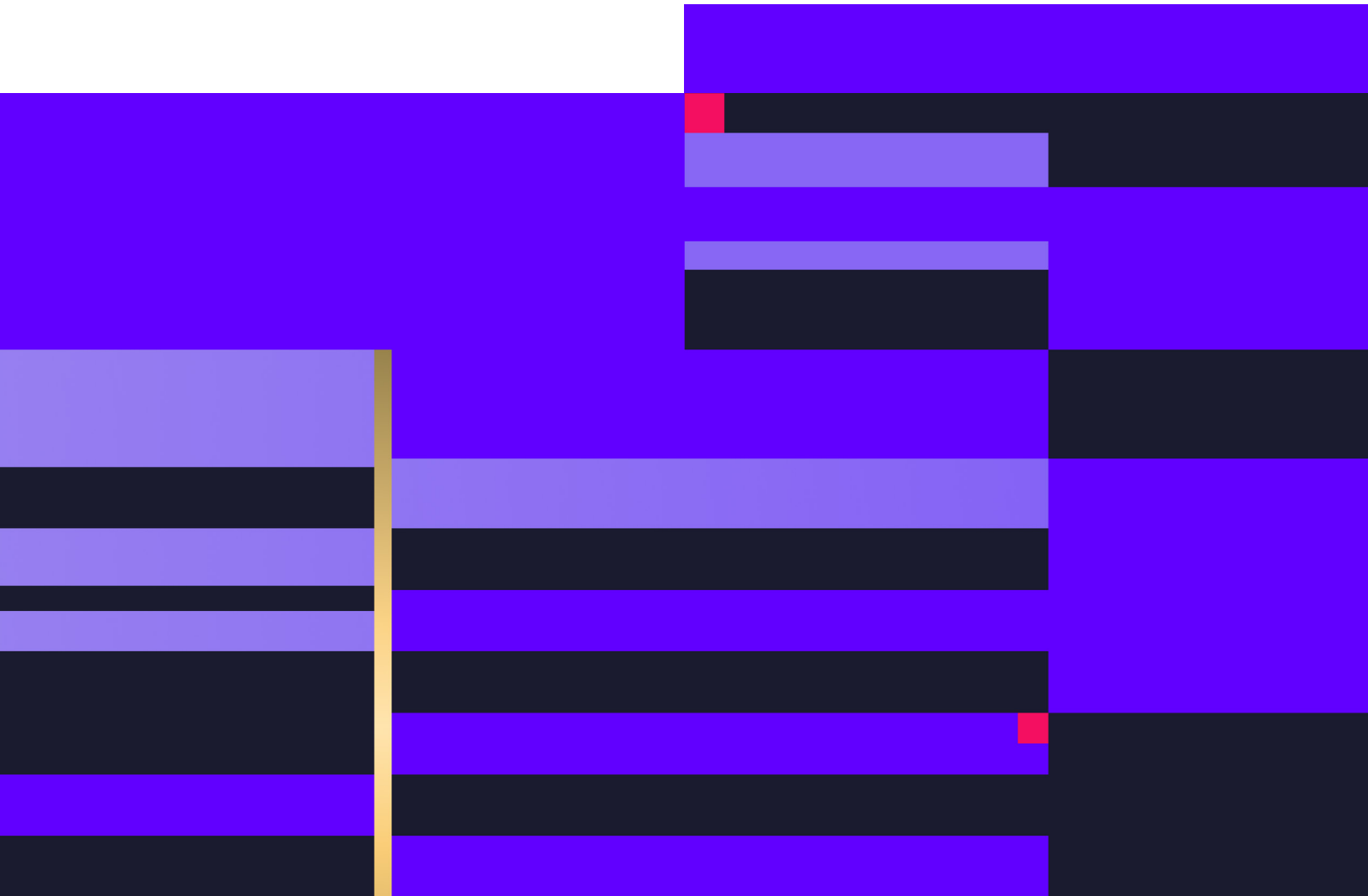
SentinelOne

FY2024 Annual Report



UNITED STATES
SECURITIES AND EXCHANGE COMMISSION

Washington, D.C. 20549

FORM 10-K

(Mark One)

☒ **ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the fiscal year ended January 31, 2024

OR

☐ **TRANSITION REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934**

For the transition period from to

Commission file number 001-40531

SENTINELONE, INC.

(Exact name of registrant as specified in its charter)

Delaware	**99-0385461**
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification No.)

444 Castro Street, Suite 400
Mountain View, California 94041
(Address of Principal Executive Offices)

(855) 868-3733
(Registrant's telephone number, including area code)

Securities registered pursuant to Section 12(b) of the Act:

Title of each class	Trading Symbol(s)	Name of each exchange on which registered
Class A common stock, par value $0.0001	**S**	**The New York Stock Exchange**

Securities registered pursuant to section 12(g) of the Act: None.

Indicate by check mark if the registrant is a well-known seasoned issuer, as defined in Rule 405 of the Securities Act. Yes ☒ No ☐

Indicate by check mark if the registrant is not required to file reports pursuant to Section 13 or Section 15(d) of the Act. Yes ☐ No ☒

Indicate by check mark whether the registrant: (1) has filed all reports required to be filed by Section 13 or 15(d) of the Securities Exchange Act of 1934 during the preceding 12 months (or for such shorter period that the registrant was required to file such reports); and (2) has been subject to such filing requirements for the past 90 days. Yes ☒ No ☐

Indicate by check mark whether the registrant has submitted electronically every Interactive Data File required to be submitted pursuant to Rule 405 of Regulation S-T (§232.405 of this chapter) during the preceding 12 months (or for such shorter period that the registrant was required to submit such files). Yes ☒ No ☐

Indicate by check mark whether the registrant is a large accelerated filer, an accelerated filer, a non-accelerated filer, a smaller reporting company, or an emerging growth company. See the definitions of “large accelerated filer,” “accelerated filer,” smaller reporting company,” and “emerging growth company” in Rule 12b-2 of the Exchange Act:

Large accelerated filer	☒	Accelerated filer	☐
Non-accelerated filer	☐	Smaller reporting company	☐
		Emerging growth company	☐

If an emerging growth company, indicate by check mark if the registrant has elected not to use the extended transition period for complying with any new or revised financial accounting standards provided pursuant to Section 13(a) of the Exchange Act. ☐

Indicate by check mark whether the registrant has filed a report on and attestation to its management's assessment of the effectiveness of its internal control over financial reporting under Section 404(b) of the Sarbanes-Oxley Act (15 U.S.C. 7262(b)) by the registered public accounting firm that prepared or issued its audit report. ☒

If securities are registered pursuant to Section 12(b) of the Act, indicate by check mark whether the financial statements of the registrant included in the filing reflect the correction of an error to previously issued financial statements. ☐

Indicate by check mark whether any of those error corrections are restatements that required a recovery analysis of incentive-based compensation received by any of the registrant's executive officers during the relevant recovery period pursuant to §240.10D-1(b). ☐

Indicate by check mark whether the registrant is a shell company (as defined in Rule 12b-2 of the Exchange Act). Yes ☐ No ☒

The aggregate market value of voting stock held by non-affiliates of the registrant on July 31, 2023, based on the closing price of $16.67 for shares of the Registrant's Class A common stock as reported by the New York Stock Exchange, was approximately $3.3 billion.

As of March 22, 2024, the registrant had outstanding 275,097,473 shares of Class A common stock and 34,910,310 shares of Class B common stock.

DOCUMENTS INCORPORATED BY REFERENCE

Portions of the registrant's definitive proxy statement relating to its 2024 Annual Meeting of Stockholders (Proxy Statement) are incorporated by reference into Part III of this Annual Report on Form 10-K where indicated. Such Proxy Statement will be filed with the United States Securities and Exchange Commission (SEC) within 120 days after the end of the registrant's fiscal year ended January 31, 2024 to which this Annual Report on Form 10-K relates.

TABLE OF CONTENTS

Special Note About Forward-Looking Statements

This Annual Report on Form 10-K contains forward-looking statements within the meaning of Section 27A of the Securities Act of 1933, as amended (the Securities Act), and Section 21E of the Securities Exchange Act of 1934, as amended (the Exchange Act), about us and our industry that involve substantial risks and uncertainties. All statements contained in this Annual Report on Form 10-K, other than statements of historical fact, including statements regarding our future operating results and financial condition, our business strategy and plans, market growth, and our objectives for future operations, are forward-looking statements. The words "believe," "may," "will," "potentially," "estimate," "continue," "anticipate," "intend," "could," "would," "project," "target," "plan," "expect," or the negative of these words and similar expressions are intended to identify forward-looking statements.

Forward-looking statements include, but are not limited to, statements about:

- our future financial performance, including our expectations regarding our total revenue, cost of revenue, gross profit or gross margin, operating expenses, including changes in operating expenses and our ability to achieve and maintain future profitability;
- the global political, economic, and macroeconomic climate, whether in the cybersecurity industry in general, or among specific types of customers or within particular geographies, including but not limited to, actual or perceived instability in the banking industry, supply chain disruptions, a potential recession, inflation, potential uncertainty with respect to the federal debt ceiling and budget, and potential government shutdowns related thereto, and interest rate volatility;
- the impact of natural or man-made global events on our business, including wars and other regional geopolitical conflicts, including the conflicts in Ukraine, the Middle East and tensions between China and Taiwan;
- the impact of actions that we are taking to improve operational efficiencies and operating costs, including the restructuring plan we approved in June 2023;
- our business plan and our ability to effectively manage our growth;
- our total market opportunity;
- anticipated trends, growth rates, and challenges in our business and in the markets in which we operate;
- our ability to maintain the security and availability of our platform;
- market acceptance of our platform and our ability to increase adoption of our platform;
- beliefs and objectives for future operations;
- our ability to further penetrate our existing customer base and attract, retain, and expand our customer base;
- our ability to timely and effectively scale and adapt our platform;
- future acquisitions or investments in complementary companies, products, services, or technologies and our ability to integrate such acquisitions or investments, including our recent acquisitions of the Krebs Stamos Group LLC (KSG) in November 2023 and both PingSafe Pte. Ltd. (PingSafe) and Stride Security Ltd. (Stride) in February 2024;
- cybersecurity incidents;
- our ability to develop new products and services and bring them to market in a timely manner and make enhancements to our platform;
- the ultimate success of technologies aimed at enhancing our platform, including through artificial intelligence (AI);

- our expectations concerning relationships with third parties;
- our ability to maintain, protect, and enhance our intellectual property;
- our ability to continue to expand internationally;
- the effects of increased competition in our markets and our ability to compete effectively;
- our ability to stay in compliance with laws and regulations that currently apply or become applicable to our business both in the United States (US) and internationally;
- economic and industry trends, projected growth, or trend analysis;
- expenses associated with being a public company; and
- other statements regarding our future operations, financial condition, and prospects and business strategies.

We caution you that the foregoing list may not contain all of the forward-looking statements made in this Annual Report on Form 10-K.

These forward-looking statements are subject to a number of risks, uncertainties, and assumptions, including those described in the section titled “Risk Factors” and elsewhere in this Annual Report on Form 10-K. Moreover, we operate in a very competitive and rapidly changing environment, and new risks emerge from time to time. It is not possible for our management to predict all risks, nor can we assess the impact of all factors on our business or the extent to which any factor, or combination of factors, may cause actual results to differ materially from those contained in any forward-looking statements we may make. In light of these risks, uncertainties, and assumptions, the forward-looking events and circumstances discussed in this Annual Report on Form 10-K may not occur, and actual results could differ materially and adversely from those anticipated or implied in the forward-looking statements.

You should not rely upon forward-looking statements as predictions of future events. The events and circumstances reflected in the forward-looking statements may not be achieved or occur. We undertake no obligation to update publicly any of these forward-looking statements for any reason after the date of this Annual Report or to conform these statements to actual results or to changes in our expectations, except as required by law. Our forward-looking statements do not reflect the potential impact of any future acquisitions, partnerships, mergers, dispositions, joint ventures, or investments we may make.

You should read this Annual Report on Form 10-K and the documents that we reference in this Annual Report on Form 10-K and have filed with the SEC as exhibits to this report with the understanding that our actual future results, performance, and events and circumstances may be materially different from what we expect.

PART I

ITEM 1. BUSINESS

Overview

Cybersecurity is indispensable to our digital way of life, with millions of cyberattacks occurring every year resulting in trillions of dollars in damages. We are in the midst of a generational shift in cybersecurity, ushered in by the ongoing digital transformation of the enterprise. Attacks can inflict damages that span operational disruption, leadership change, loss of customer trust, and intellectual property theft, among others. The rise and persistence of cyberattacks clearly shows that there is a long way to go from here. Enterprises must deploy solutions that enable them to stay one step ahead of attackers and address intrusion attempts in real-time at machine speed—empowering human operators with the speed, scale, visibility, and precision of technology.

We envisioned a revolutionary data and AI paradigm where technology alone could autonomously prevent, detect, and respond to cyberattacks. It is time to fight machine with machine. We pioneered the world's first purpose-built AI-powered Extended Detection and Response (XDR) platform to make cybersecurity defense truly autonomous, from the endpoint and beyond. By leveraging AI and our fully unified security data lake for analytics, our Singularity Platform instantly defends against cyberattacks—performing at a faster speed, greater scale, and higher accuracy than otherwise possible from any single human or even a crowd. Purple AI unifies the entire platform experience, supercharges the security operations, and delivers improved efficiency with threat-hunting capabilities across multiple attack vectors.

Our Singularity Platform ingests, correlates, and queries petabytes of structured and unstructured data from a myriad of ever-expanding disparate external and internal sources in real-time. We build rich context and deliver greater visibility by constructing a dynamic representation of data across an organization. As a result, our AI models are highly accurate, actionable, and autonomous. Our distributed AI models run both locally on every endpoint and every cloud workload, as well as on our cloud platform. Our Static and vector-agnostic Behavioral AI models, which run on the endpoints themselves, provide our customers with protection even when their devices are not connected to the cloud. In the cloud, our Streaming AI detects anomalies that surface when multiple data feeds are correlated.

Furthermore, our platform provides visibility across an organization's digital assets through a fully-integrated console, making it easy and very fast for analysts to search through petabytes of data to investigate incidents and hunt threats. Our Singularity Platform offers multi-tenancy and can be deployed on a diverse range of environments that our customers choose, including public, private, or hybrid clouds.

For each endpoint, cloud workload, and user identity, we run highly optimized AI models in a single lightweight software agent. Our Static AI model predicts file-based attacks of all types, even previously unknown threats, often referred to as "zero-day attacks," with extreme precision in milliseconds. Our Behavioral AI model maps, monitors, and links all behaviors to create rich, contextual narratives that we call Storylines. These high-fidelity Storylines are continuously evaluated by our Behavioral AI model. When activity is deemed a threat, our software autonomously takes action to kill the attack. Because Storylines contain a complete record of unauthorized changes made during an attack, we are ready to remediate or roll back these changes.

The power to turn back time on a device is unique in the market. It is the ultimate safety net and exemplifies autonomous cybersecurity. Therefore, our software eliminates manual, expensive, and time-consuming incident cleanup. In the cloud, our platform aggregates Storylines. Our Streaming AI detects anomalies that surface when multiple data feeds are correlated with additional external and internal data. By providing full visibility into the Storyline of every secured device across the organization through one console, our platform makes it very fast for analysts to easily search through petabytes of data to investigate incidents and proactively hunt threats.

Our protection and visibility extend across critical enterprise surfaces, including traditional endpoints, cloud workloads, identity credentials, unmanaged devices, and Internet of Things (IoT) devices. This empowers security analysts of all skill levels to hunt, investigate, and remediate even the most sophisticated threats across the network leveraging automated context provided by our Storylines. Our proprietary data stack, Singularity Data Lake, and cloud architecture enable us to retain this rich, contextual data on behalf of our customers for extended periods of

time in a highly cost-efficient manner. All of this threat intelligence is fed back into our AI model and further strengthens our algorithms, creating a strong flywheel effect and deepening our competitive moat.

Our Singularity Platform can be flexibly deployed on the environments that our customers choose, including public, private, or hybrid clouds. Our feature parity across Windows, macOS, Linux, and Kubernetes offers best-of-breed protection, visibility, and control across today's heterogeneous information technology (IT) environments. Together, these capabilities make our platform the logical choice for organizations of all sizes, industry verticals, and compliance requirements. Our platform offers true multi-tenancy, which enables the world's largest organizations and provides our managed security providers and incident response partners with an excellent management experience. Our customers realize improved cybersecurity outcomes with fewer people.

Our Singularity Platform is used globally by organizations of all sizes across a broad range of industries. Our AI and automation driven approach to cybersecurity has been adopted by some of the world's largest organizations. As a result, we have grown rapidly since our inception. Our revenue for fiscal 2024 and 2023 was $621.2 million and $422.2 million, respectively, representing year-over-year growth of 47%. During this period, we continued to invest in growing our business to capitalize on our market opportunity. As a result, our net loss for fiscal 2024 was $338.7 million compared with net loss of $378.7 million in fiscal 2023.

Industry Background

Cybersecurity is fundamentally a data problem. Advances in AI, specifically machine learning, where algorithms use data to make decisions with minimal human intervention, are already revolutionizing fields such as healthcare, advertising, and securities trading. We believe that AI is ripe for revolutionizing cybersecurity. First, organizations need to ingest, normalize, and correlate petabytes of structured and unstructured data from a myriad of external and internal data in a cost efficient manner. Second, organizations need to apply powerful AI models on this high-fidelity contextual data to automatically detect known and unknown threats, then autonomously remediate and neutralize such threats. It is critical that we harness the power of data and AI to protect our digital way of life.

Stakes are high for organizations and cybercriminals. The exponential growth of sensitive customer and business data has simultaneously made many organizations and governments the target of highly sophisticated cybercriminals. Powered by very large networks of individual attackers distributed worldwide, cybercrime is practically infinite in scale and transcends geographical boundaries. To gain access to an organization's data, cybercriminals target endpoints, applications, and user credentials and deploy a variety of sophisticated methods in the form of attack frameworks, machine learning, weaponized exploits, fileless techniques, and social engineering. As a result, solutions that help strengthen and scale cyber defenses cost effectively is a top-level priority for organizations today.

Tectonic shifts in IT require a "Zero Trust" operating procedure. With millions of remote devices accessing thousands of applications running in public, private and hybrid clouds, traditional perimeter-based security controls are bypassed, and organizations have to operate in a "Zero Trust" IT environment. The attack surface has expanded considerably, and the notion of a corporate perimeter protected by firewalls is a relic of the past, making the endpoint the epicenter, and endpoint protection software the first, and last, line of defense. Several tectonic shifts in IT have increasingly left companies vulnerable including:

- ***Rapid adoption of cloud computing.*** Cloud computing has become a strategic imperative for organizations to accelerate their digital transformation. Security and compliance is a shared responsibility model between cloud infrastructure providers and their customers, and organizations are looking for technology solutions that protect their growing cloud workloads while enabling flexible deployment options across public, private and hybrid clouds.

- ***The operating system landscape is more complex than ever before.*** The diversification of IT and bring your-own-device policies brought Macs and other devices into today's organizations. Organizations are looking for cybersecurity solutions that deliver comprehensive defense capabilities and feature parity across a large variety of operating systems, including Windows, macOS, and Linux, without burdening their IT teams.

- ***Proliferation of connected devices.*** Billions of connected devices are online today and the numbers are only expected to increase. Many of these devices will have little to no built-in security capabilities. Cybercriminals are increasingly exploiting inherent vulnerabilities in these devices to breach organizations. Unmanaged devices are especially vulnerable. As a result, the attack surface has exploded. Visibility across connected devices and continuous assessment of their risk profiles have become top priorities for organizations.

- ***Remote and hybrid work is here to stay.*** As companies continue to adopt and maintain remote work practices, the risk of cyberattacks has increased. As a result of the accelerated structural shift towards a distributed workforce, organizations are increasingly looking for cybersecurity solutions that safeguard their remote workforce and employee credentials.

Sophisticated cyberattacks circumvent existing security controls. Cyberattacks have evolved from malware to highly sophisticated, organized and large-scale attacks by malicious insiders, criminal syndicates, and nation-states seeking to circumvent existing security controls and undermine critical societal functions through a variety of attacks that are fast acting that take only seconds to breach organizations, exfiltrate data, demand ransoms, and disrupt operations. Alternatively, some attacks, such as advanced persistent attacks and targeted attacks, are designed to breach the organization and stealthily infiltrate across assets to steal data, facilitate future attacks, or cause other harm over a long period of time, all while operating undetected. In addition, threat actors are using generative AI to increase the sophistication, frequency, and speed of cyberattacks. The new challenges in security landscape require autonomous security powered by AI and machine learning.

Cybersecurity teams are unable to scale. While the number of connected devices, applications and cyber threats have increased exponentially, organizations are facing an acute shortage of skilled cybersecurity talent. The large number of security solutions that companies have deployed over time generate large volumes of alerts that overwhelm security teams as they must sift through and analyze. Out of necessity, organizations are demanding solutions that do not require human intervention to prevent, detect, and remediate cyber threats.

Limitations of Legacy Solutions

Organizations must deploy solutions that enable them to stay one step ahead of attackers and address intrusion attempts in real-time. As attackers up the ante, developing new skills and deploying new tactics and techniques, legacy tools are often unable to prevent and respond effectively to breaches. The result is a rising number of successful high-profile attacks.

Key limitations of legacy tools are that they:

- ***Cover a limited spectrum of cyber threats.*** Legacy tools, such as signature-based approaches, human-powered monitoring, application whitelisting and sandboxing, are each effective under limited circumstances, but lack the ability to detect the full spectrum of threats that organizations face. For example, signature-based approaches can detect attacks that have been seen previously, but are incapable of preventing a wide range of attacks, such as unknown malware, ransomware, modified versions of previously known attacks and the exploitation of zero day vulnerabilities. In addition, they lack the ability to detect and prevent an increasing number of fileless attacks, that deposit no malware, but instead exploit operating system vulnerabilities and use trusted tools within IT environments. In general, enterprises need to take a more holistic view of security protection across endpoints, cloud environments, and identity credentials. A unified platform approach is needed to deliver comprehensive protection, visibility, and user experience. As a result, despite deploying a myriad of point solutions, organizations have continued to suffer huge losses from cyberattacks.

- ***Utilize AI approaches that rely on humans to power protection mechanisms.*** First-generation AI tools cannot handle the volume, variety, and velocity of data that must be ingested and analyzed, in real-time, to effectively prevent breaches. These tools often rely on ineffective pattern-matching algorithms in the cloud that generate so much “noise” that human intervention is required to extract useful “signals.” Without curated, contextual data, these tools only generate more alerts that need to be analyzed by humans. They cannot take action at machine speed and are thus unable to detect and prevent or stop many fast-acting

attacks. Additionally, due to communication latency with the cloud, these tools cannot generate actionable insights in real-time, which is required to stop many current threats.

- ***Lack long-term data visibility to proactively investigate advanced threats.*** Existing endpoint detection and response (EDR) tools lack the capability to store large sets of historical data cost efficiently, and consequently often only offer limited data retention capabilities. This results in only partial datasets being available for threat hunting and time bound retrospective forensic analysis. Limited historical EDR data makes full incident investigation challenging for security personnel, as they are unable to go back in time and see how the attack breached the organization and progressed.

- ***Struggle to protect complex modern IT environments.*** Legacy tools were not designed to protect today's multi-cloud, multi-device, and multi-operating system IT environments. Vendors have extended their existing solutions by bolting on functionalities, which has led to a wide disparity of capabilities across endpoints and operating systems. Legacy tools further lack the ability to identify unmanaged IoT devices which often have very limited, if any, built-in security capabilities and can be used by attackers to access the networks of target organizations. This lack of unified visibility and control over endpoints, cloud workloads, and IoT devices results in gaps in security coverage for organizations.

- ***Lack deployment flexibility for organizations.*** Organizations struggle with the limited deployment methods mandated by legacy tools. On-premise tools impose complexity and maintenance burdens on organizations. These tools typically lack the ability to quickly adapt to organizations' rapidly evolving IT environments, which requires significant upfront investments and configuration and integration efforts. On the other hand, cloud-only cybersecurity vendors are unsuitable for many large and complex enterprises and governments that need private or hybrid cloud solutions to meet their security, regulatory, and compliance requirements.

- ***Inhibit technology workflow automation.*** Many legacy tools lack out-of-the box APIs and rely heavily on professional services, which makes the integration and implementation process long, expensive, and often unattainable. The lack of flexible workflow integrations limits organizations' ability to reduce overhead by automating processes and improving their security by ensuring that process steps are done quickly, consistently, and according to their predefined requirements.

A new paradigm for cybersecurity is needed to autonomously protect organizations and their heterogeneous IT footprints from highly sophisticated, machine-based attacks in a holistic, seamless, and automated manner.

Our Revolutionary Autonomous Approach to Cybersecurity

Our AI-powered Singularity Platform defines and delivers enterprise-wide security across diverse attack vectors — powered by a single, unified data and security architecture. Our platform ingests, correlates, and queries petabytes of structured and unstructured data from a myriad of disparate external and internal sources in real-time. We build rich context by constructing a dynamic representation of data across an organization. As a result, our AI models are highly accurate, actionable, and autonomous. Furthermore, our platform provides visibility across an organization's digital assets through one console, making it easy and very fast for analysts to search through petabytes of data to investigate incidents and hunt threats. Our Singularity Platform offers multi-tenancy and can be deployed on a diverse range of environments that our customers choose, including public, private, or hybrid clouds.

Singularity Platform Capabilities and Our Competitive Strengths

- ***Protects against present and future cyber threats.*** A combination of our powerful Static AI and Behavioral AI locally on the device with Streaming AI models in the cloud addresses the spectrum of attacks in an evolving threat landscape, including ransomware, known and unknown malware, trojans, hacking tools, memory exploits, script misuse, bad macros, and "living off the land," or file-less, attacks. When our on-device machine learning models assess how an endpoint behaves, they are completely independent of the attack vector itself or any further updates and configurations.

- ***One Platform approach enables protection and visibility across all digital assets.*** Our Singularity Platform provides organizations with our full suite of real-time threat prevention, detection, and remediation capabilities across their endpoints, cloud workloads, servers, operating systems, and user credentials. Our platform further leverages our agents, combined with passive and active network discovery methods, to provide our customers with organization-wide visibility into their network assets, managed and unmanaged. Our platform approach helps enterprise consolidate security tools while enhancing enterprise-wide coverage.

- ***Provides autonomous protection and remediation.*** Powered by our AI and Storyline technology, our agents defend and heal endpoints autonomously and in real-time by stopping malicious processes, quarantining, remediating, and even rolling back events to surgically keep endpoints clean. Rollbacks are performed autonomously and in real-time, eliminating the need for manual, expensive, and time-consuming incident cleanup.

- ***Enables facilitated, as well as fully automated, incident investigation and proactive threat hunting.*** Our platform gives security teams the ability to search their IT assets for behavioral indicators via a single-click interface. Our deep visibility and contextual data empower security analysts of all skill levels to run queries at very fast speeds, and quickly understand the root causes behind the most complex threats. Purple AI supercharges the security analyst experience, with simplified user experience, improved efficiency, and more holistic hunting capabilities.

- ***Provides full forensic recall for complete remediation.*** We offer our customers the ability to retain rich, contextual data for extended periods of time in a highly cost-efficient manner. For compliance and security, enterprises need cost effective data retention for longer periods of time. This forensic data helps our customers investigate breaches that have stealthily infiltrated their organization and potentially operated undetected for many months giving them the ability to ensure that any incident has been fully remediated without the need to re-image or replace elements of their IT infrastructure.

- ***Provides a superior customer experience.*** We put the user at the center of our product development and engineering processes. The combination of our intuitive and clean user interface, our ability to provide context with one click, and a high degree of automation empowers our customers to use Singularity platform independent of their expertise level.

- ***Proprietary data stack.*** Our modern, innovative, and extensible data stack, Singularity Data Lake, enables us to ingest, process and analyze massive amounts and a wide variety of data types efficiently. Our independent, component-driven architecture allows us to evolve rapidly leveraging continued innovations of public cloud infrastructure, while controlling every aspect of our innovation roadmap and customer experience.

- ***Deeply embedded within our customers' IT stacks.*** Our API-first approach and Singularity Marketplace allow our customers to easily integrate intelligence, analytics, automation, and other third-party business applications with our platform. Security teams often need to integrate different security tools to address gaps and improve security posture. Our Singularity Marketplace offers no-code automation that allows customers to seamlessly ingest data from third-party applications into our Singularity Platform.

- ***Flexible deployment model that delivers rapid time to value.*** Our Singularity Platform can be quickly and easily deployed on a diverse range of environments of our customers, and without extensive configuration or maintenance, including the public, private or hybrid cloud, making it relevant for organizations of all sizes with varying compliance and regulatory requirements.

- ***Rich partner ecosystem.*** We have deep partnerships with many of the leading Independent Software Vendors (ISVs), alliance partners whom we engage with on joint technology and/or go-to-market strategies; and channel partners, such as distributors, resellers, Managed Service Providers (MSPs), Managed Security Service Providers (MSSPs), Managed Detection and Response Providers (MDRs), Original Equipment Manufacturers (OEMs), and Incident Response (IR) firms. Our partner relationships provide us with significantly broader market reach. In particular, we do not currently have a services offering that competes with our IR partners. Therefore, they seek to bring us into remediation situations where their customers often become our customers. As a result, many of our partners act as force multipliers and broaden our market reach. By empowering MSPs, MSSPs, MDRs, and IR firms with our technology and through our deep partnerships with them, we benefit from the market penetration of those entities.

- ***Quality and access of cybersecurity and AI talent.*** Our thought leadership in security and AI, combined with our award-winning culture, allows us to attract and retain some of the best talent at a global scale. It allows us to develop state-of-the-art solutions, innovate faster, and solve many of the industry's most complex problems.

We believe our leading security and platform breadth position us well to consolidate and unify cybersecurity spend across multiple categories. Over time, we believe this unification and re-architecture of the prevention, detection and response paradigm will create new opportunities for additional products and features.

Growth Strategy

Key elements of our growth strategy include:

- ***Continue to innovate and enhance our cybersecurity and data platform.*** We will continue to expand our platform by developing new modules to include greater functionality and address additional use cases. As a pioneer in autonomous and AI-based cybersecurity, we have established a track record for expanding our platform capabilities with new modules. Through convergence of cybersecurity and data, we intend to bring our customers and prospects a variety of differentiated cybersecurity-first, AI powered, and enhanced data analytics offerings. Having access to some of the world's top cybersecurity and AI talent through our distributed workforce model and our research and development centers across North America, Europe, the Middle East, and Asia allows us to continue hiring top technical talent and innovate to maintain our leading position.

- ***Drive new customer acquisition.*** We have customers, ranging from large enterprises, such as Fortune 500 companies, to small and medium-sized businesses around the world. We intend to continue to add new customers through a product-first approach. This approach enables us to build trusted relationships with a large and rapidly growing group of highly influential managed service and incident response providers, as opposed to creating a dynamic of competition that creates friction between product vendors and service providers. We are currently certified under the Federal Risk and Authorization Management Program (FedRAMP), and we intend to further grow our footprint within the US federal government. We intend to continue to build our relationships with our channel partners, including MSPs, MSSPs, MDRs, OEMs, and IR firms, as well as our alliance partners to expand our market reach.

- ***Increase adoption within our customer base.*** We have successfully grown our revenue from our customer base as they deploy additional licenses and expand the use of our platform by adoption of adjacent solutions. As we enhance our platform functionality and value proposition, we expect many of our customers to adopt additional platform functionalities and Singularity modules to address all of their cybersecurity use cases through the same platform. Our customers can seamlessly activate additional modules to adopt more platform capabilities. Module-driven growth has been broad-based with notable strength from our cloud and data modules. Our platform also enables us to show in-product promotions and trials and to drive the expansion of our Singularity Modules. The success of our land-and-expand strategy is evidenced by our dollar-based net retention rate of 114% as of January 31, 2024.

- ***Expand our global footprint.*** Revenue generated outside of the US was 36% for fiscal 2024, compared to 35% for fiscal 2023. We intend to continue to grow our international customer base by increasing our investments in international operations. We are continuing to invest and hire talent to expand our business in Asia-Pacific and Europe, the Middle East and Africa, and Latin America.

- ***Expand our total addressable market through acquisitions.*** We evaluate acquisition prospects that align with our platform, customers, and strategic market opportunities. We intend to use these opportunities to extend the reach of our Singularity Platform into adjacencies that complement our core offerings. We are committed to innovation, automation, and securing data wherever it resides with a front-row seat into cutting-edge cybersecurity technologies. For example, in November 2023, through our acquisition of KSG, a strategic advisory group, we launched PinnacleOne to address multifaceted security challenges for enterprises. PinnacleOne will focus on helping companies and their executives holistically understand the evolving risks of operating in the modern global business landscape through personalized access to expert intelligence, insights, and transformative risk management strategies. Further, in February 2024, we acquired PingSafe, a cloud native application protection platform (CNAPP) to bolster our existing cloud security product suite. By adding PingSafe's CNAPP to our Cloud Workload Security (CWS), we can now provide enterprises with a comprehensive cloud security coverage that drives comprehensive security, improved posture, and autonomous protection across their entire cloud footprint.

Our Singularity Platform

Our Singularity Platform delivers AI-powered autonomous threat prevention, detection, and response capabilities across an organization's endpoints, cloud workloads, and identity credentials, enable seamless and autonomous protection against a full spectrum of cyber threats. We built our platform to be deployed as a cloud service in public, private, and hybrid cloud environments. We further offer customers a broad set of capabilities through our Singularity Modules. We price our modules as a subscription on a per agent basis.

Our platform capabilities are connected through three key patented technologies:

- ***Data Analytics.*** Our data analytics technology can ingest, correlate, and query petabytes of structured and unstructured data from disparate external and internal sources at machine speed.

- ***AI.*** Our Static, Behavioral, and Streaming AI technologies that run in a distributed manner on our data cloud as well as on every endpoint and every cloud workload we protect. We overlay the entire user experience with Purple AI, improving the efficiency and effectiveness of security analyst operations.

- ***Storyline.*** Our Storyline technology builds a model of real-time running processes and their behaviors, to create rich, contextual data narratives which become the input to our Behavioral AI model. Storyline powers our unified Endpoint Protection Platform (EPP), EDR, or XDR functionalities. Storyline is the foundation of our EPP providing unprecedented levels of visibility, with contextual information for benign and malicious processes. We extend our fundamental protection, visibility and response capabilities well beyond the endpoint to cloud, and third-party solutions in our Singularity Platform.

Proprietary Security Data Lake

Singularity Data Lake (SDL), formerly DataSet, is our fully integrated security data lake that seamlessly fuses together the data, access, control, and integration planes of EPP, EDR, CWS, Identity Protection, and IoT security into a centralized platform. With our Singularity Platform, enterprises gain visibility and access to their security data through a single pane of glass across multiple sources. SDL was designed with the goal of optimizing scale, cost and performance - what we call the Golden Ratio of Big Data. This is achieved using innovative data structures, storage systems, and algorithms:

- ***Ingest.*** Our platform can ingest structured and unstructured data from any source, with little to no manual configuration and at unprecedented speed and scale.

- ***Normalize***. Aligns every data point to extract the shared elements regardless of origin and to produce true insights.

- ***Correlate.*** We correlate events from multiple sources into Storylines which contains event data, both benign and malicious, in a context-rich format for easy understanding.

- ***Analyze.*** Our Singularity Platform enriches and visualizes every Storyline with information from Threat Intelligence sources, both homegrown and through integrations with third-party intelligence information services.

Multi-tenancy Architecture

We offer complete multi-tenancy with four tiers—Global, Account, Site, and Group. Policies set at the higher tier of the hierarchy are automatically inherited by the lower levels, but administrators may override them to create local policies at any tier. We also support fully customizable Role Based Access Control, that allows organizations to create specific rules controlling console permissions at a granular level. This enables large, distributed teams to work independently while at the same time providing a global view for the chief information officer and other stakeholders. It further enables our platform adoption by the world's largest organizations, MSPs, MSSPs, MDRs, OEMs, and IR firms.

XDR Integrations

Singularity XDR unifies and extends detection, investigation, and response capability across the entire enterprise, providing security teams with centralized end-to-end enterprise visibility, powerful analytics, and automated responses across the technology stack. This empowers security teams to see data collected by disparate security solutions from all platforms, including endpoints, cloud workloads, network devices, email, identity, and more, within a single dashboard. It enables customers to seamlessly extend the power of the Singularity Platform across the entire IT stack—regardless of vendor—to automate response actions. Our XDR integrations give customers the flexibility to operate our platform as a platform-as-a-service in their own customized graphical user interface and workflows simply by leveraging our robust, well-documented and easy-to-use APIs.

IT and Security Operations

Our Singularity Platform enables security and IT teams to identify software or application vulnerabilities, fix insecure configurations, and manage endpoints. Vulnerable and misconfigured applications make it easier for attackers to gain entry and evade detection. Addressing these vulnerabilities and misconfigured settings strengthens the security risk profile of our customers. Our platform has the following capabilities:

- ***Application Inventory.*** Maintains a software application inventory in real-time across an entire organization and their attributes such as their version numbers, install date, and publisher. Customers can quickly perform software frequency analysis and compliance checks.

- ***Scanless Vulnerability Assessment.*** Using our real-time organization-wide Application Inventory database, our solution can provide highly accurate and dynamic Vulnerability Management information without the need to deploy another solution.

- ***Device Control.*** Allows maximum granularity and flexibility when defining Device Control policies to prevent data exfiltration and malware entry. Our Device Control capability provides granular control for Bluetooth devices in conjunction with other forms of USB media.

- ***Native Operating System Host Firewall Control.*** Firewall control provides visibility, malware prevention, and network segmentation by utilizing the native firewall capabilities on Windows, macOS, and Linux devices.

- ***File Integrity Monitoring.*** Our File Integrity solution (FIM) is able to automatically alert or remediate unauthorized changes to these files. Organizations use our FIM to be compliant with Payment Card

Industry Data Security Standard (also known as "PCI DSS") and other regulatory requirements while eliminating other agents, products, and spend.

Singularity Platform Product Offerings

Our Singularity Platform offers a highly flexible deployment model. It is primarily hosted in Amazon Web Services (AWS) in multiple regions - North America, Europe, Asia Pacific, and AWS GovCloud. Our platform can also be hosted in Google Cloud, as well as customers' on-premise data centers, and private and hybrid cloud environments for organizations with specialized hosting and data sovereignty needs.

Our Singularity Platform provides feature parity across Windows, macOS, and Linux. It provides customers with full flexibility through a multi-tier offering priced on a per agent basis, which generally corresponds with an endpoint, server, virtual machine, or host. The tiers of our Singularity Platform include:

- ***Singularity Core.*** Our entry level security solution for organizations that want to replace antivirus tools with our EPP which we believe is more effective and easier to manage than legacy antivirus and next-generation antivirus products. Singularity Core includes our Static and Behavioral AI models and autonomous threat response and rollback features.

- ***Singularity Control.*** Made for organizations seeking best-of-breed security with the addition of our "security suite" features for endpoint management. It provides additional features for control network connectivity, USB and Bluetooth peripherals, and uncovering rogue devices.

- ***Singularity Complete.*** Our flagship offering that includes a comprehensive suite of product capabilities.

- ***Singularity Commercial.*** Provides a solid foundational security solution across endpoints, cloud, and identities, ensuring that an organization has the necessary tools to stay secure.

- ***Singularity Enterprise.*** Provides comprehensive protection across endpoints, cloud, and identities as well as threat intelligence, vulnerability, and diverse set of services.

Endpoint Protection (EPP)

Our next-generation cybersecurity technology provides autonomous real-time protection across all operating systems, including Windows, Linux, macOS, and cloud-native and containerized workloads. Our endpoint protection is powered by distributed AI which resides both on devices as well as in the cloud for always-on, machine-speed protection. It is capable of autonomous decision making on the device and stopping threats in milliseconds rather than minutes, hours or even days. We are able to provide superior performance compared to traditional signature-based antivirus tools and earlier next-generation antivirus products with the following three key capabilities:

- ***Static AI.*** Our on-device AI model can detect file-based attacks, even those that are previously unknown zero-day exploits, with extreme precision in milliseconds. Our Static AI model is the output of a supervised machine learning cycle that is trained on a continuously evolving data set from billions of files coupled with the data from multiple threat intelligence sources, including our proprietary Embedded Threat Intelligence.

- ***Behavioral AI.*** Our on-device AI model continuously scores Storylines from the device to precisely classify individual or group behaviors as benign or malicious. The accuracy of our Behavioral AI is powered by the rich contextual information that is encoded in each Storyline that is being scored. As a result, our Behavioral AI is attack vector agnostic because it is not limited to any particular pathway used by attackers to penetrate a system, such as zero-day vulnerability exploits and living off the land attacks.

- ***Embedded Threat Intelligence.*** Our cloud threat intelligence system combines threat information from our data analytics and research teams, Vigilance MDR and IR services, and other commercial and proprietary threat feeds. Our Purple AI for Threat Intelligence expands and accelerates an organization's ability to deliver deep insights needed to proactively protect against threats and mitigate risk.

Endpoint Detection and Response (EDR)

Unlike first-generation EDR products that are reactive and mainly focused on collecting data, our ActiveEDR solutions leverage Storylines to reduce analysis time and to automate response actions by significantly minimizing the time between detection and response through technology automation. It enables on-device behavioral analysis, auto-remediation, and response in a fully autonomous fashion. ActiveEDR reduces analysis time and requirements for specialized skills by providing technology-generated context which would otherwise need to be produced by highly skilled people manually in a time-intensive and error prone fashion. ActiveEDR excels at visualizing context, pinpointing anomalies, and providing a variety of granular responses. The main capabilities of ActiveEDR are:

- ***Deep Visibility Threat Hunting*.** Deep Visibility Threat Hunting provides an easy-to-use search interface on top of our Deep Visibility dataset. The Storylines shown within Deep Visibility hunts enable one-click responses, which are far easier and faster to execute than manually scripting responses. As a result, both entry level and highly skilled analysts can analyze results faster, review more alerts, and be more productive with the power of technology.

- ***Response Capabilities*.** Our Singularity Platform offers one of the broadest sets of response actions in the EDR market. Leveraging Storylines, we automate responses or make them optionally initiated by operators. Our response capabilities enable security analyst to *Kill, Quarantine, Remediate, Remote Shell, and Rollback*.

Singularity Data Lake

Building upon the acquisition of Scalyr, Inc., Singularity Data Lake is a revolutionary live enterprise data platform for data queries, analytics, insights, and retention. It expands our capabilities beyond cybersecurity use cases, such as data analytics. Singularity Data Lake takes a security-first perspective to data analytics. It is a cloud-native flexible enterprise data platform built for all types of data live or historical, at petabyte scale. By eliminating data schema requirements from the ingestion process and index limitations from querying, Singularity Data Lake can process massive amounts of live data in real time, delivering log management, data analytics, and alerting with unparalleled speed, performance, and efficiency built on a security and privacy-first foundation.

As a software as a service (SaaS) platform, it can be deployed in minutes and is easy to operate without any maintenance requirement. Singularity Data Lake is built for the cloud and offered as a cloud service freeing up engineering resources from managing data refineries. It is built with the security and controls that enterprises require for their most precious asset: data.

Cloud Security

We offer both agent and agentless cloud security capabilities in a comprehensive CNAPP. Offering these in a unified security platform helps reduce operational complexity and improve integrated protection and remediation capabilities.

Our CWS solution extends distributed, autonomous endpoint protection, detection, and response to compute workloads running in public clouds, private clouds, and on-premise data centers. Our runtime protection delivers prevention, detection, response and hunting functionalities purpose-built for these environments. We offer full-fledged EPP and EDR for servers, virtual machines, and containerized workloads. Our Cloud Application Control locks down the running image of servers and containers to prevent configuration drift and protect against unauthorized changes, in line with best practices for cloud workload security.

Our Cloud Security Posture Management (CSPM) solution automatically and continuously identifies and responds to cloud misconfigurations and reports on compliance with industry benchmarks like NIST, MITRE, CIS, PCI-DSS, and more. Furthermore, it detects vulnerabilities in cloud infrastructure including infrastructure as a code (IoC) scanning, secret scanning, and code to runtime monitoring across major cloud services (AWS, GCP, Azure, Oracle, Alibaba, and more).

Our Cloud Data Security solution protects cloud environments from the spread of malware through automated file threat analysis. Customers receive protection from malicious files in Amazon Simple Storage Service (S3) and NetApp. Our AI-powered threat detection delivers unparalleled visibility and proactive protection against advanced threats, ensuring security and compliance.

Identity Security

Our identity security portfolio acts as a force multiplier for security teams, allowing them to assume a more robust security posture and extend the capabilities of the Singularity Platform to protect user credentials. Our Singularity Identity solution detects and responds to identity-based attacks and finds attackers early, before they can exploit identities. Our identity solution also reduces the potential attack surface and proactively increases security by identifying misconfigurations and credential exposures that create attack paths for attackers to move laterally. Our identity security portfolio includes:

- ***Singularity Identity*** detects real-time identity attacks across the enterprise that target Active Directory and Active Directory (Azure AD). It delivers holistic identity threat detection and response including credential theft, privilege escalation, lateral movement, data cloaking, identity exposure, and more for zero trust cybersecurity.

- ***Singularity Ranger Active Directory*** uncovers vulnerabilities in Active Directory and Azure AD with a cloud-delivered, continuous identity assessment solution. It provides instant Active Directory visibility of misconfigurations, suspicious password changes, credential harvesting, unauthorized access, and more.

- ***Singularity Hologram*** lures network and insider threat actors into revealing themselves. Through misdirection of the attack with tactics including breadcrumbs and decoy accounts, files and IPs, organizations gain the advantage of time to detect, analyze, and stop an attacker without impacting enterprise assets.

Attack Surface Management

Our Ranger module enables control of the enterprise network attack surface in real time by discovering, identifying, and containing any device-based threat. Ranger leverages the presence of our software in an organization's network to track assets, create an Enterprise Asset Map, perform network segmentation, deploy our agents to unprotected devices, and provide risk scores. Ranger provides organization-wide inventory and control of IoT devices by discovering connected devices, including virtual machines, containers, and IoT devices such as printers, smart TVs, and thermostats. Ranger has four key component features:

- ***Rogue Discovery.*** Enables administrators to identify unprotected or "rogue" assets and verifies our agent is installed on all corporate assets.

- ***Ranger Insight.*** Provides a clear picture of the inventory and risk in the IoT environment, including open ports, header and application versions, and vulnerability information,

- ***Rogue Control.*** Creates network segments to restrict access to a corporate network. Rogue Control prevents unsanctioned devices, such as guest machines, from connecting to authorized networks.

- ***Ranger Auto-Deploy.*** Rapidly deploys our agents using service credentials to unprotected endpoints with no additional IT infrastructure or software. Auto-Deploy provides security teams with complete, instant asset coverage.

Mobile Endpoint Security

Our Singularity Mobile module enables customers to manage mobile devices through behavioral AI-driven protection, detection, and response directly for iOS, Android, and ChromeOS devices. It delivers mobile threat defense that is local, adaptive, and real-time, to thwart mobile malware and phishing attacks at the device, with or without a cloud connection. It is the industry's leading on-device behavioral AI product that dynamically detects never before seen malware, phishing, exploits, and man-in-the-middle attacks. Singularity Mobile provides security and data privacy to support zero trust.

XDR Power Tools

Our Singularity XDR Power Tools modules complement and extend Singularity EDR & XDR capabilities for organizations seeking advanced investigative workflows and a long, retrospective look back to support comprehensive incident response. These modules include:

- ***Binary Vault.*** Enables customers to store and download copies of any file that has been executed in their environment for forensic review and reverse engineering. Binary Vault can store a copy of every known binary, both benign and malicious, that executes across an enterprise. This enables advanced security analysts to download a copy of any file that has been executed in their environment for forensic review and reverse engineering, and provides them with access to a broader dataset and more complete lookback capabilities than any of our competitors.

- ***Remote Script Orchestration (RSO).*** Enables enterprises and incident responders to investigate and respond to threats on multiple endpoints across the organization remotely, enabling them to easily manage their entire fleet. In incident response situations, rapid artifact extraction and endpoint state querying across the entire enterprise is critical. Our remote script orchestration module allows concurrent execution of custom and preset scripts across an enterprise, instead of having to triage with a device-by-device approach. By converging our protection, detection, and response capabilities with remote script orchestration, our platform is the only solution that is needed to respond to a breach.

- ***Storyline Active Response (STAR).*** STAR gives users the capability to set custom Indicators of Compromise (IOC) based rules for real-time analysis, alerting, and automatic response workflows. Our STAR module is also capable of ingesting threat intelligence feeds to enhance and correlate analyses. The STAR module uses Streaming AI technology to match billions of events to tens of millions of IOCs at the time of ingestion. STAR is a threat hunting and workflow orchestration force multiplier. Without STAR, it is difficult for security analysts to keep pace with the number and complexity of emerging threats from an EDR perspective.

- ***Data Retention.*** Offers data retention from one month to three years and beyond. Modern attacks can take days and weeks to initiate after infiltration. Therefore, it is critical for an EDR solution to provide visibility for extended periods of time. This enhances both retrospective analysis and proactive hunting measures. Our platform has been designed and built to support extended data retention to time periods that far exceed what others are able to offer, and we do so on a cost-efficient basis due to our data retention architecture. We offer data retention for up to three years to provide maximum value from our Deep Visibility Threat Hunting module.

- ***Cloud Funnel.*** Allows organizations to export their XDR data in real-time to their private data lakes, whether locally-hosted or in the cloud. Moreover, it securely streams a copy of all endpoint EDR telemetry to a customer's local data lake for further correlation with other security tools, while allowing offline data storage for audit and compliance.

WatchTower

WatchTower delivers threat hunting and insights to help customers understand the nature of threats, targeted attacks, threat actors, and risk reduction. It provides intelligence-driven, cross-platform threat hunting to help customers adapt to the modern threat landscape through visibility and actionability to novel attacker techniques, global APT, campaigns, and emerging cybercrimes. As we track threat actors globally, WatchTower parses, consolidates, and contextualizes threat intelligence sources and hunts for threats in our customers' environments. WatchTower distills intelligence down to its most valuable insights, such as a summary bulletin of the threat, its impact on our customers' organizations, and how the threat can be addressed.

Vigilance MDR

Vigilance MDR leverages the expertise of our in-house security analysts to review, act upon, and document every threat that our Singularity Platform autonomously identifies. It adds a human lens to cybersecurity understanding and augments our customers' in-house security teams. Due to the autonomous nature of our Singularity Platform, Vigilance MDR provides rapid response times to threats. Our technology-powered digital forensics analysis and incident response offering takes Vigilance MDR two steps further and provides customers with a full-service solution and enables customers to benefit from world-class SOC operations with customized threat annotation and response. Vigilance MDR helps customers of all sizes augment their cybersecurity staff with a 24/7/365 globally-distributed operation which operates under the industry's only publicly available Service Level Agreement.

Our Customers

As of January 31, 2024, we had customers using our Singularity Platform in approximately 80 countries. We are protecting the digital infrastructures of thousands of customers around the world, including large global enterprises, small and medium sized businesses, and government organizations. Our business does not depend on any single end customer. For a definition of customer, see the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations—Key Business Metrics—Customers with ARR of $100,000 or More."

Seasonality

We experience seasonal fluctuations in our financial results due to the annual budget approval process of many of our customers. We typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in our fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers.

Human Capital Resources

Our Team

As of January 31, 2024, we had over 2,300 full-time employees worldwide. We also engage temporary employees and consultants as needed to support our operations.

Our US-based employees include team members in all key functions, including go-to-market, customer success, technology, product, and support. Each of our US offices has a different functional focus but shares a driven, customer-centric culture. Our headquarters in Mountain View, California is where the majority of our executive team, marketing, finance, legal, people and talent, and sales operations is located, which supports cross functional collaboration.

Our office in Tel Aviv, Israel benefits from Israel's concentration of cybersecurity experts. This team draws from a deep pool of Israeli military cybersecurity and intelligence experts, product mavens, and general technical talent. Our office in Prague, Czech Republic houses research and product development functions to augment current teams across the globe and the expansion of our global engineering organization.

Our European head office is in Amsterdam, Netherlands, which we chose for its talent pool, language versatility, diversity, labor and tax laws, and central location in relation to our offices in the US and Israel.

Our Dubai office is primarily focused on go-to-market activities in the Middle East and Africa and supports our new business efforts in connecting with both customers and partners across these regions.

Our Bangalore, India office houses engineering talent as well as supportive functions across general, administrative and go-to-market. The economic climate in India continues to expand with endless potential. We are excited to continue our investment across this beautiful country.

None of our employees are represented by a labor union or are a party to a collective bargaining arrangement. We have not experienced any work stoppages and we believe that our employee relations are strong.

Our Culture

Our mission is to Secure Tomorrow™ and our purpose is to be a Force for Good. Our core values are at the foundation of our equitable culture and guide our approach on how we build and grow our business with all stakeholders:

- ***Trust***. Be dependable. Conduct yourself with the highest integrity at all times.
- ***Accountability***. Be reliable in all your actions and words. Put customers first. Be the owner.
- ***OneSentinel***. Be passionate about driving team success and collaboration across our company.
- ***Relentlessness***. Act with unwavering purpose and determination in everything you do.
- ***Ingenuity***. Encourage innovative approaches to problem-solving and market leadership. Embrace diverse perspectives. Hustle.
- ***Community***. Be kind to one another. Think about how your actions will affect others. Together.

Our Employee Value Proposition was designed using feedback from employees around the globe. It is our promise to all Sentinels and candidates on what to expect while working at SentinelOne. *Here you will drive innovation*, pushing the boundaries of cybersecurity to determine what's next. *Here you will build your future*, with amazing benefits and tools to grow. *Here you will enjoy your work*, in a culture that is built on equity, integrity and autonomous action.

We value transparent and respectful communication as key components of our continuous feedback culture, something that we view as a key driver of our business success. We benefit from the varied perspectives that come from our global workforce. We believe in the strengths of diversity and are committed to building out a diverse talent base. We plan to continue investing in hiring employees both in and outside of the US.

We received multiple workplace accolades in 2023.

- Fortune recognized SentinelOne as a Best Workplace in Technology, Best Medium Workplace, Best Workplace for Millennials, and Best Workplace in the Bay Area.
- Dun's 100 list acknowledged SentinelOne as one of the Best High Tech Companies to Work for in 2023.
- SentinelOne also achieved Great Place to Work certification (December 2023 - December 2024) for the US, UK, France, India, Netherlands, Australia, Canada, Slovakia, Germany, Italy, UAE, Poland, Spain, Czechia, and Singapore.
- SentinelOne received the Best Workplaces in Tech in the UK, Best Workplaces for Women in the UK and Best workplaces in Technology in France.

Our presence and engagement across all social media platforms continue to grow rapidly, a reflection of the market's perception of us and our leadership as innovators in the cybersecurity space. We pride ourselves on offering employees an award-winning culture centered around trust and integrity, as together, we work to defeat every cyberattack with autonomous technology.

Retention and Talent Development

We believe that motivating and retaining talent at all levels is vital to our success. Our compensation and benefits program is intended to anticipate and meet the needs of our employees. In addition to base salary, these programs, which vary by country and region, include bi-annual bonuses, equity awards, an employee stock purchase plan, a 401(k) plan, including a 401(k) match in the US, healthcare and insurance benefits, health savings and flexible spending accounts, unlimited vacation, wellness reimbursement, 16 weeks of gender-neutral parental leave and more. We have increased our investment in training and development and have rolled out several key programs as well as enabling our employees to access over 1,000 on demand webinars in technical and soft skills areas.

We continue to globally align our benefits to focus on business continuity and employee well-being. We have been very intentional with our efforts to support employees while working from home and in their return to the office. Further, we have enhanced and promoted programs to support employees' physical and mental health and well-being. We have built a company that we believe thrives whether our employees are in offices or remote.

Diversity, Equity and Inclusion

We aim to cultivate and foster an inclusive workplace that is diverse, equitable, and inclusive, where Sentinels can fulfill their potential. We have developed a SentinelOne Diversity, Equity, and Inclusion (DEI) framework that includes a commitment statement and a three-year roadmap focused on moving towards our long term DEI goals. We also have five key pillars to support our DEI initiatives.

- Diversifying our talent pipeline including targeting hiring diverse slates across key functional areas and targeting underrepresented groups through our University Recruiting program.
- Amplifying the power of communities through our Inclusion Networks including Women's Inclusion Network, WIN@sentinelone; Black Inclusion Network, BLK@sentinelone; Pride Inclusion Network, Out@sentinelone; Latino Inclusion Network, Latinos@sentinelone and Veteran's Inclusion Network, Served@sentinelone.
- Holding ourselves accountable through data and insights and publishing a DEI dashboard.
- Creating an equitable culture for all through strategic partnerships including Women in Cybersecurity (also known as "WiCys"). Through the S Foundation, we offer grants and scholarships to organizations within our communities. And we have established partnerships that support and advocate for underrepresented groups in the workforce.
- Hearing all voices through our internal celebrations including Black History Month, Women's History Month, Pride, and Hispanic Heritage Month. In addition, the MentorOne program provides Sentinels the opportunity to mentor and be mentored to develop professionally.

Research and Development

Our research and development organization is responsible for the design, development, testing, and delivery of new technologies, features and integrations of our platform, as well as the continued improvement and iteration of our existing products. It is also responsible for operating and scaling our platform including its underlying infrastructure. Our most significant investments are in research and development to drive core technology innovation and bring new products to market. Research and development employees are located primarily in our Israel, India, and Czech Republic offices, and remotely.

We have a proven team that constantly works to expand our market, customer and user reach and impact with new, innovative products. We intend to continue to invest in our research and development capabilities to extend our platform and products.

Our Go-To-Market Strategy

Our sales and marketing organizations partner to create brand awareness, drive demand, and develop customer relationships to deliver strong sales pipeline coverage and revenue growth.

Sales

We sell subscriptions to our Singularity Platform through our direct sales team, which is composed of field sales and inside sales professionals. Our sales team leverages our global network of channel and alliance partners for prospect access and fulfillment. For specific market segments, our channel partners independently manage the complete sales cycle resulting in a highly scaled and leveraged sales experience. Our sales team also identifies existing customers who may be interested in free trials of additional platform modules, which serves as a powerful driver of our "land and expand" growth model. Through segmenting our sales teams by customer size, we can deploy an efficient and scalable sales model which enables rapid prospect engagement, thorough technology evaluations, and yields lasting customer relationships.

Marketing

Our marketing organization is focused on building our brand reputation, increasing the awareness of our platform, and driving prospect and customer demand. To support these efforts, we deliver broad based brand campaigns to build awareness of our solutions and our company. We also deliver targeted and situational content to demonstrate thought leadership in the security industry, including speaking engagements with the security industry's foremost organizations to provide expert advice, educating the public about the cyber threats, and identifying threat research discoveries that illustrate the business outcomes and differentiation of our solution. We engage in paid media, web marketing, out of home media advertising, industry and trade conferences, analyst engagements, producing whitepapers, demand generation via digital and web, telemarketing, and targeted displacement campaigns. We employ a wide range of digital programs, including search engine marketing, online and social media initiatives, and content syndication to increase traffic to our website and encourage new customers to request an expertly guided trial of our Singularity Platform. Additionally, we engage in joint marketing activities with our channel and alliance partners. Over the past several years, we have experienced significant increases in our brand relevance as demonstrated by coverage in leading global press, analyst publications, website traffic, web demo requests, and channel partner engagement.

Partnership Ecosystem

We work with a number of partners to create "better together" technology solutions for mutual customers, many of which we then leverage in joint go-to-market strategies. These partnerships include many of the leading ISVs, alliance partners, MSPs, MSSPs, MDRs, OEMs, and IR firms. We provide our partners with our differentiated technology and platform to enable them to provide the best security service to their own customers.

Our Singularity Platform offers our partners complete multi-tenancy and a superior level of management capability and flexibility with tiering, policy inheritance, and customizable role-based access control from the same console. Our data model and open architecture enable our partners to rapidly build and innovate across a wide range of use cases and deliver their products on top of our technology. As such, our partners are not our competitors but instead, act as force multipliers for our go-to-market investments.

Our partner integrations deliver more secure solutions and an improved end user experience to their customers. Our ISV and alliance partnerships focus on security analytics, network and infrastructure security, threat platforms and orchestration, automation, and other mainstream technology integrations.

Singularity Marketplace

Singularity Marketplace is an open application ecosystem that enables customers to seamlessly integrate dozens of applications. Organizations can gain visibility over data across historically disparate security solutions without the need for custom business logic, coding, or complex configuration. Organizations can integrate any security applications and tools regardless of vendor into a single platform without coding or scripting required. Singularity

Marketplace extends the power of our platform across the entire security and IT stack to build an effective threat defense posture with layered security, collaborative processes, and integrated products.

Singularity Marketplace enables security teams to converge on a single pane-of-glass for extended detection and response workflows to minimize context switching and distractions during triage and incident response. It helps them gain insights from shared security events without requiring a massive time investment in custom business logic, code, and complex configuration. It allows security teams to drive a unified, orchestrated response among security tools in different domains.

Competition

The market for our solutions is competitive and characterized by an evolving IT environment, customer requirements, industry standards, frequent new product and service offerings, and improvements. We compete with an array of established and emerging security solution vendors.

Our competitors include the following:

- endpoint security providers, such as CrowdStrike Holdings, Inc. (CrowdStrike) and VMware, Inc. (Carbon Black);
- legacy antivirus providers such as Trellix (formerly McAfee Corp.), Symantec (a subsidiary of Broadcom, Inc.) (Symantec), and Microsoft Corporation (Microsoft); and
- providers of general network security products and services who offer a broad portfolio of solutions, such as Palo Alto Networks, Inc. (Palo Alto Networks)

We compete on the basis of a number of factors, including but not limited to our:

- ability of our technology to detect, prevent, and block threats;
- breadth of our functionality;
- ability to automate threat prevention and remediation with limited human intervention;
- performance of our platform;
- speed of our threat hunting capabilities;
- support for cloud, hybrid, and on-premise deployments;
- support for various operating systems;
- platform data retention capabilities;
- ability to integrate with other participants in the security ecosystem;
- ease of use to deploy, manage, and maintain our platform;
- quality of our MDR service;
- strength of sales, marketing, and channel partner relationships; and
- customer support.

Although certain of our competitors enjoy greater brand awareness and recognition, deep customer relationships, and larger existing customer bases, we believe that we compete favorably with respect to our autonomous and AI-powered threat prevention, detection, response, and hunting capabilities.

Intellectual Property

The protection of our technology and intellectual property is an important aspect of our business. We rely upon a combination of trademarks, trade secrets, know-how, copyrights, patents, confidentiality procedures, contractual commitments, domain names, and other legal rights to establish and protect our intellectual property. We generally enter into confidentiality agreements and invention or work product assignment agreements with our officers, employees, agents, contractors, and business partners to control access to, and clarify ownership of, our proprietary information.

As of January 31, 2024, we had 66 issued patents and 5 pending patent applications in the US and abroad. These patents and patent applications seek to protect our proprietary inventions relevant to our business. These issued patents are scheduled to expire on or around the years between 2034 and 2042 and cover various aspects of our platform and technology.

As of January 31, 2024, we had 11 trademark registrations in the US, including registrations for "SentinelOne" and our logo. We also had 60 trademark registrations and applications in certain foreign jurisdictions. Additionally, we are the registered holder of a number of domain names, including sentinelone.com and dataset.com.

Government Regulation

We are subject to many varying laws and regulations in the US, the United Kingdom (UK), the European Union (EU) and throughout the world, including those related to privacy, data protection, intellectual property, consumer protection, marketing, advertising, employment and labor, competition, customs and international trade, taxation, and more. As we grow and expand our geographical reach, we may become subject to additional regulations in the US and internationally.

These laws often require companies to implement specific information security controls to protect certain types of information, such as personal data. These laws and regulations are constantly evolving and may be interpreted, applied, created, or amended in a manner that could harm our current or future business. Our compliance with these laws and regulations may be onerous and could, individually or in the aggregate, increase our cost of doing business, impact our competitive position relative to our peers, and/or otherwise adversely affect our business, reputation, operating results, and financial condition. However, we believe we are currently in material compliance with such laws and regulations to which we are subject and do not currently expect continued compliance to have a material impact on our capital expenditures, earnings, or competitive position. See the section titled "Risk Factors" for additional information about the laws and regulations we are subject to and the risks of our business associated with such laws and regulations.

Corporate Information

We were incorporated in the State of Delaware as Sentinel Labs, Inc. in January 2013. We changed our name to SentinelOne, Inc. in March 2021. Our principal executive offices are located at 444 Castro Street, Suite 400, Mountain View, California 94041. Our telephone number is (855) 868-3733. We completed our initial public offering (IPO) of shares of our Class A common stock in July 2021.

SentinelOne, the SentinelOne logo, and other registered or common law trade names, trademarks, or service marks of SentinelOne appearing in this prospectus are the property of SentinelOne. This prospectus contains additional trade names, trademarks, and service marks of ours and of other companies. We do not intend our use or display of other companies' trade names, trademarks, or service marks to imply a relationship with these other companies, or endorsement or sponsorship of us by these other companies. Other trademarks appearing in this prospectus are the property of their respective holders. Solely for convenience, our trademarks and trade names referred to in this prospectus appear without the ® and ™ symbols, but those references are not intended to indicate, in any way, that we will not assert, to the fullest extent under applicable law, our rights, or the right of the applicable licensor, to these trademarks and trade names.

Available Information

We file electronically with the SEC our Annual Report on Form 10-K, Definitive Proxy Statements on Schedule 14A, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, and amendments to reports filed or furnished pursuant to Section 13(a) or 15(d) of the Exchange Act. The SEC maintains a website at www.sec.gov that contains reports, proxy and information statements and other information that we file with the SEC electronically. We will make available on our website at www.sentinelone.com, free of charge, copies of these reports and other information as soon as reasonably practicable after we electronically file such material with, or furnish it to, the SEC.

We use our investor relations page on our website (www.sentinelone.com), press releases, public conference calls, public webcasts, our X account (@SentinelOne), our Facebook page, and our LinkedIn page as means of disclosing material non-public information and for complying with our disclosure obligations under Regulation FD. The information disclosed by the foregoing channels could be deemed to be material information. As such, we encourage investors, the media, and others to follow the channels listed above and to review the information disclosed through such channels. Any updates to the list of disclosure channels through which we will announce information will be posted on the investor relations page on our website.

The contents of the websites referred to above are not incorporated into this filing. Further, our references to the URLs for these websites are intended to be inactive textual references only.

ITEM 1A. RISK FACTORS

Investing in our Class A common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, together with all of the other information in this Annual Report on Form 10-K, including the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations," and our consolidated financial statements and the accompanying notes included before making a decision to invest in our Class A common stock. Our business, financial condition, operating results, or prospects could also be adversely affected by risks and uncertainties that are not presently known to us or that we currently believe are not material. If any of the risks actually occur, our business, financial condition, operating results, and prospects could be adversely affected. In that event, the market price of our Class A common stock could decline, and you could lose all or part of your investment.

Summary Risk Factors

Our business is subject to numerous risks and uncertainties, including those risks more fully described below. These risks include, among others, the following, which we consider our most material risks:

Risks Related to Our Business and Industry

- We have a limited operating history, which makes it difficult to evaluate our current business and future prospects and increases the risks associated with your investment.
- We have a history of losses, anticipate increases in our operating expenses in the future, and may not achieve or sustain profitability. If we cannot achieve and sustain profitability, our business, operating results, and financial condition will be adversely affected.
- We face intense competition and could lose market share to our competitors, which would adversely affect our business, operating results, and financial condition.
- Our operating results may fluctuate significantly, which could make our future results difficult to predict and could cause our operating results to fall below expectations.
- Adverse global macroeconomic conditions or reduced information technology spending could adversely affect our business, operating results, and financial condition.
- A network or data security incident against us, whether actual, alleged, or perceived, would harm our reputation, create liability, and regulatory exposure, and adversely affect our business, operating results, and financial condition.
- Defects, errors, or vulnerabilities in our platform, the failure of our platform to block malware or prevent a security breach, misuse of our platform, or risks of product liability claims would harm our reputation and adversely affect our business, operating results, and financial condition.
- Existing and future acquisitions, strategic investments, partnerships, or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, operating results, and financial condition.
- If we are unable to retain our customers, renew and expand our relationships with them, and add new customers, we may not be able to sustain revenue growth, and we may not achieve or maintain profitability in the future.
- If our platform is not effectively interoperated within our customers' IT infrastructure, deployments could be delayed or canceled, which would adversely affect our business, operating results, and financial condition.
- Disruptions or other business interruptions that affect the availability of our platform could adversely affect our customer relationships and overall business.

- We may not be able to timely and cost-effectively scale and adapt our existing technology to meet our customers' performance and other requirements.
- If we are unable to maintain successful relationships with our channel partners and alliance partners, or if our channel partners or alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, operating results, and financial condition will be harmed.

Risks Related to Regulatory Matters

- If we fail to adequately protect personal information or other information we collect, process, share, or maintain under applicable laws, our business, operating results, and financial condition could be adversely affected.

Risks Related to Our People

- We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to hire, integrate, train, manage, retain, and motivate qualified personnel, including members of our board of directors, could harm our business.

Risks Related to Our Intellectual Property

- Our proprietary rights may be difficult to enforce, which could enable others to copy or use aspects of our platform without compensating us.
- Third parties have claimed and may claim in the future that our platform infringes their intellectual property rights, and this may create liability for us or otherwise adversely affect our business, operating results, and financial condition.

Risks Related to Ownership of Our Class A Common Stock

- The market price of our Class A common stock may be volatile, and you could lose all or part of your investment.
- The dual class structure of our common stock has the effect of concentrating voting control with certain stockholders who held our capital stock prior to the completion of our IPO, including our directors, executive officers, and other beneficial owners who hold in the aggregate approximately 72% of the voting power of our capital stock, which will limit or preclude your ability to influence corporate matters, including the election of directors and the approval of any change of control transaction.

Risks Related to Our Business and Industry

We have a limited operating history, which makes it difficult to evaluate our current business and future prospects and increases the risks associated with your investment.

We were founded in January 2013 and released our first endpoint security solution in February 2015. Our limited operating history and financial data may make it difficult to evaluate our current business, future prospects and other trends. We have encountered, and will continue to encounter, risks and uncertainties frequently experienced by growing companies in rapidly changing industries and sectors, such as the risks and uncertainties described herein. Any predictions about our future revenue and expenses may not be as accurate as they would be if we had a longer operating history or operated in a more predictable or established market. If our assumptions regarding these risks and uncertainties are incorrect or change due to fluctuations in our markets or otherwise, or if we do not address these risks successfully, our operating and financial results could differ materially from our expectations, and our business and operating results would be adversely affected. We cannot assure you that we will be successful in addressing these and other challenges we may face in the future. The risks associated with having a limited operating history may be exacerbated by current global macroeconomic conditions.

We have a history of losses, anticipate increases in our operating expenses in the future, and may not achieve or sustain profitability. If we cannot achieve and sustain profitability, our business, operating results, and financial condition will be adversely affected.

We have incurred net losses in all periods since our inception, and we may not achieve or maintain profitability in the future. We experienced a net loss of $338.7 million and $378.7 million for the fiscal years ended January 31, 2024 and 2023, respectively. As of January 31, 2024, we had an accumulated deficit of $1.3 billion. While we have historically experienced significant growth in revenue, we cannot predict when or whether we will reach or maintain profitability. We also expect our operating expenses to increase in the future as we continue to invest for our future growth, including expanding our research and development function to drive further development of our platform, expanding our sales and marketing activities, developing the functionality to expand into adjacent markets, and reaching customers in new geographic locations, which will negatively affect our operating results if our total revenue does not increase. In addition to the anticipated costs to grow our business, we have incurred and expect to continue to incur significant additional legal, accounting, and other expenses as a public company, particularly now that we are no longer an emerging growth company. Our revenue growth is expected to slow as we grow and our revenue may decline for a number of other reasons, including reduced demand for our platform, increased competition, a decrease in the growth or reduction in size of our overall market, or if we cannot capitalize on growth opportunities, including acquisitions, new products, services, and feature releases. While we consistently evaluate opportunities to reduce our operating costs and optimize efficiencies, including, for example, our restructuring plan in June 2023, we cannot guarantee that these efforts will be successful or that we will not re-accelerate operating expenditures in the future in order to capitalize on growth opportunities. If we fail to increase our revenue to offset increases in our operating expenses or manage our costs as we invest in our business, we may not achieve or sustain profitability.

We face intense competition and could lose market share to our competitors, which would adversely affect our business, operating results, and financial condition.

The market for cybersecurity products and services is intensely competitive, fragmented and is rapidly evolving, characterized by changes in technology, customer requirements, industry standards, increasingly sophisticated attackers, and frequent introductions of new or improved products and services. We expect to continue to face intense competition from current competitors, as well as from new entrants into the market, as our competitors complete strategic acquisitions or form cooperative relationships and/or customer requirements evolve. If we are unable to anticipate or react to these challenges, our competitive position could weaken, and we would experience a decline in revenue or reduced revenue growth, and loss of market share that would adversely affect our business, operating results, and financial condition. For a description of our competitors, see the section titled “Business—Competition.”

Our ability to compete effectively depends upon numerous factors, many of which are beyond our control, including, but not limited to:

- our ability to attract and retain new customers, expand our platform or sell additional products and services to our existing customers;
- our ability to attract, train, retain, and motivate talented employees;
- our ability to successfully incorporate new technologies into our platform, including AI;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of our customers, including any slowdown in technology spending due to US and general global macroeconomic conditions;
- general global macroeconomic and political conditions, both domestically and in our foreign markets that could impact some or all regions where we operate, including global economic slowdowns, actual or perceived global banking and finance related issues, increased risk of inflation, potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto, interest rate volatility, supply chain disruptions, labor shortages, and potential global recession;

- the impact of natural or man-made global events on our business, including wars and other armed conflict, such as the conflicts in the Middle East, Ukraine and the tensions between China and Taiwan;
- changes in customer, distributor or reseller requirements or market needs;
- price competition;
- the timing and success of new product and service introductions by us or our competitors or any other change in the competitive landscape of our industry, including consolidation among our competitors or customers and strategic partnerships entered into by and between our competitors;
- changes in our mix of products, subscriptions and services sold, including changes in the average contract length for subscriptions and support;
- our ability to successfully and continuously expand our business domestically and internationally;
- changes in the growth rate of endpoint security, cloud security, and overall cybersecurity product platform and services sectors;
- deferral of orders from customers in anticipation of new or enhanced products and services announced by us or our competitors;
- significant security breaches of, technical difficulties with, or interruptions to the use of our platform;
- the timing and costs related to the development or acquisition of technologies, businesses, or strategic partnerships;
- our ability to execute, complete, or efficiently integrate any acquisitions that we may undertake;
- increased expenses, unforeseen liabilities, or write-downs and any impact on our operating results from any acquisitions we consummate;
- our ability to increase the size and productivity of our distribution channels;
- decisions by potential customers to purchase security solutions from larger, more established security vendors or from their primary network equipment vendors;
- timing of revenue recognition and revenue deferrals;
- insolvency or credit difficulties confronting our customers, which could increase due to US and global macroeconomic issues, including actual or perceived global banking and finance related issues, inflation, interest rate volatility, and market downturns, which would adversely affect their ability to purchase or pay for our platform, products, and services in a timely manner or at all;
- the cost and potential outcomes of litigation or other proceedings, which could have a material adverse effect on our business;
- future accounting pronouncements or changes in our accounting policies; and
- increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates.

Many of our competitors have greater financial, technical, marketing, sales, and other resources, greater name recognition, longer operating histories, and a larger base of customers than we do. Our competitors may be able to devote greater resources to the development, promotion and sale of their products and services than we can, and they may offer lower pricing than we do or bundle certain competing products and services at lower prices. Our competitors may also have greater resources for research and development of new technologies, customer support and to pursue acquisitions, or they may have other financial, technical, or other resource advantages. Our larger competitors have substantially broader and more diverse product and service offerings and more mature distribution

and go-to-market strategies, which allows them to leverage their existing customer and distributor relationships to gain business in a manner that discourages potential customers from purchasing our platform.

Conditions in our market could change rapidly and significantly as a result of technological advancements, including but not limited to increased advancements and proliferation in the use of open artificial intelligence applications, partnering or acquisitions by our competitors or continuing market consolidation. Some of our competitors have recently made or could make acquisitions of businesses or have established cooperative relationships that may allow them to offer more directly competitive and comprehensive products and services than were previously offered and adapt more quickly to new technologies and customer needs. These competitive pressures in our market or our failure to compete effectively may result in price reductions, fewer orders, reduced revenue and gross margin, increased net losses, and loss of market share. Even if there is significant demand for endpoint and cloud security solutions like ours, if our competitors include functionality that is, or is perceived to be, equivalent to or better than ours in legacy products that are already generally accepted as necessary components of an organization's IT security architecture, we will have difficulty increasing the market penetration of our platform. Furthermore, even if the functionality offered by other cybersecurity providers is different and more limited than the functionality of our platform, organizations may elect to accept such limited functionality in lieu of purchasing products and services from additional vendors like us. If we are unable to compete successfully, or if competing successfully requires us to take aggressive action with respect to pricing or other actions, our business, financial condition, and operating results would be adversely affected.

Our operating results may fluctuate significantly, which could make our future results difficult to predict and could cause our operating results to fall below expectations.

Our operating results have varied significantly from period to period in the past, and we expect that our operating results will continue to vary significantly in the future such that period-to-period comparisons of our operating results may not be meaningful. This could adversely affect our business, operating results, and financial condition. Accordingly, our financial results in any one quarter should not be relied upon as indicative of future performance. Fluctuations in quarterly results may negatively impact the trading price of our Class A common stock. Our quarterly financial results may fluctuate as a result of a number of factors, many of which are outside of our control and may be difficult to predict, including, without limitation:

- general global macroeconomic and political conditions, both domestically and in our foreign markets that could impact some or all regions where we operate, including global economic slowdowns, actual or perceived global banking and finance related issues, increased risk of inflation, potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto, interest rate volatility, supply chain disruptions, labor shortages and potential global recession;
- the impact of natural or man-made global events on our business, including wars and other armed conflict, such as the conflicts in the Middle East, Ukraine and tensions between China and Taiwan;
- our ability to attract new and retain existing customers or sell additional features to existing customers;
- the budgeting cycles, seasonal buying patterns, and purchasing practices of customers;
- the timing and length of our sales cycles;
- changes in customer or channel partner requirements or market needs;
- changes in the growth rate of the cybersecurity market generally and market for endpoint security;
- the timing and success of new product and service introductions by us, including PinnacleOne, our strategic risk analysis and advisory group, and Singularity Data Lake, our live enterprise data platform for data queries, analytics, insights, and retention, or our competitors or any other competitive developments, including consolidation among our customers or competitors;
- the level of awareness of cybersecurity threats, particularly advanced cyberattacks, and the market adoption of our platform;

- our ability to successfully expand our business domestically and internationally;
- decisions by organizations to purchase security solutions from larger, more established security vendors or from their primary IT equipment vendors;
- changes in our pricing policies or those of our competitors;
- any disruption in our relationship with ISVs, channel partners, MSPs, MSSPs, MDRs, OEMs, and IR firms;
- insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solution;
- significant security breaches of, technical difficulties with, or interruptions to, the use of our platform or other cybersecurity incidents;
- extraordinary expenses such as litigation or other dispute-related settlement payments or outcomes, taxes, regulatory fines or penalties;
- future accounting pronouncements or changes in our accounting policies or practices;
- negative media coverage or publicity;
- the amount and timing of operating costs and capital expenditures related to the expansion of our business; and
- increases or decreases in our expenses caused by fluctuations in foreign currency exchange rates.

In addition, we experience seasonal fluctuations in our financial results as we typically receive a higher percentage of our annual orders from new customers, as well as renewal orders from existing customers, in our fourth fiscal quarter as compared to other quarters due to the annual budget approval process of many of our customers.

Any of the above factors, individually or in the aggregate, may result in significant fluctuations in our financial and other operating results from period to period. As a result of this variability, our historical operating results should not be relied upon as an indication of future performance. Moreover, this variability and unpredictability could result in our failure to meet our operating plan or the expectations of investors or analysts for any period. If we fail to meet such expectations for the reasons described above or other reasons, our stock price could fall substantially, and we could face costly lawsuits, including securities class action lawsuits.

Adverse global macroeconomic conditions or reduced information technology spending could adversely affect our business, operating results, and financial condition.

Our business depends on the overall demand for information technology and on the economic health of our current and prospective customers. In addition, the purchase of our platform is often discretionary and may involve a significant commitment of capital and other resources. Weak global and regional economic conditions, including US and global macro-economic issues, actual or perceived global banking and finance related issues, labor shortages, supply chain disruptions, rising interest rates and inflation, spending environments, geopolitical instability, warfare and uncertainty, weak economic conditions in certain regions or a reduction in information technology spending regardless of macro-economic conditions, including the effects of the conflicts in the Middle East, Ukraine, and tensions between China and Taiwan and judicial reform in Israel, could adversely affect our business, operating results, and financial condition, including resulting in longer sales cycles, a negative impact on our ability to attract and retain new customers or expand our platform or sell additional products and services to our existing customers, lower prices for our platform, higher default rates among our channel partners, reduced sales to new or existing customers and slower or declining growth. For example, as a result of current uncertainty in macroeconomic conditions and related higher cost consciousness around IT budgets, we have recently experienced certain impacts on our business, including a decline in usage and consumption patterns from certain customers, especially larger enterprise customers, longer sales cycles, and deal downsizing by new customers and of renewals by existing

customers, especially larger enterprises. We expect the global macroeconomic conditions impacting demand to persist in the near term. Deterioration in economic conditions in any of the countries in which we do business could also cause slower or impaired collections on accounts receivable, which may adversely impact our liquidity and financial condition.

Moreover, the US capital markets have experienced and continue to experience extreme volatility and disruption. Inflation rates in the US significantly increased in 2021 and 2022, resulting in federal action to increase interest rates, adversely affecting capital markets activity. Further deterioration of the macroeconomic environment and regulatory action may adversely affect our business, operating results, and financial condition.

We are investing in expanding our platform, including our cloud security products, and it is difficult to predict adoption and demand.

We are meaningfully investing in our platform, including growing our cloud security product. For example, in November 2023, through the acquisition of KSG, we launched PinnacleOne, a strategic advisory group also operating as a think tank for hire, focused on helping companies and their executives holistically understand the evolving risks of operating in the modern global business landscape through personalized access to experts' intelligence, insight, and transformative risk management strategies. Further, in February 2024, we acquired PingSafe, a cloud security platform, which we expect will enable us to couple PingSafe's CNAPP with our cloud workload security and cloud data security capabilities.

It is difficult to predict customer adoption and demand for our platform, the size and growth rate of this market, the entry of competitive products and services or the success of existing competitive products and services.

Any expansion in our market depends on a number of factors, including the cost, performance and perceived value associated with, and customer adoption of, our platform. If the market for our platform does not achieve widespread adoption or there is a reduction in demand for our software or our services caused by a lack of customer acceptance, implementation challenges for deployment, technological challenges, competing technologies and services, decreases in corporate spending, weakening economic conditions, or otherwise, it could result in reduced customer orders and decreased revenue, which would adversely affect our business operations and financial condition.

Our platform interoperates with, but does not necessarily replace, other security and log analytics products. Businesses that use other cybersecurity products and services may be hesitant to purchase our platform if they believe their existing products and services provide a level of security that is sufficient to meet their needs. If we do not succeed in convincing customers that our platform should be an integral part of their overall approach to security, our sales will not grow as quickly as anticipated, or at all, which would have an adverse impact on our business, operating results, and financial condition.

If businesses do not continue to adopt our platform for any of the reasons discussed above or for other reasons not contemplated, our sales would not grow as quickly as anticipated, or at all, and our business, operating results, and financial condition would be adversely affected.

We may not be successful in our artificial intelligence initiatives, which could adversely affect our business, reputation, or financial results.

We have recently begun incorporating generative AI into our offerings, including our Purple AI solution dedicated to threat-hunting, analysis and response. As with many innovations, generative AI presents risks, challenges, and unintended consequences that could impact our successful ability to incorporate the use of generative AI in our business. For example, language models may provide flawed results or misinterpret prompts. Further, data practices by us or others that result in controversy could also impair the acceptance of AI solutions. This is turn could undermine confidence in the decisions, predictions, analyses or other content that our AI-initiatives produce. In addition, our competitors or other third parties may incorporate generative AI solutions into their products more successfully than us, and their solutions may achieve higher market acceptance than ours, which may result in us failing to recoup our investments in developing generative AI-powered offerings. We have made and expect to continue to make significant investments in our AI technology, including in our Purple AI solution. Our ability to employ AI, or the ability of our competitors to do so more successfully, may negatively impact our gross margins, impair our ability to compete effectively, result in reputational harm and have an adverse impact on our operating results.

Moreover, AI may give rise to litigation risk, including potential intellectual property, privacy, or cybersecurity liability. Because AI is an emerging technology, there is not a mature body of case law construing the appropriateness of certain of its uses of data - whether through the employment of large language models or other models leveraging data found on the Internet - and the evolution of this law may limit our ability to exploit artificial intelligence tools, or expose us to litigation. Further, AI presents emerging ethical issues and if our use of AI algorithms draws controversy due to their perceived or actual impact on society, we may experience brand or reputational harm, competitive harm or legal liability.

In addition, given the complex nature of AI technology, we face an evolving regulatory landscape. For example, in October 2023, President Biden issued an Executive Order that establishes new standards for, among other things, AI safety, security, and privacy. Moreover, we are subject to significant competition from other companies, some of which have longer operating histories and significantly greater financial, technical, marketing, distribution, professional services, or other resources than us. Our competitors may incorporate AI into their products more quickly or more successfully than us, which could impair our ability to compete effectively and adversely affect our financial results. Any of the foregoing could adversely affect our business, reputation, or financial results.

A network or data security incident against us, whether actual, alleged, or perceived, would harm our reputation, create liability and regulatory exposure, and adversely impact our business, operating results, and financial condition.

Companies are subject to an increasing number and wide variety of attacks on their networks on an ongoing basis. Traditional computer “hackers,” malicious code (such as viruses and worms), phishing attempts, ransomware, account takeover, business email compromise, employee fraud, theft or misuse, denial of service attacks, and sophisticated nation-state and nation-state supported actors engage in intrusions and attacks that create risks for our internal networks and cloud deployed products and the information they store and process. Cybersecurity companies face particularly intense attack efforts, and we have faced, and will continue to face, cyber threats and attacks from a variety of sources. The research that we conduct and report may make us, or our customers, a further target for attacks of all kinds. State-supported and geopolitical-related cyberattacks may rise in connection with regional geopolitical conflicts such as the conflicts in the Middle East, Ukraine and tensions between China and Taiwan. In addition, our cybersecurity product is likely considered a valuable target for lateral attacks because of its highly privileged access. Moreover, the ongoing war in Ukraine and associated activities in Ukraine and Russia have increased the risk of cyberattacks on various types of infrastructure and operations, and the US government has warned companies to be prepared for a significant increase in Russian cyberattacks in response to the sanctions on Russia. There may also be increased risks of cybersecurity attacks as a result of the unfolding events in the Middle East. Additionally, bad actors are beginning to utilize AI-based tools to execute attacks, creating unprecedented cybersecurity challenges.

Although we have implemented security measures to prevent such attacks, our networks and systems may be breached due to the actions of outside parties, human or employee error, insufficient cybersecurity controls, malfeasance, a combination of these, or otherwise, and as a result, an unauthorized party may obtain access to our and/or our customers' systems, networks, or data. We may face difficulties or delays in identifying or otherwise responding to any attacks or actual or potential security breaches or threats. These risks are exacerbated by developments in generative AI. A breach in our data security or an attack against our platform could impact our networks or the networks and data of our customers that are secured by our platform, creating system disruptions or slowdowns and providing access to malicious parties to information stored on our networks or the networks of our customers, resulting in data being publicly disclosed, misused, altered, lost, or stolen, which could subject us to liability and adversely affect our financial condition. If compromised, our own systems could be used to facilitate or magnify an attack. Further, the increase in remote work by companies and individuals in recent years has generally increased the attack surface available to bad actors for exploitation, and as such, the risk of a cybersecurity incident potentially occurring has increased. We have accordingly increased our investments in protective measures and risk mitigation strategies, but we cannot guarantee that our efforts, or the efforts of those upon whom we rely and partner with, will be successful in preventing any such information security incidents. Protecting our own assets has become more expensive from a dollar investment and time perspective and these costs may increase as the threat landscape increases, including as a result of use by bad actors of AI.

Any actual, alleged, or perceived security breach in our systems or networks, or any other actual, alleged or perceived data security incident we suffer, could result in damage to our reputation, negative publicity, loss of customers and sales, loss of competitive advantages over our competitors, increased costs to remedy any problems and otherwise respond to any incident, regulatory investigations and enforcement actions, fines and penalties, costly litigation, and other liability. We would also be exposed to a risk of loss or litigation and potential liability under laws, regulations, and contracts that protect the privacy and security of personal information. For example, the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act (CPRA), imposes a private right of action for security breaches that could lead to some form of remedy including regulatory scrutiny, fines, private right of action settlements, and other consequences. Where a security incident involves a breach of security leading to the accidental or unlawful destruction, loss, alternation, unauthorized disclosure of, or access to, personal data from the European Economic Area (EEA) or the UK in respect of which we are a controller or processor under the General Data Protection Regulation (GDPR), and the UK General Data Protection Regulation and UK Data Protection Act 2018 (UK GDPR), this could result in fines of up to €20 million or 4% of annual global turnover, whichever is greater, under the GDPR or up to £17.5 million or 4% of annual global turnover, whichever is greater, in the case of the UK GDPR. We may also be required to provide notice of such breaches to regulators and/or individuals which may result in us incurring additional costs, penalties, fines or litigation. Further, on July 26, 2023, the SEC adopted cybersecurity disclosure rules for public companies that require disclosure regarding cybersecurity risk management (including the board's role in overseeing cybersecurity risks, management's role and expertise in assessing and managing cybersecurity risks and processes for assessing, identifying and managing cybersecurity risks) in annual reports on Form 10-K. These cybersecurity disclosure rules also require the disclosure of material cybersecurity incidents by Form 8-K, within four business days of determining an incident is material. Any public disclosure relating to a material cybersecurity incident, whether as a result of the new SEC rules or otherwise, harm our reputation, result in litigation and adversely impact our business, operating results, and financial condition.

In addition, certain of our customer agreements may require us to promptly report security breaches involving their data on our systems or those of subcontractors processing such data on our behalf. This mandatory disclosure could be costly, result in litigation, harm our reputation, erode customer trust, and require significant resources to mitigate issues stemming from actual or perceived security breaches.

In addition, we may incur significant financial and operational costs to investigate, remediate, eliminate and put in place additional tools and devices designed to prevent actual or perceived security breaches and other security incidents, as well as costs to comply with any notification obligations resulting from any security incidents. Any of these negative outcomes could adversely affect the market perception of our platform and customer and investor confidence in our company, and would adversely affect our business, operating results, and financial condition.

Defects, errors, or vulnerabilities in our platform, the failure of our platform to block malware or prevent a security breach, misuse of our platform, or risks of product liability claims would harm our reputation and adversely impact our business, operating results, and financial condition.

Our platform and product features are multi-faceted and may be deployed with material defects, software "bugs" or errors that are not detected until after their commercial release and deployment to our customers. From time to time, certain of our customers have reported defects in our platform related to performance, scalability, and compatibility. Our platform and product features also provide our customers with the ability to customize a multitude of settings, and it is possible that a customer could misconfigure our platform or otherwise fail to configure our products in an optimal manner. Such defects and misconfigurations of our platform could cause our platform to operate at suboptimal efficacy, cause it to fail to secure customers' computing environments and detect and block threats, or temporarily interrupt our customers' computing environments. We also make frequent updates to our platform, which may fail, resulting in temporary vulnerability that increases the likelihood of a material defect.

In addition, because the techniques used by computer hackers to access or sabotage target computing environments change frequently and generally are not recognized until launched against a target, there is a risk that an advanced attack could emerge that our platform is unable to detect or prevent. Furthermore, as a well-known provider of security solutions, our networks, platform, products, including cloud-based technology, and customers could be targeted by attacks specifically designed to disrupt our business, harm our reputation or use our technology to gain unauthorized access. In addition, regional geopolitical conflicts such as the conflicts in the Middle East, Ukraine and tensions between China and Taiwan, may result in increased cyberattacks against our customers, resulting in an increased risk of a security breach of our customers' systems. In addition, defects or errors in our platform could result in a failure to effectively update customers' cloud-based products. Our data centers and networks may experience technical failures and downtime, may fail to distribute appropriate updates, or may fail to meet the increased requirements of a growing customer base, any of which could temporarily or permanently expose our customers' computing environments, leaving their computing environments unprotected against cyber threats. Any of these situations could result in negative publicity to us, damage our reputation, and increase expenses and customer relations issues, which would adversely affect our business, financial condition, and operating results.

Advances in computer capabilities, discoveries of new weaknesses and other developments with software generally used by the Internet community may increase the risk we will suffer a security breach. Furthermore, our platform may fail to detect or prevent malware, ransomware, viruses, worms or similar threats for any number of reasons, including our failure to enhance and expand our platform to reflect industry trends, new technologies and new operating environments, the complexity of the environment of our clients and the sophistication of malware, viruses and other threats. Our platform may fail to detect or prevent threats in any particular test for a number of reasons. We or our service providers may also suffer security breaches or unauthorized access to personal information, financial account information, and other confidential information due to employee error, rogue employee activity, unauthorized access by third parties acting with malicious intent or who commit an inadvertent mistake or social engineering. If we experience, or our service providers experience, any breaches of security measures or sabotage or otherwise suffer unauthorized use or disclosure of, or access to, personal information, financial account information or other confidential information, we might be required to expend significant capital and resources to address these problems. We may not be able to remedy any problems caused by hackers or other similar actors in a timely manner, or at all. To the extent potential customers, industry analysts or testing firms believe that the failure to detect or prevent any particular threat is a flaw or indicates that our platform does not provide significant value, our reputation and business would be harmed. Any real or perceived defects, errors or vulnerabilities in our platform, or any other failure of our platform to detect an advanced threat, could result in:

- a loss of existing or potential customers;
- delayed or lost revenue and adverse impacts to our business, operating results, and financial condition;
- a delay in attaining, or the failure to attain, market acceptance;

- the expenditure of significant financial and research and development resources in efforts to analyze, correct, eliminate, or work around errors or defects, and address and eliminate vulnerabilities;
- an increase in resources devoted to customer service and support, which could adversely affect our gross margin;
- harm to our reputation or brand; and
- claims and litigation, regulatory inquiries, or investigations, enforcement actions, and other claims and liabilities, all of which may be costly and burdensome and further harm our reputation.

Because techniques used to obtain unauthorized access or to sabotage systems change frequently and generally are not recognized until after they are launched against a target, we and our service providers may be unable to anticipate these techniques or to implement adequate preventative measures. Moreover, if a high-profile cybersecurity incident occurs with respect to another SaaS provider, customers may lose trust in the security of the SaaS business model generally, which could adversely affect our ability to retain existing customers or attract new ones. In the last few years there have been many successful advanced cybersecurity incidents that have damaged several prominent companies despite strong information security measures. We expect that the risks associated with cybersecurity incidents and the costs of preventing such attacks will continue to increase in the future.

In addition, we cannot assure you that any limitation of liability provisions in our customer agreements, contracts with third-party vendors and service providers, or other contracts would be enforceable or adequate or would otherwise protect us from any liabilities or damages with respect to any particular claim relating to a security breach or other security-related matter or as a result of federal, state, or local laws or ordinances, or unfavorable judicial decisions in the US, or other countries. We maintain insurance to protect against certain claims associated with the use of our platform, but our insurance coverage may not adequately cover any claim asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management's time and other resources, and harm our reputation. We also cannot be certain that our insurance coverage will be adequate for data handling or data security liabilities actually incurred, that insurance will continue to be available to us on economically reasonable terms, or at all, or that any future claim will not be excluded or otherwise be denied coverage by any insurer. The successful assertion of one or more large claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co-insurance requirements, could adversely affect our business, operating results, and financial condition.

Existing and future acquisitions, strategic investments, partnerships or alliances could be difficult to identify and integrate, divert the attention of key management personnel, disrupt our business, dilute stockholder value and adversely affect our business, operating results, and financial condition.

As part of our business strategy, we have in the past and expect to continue to make investments in and/or acquire complementary companies, services, products, technologies, or talent. For example, in February 2021 we acquired Scalyr, a data analytics company, in May 2022 we acquired Attivo, a leading identity security and lateral movement protection company, in November 2023 we acquired KSG, a strategic advisory group, and in February 2024 we acquired both PingSafe, a cloud security platform, and Stride, a security automation company. We have also invested in certain privately held companies through our S Ventures fund, and we may not realize a return on these investments. All of our venture investments are subject to a risk of partial or total loss of investment capital. Our ability as an organization to acquire and integrate other companies, services or technologies in a successful manner is not guaranteed.

In the future, we may not be able to find suitable acquisition candidates, and we may not be able to complete such acquisitions on favorable terms, if at all. Our due diligence efforts may fail to identify all of the challenges, problems, liabilities or other shortcomings involved in an acquisition. If we do complete acquisitions, we may not ultimately strengthen our competitive position or ability to achieve our business objectives, and any acquisitions we announce or complete could be viewed negatively by our customers or investors.

In addition, if we are unsuccessful at integrating existing and future acquisitions, or the technologies and personnel associated with such acquisitions, into our company, the revenue and operating results of the combined company could be adversely affected. Any integration process may require significant time and resources, and we may not be able to manage the process successfully. We may not successfully evaluate or utilize the acquired technology or personnel, or accurately forecast the financial impact of an acquisition transaction, causing unanticipated write-offs or accounting charges. Additionally, integrations could take longer than expected, or if we move too quickly in trying to integrate an acquisition, strategic investment, partnership, or other alliance, we may fail to achieve the desired efficiencies.

We have, and may in the future have, to pay cash, incur debt, or issue equity securities to pay for any such acquisition, each of which could adversely affect our financial condition and the market price of our Class A common stock. The sale of equity or issuance of debt to finance any such acquisitions could result in dilution to our stockholders, which depending on the size of the acquisition, may be significant. The incurrence of indebtedness would result in increased fixed obligations and could also include covenants or other restrictions that would impede our ability to manage our operations.

Additional risks we may face in connection with acquisitions include:

- diversion of management's time and focus from operating our business to addressing acquisition integration challenges;
- the inability to coordinate research and development and sales and marketing functions;
- the inability to integrate product and service offerings;
- retention of key employees from the acquired company;
- changes in relationships with strategic partners or the loss of any key customers or partners as a result of product acquisitions or strategic positioning resulting from the acquisition;
- cultural challenges associated with integrating employees from the acquired company into our organization;
- integration of the acquired company's accounting, customer relationship management, management information, human resources and other administrative systems;
- the need to implement or improve controls, procedures and policies at a business that prior to the acquisition may have lacked sufficiently effective controls, procedures and policies;
- unexpected security risks or higher than expected costs to improve the security posture of the acquired company;
- higher than expected costs to bring the acquired company's IT infrastructure up to our standards;
- additional legal, regulatory, or compliance requirements;
- financial reporting, revenue recognition or other financial or control deficiencies of the acquired company that we don't adequately address and that cause our reported results to be incorrect;
- liability for activities of the acquired company before the acquisition, including intellectual property infringement claims, violations of laws, commercial disputes, tax liabilities, and other known and unknown liabilities;
- failing to achieve the expected benefits of the acquisition or investment; and
- litigation or other claims in connection with the acquired company, including claims from or against terminated employees, customers, current and former stockholders, or other third parties.

Our failure to address these risks or other problems encountered in connection with acquisitions and investments could cause us to fail to realize the anticipated benefits of these acquisitions or investments, cause us to incur unanticipated liabilities, and harm our business generally.

If we are unable to retain our customers, renew and expand our relationships with them, and add new customers, we may not be able to sustain revenue growth, and we may not achieve or maintain profitability in the future.

Historically, we have experienced rapid growth in the adoption of our platform, customer base, and revenue. However, we may not return to our prior growth rates or grow at the same rate in the future. Any success that we may experience in the future will depend, in large part, on our ability to, among other things:

- maintain, renew and expand our existing customer base;
- continue to attract new customers;
- induce customers to expand deployment of the initially adopted module(s) of our platform across their organizations and infrastructure, and to adopt additional modules of our platform and services;
- improve the capabilities of our platform through research and development;
- continue to successfully expand our business domestically and internationally; and
- successfully compete with other companies in the endpoint security industry.

Our customers have no obligation to renew their subscription for our platform after the expiration of their contractual subscription period, which is generally one to three years, and in the normal course of business, some customers have elected not to renew. In addition, our customers may renew for shorter contract subscription lengths or cease using certain features. Our customer retention and expansion may decline or fluctuate as a result of a number of factors, including our customers' satisfaction with our services, our pricing, customer security and networking issues and requirements, our customers' spending levels, decreases in the number of endpoints to which our customers deploy our solution, mergers and acquisitions involving our customers, industry developments, competition, general economic conditions, or the perceived decline in the incidence of cyberattacks. If our efforts to maintain and expand our relationships with our existing customers are not successful, our business, operating results, and financial condition will materially suffer.

If our platform is not effectively interoperated within our customers' IT infrastructure, deployments could be delayed or canceled, which would adversely impact our business, operating results, and financial condition.

Our platform must effectively interoperate with our customers' existing IT infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products and services from multiple vendors, and contains multiple generations of products and services that have been added over time. As a result, our solutions can sometimes encounter interoperability issues on deployment or over time, which require additional support and problem solving with customers, in some cases, at a substantial cost to us. We may modify our software or introduce new capabilities so that our platform interoperates with a customer's infrastructure. These issues could cause longer deployment and integration times for our platform, leading to customer churn, which would adversely affect our business, operating results, and financial condition. In addition, government and other customers may require our platform to comply with certain security or other certifications and standards. If we are unable to achieve, or are delayed in achieving, compliance with these certifications and standards, we may be disqualified from selling our platform to such customers, or may otherwise be at a competitive disadvantage, either of which could adversely affect our business, operating results, and financial condition.

Disruptions or other business interruptions that affect the availability of our platform could adversely impact our customer relationships and overall business.

Our platform is hosted by third-party cloud hosting providers including AWS. Our software and systems are designed to use computing, storage capabilities, bandwidth, and other services provided by such cloud hosting providers, and currently our cloud service infrastructure is primarily run on AWS. We have experienced, and expect in the future that we may experience from time to time, interruptions, delays or outages in service availability due to a variety of factors. Capacity constraints could arise from a number of causes such as technical failures, natural disasters, fraud, or security attacks. The level of service provided by our cloud hosting providers, or regular or prolonged interruptions in that service, could also impact the use of, and our customers' satisfaction with, our platform and could harm our business and reputation. In addition, hosting costs are expected to increase as our customer base grows, which could adversely affect our business, operating results, and financial condition.

Furthermore, AWS has discretion to change and interpret its terms of service and other policies with respect to us, including on contract renewal, and those actions may be unfavorable to our business operations. AWS, and other cloud hosting providers, may also take actions beyond our control that could seriously harm our business, including discontinuing or limiting our access to one or more services, increasing pricing terms, competing with us, terminating or seeking to terminate our contractual relationship altogether, or altering how we are able to process data on their system in a way that is unfavorable or costly to us. Although we obtain services from other cloud hosting providers, if our current arrangement with AWS were to be terminated, we could experience interruptions on our platform and in our ability to make our content available to customers, as well as delays and additional expenses in arranging for expansion and transition to alternative cloud hosting and infrastructure services. Such a transition could require further technical changes to our platform, including, but not limited to, our cloud service infrastructure which was initially designed to run on AWS. Making such changes could be costly in terms of time and financial resources.

Any of these factors could reduce our revenue, subject us to liability, and cause our customers to decline to renew their subscriptions, any of which would harm our business and operating results.

We may not timely and cost-effectively scale and adapt our existing technology to meet our customers' performance and other requirements.

Our future growth is dependent upon our ability to continue to meet the needs of new customers and the expanding needs of our existing customers as their use of our solutions grows. As our customers gain more experience with our platform, the number of endpoints and events, the amount of data transferred, processed and stored by us, and the number of locations where our platform is being accessed, have in the past, and may in the future, expand rapidly. In order to meet the performance and other requirements of our customers, we intend to continue to make significant investments to increase capacity and to develop and implement new technologies in our service and cloud infrastructure operations. These technologies, which include databases, applications, and server optimizations, network and hosting strategies, and automation, are often advanced, complex, new and untested. We may not be successful in developing or implementing these technologies. In addition, it takes a significant amount of time to plan, develop and test improvements to our technologies and infrastructure, and we may not be able to accurately forecast demand or predict the results we will realize from such improvements. In some circumstances, we may also determine to scale our technology through the acquisition of complementary businesses and technologies rather than through internal development, which may divert management's time and resources. To the extent that we do not effectively scale our operations to meet the needs of our growing customer base and to maintain performance as our customers expand their use of our solution, we will not be able to grow as quickly as we anticipate, our customers may reduce or cancel use of our solutions and we will be unable to compete as effectively and our business and operating results will be adversely affected.

If we do not accurately anticipate and promptly respond to changes in our customers' technologies, business plans or security needs, our competitive position and prospects will be adversely impacted.

The cybersecurity market has grown quickly and is expected to continue to evolve rapidly. Moreover, many of our customers operate in markets characterized by rapidly changing technologies and business plans, which require

them to add numerous network-connected endpoints and adapt to increasingly complex IT environments, incorporating a variety of hardware, software applications, operating systems, and networking protocols. As their technologies and business plans grow more complex, we expect these customers to face new and increasingly sophisticated methods of attack. We face significant challenges in ensuring that our platform effectively identifies and responds to these advanced and evolving attacks, including as a result of the evolving AI landscape. As a result of the continued rapid innovations in the technology industry, including the rapid growth of smartphones, tablets and other devices, enterprise employees using personal devices for work, the rapidly evolving Internet of Things and AI, we expect the networks of our customers to continue to change rapidly and become more complex. There can be no assurance that we will be successful in developing and marketing, on a timely basis, enhancements to our platform that adequately address the changing needs of our customers. In addition, any enhancements to our platform could involve research and development processes that are more complex, expensive and time-consuming than we anticipate. We may experience unanticipated delays in the availability of enhancements to our platform and may fail to meet customer expectations with respect to the timing of such availability. If we do not quickly respond to the rapidly changing and rigorous needs of our customers by developing and releasing updates to our platform on a timely basis that can adequately respond to advanced threats and our customers' evolving needs, our business, operating results, and financial condition will be adversely affected.

If we are not able to maintain and enhance our brand and reputation, our business and operating results may be adversely affected.

We believe that maintaining and enhancing our brand and our reputation as a leading provider of endpoint and platform security solutions is critical to our relationship with our existing customers, channel partners, and alliance partners and our ability to attract new customers and partners. The successful promotion of our brand will depend on a number of factors, including our ability to continue to develop additional features for our platform, our ability to successfully differentiate our platform from competitive cloud-based or legacy security solutions, our marketing efforts, and, ultimately, our ability to detect and stop breaches. Although we believe it is important for our growth, our brand promotion activities may not be successful or yield increased revenue.

Under certain circumstances, our employees may have access to our customers' platforms. An employee may take advantage of such access to conduct malicious activities. Any such misuse of our platform could result in negative press coverage and negatively affect our reputation, which could result in harm to our business, reputation, and operating results.

In addition, independent industry and research firms often evaluate our solutions and provide reviews of our platform, as well as the products of our competitors, and perception of our platform in the marketplace may be significantly influenced by these reviews. If these reviews are negative, or less positive as compared to those of our competitors' products, our brand may be adversely affected. Our solutions may fail to detect or prevent threats in any particular test for a number of reasons that may or may not be related to the efficacy of our solutions in real world environments. To the extent potential customers, industry analysts or research firms believe that the occurrence of a failure to detect or prevent any particular threat is a flaw or indicates that our solutions or services do not provide significant value, we may lose customers, and our reputation, financial condition and business would be harmed.

Moreover, the performance of our channel partners and alliance partners may affect our brand and reputation if customers do not have a positive experience with these partners. In addition, we have in the past worked, and continue to work, with high profile customers as well as assist in analyzing and remediating high profile cyberattacks. Our work with such customers has exposed us to publicity and media coverage. Negative publicity about us, including about our management, the efficacy and reliability of our platform, our products offerings, our professional services, and the customers we work with, even if inaccurate, could adversely affect our reputation and brand.

If we are unable to maintain successful relationships with our channel partners and alliance partners, or if our channel partners or alliance partners fail to perform, our ability to market, sell and distribute our platform will be limited, and our business, operating results, and financial condition will be harmed.

Substantially all of our sales are fulfilled through our channel partners, including resellers, distributors, MSPs, MSSPs, MDRs, OEMs, and IR firms, and we expect that we will continue to generate a significant portion of our revenue from channel partners for the foreseeable future. Our agreements with our channel partners are non-exclusive, do not last for set terms, and may be terminated by either party at any time. Further, channel partners fulfill our sales on a purchase order basis and do not impose minimum purchase requirements or related terms on sales. Additionally, we have entered, and intend to continue to enter, into alliance partnerships with third parties to support our future growth plans. The loss of a substantial number of our channel partners or alliance partners, or the failure to recruit additional partners, would adversely affect our business, operating results, and financial condition.

To the extent our partners are unsuccessful in selling our platform, or if we are unable to enter into arrangements with and retain a sufficient number of high-quality partners in each of the regions in which we sell or plan to sell our platform, we are unable to keep them motivated to sell our platform, or our partners shift focus to other vendors and/or our competitors, our ability to sell our platform and operating results will be harmed. The termination of our relationship with any significant partner may adversely affect our sales and operating results. Our ability to achieve revenue growth in the future will depend in part on our ability to maintain successful relationships with our channel partners and in training our channel partners to independently sell and deploy our platform.

We are also exposed to credit and liquidity risks and our operating results will be harmed if our partners were to become unable or unwilling to pay us at all or in a timely manner, terminate their relationships with us or go out of business. Although we have programs in place that are designed to monitor and mitigate such risks, we cannot guarantee these programs will be effective in reducing our risks. If we are unable to adequately control these risks, our business, operating results, and financial condition would be harmed. If partners fail to pay us under the terms of our agreements or we are otherwise unable to collect on our accounts receivable from these partners, we may be adversely affected both from the inability to collect amounts due and the cost of enforcing the terms of our contracts, including litigation. Our partners may seek bankruptcy protection or other similar relief and fail to pay amounts due to us, or pay those amounts more slowly, either of which would adversely affect our business, operating results, and financial condition. We may be further impacted by consolidation of our existing channel partners. In such instances, we may experience changes to our overall business and operational relationships due to dealing with a larger combined entity, and our ability to maintain such relationships on favorable contractual terms may be more limited. We may also become increasingly dependent on a more limited number of channel partners, as consolidation increases the relative proportion of our business for which each channel partner is responsible, which may magnify the risks described in the preceding paragraphs.

Our business depends, in part, on sales to government organizations, and significant changes in the contracting or fiscal policies of such government organizations could adversely affect our business and operating results.

Our future growth depends, in part, on increasing sales to government organizations. Demand from government organizations is often unpredictable and subject to budgetary uncertainty. We have made significant investments to address the government sector, but we cannot assure you that these investments will be successful, or that we will be able to maintain or grow our revenue from the government sector. Although we anticipate that they may increase in the future, sales to governmental organizations have not accounted for, and may never account for, a significant portion of our revenue. Sales to governmental organizations are subject to a number of challenges and risks that may adversely affect our business and operating results, including the following risks:

- selling to governmental agencies can be highly competitive, expensive, and time consuming, often requiring significant upfront time and expense without any assurance that such efforts will generate a sale;
- government certification, software supply chain or source code transparency requirements applicable to us or our platform may change and, in doing so, restrict our ability to sell into the governmental sector until we have attained the revised certification or meet other new requirements. For example, although we are

currently FedRAMP authorized, such authorization is costly to maintain and subject to rigorous compliance and if we lose our authorization, it will restrict our ability to sell to government customers;

- government demand and payment for our platform may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our platform, including as a result of sudden, unforeseen and disruptive events such as government shutdowns, governmental defaults on indebtedness, war, regional geopolitical conflicts around the world, incidents of terrorism, natural disasters, and public health concerns or epidemics;
- governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our platform, which would adversely impact our revenue and operating results, or institute fines or civil or criminal liability if an investigation, audit, or other review, were to uncover improper or illegal activities;
- governments may require certain products to be manufactured, produced, hosted or accessed solely in their country or in other relatively high-cost locations, and we may not produce or host all products in locations that meet these requirements, affecting our ability to sell these products to governmental agencies; and
- refusal to grant certain certifications or clearance by one government agency, or decision by one government agency that our products do not meet certain standards, may cause reputational harm and cause concern with other government agencies.

The occurrence of any of the foregoing could cause governmental organizations to delay or refrain from purchasing our solutions in the future or otherwise adversely affect our business and operating results.

Our long-term success depends, in part, on our ability to expand the sale of our platform to customers located outside of the US and our current, and any further, expansion of our international operations exposes us to risks that could have a material adverse effect on our business, operating results, and financial condition.

We are generating a growing portion of our revenue outside of the US, and conduct our business activities in various foreign countries, including some emerging markets where we have limited experience, where the challenges of conducting our business can be significantly different from those we have faced in more developed markets and where business practices may create internal control risks including:

- fluctuations in foreign currency exchange rates, which could add volatility to our operating results;
- new, or changes in, regulatory requirements;
- tariffs, export and import restrictions, restrictions on foreign investments, sanctions, and other trade barriers or protection measures;
- exposure to numerous, increasing, stringent (particularly in the EU), and potentially inconsistent laws and regulations relating to privacy, data protection, and information security;
- costs of localizing products and services (including, but not limited to data localization requirements);
- lack of acceptance of localized products and services;
- the need to make significant investments in people, solutions and infrastructure, typically well in advance of revenue generation;
- challenges inherent in efficiently managing an increased number of employees over large geographic distances, including the need to implement appropriate systems, policies, benefits, and compliance programs;
- difficulties in maintaining our corporate culture with a dispersed and distant workforce;

- treatment of revenue from international sources, evolving domestic and international tax environments, and other potential tax issues, including with respect to our corporate operating structure and intercompany arrangements;
- different or weaker protection of our intellectual property, including increased risk of theft of our proprietary technology and other intellectual property;
- economic weakness or currency-related crises;
- compliance with multiple, conflicting, ambiguous or evolving governmental laws and regulations, including employment, tax, data privacy, anti-corruption, import/export, antitrust, data transfer, storage and protection, and industry-specific laws and regulations, including rules related to compliance by our third-party resellers and our ability to identify and respond timely to compliance issues when they occur and regulations applicable to us and our third party data providers from whom we purchase and resell syndicated data;
- vetting and monitoring our third-party channel partners in new and evolving markets to confirm they maintain standards consistent with our brand and reputation;
- generally longer payment cycles and greater difficulty in collecting accounts receivable;
- our ability to adapt to sales practices and customer requirements in different cultures;
- the lack of reference customers and other marketing assets in regional markets that are new or developing for us, as well as other adaptations in our market generation efforts that we may be slow to identify and implement;
- dependence on certain third parties, including channel partners with whom we do not have extensive experience;
- natural disasters, acts of war, terrorism, or pandemics, including the armed conflicts in the Middle East, Ukraine and tensions between China and Taiwan;
- actual or perceived instability in the global banking system;
- cybersecurity incidents;
- corporate espionage; and
- political instability and security risks in the countries where we are doing business and changes in the public perception of governments in the countries where we operate or plan to operate.

We have undertaken, and will continue to undertake, additional corporate operating restructurings from time to time that involve our group of foreign country subsidiaries through which we do business abroad. We consider various factors in evaluating these restructurings, including the alignment of our corporate legal entity structure with our organizational structure and its objectives, the operational and tax efficiency of our group structure, and the long-term cash flows and cash needs of our business. Such restructurings increase our operating costs, and if ineffectual, could increase our income tax liabilities and our global effective tax rate.

We have experienced rapid growth in recent periods, and if we do not effectively manage our future growth, our business, operating results, and financial condition may be adversely affected.

We have experienced rapid growth in recent periods, and we expect to continue to invest broadly across our organization to support our growth. For example, our headcount grew from over 2,100 employees as of January 31, 2023, to over 2,300 employees as of January 31, 2024. Although we have experienced rapid growth historically, we may not sustain our growth rates, nor can we assure you that our investments to support our growth will be successful. The growth and expansion of our business will require us to invest significant financial and operational resources and the continuous dedication of our management team.

In addition, as we have grown, our number of customers has also increased significantly, and we have increasingly managed more complex deployments of our platform in more complex computing environments. The rapid growth and expansion of our business places a significant strain on our management, operational, and financial resources. To manage any future growth effectively, we must continue to improve and expand our information technology and financial infrastructure, our operating and administrative systems and controls, and our ability to manage headcount, capital, and processes in an efficient manner. As a result of recent macroeconomic conditions, in June 2023, we approved a restructuring plan designed to improve operational efficiencies and operating costs and better align our workforce and operations with current business needs, priorities, and near-term growth expectations.

If we continue to experience rapid growth, we may not be able to successfully implement or scale improvements to our systems, processes, and controls in an efficient or timely manner. For example, as we grow, we may experience difficulties in managing improvements to our systems, processes, and controls or in connection with third-party software licensed to help us with such improvements. As we grow, our existing systems, processes, and controls may not prevent or detect all errors, omissions, or fraud. Any future growth will continue to add complexity to our organization and require effective coordination throughout our organization. Failure to manage any future growth effectively could result in increased costs, cause difficulty or delays in deploying new customers, reduce demand for our platform, cause difficulties in introducing new features or other operational difficulties, and any of these difficulties would adversely affect our business, operating results, and financial condition.

Our sales cycles can be long and unpredictable, and our sales efforts require considerable time and expense.

Our revenue recognition is difficult to predict because of the length and unpredictability of the sales cycle for our platform, particularly with respect to large organizations and government entities. For example, in light of current macroeconomic conditions, we have observed a lengthening of the sales cycle for some prospective customers that we attribute to higher cost-consciousness around IT budgets, which has become more pronounced recently. Customers often view the subscription to our platform as a significant strategic decision and, as a result, frequently require considerable time to evaluate, test and qualify our platform prior to entering into or expanding a relationship with us. Large enterprises and government entities in particular often undertake a significant evaluation process that further lengthens our sales cycle.

Our direct sales team develops relationships with our customers, and works with our channel partners on account penetration, account coordination, sales and overall market development. We spend substantial time and resources on our sales efforts without any assurance that our efforts will produce a sale. Security solution purchases are frequently subject to budget constraints, multiple approvals and unanticipated administrative, processing and other delays. As a result, it is difficult to predict whether and when a sale will be completed. The failure of our efforts to secure sales after investing resources in a lengthy sales process would adversely affect our business, operating results, and financial condition.

The sales prices of our platform may decrease, or the mix of our sales may change, which may reduce our gross profits and adversely affect our business, operating results, and financial condition.

We have limited experience with respect to determining the optimal prices for our platform. As the market for endpoint security matures, or as new competitors introduce new products or services that are similar to or compete with ours, we may be unable to effectively optimize our prices through increases or decreases, attract new customers at our offered prices or based on the same pricing model as we have used historically. Further, competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products or services that compete with ours or may bundle them with other products and services. This could lead customers to demand greater price concessions or additional functionality at the same price levels. As a result, in the future we may be required to reduce our prices or provide more features without corresponding increases in price, which would adversely affect our business, operating results, and financial condition.

Because we recognize revenue from subscriptions to our platform over the term of the subscription, downturns or upturns in new business will not be immediately reflected in our operating results.

We generally recognize revenue from customers ratably over the term of their subscription, which is generally one to three years. As a result, a substantial portion of the revenue we report in each period is attributable to the recognition of deferred revenue relating to agreements that we entered into during previous periods. Consequently, any increase or decrease in new sales or renewals in any one period will not be immediately reflected in our revenue for that period. Any such change, however, would affect our revenue in future periods. Accordingly, the effect of downturns or upturns in new sales and potential changes in our rate of renewals will not be fully reflected in our operating results until future periods. We may also be unable to timely reduce our cost structure in line with a significant deterioration in sales or renewals that would adversely affect our business, operating results, and financial condition.

We provide service level commitments under some of our customer contracts. If we fail to meet these contractual commitments, we could be obligated to provide partial refunds or our customers could be entitled to terminate their contracts and our business would suffer.

Certain of our customer agreements contain service level commitments, which contain specifications regarding the availability of our platform and our support services. Failure of or disruption to our infrastructure or third-party hosting service providers could impact the performance of our platform and the availability of services to customers. If we are unable to meet our stated service level commitments or if we suffer extended periods of poor performance or unavailability of our platform, we may be contractually obligated to provide affected customers with credit, partial refunds or termination rights. To date, there has not been a material failure to meet our service level commitments, and we do not currently have any material liabilities accrued on our consolidated balance sheets for such commitments. Our business, operating results, and financial condition would be adversely affected if we suffer performance issues or downtime that exceeds the service level commitments under our agreements with our customers.

Our business is subject to the risks of warranty claims, product returns and product defects from real or perceived defects in our solutions or their misuse by our customers or third parties and indemnity provisions in various agreements potentially expose us to substantial liability for intellectual property infringement and other losses.

We may be subject to liability claims for damages related to errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our platform will harm our business and operating results. Although we generally have limitation of liability provisions in our terms and conditions of sale, they may not fully or effectively protect us from claims as a result of federal, state or local laws or ordinances, or unfavorable judicial decisions in the US or other countries. The sale and support of our platform also entails the risk of product liability claims. We employ measures in the form of policy and technical controls to limit unauthorized access to our platform by our employees, customers and third parties, however, these measures may not fully or effectively protect our platform from unauthorized access.

Additionally, we typically provide indemnification to customers, partners or other third parties we do business with for certain losses suffered or expenses incurred as a result of third-party claims arising from our infringement of a third party's intellectual property. We also provide unlimited liability for certain breaches of confidentiality, as defined in our master subscription agreement. We also provide limited liability in the event of certain breaches of our master subscription agreement. Certain of these contractual provisions survive termination or expiration of the applicable agreement. However, as we continue to grow, indemnification claims against us for the obligations listed may increase.

When our customers or other third parties we do business with make intellectual property rights or other indemnification claims against us, we incur significant legal expenses and may have to pay damages, license fees and/or stop using technology found to be in violation of the third party's rights. We may also have to seek a license for the technology. Such licenses may not be available on reasonable terms, if at all, and may significantly increase our operating expenses or may require us to restrict our business activities and limit our ability to deliver certain solutions or features. We may also be required to develop alternative non-infringing technology, which could require

significant effort and expense and/or cause us to alter our platform, which could harm our business. Large indemnity obligations, whether for intellectual property or in certain limited circumstances, other claims, would harm our business, operating results and financial condition.

Additionally, our platform may be used by our customers and other third parties who obtain access to our solutions for purposes other than for which our platform was intended.

We maintain insurance to protect against certain claims associated with the use of our platform, but our insurance coverage may not adequately cover the claims asserted against us. In addition, even claims that ultimately are unsuccessful could result in our expenditure of funds in litigation, divert management's time and other resources, and harm our business and reputation. We have offered some of our customers a limited warranty, subject to certain conditions. Any failure or refusal of our insurance providers to provide the expected insurance benefits to us after we have remediated warranty claims would cause us to incur significant expense or cause us to cease offering warranties which could damage our reputation, cause us to lose customers, expose us to liability claims by our customers, negatively impact our sales and marketing efforts, and have an adverse effect on our business, operating results, and financial condition. Further, although the terms of the warranty do not allow those customers to use warranty claim payments to fund payments to persons on the US Treasury Department's Office of Foreign Assets Control (OFAC), list of Specially Designated Nationals and Blocked Persons or who are otherwise subject to US sanctions, we cannot assure you that all of our customers will comply with our warranty terms or refrain from taking actions, in violation of our warranty and applicable law.

Key business metrics and other estimates are subject to inherent challenges in measurement and to change as our business evolves, and our business, operating results, and financial condition could be adversely affected by real or perceived inaccuracies in those metrics or any changes in metrics we disclose.

We regularly review key business metrics, including our ARR, number of customers with ARR of $100,000, NRR, and other measures to evaluate growth trends, measure our performance, and make strategic decisions. These key metrics are calculated using internal company data and have not been validated by an independent third party. While these numbers are based on what we believe to be reasonable estimates for the applicable period of measurement at the time of reporting, there are inherent challenges in such measurements. If we fail to maintain effective processes and systems, our key metrics calculations may be inaccurate, and we may not be able to identify those inaccuracies. We regularly review our processes for calculating these metrics, and from time to time we make adjustments to improve their accuracy. Moreover, we may periodically change the definition or methodology underlying our key metrics. For example, as a result of a decline in usage and consumption in the quarter ended April 30, 2023, we decided to change our methodology of calculating ARR for consumption and usage-based agreements to reflect committed contract values as opposed to based on consumption and usage. In addition, as part of our quarterly review of ARR in connection with the preparation of our condensed consolidated financial statements for the quarter ended April 30, 2023, we discovered some historical inaccuracies relating to ARR on certain contracts, which we have corrected. As a result, we made a one-time adjustment of approximately 5% of total ARR, which we reflected in our total ARR as of April 30, 2023. If our key metrics are inaccurate or if investors perceive any changes to our key business metrics or the methodologies for calculating these metrics negatively, our business could be adversely affected.

Risks Related to our People

We rely on our management team and other key employees and will need additional personnel to grow our business, and the loss of one or more key employees or our inability to hire, integrate, train, manage, retain, and motivate qualified personnel, including members of our board of directors, could harm our business.

Our future success is dependent, in part, on our ability to hire, integrate, train, manage, retain, and motivate the members of our management team and other key employees throughout our organization. The loss of key personnel, including key members of our management team or members of our board of directors, as well as certain of our key marketing, sales, finance, support, product development, people team, or technology personnel, could disrupt our operations and have an adverse effect on our ability to grow our business. In particular, we are highly dependent on the services of Tomer Weingarten, our co-founder, Chairman of the Board of Directors, President, and Chief

Executive Officer, who is critical to the development of our technology, platform, future vision, and strategic direction. From time to time, there have been and may in the future be changes in our management team. While we seek to manage any such transitions carefully, such changes may result in a loss of institutional knowledge, cause disruptions to our business and negatively affect our business. Further, we maintain an office in Tel Aviv, Israel and had approximately 13% of our personnel in Israel as of January 31, 2024. We are closely monitoring the unfolding events of the armed conflict in Israel which began in October 2023. While this conflict is still evolving, to date, the conflict has not had an adverse impact on our workforce and we have implemented continuity measures to address the safety of our employees and continue our operations in the event of reduced employee availability in the conflict region. However, if our continuity measures fail or the conflict continues to worsen or intensify, any business interruptions or spillover effects could adversely affect our business and operations.

Competition for highly skilled personnel is intense, especially in the San Francisco Bay Area, where we have a substantial presence and need for highly skilled personnel, and we may not be successful in hiring or retaining qualified personnel to fulfill our current or future needs. More generally, the technology industry, and the cybersecurity industry more specifically, is also subject to substantial and continuous competition for engineers with high levels of experience in designing, developing and managing software and related services. Moreover, the industry in which we operate generally experiences high employee attrition. We have, from time to time, experienced, and we expect to continue to experience, difficulty in hiring and retaining highly skilled employees with appropriate qualifications. For example, in recent years, recruiting, hiring and retaining employees with expertise in the cybersecurity industry has become increasingly difficult as the demand for cybersecurity professionals has increased as a result of recent cybersecurity attacks on global corporations and governments. We may be required to provide more training to our personnel than we currently anticipate. Further, labor is subject to external factors that are beyond our control, including our industry's highly competitive market for skilled workers and leaders, cost inflation, overall macroeconomics and workforce participation rates. Should our competitors recruit our employees, our level of expertise and ability to execute our business plan would be negatively impacted.

In June 2023, we approved a restructuring plan, which impacted approximately 5% of our workforce. This reduction may adversely impact our ability to achieve our future operational targets. In the future, we may be unable to hire qualified employees and may be unable to successfully train those employees that we are able to hire, and as a result, employees may not become fully productive on the timelines that we have projected or at all. Further, the reduction could yield unanticipated consequences or disruptions in our day-to-day operations, such as attrition beyond planned staff reductions.

Additionally, restrictive immigration policies or legal or regulatory developments relating to immigration may also negatively affect our efforts to attract and hire new personnel as well as retain our existing personnel. Changes in US immigration and work authorization laws and regulations can be significantly affected by political forces and levels of economic activity. Our business may be adversely affected if legislative or administrative changes to immigration or visa laws and regulations impair our hiring processes.

Moreover, many of the companies with which we compete for experienced personnel have greater resources than we have. Our competitors also may be successful in recruiting and hiring members of our management team, sales team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. We have in the past, and may in the future, be subject to allegations that employees we hire have been improperly solicited, or that they have divulged proprietary or other confidential information or that their former employers own such employees' inventions or other work product, or that they have been hired in violation of non-compete provisions or non-solicitation provisions.

In addition, job candidates and existing employees often consider the value of the equity awards and other compensation they receive in connection with their employment. If the perceived value of our compensatory package declines, it may adversely affect our ability to attract and retain highly skilled employees. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and future growth prospects would be severely harmed. Further, our competitors may be successful in recruiting and hiring members of our management team or other key employees, and it may be difficult for us to find suitable replacements on a timely basis, on competitive terms, or at all. In recent years, the increased availability of hybrid or remote working arrangements has expanded the pool of companies that can compete for our employees and employment candidates.

Although we have entered into employment agreements with our key employees, these agreements are on an "at-will" basis, meaning they are able to terminate their employment with us at any time. If we fail to attract new personnel or fail to retain and motivate our current personnel, our business and future growth prospects would be severely harmed.

If we do not effectively integrate, train, manage, and retain sales personnel, and expand our sales and marketing capabilities, we may be unable to increase our customer base and increase sales to our existing customers.

Our ability to increase our customer base and achieve broader market adoption of our platform will depend to a significant extent on our ability to continue to expand our sales and marketing operations. We have and plan to continue to dedicate significant resources to sales and marketing programs and to expand our sales and marketing capabilities to target additional potential customers, but there is no guarantee that we will be successful in attracting and maintaining additional customers. If we are unable to find efficient ways to deploy our sales and marketing investments or if our sales and marketing programs are not effective, our business and operating results would be adversely affected.

Furthermore, we plan to continue expanding our sales force and there is significant competition for sales personnel with the skills and technical knowledge that we require. Our ability to achieve revenue growth will depend, in part, on our success in hiring, integrating, training, managing, and retaining sufficient numbers of sales personnel to support our growth, particularly in international markets. New hires require significant training and may take extended time before they are productive. Our recent hires and planned hires may not become productive as quickly as we expect, or at all, and we may be unable to hire or retain sufficient numbers of qualified individuals in the markets where we do business or plan to do business. Moreover, our international expansion may be slow or unsuccessful if we are unable to retain qualified personnel with international experience, language skills and cultural competencies in the geographic markets which we target.

If we are unable to hire, integrate, train, manage, and retain a sufficient number of effective sales personnel, or the sales personnel we hire are not successful in obtaining new customers or increasing sales to our existing customer base, our business, operating results and financial condition will be adversely affected.

Any inability to maintain a high-quality customer support organization could lead to a lack of customer satisfaction, which could hurt our customer relationships and adversely affect our business, operating results, and financial condition.

Once our platform is deployed within our customers' computing environments, our customers rely on our technical support services to assist with service customization and optimization and to resolve certain issues relating to the implementation and maintenance of our platform and advanced services. If we do not effectively assist our customers in deploying our platform, succeed in helping our customers quickly resolve technical issues, or provide effective ongoing support, our ability to sell additional products and services as part of our platform to existing customers would be adversely affected and our reputation with potential customers could be damaged.

In addition, our sales process is highly dependent on our product and business reputation and on positive recommendations, referrals, and peer promotions from our existing customers. Any failure to maintain high-quality technical support, or a market perception that we do not maintain high-quality support, could adversely affect our reputation, our ability to sell our services to existing and prospective customers, and our business, operating results and financial condition.

We believe that our corporate culture has contributed to our success, and if we cannot maintain this culture as we grow, we could lose the innovation, creativity, and teamwork fostered by our culture, and our business may be harmed.

We believe that our corporate culture has been, and will continue to be a key contributor to our success. If we do not continue to develop our corporate culture as we grow and evolve, it could harm our ability to foster the innovation, inclusion, creativity, and teamwork that we believe is important to support our growth. As we implement more complex organizational structures, we may find it increasingly difficult to maintain the beneficial aspects of

our corporate culture, which could negatively impact our future success. We are also taking steps to develop a more inclusive and diverse workforce, however, there is no guarantee that we will be able to do so.

Risks Related to Our Intellectual Property

Our proprietary rights may be difficult to enforce, which could enable others to copy or use aspects of our platform without compensating us.

We rely primarily on patent, trademark, copyright and trade secrets laws, and confidentiality agreements and contractual provisions to protect our technology. Valid patents may not issue from our pending applications, and the claims eventually allowed on any patents may not be sufficiently broad to protect our technology or platform. Any issued patents may be challenged, invalidated or circumvented, and any rights granted under these patents may not actually provide adequate defensive protection or competitive advantages to us. Patent applications in the US are typically not published until at least 18 months after filing, or, in some cases, not at all, and publications of discoveries in industry-related literature lag behind actual discoveries. We cannot be certain that we were the first to make the inventions claimed in our pending patent applications or that we were the first to file for patent protection. Additionally, the process of obtaining patent protection is expensive and time-consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner. In addition, recent changes to the patent laws in the US may bring into question the validity of certain software patents and may make it more difficult and costly to prosecute patent applications. Such changes may lead to uncertainties or increased costs and risks surrounding the prosecution, validity, ownership, enforcement, and defense of our issued patents and patent applications and other intellectual property, the outcome of third-party claims of infringement, misappropriation, or other violation of intellectual property brought against us and the actual or enhanced damages (including treble damages) that may be awarded in connection with any such current or future claims, and could have a material adverse effect on our business, operating results, and financial condition.

Despite our efforts to protect our proprietary rights, unauthorized parties may attempt to copy aspects of our platform or obtain and use information that we regard as proprietary. We generally enter into confidentiality or license agreements with our employees, consultants, vendors, and customers, and generally limit access to and distribution of our proprietary information. However, such agreements may not be enforceable in full or in part in all jurisdictions and any breach could negatively affect our business and our remedy for such breach may be limited. The contractual provisions that we enter into may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property rights and may not provide an adequate remedy in the event of unauthorized use or disclosure of our proprietary technology or intellectual property rights. Lastly, the measures we employ to limit the access and distribution of our proprietary information may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property. As such, we cannot guarantee that the steps taken by us will prevent misappropriation of our technology. Policing unauthorized use of our technology or platform is difficult. In addition, the laws of some foreign countries do not protect our proprietary rights to the same extent as the laws of the US, and many foreign countries do not enforce these laws as diligently as government agencies and private parties in the US. For example, many foreign countries limit the enforceability of patents against certain third parties, including government agencies or government contractors. In these countries, patents may provide limited or no benefit. Effective trade secret protection may also not be available in every country in which our products are available or where we have employees or independent contractors. The loss of trade secret protection could make it easier for third parties to compete with our products by copying functionality. In addition, any changes in, or unexpected interpretations of, the trade secret and employment laws in any country in which we operate may compromise our ability to enforce our trade secret and intellectual property rights. From time to time, legal action by us may be necessary to enforce our patents and other intellectual property rights, to protect our trade secrets, to determine the validity and scope of the proprietary rights of others or to defend against claims of infringement or invalidity. Moreover, the availability of copyright protection and other legal protections for intellectual property generated by certain technologies, such as generative AI, is uncertain. The use of generative AI and other forms of AI may expose us to risks because the intellectual property ownership and license rights, including copyright, of generative and other AI output, has not been fully interpreted by US courts or been fully addressed by US federal or state regulation, as well as in foreign jurisdictions.

Such litigation could result in substantial costs and diversion of resources and could negatively affect our business, operating results and financial condition. If we are unable to protect our proprietary rights (including aspects of our software and platform protected other than by patent rights), we will find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create our platform and other innovative products that have enabled us to be successful to date. Moreover, we may need to expend additional resources to defend our intellectual property rights in foreign countries, and our inability to do so could impair our business or adversely affect our international expansion.

Third parties have claimed and may claim that our platform infringes their intellectual property rights and this may create liability for us or otherwise adversely affect our business, operating results, and financial condition.

Third parties have claimed, and may claim in the future, that our current or future products and services infringe their intellectual property rights, and such claims may result in legal claims against our channel partners, our alliance partners, our customers and us. These claims may damage our brand and reputation, harm our customer relationships, and create liability for us. Contractually, we are expected to indemnify our partners and customers for these types of claims. We expect the number of such claims to increase as the number of products and services and the level of competition in our market grows, as the functionality of our platform overlaps with that of other products and services, and as the volume of issued software patents and patent applications continues to increase. We generally agree in our customer and partner contracts to indemnify customers for certain expenses or liabilities they incur as a result of third-party intellectual property infringement claims associated with our platform. To the extent that any claim arises as a result of third-party technology we have licensed for use in our platform, we may be unable to recover from the appropriate third party any expenses or other liabilities that we incur.

Companies in the software and technology industries, including some of our current and potential competitors, own large numbers of patents, copyrights, trademarks, and trade secrets and frequently enter into litigation based on allegations of infringement or other violations of intellectual property rights. In addition, many of these companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. Furthermore, patent holding companies, non-practicing entities, and other adverse patent owners that are not deterred by our existing intellectual property protections may seek to assert patent claims against us. From time to time, third parties, including certain of these leading companies, have invited us to license their patents and may, in the future, assert patent, copyright, trademark, or other intellectual property rights against us, our channel partners, our alliance partners, or our customers. We have received, and may in the future receive, notices that claim we have misappropriated, misused, or infringed other parties' intellectual property rights, and, to the extent we gain greater market visibility, we face a higher risk of being the subject of intellectual property infringement claims.

There may be third-party intellectual property rights, including issued or pending patents and trademarks, that cover significant aspects of our technologies or business methods and assets. We may also face exposure to third-party intellectual property infringement, misappropriation, or violation actions if we engage software engineers or other personnel who were previously engaged by competitors or other third parties and those personnel inadvertently or deliberately incorporate proprietary technology of third parties into our products. In addition, we may lose valuable intellectual property rights or personnel. A loss of key personnel or their work product could hamper or prevent our ability to develop, market, and support potential products or enhancements, which could severely harm our business. Any intellectual property claims, with or without merit, could be very time-consuming, could be expensive to settle or litigate, and could divert our management's attention and other resources. These claims could also subject us to significant liability for damages, potentially including treble damages if we are found to have willfully infringed patents or copyrights, and may require us to indemnify our customers for liabilities they incur as a result of such claims. These claims could also result in our having to stop using technology found to be in violation of a third party's rights. We might be required to seek a license for the intellectual property, which may not be available on reasonable terms or at all. Even if a license were available, we could be required to pay significant royalties, which would increase our operating expenses. Alternatively, we could be required to develop alternative non-infringing technology, which could require significant time, effort, and expense, and may affect the performance or features of our platform. If we cannot license or develop alternative non-infringing substitutes for any infringing technology used in any aspect of our business, we would be forced to limit or stop sales of our

platform and may be unable to compete effectively. Any of these results would adversely affect our business, operating results, and financial condition.

We license technology from third parties, and our inability to maintain those licenses could harm our business.

We currently incorporate, and will in the future incorporate, technology that we license from third parties, including software, into our solutions. Licensing technologies from third parties exposes us to increased risk of being the subject of intellectual property infringement and vulnerabilities due to, among other things, our lower level of visibility into the development process with respect to such technology and the care taken to safeguard against risks. We cannot be certain that our licensors do not or will not infringe on the intellectual property rights of third parties or that our licensors have or will have sufficient rights to the licensed intellectual property in all jurisdictions in which we may sell our platform. Some of our agreements with our licensors may be terminated by them for convenience, or otherwise provide for a limited term. If we are unable to continue to license technology because of intellectual property infringement claims brought by third parties against our licensors or against us, or if we are unable to continue our license agreements or enter into new licenses on commercially reasonable terms, our ability to develop and sell solutions and services containing or dependent on that technology would be limited, and our business, including our financial conditions, cash flows and results of operations could be harmed. Additionally, if we are unable to license technology from third parties, we may be forced to acquire or develop alternative technology, which we may be unable to do in a commercially feasible manner, or at all, and may require us to use alternative technology of lower quality or performance standards. This could limit or delay our ability to offer new or competitive solutions and increase our costs. Third-party software we rely on may be updated infrequently, unsupported or subject to vulnerabilities that may not be resolved in a timely manner, any of which may expose our solutions to vulnerabilities. As a result, our business, operating results, and financial condition would be adversely affected.

Some of our technology incorporates "open source" software, which could negatively affect our ability to sell our platform and subject us to possible litigation.

Our platform contains third-party open source software components, and failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our products and subscriptions. The use and distribution of open source software may entail greater risks than the use of third-party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code, which they are not typically required to maintain and update, and they can change the license terms on which they offer the open source software. Although we monitor our use of open source software in an effort both to comply with the terms of the applicable open source licenses and to avoid subjecting our products to conditions we do not intend, many of the risks associated with use of open source software cannot be eliminated and could negatively affect our business. In addition, the wide availability of source code used in our solutions could expose us to security vulnerabilities.

Some open source licenses contain requirements that we make available as source code for modifications or derivative works we create based upon our use and distribution of the open source software. If we combine and distribute our proprietary software with open source software in a certain manner, we could, under certain open source licenses, be required to release combined the source code of our proprietary software to the public, including authorizing further modification and redistribution, or otherwise be limited in the licensing of our services, each of which could provide an advantage to our competitors or other entrants to the market, create security vulnerabilities in our solution, require us to re-engineer all or a portion of our platform, and reduce or eliminate the value of our services. This would allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us.

The terms of many open source licenses have not been interpreted by US courts, and there is a risk that these licenses could be construed in ways that could impose unanticipated conditions or restrictions on our ability to commercialize products and subscriptions incorporating such software. Moreover, we cannot assure you that our processes for controlling our use of open source software in our products and subscriptions will be effective. From time to time, we may face claims from third parties asserting ownership of, or demanding release of, the open source software or derivative works that we developed using such software (which could include our proprietary source

code), or otherwise seeking to enforce the terms of the applicable open source license. These claims, regardless of validity, could result in time consuming and costly litigation, divert management's time and attention away from developing the business, expose us to customer indemnity claims, or force us to disclose source code. Litigation could be costly for us to defend, result in paying damages, entering into unfavorable licenses, have a negative effect on our operating results and financial condition, or cause delays by requiring us to devote additional research and development resources to change our solution.

Risks Related to Legal and Regulatory Matters

We are subject to laws and regulations, including governmental export and import controls, sanctions and anti-corruption laws, that could impair our ability to compete in our markets and subject us to liability if we are not in full compliance with applicable laws.

We are subject to laws and regulations, including governmental export and import controls, that could subject us to liability or impair our ability to compete in our markets. Our platform and related technology are subject to US export controls, including the US Department of Commerce's Export Administration Regulations (also known as "EAR"), and we and our employees, representatives, contractors, agents, intermediaries, and other third parties are also subject to various economic and trade sanctions regulations administered by OFAC and other US government agencies. We incorporate standard encryption algorithms into our platform, which, along with the underlying technology, may be exported outside of the US only with the required export authorizations, including by license, license exception or other appropriate government authorizations, which may require the filing of an encryption registration and classification request. We also offer certain customers a ransomware warranty in addition to their subscriptions, providing coverage in the form of a limited monetary payment if they are affected by a ransomware attack (as specified in our ransomware warranty agreement), and though the terms of the warranty do not allow those customers to use warranty claim payments to fund payments to persons on OFAC's list of Specially Designated Nationals and Blocked Persons or who are otherwise prohibited to receive such payments under US sanctions, we cannot assure you that all of our customers will comply with our warranty terms or refrain from taking actions in violation of our warranty and applicable law. Furthermore, US export control laws and economic sanctions prohibit the export and re-export of certain hardware and software and the provision of certain cloud-based solutions to certain countries, governments and persons targeted by US sanctions and for certain end-uses. As an example, following Russia's invasion of Ukraine, the US and other countries imposed economic sanctions and severe export control restrictions against Russia and Belarus. The US and its allies could expand and strengthen these sanctions and export restrictions and take other actions should the conflict further escalate. These restrictions would further impact our ability to do business in certain parts of the world and to do business with certain persons and entities, including selling our services and using local developers. We also collect information about cyber threats from open sources, intermediaries and third parties that we make available to our customers in our threat industry publications. Further, regulators in the US and elsewhere have signaled an increased emphasis on sanctions and export control enforcement, including several recent high-profile enforcement actions and increased pressure for companies to self-disclose potential violations. While we have implemented certain procedures to facilitate compliance with applicable laws and regulations in connection with the collection and distribution of this information, we cannot assure you that these procedures have been effective or that we, or third parties who we do not control, have complied with all laws or regulations in this regard. Failure by our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties to comply with applicable laws and regulations in the collection and distribution of this information also could have negative consequences to us, including reputational harm, government investigations, and penalties.

Although we take precautions to prevent our information collection practices and services from being provided in violation of such laws, our information collection practices and services may have been in the past, and could in the future be, provided in violation of such laws. If we or our employees, representatives, contractors, channel partners, agents, intermediaries, or other third parties fail to comply with these laws and regulations, we could be subject to civil or criminal penalties, including the possible loss of export privileges and fines. We may also be adversely affected through reputational harm, loss of access to certain markets or otherwise. Obtaining the necessary authorizations, including any required license, for a particular transaction may be time-consuming, is not guaranteed and may result in the delay or loss of sales opportunities.

Various countries regulate the import of certain encryption technology, including through import permit and license requirements, and have enacted laws that could limit our ability to distribute our platform or could limit our customers' ability to implement our platform in those countries. Additionally, export restrictions imposed on Russia and Belarus specifically limit the export of encryption hardware, software and related source code and technology to these locations which could limit our ability to provide our software and services to these countries. Changes in our platform, and changes in or promulgation of new export and import regulations may create delays in the introduction of our platform into international markets, prevent our customers with international operations from deploying our platform globally or, in some cases, prevent the export or import of our platform to certain countries, governments or persons altogether. Any change in export or import regulations, economic sanctions or related legislation, shift in the enforcement or scope of existing regulations, or change in the countries, governments, persons or technologies targeted by such regulations, could result in decreased use of our platform by, or in our decreased ability to export or sell our platform to, existing or potential customers with international operations. Any decreased use of our platform or limitation on our ability to export or sell our platform would adversely affect our business, operating results, and financial condition.

We are also subject to the United States Foreign Corrupt Practices Act of 1977 (FCPA), as amended, the United Kingdom Bribery Act 2010 (the Bribery Act), and other anti-corruption, sanctions, anti-bribery, anti-money laundering and similar laws in the US and other countries in which we conduct activities. Anti-corruption and anti-bribery laws, which have been enforced aggressively and are interpreted broadly, prohibit companies and their employees, agents, intermediaries and other third parties from promising, authorizing, making or offering improper payments or other benefits to government officials and others in the public, and in certain cases, private sector. We leverage third parties, including intermediaries, agents and channel partners, to conduct our business in the US and abroad, to sell subscriptions to our platform and to collect information about cyber threats. We and these third parties may have direct or indirect interactions with officials and employees of government agencies or state-owned or affiliated entities and we may be held liable for the corrupt or other illegal activities of these third-party business partners and intermediaries, our employees, representatives, contractors, channel partners, agents, intermediaries and other third parties, even if we do not explicitly authorize such activities. While we have policies and procedures to address compliance with FCPA, Bribery Act and other anti-corruption, sanctions, anti-bribery, anti-money laundering and similar laws, we cannot assure you that they will be effective, or that all of our employees, representatives, contractors, channel partners, agents, intermediaries or other third parties have not taken, or will not take actions, in violation of our policies and applicable law, for which we may be ultimately held responsible. As we increase our international sales and business, including our business with government organizations, our risks under these laws may increase. Noncompliance with these laws could subject us to investigations, severe criminal or civil sanctions, settlements, prosecution, loss of export privileges, suspension or debarment from US government contracts, other enforcement actions, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, whistleblower complaints, adverse media coverage and other consequences. Any investigations, actions or sanctions could harm our reputation, business, operating results, and financial condition.

Moreover, the rapid evolution of AI, including potential government regulation of AI, may require significant additional resources to develop, test, and maintain our platform. Our AI-related initiatives may result in new or enhanced governmental or regulatory scrutiny, including regarding the use of AI in our products and the marketing of products using AI, litigation, customer reporting or documentation requirements, ethical or social concerns, or other complications and may also introduce risks related to accuracy, bias, toxicity, privacy, and security and data provenance. For example, the European Commission's proposed Artificial Intelligence Act could also impose new obligations or limitations affecting our business, if and when it enters into force.

If we fail to adequately protect personal information or other information we collect, process, share or maintain under applicable laws, our business, operating results, and financial condition could be adversely affected.

We receive, store, and process personal information from our employees, customers, the employees of our customers, and our end users. This personal information is hosted by our third-party service providers. A wide variety of state, national, and international laws, as well as regulations and industry standards apply to the collection, use, retention, protection, disclosure, transfer and other processing of personal information and other information, the scope of which are changing, subject to differing interpretations, and may be inconsistent across countries or conflict with other rules. Data protection and privacy-related laws and regulations are evolving and may result in

increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. Failure to comply with laws, regulations and industry standards regarding personal information or other information could adversely affect our business, operating results, and financial condition.

Complying with these various laws and regulations could cause us to incur substantial costs or require us to change our business practices, systems, and compliance procedures in a manner adverse to our business.

In the US, there are numerous federal and state consumer, privacy, and data security laws and regulations governing the collection, use, disclosure, and protection of personal information, including security breach notification laws and consumer protection laws. Each of these laws is subject to varying interpretations and constantly evolving. Notably, but not necessarily limited to, we may be subject to:

- Controlling the Assault of Non-Solicited Pornography And Marketing Act (also known as the "CAN-SPAM Act") and similar state consumer protection laws regarding the use of telephones and text messaging for marketing purposes.
- Section 5(a) of the Federal Trade Commission (FTC) Act for violating consumers' privacy rights or failing to take appropriate steps to keep consumers' personal information secure, resulting in a finding of an unfair act or practice.
- The CCPA, effective since January 1, 2020, which created new data privacy obligations for covered businesses and provided new privacy rights to California residents, including the right to opt out of certain disclosures of their information and receive detailed information about how their personal information is used. The CCPA provides for civil penalties for violations, as well as a private right of action for data breaches that is expected to increase data breach litigation. A ballot initiative called the California Privacy Rights Act (CPRA) went into force July 1, 2023, and significantly modifies the CCPA, including by expanding consumers' rights with respect to certain sensitive personal data. The CPRA also creates a new state agency, known as the California Privacy Protection Agency, which is vested with the authority to implement and enforce the CCPA and the CPRA. Potential uncertainty surrounding the CCPA and CPRA may increase our compliance costs and potential liability, particularly in the event of a data breach, and could have a material adverse effect on our business.
- Other states have enacted consumer privacy laws comparable to the CCPA that came into effect in 2023: Virginia enacted the Virginia Consumer Data Protection Act which became effective January 1, 2023; Colorado and Connecticut enacted the Colorado Privacy Act and the Connecticut Personal Data Privacy and Online Monitoring Act, which both became effective July 1, 2023; Utah enacted the Utah Consumer Privacy Act, which became effective December 31, 2023. In addition, as of December 31, 2023, eight other states (Delaware, Indiana, Iowa, Florida, Montana, Oregon, Tennessee and Texas) enacted privacy legislation which will become effective between July 1, 2024 and January 1, 2026. Numerous other states also have pending consumer privacy legislation under review, which if enacted, would add additional costs and expense of resources to maintain compliance.

In certain circumstances, we may also be subject to the GDPR (established in 2018 and implemented by countries in the EEA) and the UK GDPR, which respectively govern the collection, use, disclosure, transfer or other processing of personal data of natural persons, and it applies extra-territorially and imposes onerous requirements on controllers and processors of personal data, including, for example: (i) accountability and transparency requirements, and enhanced requirements for obtaining valid consent; (ii) obligations to consider data protection as any new products or services are developed and to limit the amount of personal data processed; (iii) obligations to comply with data protection rights of data subjects; and (iv) reporting of personal data breaches to the supervisory authority without undue delay (and no later than 72 hours).

Companies that must comply with the GDPR face increased compliance obligations and risk, including more robust regulatory enforcement of data protection requirements and potential fines for noncompliance of up to €20 million or 4% of the annual global turnover of the noncompliant company, whichever is greater. Additionally, following the withdrawal by the UK from the EU and the EEA, companies must comply with both the GDPR and the UK GDPR as incorporated into UK national law, the latter regime having the ability to separately fine up to the

greater of £17.5 million or 4% of global annual turnover. In addition to the foregoing, a breach of the GDPR or UK GDPR could result in regulatory investigations, reputational damage, orders to cease or change our processing of our data, enforcement notices, and/or assessment notices (for a compulsory audit). We may also face civil claims including representative actions and other class action type litigation (where individuals have suffered harm), potentially amounting to significant compensation or damages liabilities, as well as associated costs, diversion of internal resources, and reputational harm.

The GDPR and UK GDPR requires, among other things, that personal data only be transferred outside of the EEA, or the UK, respectively to jurisdictions that have been deemed adequate (also known as "Third Countries,") by the European Commission or by the UK data protection regulator, respectively. Accordingly, personal data may not be transferred to those jurisdictions that have not been deemed adequate, unless steps are taken to legitimize those data transfers. Switzerland follows similar legal practices. We rely on the use of Standard Contractual Clauses (SCCs), a standard form of contract approved by the European Commission, as an adequate personal data transfer mechanism for the transfer of personal data to Third Countries; however, the SCCs may not be alone sufficient to protect data transferred to the US or other Third Countries under certain circumstances without making a case-by-case basis assessment of the legal regime applicable in the destination country according to the CJEU. On June 28, 2021, the European Commission issued an adequacy decision for personal data transfers from the EEA to the UK, with a sunset clause of four years, meaning that the European Commission will review and renew only if the European Commission considers that the UK continues to ensure an adequate level of data protection. Notably, the European Commission reserved a right to intervene at any time during the four-year adequacy period if the UK deviates from the level of protection then in place. If this adequacy decision is reversed by the European Commission, we would have to implement protection measures such as the SCCs for personal data transfers between the EU and the UK or find alternative solutions for the compliant transfer of personal data from the EU into the UK In March 2022, the UK Information Commissioner's Office adopted an International Data Transfer Agreement (IDTA) for transfers of personal data out of the UK to so-called third countries, as well as an international data transfer addendum (UK SCC Addendum) that can be used with the SCCs for the same purpose.

To add to this complexity, effective on July 10, 2023, the European Commission adopted the new EU-US Data Privacy Framework (DPF) which allows for transfers of personal data from the EU to certified companies in the US without the need for additional privacy safeguards as an alternative to the SCCs. In October 2023, a UK extension to the DPF (the UK – US Data Bridge) was adopted enabling the transfer of personal data between the UK and US entities without the need for an IDTA or UK SCC Addendum. However, the DPF and the UK – US Data Bridge could be subject to further legal challenge which could cause the legal requirements for personal data transfers from the EU and the UK to the US to become uncertain once again.

Some countries (including some outside the EEA) also are considering or have passed legislation requiring local storage and processing of data, or similar requirements, which could increase the cost and complexity of delivering our products and services if we were to operate in those countries. If we are required to implement additional measures to transfer data from the EEA, this could increase our compliance costs, and could adversely affect our business, financial condition and results of operations.

The myriad of international and US privacy and data breach laws are not consistent, and compliance in the event of a widespread data breach is difficult and may be costly. In many jurisdictions, enforcement actions and consequences for noncompliance are also rising. In addition to government regulation, privacy advocates and industry groups may propose new and different self-regulatory standards that either legally or contractually apply to us.

As supervisory authorities continue to issue further guidance on personal information transfers (including regarding data export and circumstances in which we cannot use the SCCs), we could suffer additional costs, complaints, or regulatory investigations or fines. If we are otherwise unable to transfer personal data between and among countries and regions in which we operate, it could affect the manner in which we provide our services, adversely affecting our financial results, and possibly making it necessary to establish localized storage systems in the EEA, Switzerland, and the UK to maintain personal data originating from those jurisdictions that adds expenses and may create distractions from our other business pursuits. Loss, retention or misuse of certain information and alleged violations of laws and regulations relating to privacy and data security, and any relevant claims, may expose

us to potential liability and may require us to expend significant resources on data security and in responding to and defending such allegations and claims.

We are also subject to evolving EU and UK privacy laws on cookies and electronic marketing. In the EU and the UK, informed opt-in consent is required for the placement of a cookie or similar technologies on a user's device and for direct electronic marketing. The GDPR also imposes conditions on obtaining valid consent, such as a prohibition on pre-checked consents and a requirement to ensure separate consents are sought for each type of cookie or similar technology. While we anticipate the development of the ePrivacy Regulation to govern cookies and e-marketing, recent European court decisions and regulators' guidance are driving increased attention to cookies and tracking technologies. If regulators start to enforce the strict approach in recent guidance, this could lead to substantial costs, require significant systems changes, limit the effectiveness of our marketing activities, divert the attention of our technology personnel, adversely affect our margins, increase costs and subject us to additional liabilities. Regulation of cookies and similar technologies, and any decline of cookies or similar online tracking technologies as a means to identify and potentially target users, may lead to broader restrictions and impairments on our marketing and personalization activities and may negatively impact our efforts to understand users. Similar concerns may happen under the new CPRA regime in California and other current and soon-to-be enacted US state privacy laws.

Additionally, by expanding into the EU and UK, we may also trigger Article 3(2) of the GDPR/UK GDPR directly as we may be considered to be monitoring data subjects. To the extent we process personal data on behalf of our customers for the provision of services, we have, and may in the future, also be required to enter into data processing agreements which comply with Article 28 of the GDPR/UK GDPR.

We depend on a number of third parties in relation to the operation of our business, a number of which process personal data on our behalf or as our sub-processor. To the extent required by applicable law, we attempt to mitigate the associated risks of using third parties by performing security assessments and detailed due diligence, entering into contractual arrangements to ensure that providers only process personal data according to our instructions or comparable instructions to the instructions of our customer (as applicable), and that they have sufficient technical and organizational security measures in place. There is no assurance that these contractual measures and our own privacy and security-related safeguards will protect us from the risks associated with the third-party processing, storage and transmission of such information. Any violation of privacy, data protection, data or cybersecurity laws by our third-party processors could have a material adverse effect on our business and result in the fines and penalties under the GDPR and the UK GDPR outlined above.

In recent years, some regulators have proposed or introduced cybersecurity licensing requirements or certification regimes for specific sectors, such as critical infrastructure. These may impose new requirements on us or our current or prospective customer including, but not limited to, data processing locations, breach notification, and security standards. Such requirements may cause us to incur significant organizational costs and increase barriers of entry into new markets. New worldwide data protection laws, including in the US and European jurisdictions described above, may lead to changing definitions of personal information and other sensitive information which may also limit or inhibit our ability to operate or expand our business, including limiting strategic partnerships that may involve the sharing of data. Notably some foreign jurisdictions require that certain types of data be retained on servers within these respective jurisdictions. Our failure to comply with applicable laws, directives, and regulations may result in enforcement action against us, including fines, and damage to our reputation, any of which may have an adverse effect on our business and operating results.

Any failure or perceived failure by us, even if unfounded, to comply with applicable privacy and data security laws and regulations, our privacy policies, or our privacy-related obligations to customers, users or other third parties, or any compromise of security that results in the unauthorized release or transfer of personal information or other customer data, may result in governmental enforcement actions, fines, penalties, litigation, or public statements against us by consumer advocacy groups or others and could cause our users to lose trust in us, which would have an adverse effect on our reputation and business. For example, in 2017, we reached a consent agreement with the FTC, to resolve an investigation relating to certain disclosures in our privacy policy. The consent agreement requires us, among other things, to provide information to the FTC about our compliance with the FTC order and about representations made in our marketing materials. We may be subject to future investigations and legal proceedings

by the FTC or other regulators. As such, it is possible that a regulatory inquiry might result in changes to our policies or business practices. Violation of existing or future regulatory orders or consent decrees could subject us to substantial monetary fines and other penalties that could negatively affect our operating results and financial condition. In addition, it is possible that future orders issued by, or enforcement actions initiated by, regulatory authorities could cause us to incur substantial costs or require us to change our business practices in a manner materially adverse to our business.

Any significant change to applicable laws, regulations or industry practices regarding the use or disclosure of our customers' data, or regarding the manner in which the express or implied consent of customers for the use and disclosure of such data is obtained – or in how these applicable laws, regulations or industry practices are interpreted and enforced by state, federal and international privacy regulators – could require us to modify our services and features, possibly in a material manner, may subject us to regulatory enforcement actions and fines, and may limit our ability to develop new products, services and features that make use of the data that our customers voluntarily share with us.

Any security breach or incident, including those resulting from a cybersecurity attack, phishing attack, unauthorized access, unauthorized usage, virus, malware, ransomware, denial of service, credential stuffing attack, supply chain attack, hacking or similar breach involving our networks and systems, or those of third parties upon which we rely, could result in the loss of customer data, including personal information, disruption to our operations, significant remediation costs, lost revenue, increased insurance premiums, damage to our reputation, litigation, regulatory investigations, or other liabilities. These attacks may come from individual hackers, criminal groups, and state-sponsored organizations, and security breaches and incidents may arise from other sources, such as employee or contractor error or malfeasance. Cyber threats are evolving and becoming increasingly sophisticated and complex, increasing the difficulty of detecting and successfully defending against them. As a cybersecurity company, we have been and may continue to be specifically targeted by malicious actors for attacks intended to circumvent our security capabilities as an entry point into customers' endpoints, networks, or systems. Our industry is experiencing an increase in phishing attacks and unauthorized scans of systems searching for vulnerabilities or misconfigurations to exploit. If our security measures are breached or otherwise compromised as a result of third-party action, employee or contractor error, defect, vulnerability or bug in our products or products of third parties upon which we rely, malfeasance or otherwise, including any such breach or compromise resulting in someone obtaining unauthorized access to our confidential information, including personal information or the personal information of our customers or others, or if any of these are perceived or reported to occur, we may suffer the loss, compromise, corruption, unavailability, or destruction of our or others' confidential information and personal information, we may face a loss in intellectual property protection, our reputation may be damaged, our business may suffer and we could be subject to claims, demands, regulatory investigations and other proceedings, indemnity obligations, and otherwise incur significant liability. Even the perception of inadequate security may damage our reputation and negatively impact our ability to win new customers and retain existing customers. Further, we could be required to expend significant capital and other resources to address any security incident or breach, and we may face difficulties or delays in identifying and responding to any security breach or incident.

Techniques used to sabotage or obtain unauthorized access to systems or networks are constantly evolving and, in some instances, are not identified until launched against a target. We and our third-party vendors and service providers may be unable to anticipate these techniques, react in a timely manner, or implement adequate preventative measures. Due to political uncertainty and military actions associated with the conflicts in Ukraine, the Middle East and tensions between China and Taiwan, we and our third-party vendors and service providers are vulnerable to a heightened risk of cybersecurity attacks, phishing attacks, viruses, malware, ransomware, hacking or similar breaches from nation-state and affiliated actors, including attacks that could materially disrupt our and our third-party vendors' and service providers' systems and operations, supply chain, and ability to produce, sell and distribute our products and services as well as retaliatory cybersecurity attacks from Russian and Russian-affiliated actors against companies with a US presence. In addition, laws, regulations, government guidance, and industry standards and practices in the US and elsewhere are rapidly evolving to combat these threats. We may face increased compliance burdens regarding such requirements with regulators and customers regarding our products and services and also incur additional costs for oversight and monitoring of our own supply chain. We and our customers may also experience increased costs associated with security measures and increased risk of suffering cyberattacks,

including ransomware attacks. Should we or the third-party vendors and service providers upon which we rely experience such attacks, including from ransomware or other security breaches or incidents, our operations may also be hindered or interrupted due to system disruptions or otherwise, with foreseeable secondary contractual, regulatory, financial and reputational harms that may arise from such an incident.

Further, we cannot assure that any limitations of liability provisions in our customer agreements, contracts with third-party vendors and service providers or other contracts would be enforceable or adequate or would otherwise protect us from any liabilities or damages with respect to any particular claim relating to a security breach or other security incident. We also cannot be sure that our existing insurance coverage will continue to be available on acceptable terms or will be available in sufficient amounts to cover claims related to a security incident or breach, or that the insurer will not deny coverage as to any future claim. The successful assertion of claims against us that exceed available insurance coverage, or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or coinsurance requirements, could have a material adverse effect on our business, including our financial condition, operating results, and reputation.

Moreover, while we strive to publish and prominently display privacy policies that are accurate, comprehensive, and compliant with applicable laws, rules regulations and industry standards, we cannot ensure that our privacy policies and other statements regarding our practices will be sufficient to protect us from claims, proceedings, liability or adverse publicity relating to data privacy and security. If our public statements about our use, collection, disclosure and other processing of personal information, whether made through our privacy policies, information provided on our website, press statements or otherwise, are alleged to be deceptive, unfair or misrepresentative of our actual practices, we may be subject to potential government or legal investigation or action, including by the FTC or applicable state attorneys general.

Our compliance efforts are further complicated by the fact that data privacy and security laws, rules, regulations and standards around the world are rapidly evolving, may be subject to uncertain or inconsistent interpretations and enforcement, and may conflict among various jurisdictions. Any failure or perceived failure by us to comply with our privacy policies, or applicable data privacy and security laws, rules, regulations, standards, certifications or contractual obligations, or any compromise of security that results in unauthorized access to, or unauthorized loss, destruction, use, modification, acquisition, disclosure, release or transfer of personal information, may result in requirements to modify or cease certain operations or practices, the expenditure of substantial costs, time and other resources, proceedings or actions against us, legal liability, governmental investigations, enforcement actions, claims, fines, judgments, awards, penalties, sanctions, and costly litigation (including class actions). Any of the foregoing could harm our reputation, distract our management and technical personnel, increase our costs of doing business, adversely affect the demand for our products and services, and ultimately result in the imposition of liability, any of which could have a material adverse effect on our business, operating results, and financial condition.

We are currently in, and may in the future, become involved in litigation that may adversely affect us.

From time to time, we have been subject to claims, suits and other proceedings. For example, we are currently the subject of securities litigation and commercial litigation. For additional information regarding these litigation matters, see the section titled “Legal Proceedings.” Regardless of the outcome, legal proceedings can have an adverse impact on us because of legal costs and diversion of management attention and resources, and could cause us to incur significant expenses or liability, adversely affect our brand recognition or require us to change our business practices. The expense of litigation and the timing of this expense from period to period are difficult to estimate, subject to change and could adversely affect our business, operating results, and financial condition. It is possible that a resolution of one or more such proceedings could result in substantial damages, settlement costs, fines and penalties that would adversely affect our business, consolidated financial condition, operating results or cash flows in a particular period. These proceedings could also result in reputational harm, sanctions, consent decrees or orders requiring a change in our business practices. Because of the potential risks, expenses and uncertainties of litigation, we may, from time to time, settle disputes, even where we have meritorious claims or defenses, by agreeing to settlement agreements. Because litigation is inherently unpredictable, we cannot assure you that the results of any of these actions will not have a material adverse effect on our business, operating results,

financial condition, and prospects. Any of these consequences could adversely affect our business, operating results, and financial condition.

Risks Related to Financial and Accounting Matters

The requirements of being a public company, including maintaining adequate internal control over our financial and management systems, result in significant costs and may strain our resources, divert management's attention, and affect our ability to attract and retain executive management and qualified board members.

As a public company we incur and expect to continue to incur significant legal, accounting, and other expenses. We are subject to the reporting requirements of the Exchange Act, the Sarbanes-Oxley Act, Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 and the rules and regulations of the applicable listing standards of the New York Stock Exchange (NYSE). We expect that the requirements of these rules and regulations will continue to increase our legal, accounting, and financial compliance costs, make some activities more difficult, time-consuming, and costly, and place significant strain on our personnel, systems, and resources.

The Sarbanes-Oxley Act requires, among other things, that we maintain effective disclosure controls and procedures and internal control over financial reporting. We are continuing to develop and refine our disclosure controls, internal control over financial reporting and other procedures that are designed to ensure information required to be disclosed by us in our consolidated financial statements and in the reports that we will file with the SEC is recorded, processed, summarized and reported within the time periods specified in SEC rules and forms, and information required to be disclosed in reports under the Exchange Act is accumulated and communicated to our principal executive and financial officers.

Our current controls and any new controls we develop may become inadequate because of changes in conditions in our business. Additionally, to the extent we acquire other businesses, the acquired companies may not have a sufficiently robust system of internal controls and we may uncover new deficiencies. Further, weaknesses in our internal controls may be discovered in the future. Any failure to develop or maintain effective controls, or any difficulties encountered in their implementation or improvement, could harm our operating results, may result in a restatement of our consolidated financial statements for prior periods, cause us to fail to meet our reporting obligations, and could adversely affect the results of periodic management evaluations and annual independent registered public accounting firm attestation reports regarding the effectiveness of our internal control over financial reporting. Ineffective disclosure controls and procedures and internal control over financial reporting could also cause investors to lose confidence in our reported financial and other information, which would likely have a negative effect on the market price of our Class A common stock. Our management is also required, pursuant to Section 404 of the Sarbanes-Oxley Act, to certify financial and other information in our quarterly and annual reports and provide an annual report on the effectiveness of our internal control over financial reporting.

In addition, changing laws, regulations, and standards relating to corporate governance and public disclosure, including those related to climate change and other environmental, social, and governance (ESG)-focused disclosures, are creating uncertainty for public companies, increasing legal and financial compliance costs, and making some activities more time consuming. These laws, regulations, and standards are subject to varying interpretations, in many cases due to their lack of specificity, and, as a result, their application in practice may evolve over time as new guidance is provided by regulatory and governing bodies. This could result in continuing uncertainty regarding compliance matters and higher costs necessitated by ongoing revisions to disclosure and governance practices. We intend to continue to invest resources to comply with evolving laws, regulations, and standards, and this investment may result in increased general and administrative expenses and a diversion of management's time and attention from revenue-generating activities to compliance activities. If our efforts to comply with new laws, regulations, and standards differ from the activities intended by regulatory or governing bodies due to ambiguities related to their application and practice, regulatory authorities may initiate legal proceedings against us, and our business may be adversely affected.

We have incurred significant costs with respect to our directors' and officers' insurance coverage. In the future, it may be more expensive or more difficult for us to obtain director and officer liability insurance, and we may be required to accept reduced coverage or incur substantially higher costs to obtain coverage. These factors would also

make it more difficult for us to attract and retain qualified members of our board of directors, particularly to serve on our audit committee and compensation committee, and qualified executive officers.

Being a public company requires significant resources and management oversight. As a result, management's attention may be diverted from other business concerns, which could harm our business, operating results, and financial condition.

We could be subject to additional tax liabilities and US federal and global income tax reform could adversely affect us.

We are subject to US federal, state, local and sales taxes in the US and foreign income taxes, withholding taxes and transaction taxes in numerous foreign jurisdictions. Significant judgment is required in evaluating our tax positions and our worldwide provision for income taxes. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination is uncertain. In addition, our future income tax obligations could be adversely affected by changes in, or interpretations of, tax laws in the US or in other jurisdictions in which we operate.

For example, the US tax law legislation, commonly referred to as the Tax Cuts and Jobs Act of 2017, significantly reformed the Internal Revenue Code of 1986, as amended (the Internal Revenue Code), reducing US federal tax rates, making sweeping changes to rules governing international business operations, and imposing significant additional limitations on tax benefits, including the deductibility of interest and the use of net operating loss carryforwards. On August 16, 2022, President Biden signed the Inflation Reduction Act of 2022 (IRA) into law. The IRA contains certain tax measures, including a corporate alternative minimum tax of 15% on some large corporations and an excise tax of 1% on certain corporate stock buy-backs taking place after December 31, 2022. In addition, the Organization for Economic Cooperation and Development (OECD) Inclusive Framework of 137 jurisdictions have joined a two-pillar plan to reform international taxation rules. The first pillar is focused on the allocation of taxing rights between countries for in-scope multinational enterprises that sell goods and services into countries with little or no local physical presence and is intended to apply to multinational enterprises with global turnover above €20 billion. The second pillar is focused on developing a global minimum tax rate of at least 15 percent applicable to in-scope multinational enterprises and is intended to apply to multinational enterprises with annual consolidated group revenue in excess of €750 million. We are still evaluating the impact of the pillar two rules as they continue to be refined by the OECD and implemented by various national governments. However, it is possible that the pillar two rules, as implemented by various national governments, could adversely affect our effective tax rate or result in higher cash tax liabilities.

Due to the large and expanding scale of our international business activities, these types of changes to the taxation of our activities could impact the tax treatment of our foreign earnings, increase our worldwide effective tax rate, increase the amount of taxes imposed on our business, and harm our financial position. Such changes may also apply retroactively to our historical operations and result in taxes greater than the amounts estimated and recorded in our financial statements.

Our ability to use our net operating loss carryforwards and certain other tax attributes may be limited.

As of January 31, 2024, we had aggregate US federal and state net operating loss carryforwards of $721.2 million and $390.6 million, respectively, which may be available to offset future taxable income for US income tax purposes. If not utilized, the federal net operating loss carryforwards will begin to expire in 2031, and the state net operating loss carryforwards will begin to expire in 2025. In addition, as of January 31, 2024, we had federal research and development credit carryforwards of $5.9 million, which will begin to expire in 2037, and state research and development credit carryforwards of $2.9 million, which do not expire. We also had foreign net operating loss carryforwards of $202.8 million, as of January 31, 2024, which do not expire. Realization of these net operating loss and research and development credit carryforwards depends on future income, and there is a risk that certain of our existing carryforwards could expire unused and be unavailable to offset future income tax liabilities, which could adversely affect our operating results and financial condition.

In addition, under Sections 382 and 383 of the Internal Revenue Code, if a corporation undergoes an "ownership change," generally defined as a greater than 50% change (by value) in ownership by "5 percent

shareholders" over a rolling three-year period, the corporation's ability to use its pre-change net operating loss carryovers and other pre-change tax attributes, such as research and development credits, to offset its post-change income or taxes may be limited. Similar rules apply under US state tax laws. We have, and may in the future, experience ownership changes as a result of shifts in our stock ownership. As a result, if we earn net taxable income, our ability to use our pre-change US net operating loss carryforwards to offset US federal taxable income may be subject to limitations, which could potentially result in increased future tax liability to us.

We could be required to collect additional sales, use, value added, digital services, or other similar taxes or be subject to other liabilities with respect to past or future sales, that may increase the costs our customers would have to pay for our solutions and adversely affect our business, operating results, and financial condition.

We do not collect sales and use, value added, or similar taxes in all jurisdictions in which we have sales because we have been advised that such taxes are not applicable to our services in certain jurisdictions. Sales and use, value added, and similar tax laws and rates vary greatly by jurisdiction. Certain jurisdictions in which we do not collect such taxes may seek to impose incremental or new sales, use, value added, digital services, or assert other tax collection obligations on us that such taxes are applicable, which could result in tax assessments, penalties and interest, to us or our customers for the past amounts, and we may be required to collect such taxes in the future. If we are unsuccessful in collecting such taxes from our customers, we could be held liable for such costs, which may adversely affect our results of operations.

Further, an increasing number of US states have considered or adopted laws that attempt to impose tax collection obligations on out-of-state companies. A successful assertion by one or more US states requiring us to collect taxes where we presently do not do so, or to collect more taxes in a jurisdiction in which we currently do collect some taxes, could result in substantial liabilities, including taxes on past sales, as well as interest and penalties. Furthermore, certain jurisdictions, such as the UK, France and Canada, have enacted a digital services tax, which is generally a tax on gross revenue generated from users or customers located in in those jurisdictions, and other jurisdictions are considering enacting similar laws. A successful assertion by a US state or local government, or other country or jurisdiction that we should have been or should be collecting additional sales, use, value added, digital services or other similar taxes could, among other things, result in substantial tax payments, create significant administrative burdens for us, discourage potential customers from subscribing to our platform due to the incremental cost of any such sales or other related taxes, or otherwise harm our business.

Our corporate structure and intercompany arrangements are subject to the tax laws of various jurisdictions, and we could be obligated to pay additional taxes, which would harm our operating results and financial condition.

We are expanding our international operations and staff to support our business and growth in international markets. We generally conduct our international operations through wholly-owned subsidiaries and are or may be required to report our taxable income in various jurisdictions worldwide based upon our business operations in those jurisdictions. Our corporate structure and associated transfer pricing policies contemplate future growth in international markets, and consider the functions, risks, and assets of the various entities involved in intercompany transactions. Furthermore, increases in tax rates, new or revised tax laws, and new interpretations of existing tax laws and policies by taxing authorities and courts in various jurisdictions, could result in an increase in our overall tax obligations which could adversely affect our business. Our intercompany relationships and intercompany transactions are subject to complex transfer pricing rules administered by taxing authorities in various jurisdictions in which we operate with potentially divergent tax laws. The amount of taxes we pay in different jurisdictions will depend on the application of the tax laws of the various jurisdictions, including the US, to our intercompany transactions, international business activities, changes in tax rates, new or revised tax laws or interpretations of existing tax laws and policies by taxing authorities and courts in various jurisdictions, and our ability to operate our business in a manner consistent with our corporate structure and intercompany arrangements.

It is not uncommon for tax authorities in different countries to have conflicting views, for instance, with respect to, among other things, the manner in which the arm's length standard is applied for transfer pricing purposes, the transfer pricing and charges for intercompany services and other intercompany transactions, or with respect to the valuation of our intellectual property and the manner in which our intellectual property is utilized within our group. In 2022, we began negotiating a bilateral Advance Pricing Agreement (APA) with the US and the Israeli

governments, covering various transfer pricing matters for intercompany transactions relating to the intergroup utilization of our intellectual property among our group enterprises. An APA, if obtained, will provide us with a more predictable future business operating model, and preclude the relevant tax authorities from making certain transfer pricing adjustments within the scope of these agreements. These transfer pricing matters may be significant to our consolidated financial statements. If taxing authorities in any of the jurisdictions in which we conduct our international operations were to successfully challenge our transfer pricing, we could be required to reallocate part or all of our income to reflect transfer pricing adjustments, which could result in an increased tax liability to us. In such circumstances, if the country from where the income was reallocated did not agree to the reallocation, we could become subject to tax on the same income in both countries, resulting in double taxation. Furthermore, the relevant taxing authorities may disagree with our determinations as to the income and expenses attributable to specific jurisdictions. We believe that our tax and financial accounting positions are reasonable and our tax reserves are adequate to cover any potential liability. We also believe that our assumptions, judgements, and estimates are reasonable and that our transfer pricing for these intercompany transactions are on arm's-length terms. However, the relevant tax authorities may disagree with our tax positions, including any assumptions, judgements or estimates used for these transfer pricing matters and intercompany transactions. If any of these tax authorities determine that our transfer pricing for these intercompany transactions do not meet arm's-length criteria, and were successful in challenging our positions, we could be required to pay additional taxes, interest and penalties related thereto, which could be in excess of any reserves established therefore, and which could result in higher effective tax rates, reduced cash flows, and lower overall profitability of our operations. Our financial statements could fail to reflect adequate reserves to cover such a contingency.

We may be audited in various jurisdictions, including in jurisdictions in which we are not currently filing, and such jurisdictions may assess new or additional taxes, sales taxes and value added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have an adverse effect on our operating results or cash flows in the period or periods for which a determination is made.

If our estimates or judgments relating to our critical accounting policies prove to be incorrect or financial reporting standards or interpretations change, our operating results could be adversely affected.

The preparation of financial statements in conformity with generally accepted accounting principles (GAAP) requires management to make estimates and assumptions that affect the amounts reported in our consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as discussed in the section titled "Management's Discussion and Analysis of Financial Condition and Results of Operations." The results of these estimates form the basis for making judgments about the carrying values of assets, liabilities and equity, and the amount of revenue and expenses that are not readily apparent from other sources. Significant assumptions and estimates used in preparing our consolidated financial statements include but are not limited to those related to stock-based compensation, the period of benefit for deferred contract acquisition costs, useful lives of long-lived assets and intangibles, the valuation of intangibles acquired as part of a business combination, and accounting for income taxes. Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of industry or financial analysts and investors, resulting in a potential decline in the market price of our Class A common stock.

Additionally, we regularly monitor our compliance with applicable financial reporting standards and review new pronouncements and drafts thereof that are relevant to us. As a result of new standards, changes to existing standards and changes in their interpretation, we might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems so that they reflect new or amended financial reporting standards, or we may be required to restate our published financial statements. For example, SEC proposals on climate-related disclosures may require us to update our accounting or operational policies, processes, or systems to reflect new or amended financial reporting standards. Such changes to existing standards or changes in their interpretation may have an adverse effect on our reputation, business, financial condition and profit, or cause an adverse deviation from our revenue and operating profit target, which may adversely affect our financial results.

We are exposed to fluctuations in currency exchange rates, which could negatively affect our business, operating results, and financial condition.

Our sales contracts are denominated in US dollars, and therefore our revenue is not subject to foreign currency risk. However, strengthening of the US dollar increases the real cost of our platform to our customers outside of the US, which could lead to delays in the purchase of our platform and the lengthening of our sales cycle. If the US dollar continues to strengthen, this could adversely affect our operating results and financial condition. In addition, increased international sales in the future, including through continued international expansion, our channel partners and other partnerships, could result in foreign currency denominated sales, which would increase our foreign currency risk.

Our operating expenses incurred outside the US and denominated in foreign currencies are increasing and are subject to fluctuations due to changes in foreign currency exchange rates. These expenses are denominated in foreign currencies and are subject to fluctuations due to changes in foreign currency exchange rates. We do not currently hedge against the risks associated with currency fluctuations but may do so, or use other derivative instruments, in the future.

We may require additional capital to fund our business and support our growth, and any inability to generate or obtain such capital may adversely affect our operating results and financial condition.

In order to support our growth and respond to business challenges, such as developing new features or enhancements to our platform to stay competitive, acquiring new technologies, and improving our infrastructure, we have made significant financial investments in our business and we intend to continue to make such investments. As a result, we may need to engage in additional equity or debt financings to provide the funds required for these investments and other business endeavors. If we raise additional funds through equity or convertible debt issuances, our existing stockholders may suffer significant dilution and these securities could have rights, preferences, and privileges that are superior to those of holders of our Class A common stock. We expect that our existing cash and cash equivalents will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months. If we obtain additional funds through debt financing, we may not be able to obtain such financing on terms favorable to us. Further, the current global macroeconomic environment may make it more difficult to raise additional capital on favorable terms, it at all. Such terms may involve restrictive covenants making it difficult to engage in capital raising activities and pursue business opportunities, including potential acquisitions. The trading prices of technology companies have been highly volatile as a result of the conflict in the Middle East, Ukraine and tensions between China and Taiwan, inflation, interest rate volatility, actual or perceived instability in the banking system, and market downturns, which may reduce our ability to access capital on favorable terms or at all. In addition, a recession, depression, or other sustained adverse market event could adversely affect our business and the value of our Class A common stock. If we are unable to obtain adequate financing or financing on terms satisfactory to us when we require it, our ability to continue to support our business growth and to respond to business challenges could be significantly impaired and our business may be adversely affected, requiring us to delay, reduce, or eliminate some or all of our operations.

Risks Related to Ownership of Our Class A Common Stock

The market price of our Class A common stock may be volatile, and you could lose all or part of your investment.

Our Class A common stock price is likely to continue to be volatile and could be subject to wide fluctuations. The market price of our Class A common stock depends on a number of factors, including those described in this "Risk Factors" section, many of which are beyond our control and may not be related to our operating performance. These fluctuations could cause you to lose all or part of your investment in our Class A common stock. Factors that could cause fluctuations in the market price of our Class A common stock include the following:

- actual or anticipated changes or fluctuations in our operating results;
- the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections;

- announcements by us or our competitors of new products or new or terminated significant contracts, commercial relationships, acquisitions or capital commitments;
- rumors and market speculation involving us or other companies in our industry;
- the overall performance of the stock market or technology companies;
- the number of shares of our Class A common stock publicly owned and available for trading;
- failure of industry or financial analysts to maintain coverage of us, changes in financial estimates by any analysts who follow our company, or our failure to meet these estimates or the expectations of investors;
- litigation or other proceedings involving us, our industry or both, or investigations by regulators into our operations or those of our competitors;
- developments or disputes concerning our intellectual property rights or our solutions, or third-party proprietary rights;
- new laws or regulations or new interpretations of existing laws or regulations applicable to our business;
- any major changes in our management or our board of directors;
- the global political, economic and macroeconomic climate, including but not limited to, actual or perceived instability in the banking industry, potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto, labor shortages, supply chain disruptions, potential recession, inflation, and rising interest rates;
- other events or factors, including those resulting from war, armed conflict, including the conflicts in the Middle East, Ukraine and tensions between China and Taiwan, incidents of terrorism or responses to these events; and
- cybersecurity incidents.

In addition, the stock market in general, and the market for technology companies in particular, has experienced extreme price and volume fluctuations that have often been unrelated or disproportionate to the operating performance of those companies, particularly during the current period of global macroeconomic uncertainty, including rising inflation, increasing interest rates, labor shortages and fluctuations in international currency rates, as well as the impacts of regional geopolitical conflicts, including the conflicts in the Middle East, Ukraine and tensions between China and Taiwan. These economic, political, regulatory and market conditions have and may continue to negatively impact the market price of our Class A common stock, regardless of our actual operating performance. In addition, in the past, following periods of volatility in the overall market and the market prices of a particular company's securities, securities class action litigation has often been instituted against that company. Securities litigation, if instituted against us, could result in substantial costs and divert our management's attention and resources from our business. This could have an adverse effect on our business, operating results, and financial condition.

Sales of substantial amounts of our Class A common stock in the public markets, or the perception that they might occur, could cause the market price of our Class A common stock to decline.

Sales of a substantial number of shares of our Class A common stock into the public market, including shares of Class A common stock held by our existing stockholders that have been converted from shares of Class B common stock, and particularly sales by our directors, executive officers, and principal stockholders, or the perception that these sales might occur, could cause the market price of our Class A common stock to decline.

In addition, pursuant to our amended and restated investors' rights agreement, dated October 28, 2020, certain stockholders have the right, subject to certain conditions, to require us to file a registration statement for the public resale of such capital stock or to include such shares in registration statements that we may file for us or other

stockholders. Any registration statement we file to register additional shares, whether as a result of registration rights or otherwise, could cause the market price of our Class A common stock to decline or be volatile.

We may also issue our shares of our capital stock or securities convertible into shares of our capital stock from time to time in connection with a financing, an acquisition, an investment, or otherwise. Any such issuance could result in substantial dilution to our existing stockholders and cause the market price of our Class A common stock to decline.

The dual class structure of our common stock has the effect of concentrating voting control with the holders of our Class B common stock who held, in the aggregate, approximately 72% of the voting power of our capital stock as of January 31, 2024, which will limit or preclude your ability to influence corporate matters, including the election of directors and the approval of any change of control transaction.

Our Class B common stock has 20 votes per share, and our Class A common stock has one vote per share. As of January 31, 2024, the holders of our outstanding Class B common stock held approximately 72% of the voting power of our outstanding capital stock. Because of the twenty-to-one voting ratio between our Class B and Class A common stock, the holders of our Class B common stock collectively are expected to continue to control a majority of the combined voting power of our common stock and therefore will be able to control all matters submitted to our stockholders for approval until the earlier of (i) the date specified by a vote of the holders of 66 2/3% of the then outstanding shares of Class B common stock, (ii) seven years from the date of our prospectus filed with the SEC pursuant to Rule 424(b)(4) under the Securities Act (the Final Prospectus), or June 29, 2028, (iii) the first date following the completion of our IPO on which the number of shares of outstanding Class B common stock (including shares of Class B common stock subject to outstanding stock options) held by Tomer Weingarten, including certain permitted entities that Mr. Weingarten controls, is less than 25% of the number of shares of outstanding Class B common stock (including shares of Class B common stock subject to outstanding stock options) that Mr. Weingarten originally held as of the date of our Final Prospectus, (iv) the date fixed by our board of directors, following the first date following the completion of our IPO when Mr. Weingarten is no longer providing services to us as an officer, employee, consultant or member of our board of directors, (v) the date fixed by our board of directors following the date on which, if applicable, Mr. Weingarten is terminated for cause, as defined in our restated certificate of incorporation, and (vi) the date that is 12 months after the death or disability, as defined in our restated certificate of incorporation, of Mr. Weingarten. This concentrated control will limit or preclude your ability to influence corporate matters for the foreseeable future, including the election of directors, amendments of our organizational documents, and any merger, consolidation, sale of all or substantially all of our assets, or other major corporate transaction requiring stockholder approval. In addition, this may prevent or discourage unsolicited acquisition proposals or offers for our capital stock that you may feel are in your best interest as one of our stockholders.

Future transfers by holders of our Class B common stock will generally result in those shares converting to Class A common stock, subject to limited exceptions, such as certain transfers effected for estate planning purposes. The conversion of Class B common stock to Class A common stock will have the effect, over time, of increasing the relative voting power of those holders of our Class B common stock who retain their shares in the long term.

The dual class structure of our common stock may adversely affect the trading market for our Class A common stock.

We cannot predict whether our dual class structure will, over time, result in a lower or more volatile market price of our Class A common stock, adverse publicity, or other adverse consequences. Certain stock index providers exclude or limit the ability of multi-class share structures from being added to certain indices. In addition, several stockholder advisory firms and large institutional investors oppose the use of multiple class structures. As a result, the dual class structure of our common stock may make us ineligible for inclusion in certain indices, may discourage such indices from selecting us for inclusion (notwithstanding our automatic termination provision) may cause stockholder advisory firms to publish negative commentary about our corporate governance practices or otherwise seek to cause us to change our capital structure, and may result in large institutional investors not purchasing shares of our Class A common stock. Any exclusion from certain stock indices could result in less demand for our Class A common stock. Any actions or publications by stockholder advisory firms or institutional investors critical of our

corporate governance practices or capital structure could also adversely affect the value of our Class A common stock.

General Risk Factors

We may be adversely affected by natural disasters, pandemics, and other catastrophic events, and by man-made problems such as war and regional geopolitical conflicts around the world, that could disrupt our business operations, and our business continuity and disaster recovery plans may not adequately protect us from a serious disaster.

Natural disasters or other catastrophic events may cause damage or disruption to our operations, international commerce, and the global economy, and thus could have an adverse effect on us. Our business operations are also subject to interruption by fire, power shortages, flooding, and other events beyond our control. In addition, our global operations expose us to risks associated with public health crises, such as pandemics and epidemics, which could harm our business and cause our operating results to suffer. Further, acts of war, armed conflict, terrorism and other geopolitical unrest, such as the conflicts in the Middle East, Ukraine and tensions between China and Taiwan, could cause disruptions in our business or the businesses of our partners or the economy as a whole. We maintain an office in Tel Aviv, Israel and had approximately 13% of our personnel in Israel as of January 31, 2024. We are closely monitoring the unfolding events of the armed conflict in Israel which began in October 2023. While this conflict is still evolving, to date, the conflict has not had an adverse impact on our business results of operations and we have implemented continuity measures to address the safety of our employees and continue our operations in the event of reduced employee availability in the conflict region. However, if our continuity measures fail or the conflict continues to worsen or intensify, any business interruptions or spillover effects could adversely affect our business and operations.

In the event of a natural disaster, including a major earthquake, blizzard, or hurricane, or a catastrophic event such as a fire, power loss, cyberattack, or telecommunications failure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in development of our platform, lengthy interruptions in service, breaches of data security, and loss of critical data, all of which could have an adverse effect on our future operating results. Climate change could result in an increase in the frequency or severity of such natural disasters. Moreover, any of our office locations may be vulnerable to the adverse effects of climate change. For example, our corporate offices are located in California, a state that frequently experiences earthquakes, wildfires and resultant air quality impacts and power shutoffs associated with wildfire prevention, heatwaves, and droughts. These events can, in turn, have impacts on inflation risk, food security, water security and on our employees' health and well-being. Additionally, all the aforementioned risks will be further increased if we do not implement an effective disaster recovery plan or our partners' disaster recovery plans prove to be inadequate.

Investors' expectations of our performance relating to environmental, social and governance factors may impose additional costs and expose us to new risks.

There is an increasing focus from certain regulators, investors, employees, users and other stakeholders concerning corporate responsibility, specifically related to ESG matters both in the US and internationally. Some investors may use these non-financial performance factors to guide their investment strategies and, in some cases, may choose not to invest in us if they believe our policies and actions relating to corporate responsibility are inadequate. We may face reputational damage in the event that we do not meet the ESG standards set by various constituencies.

Further, ESG initiatives, goals or commitments could be difficult to achieve or costly to implement. If our competitors' corporate social responsibility performance is perceived to be better than ours, potential or current investors may elect to invest with our competitors instead. Moreover, California recently adopted two new climate-related bills, which require companies doing business in California that meet certain revenue thresholds to publicly disclose certain greenhouse gas emissions data and climate-related financial risk reports, and compliance with such requirements could require significant effort and resources. Additionally, in March 2024, the SEC enacted comprehensive climate change disclosure rules, which have since been challenged by various third parties. Our business may face increased scrutiny related to these activities and our related disclosures, including from the investment community, and our failure to achieve progress or manage the dynamic public sentiment and legal

landscape in these areas on a timely basis, or at all, could adversely affect our reputation, business, and financial performance.

If industry or financial analysts do not publish research or reports about our business, or if they issue inaccurate or unfavorable research regarding our Class A common stock, our stock price and trading volume could decline.

The trading market for our Class A common stock may be influenced by the research and reports that industry or financial analysts publish about us, our business, our market and our competitors. We do not control these analysts or the content and opinions included in their reports. If any of the analysts who cover us issues an inaccurate or unfavorable opinion regarding our stock price, our stock price would likely decline. If our financial results fail to meet, or significantly exceed, our announced guidance or the expectations of analysts or public investors, analysts could downgrade our Class A common stock or publish unfavorable research about us. If one or more of these analysts cease coverage of our Class A common stock or fail to publish reports on us regularly, our visibility in the financial markets could decrease, which in turn could cause our stock price or trading volume to decline.

We are currently subject to and can in the future be subject to securities class action litigation.

Securities class action litigation can be instituted against companies following periods of volatility in the market price of a company's securities. We are currently subject to securities litigation as further described in the section titled "Legal Proceedings." This type of litigation can result in substantial costs and a diversion of management's attention and resources, which could adversely affect our business, operating results, or financial condition. Additionally, the dramatic increase in the cost of directors' and officers' liability insurance may make it more expensive for us to obtain directors' and officers' liability insurance in the future and may require us to opt for lower overall policy limits and coverage or to forgo insurance that we may otherwise rely on to cover significant defense costs, settlements, and damages awarded to plaintiffs, or incur substantially higher costs to maintain the same or similar coverage. These factors could make it more difficult for us to attract and retain qualified executive officers and members of our board of directors.

We do not intend to pay dividends in the foreseeable future. As a result, your ability to achieve a return on your investment will depend on appreciation in the price of our Class A common stock.

We have never declared or paid any cash dividends on our capital stock. We currently intend to retain all available funds and any future earnings for use in the operation of our business and do not anticipate paying any dividends in the foreseeable future. Any determination to pay dividends in the future will be at the discretion of our board of directors. Accordingly, investors must rely on sales of their Class A common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments.

Provisions in our charter documents and under Delaware law could make an acquisition of us, which may be beneficial to our stockholders, more difficult and may limit attempts by our stockholders to replace or remove our current management.

Provisions in our restated certificate of incorporation and amended and restated bylaws may have the effect of delaying or preventing a merger, acquisition or other change of control of the company that the stockholders may consider favorable. In addition, because our board of directors is responsible for appointing the members of our management team, these provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors. Among other things, our restated certificate of incorporation and amended and restated bylaws include provisions that:

- provide that our board of directors is classified into three classes of directors with staggered three-year terms;
- permit our board of directors to establish the number of directors and fill any vacancies and newly created directorships;

- require super-majority voting to amend some provisions in our restated certificate of incorporation and amended and restated bylaws;
- authorize the issuance of "blank check" preferred stock that our board of directors could use to implement a stockholder rights plan;
- provide that only our chief executive officer or a majority of our board of directors will be authorized to call a special meeting of stockholders;
- eliminate the ability of our stockholders to call special meetings of stockholders;
- do not provide for cumulative voting;
- provide that directors may only be removed "for cause" and only with the approval of two-thirds of our stockholders;
- provide for a dual class common stock structure in which holders of our Class B common stock may have the ability to control the outcome of matters requiring stockholder approval, even if they own significantly less than a majority of the outstanding shares of our common stock, including the election of directors and other significant corporate transactions, such as a merger or other sale of our company or its assets;
- prohibit stockholder action by written consent, which requires all stockholder actions to be taken at a meeting of our stockholders;
- provide that our board of directors is expressly authorized to make, alter, or repeal our amended and restated bylaws; and
- establish advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon by stockholders at annual stockholder meetings.

Moreover, Section 203 of the Delaware General Corporation Law (DGCL), may discourage, delay, or prevent a change in control of our company. Section 203 imposes certain restrictions on mergers, business combinations, and other transactions between us and holders of 15% or more of our common stock.

Our restated certificate of incorporation contains exclusive forum provisions for certain claims, which may limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers, or employees.

Our restated certificate of incorporation provides that the Court of Chancery of the State of Delaware, to the fullest extent permitted by law, will be the exclusive forum for any derivative action or proceeding brought on our behalf, any action asserting a breach of fiduciary duty, any action asserting a claim against us arising pursuant to the DGCL, our restated certificate of incorporation, or our amended and restated bylaws, or any action asserting a claim against us that is governed by the internal affairs doctrine.

Moreover, Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all claims brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder. Our restated certificate of incorporation provides that the federal district courts of the US will, to the fullest extent permitted by law, be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act (Federal Forum Provision). Our decision to adopt a Federal Forum Provision followed a decision by the Supreme Court of the State of Delaware holding that such provisions are facially valid under Delaware law. While there can be no assurance that federal or state courts will follow the holding of the Delaware Supreme Court or determine that the Federal Forum Provision should be enforced in a particular case, application of the Federal Forum Provision means that suits brought by our stockholders to enforce any duty or liability created by the Securities Act must be brought in federal court and cannot be brought in state court.

Section 27 of the Exchange Act creates exclusive federal jurisdiction over all claims brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. In addition, the Federal Forum Provision applies to suits brought to enforce any duty or liability created by the Exchange Act. Accordingly, actions by our stockholders to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder must be brought in federal court.

Our stockholders will not be deemed to have waived our compliance with the federal securities laws and the regulations promulgated thereunder.

Any person or entity purchasing or otherwise acquiring or holding any interest in any of our securities shall be deemed to have notice of and consented to our exclusive forum provisions, including the Federal Forum Provision. These provisions may limit a stockholders' ability to bring a claim in a judicial forum of their choosing for disputes with us or our directors, officers, or employees, which may discourage lawsuits against us and our directors, officers, and employees. Alternatively, if a court were to find the choice of forum provision contained in our restated certificate of incorporation or amended and restated bylaws to be inapplicable or unenforceable in an action, we may incur additional costs associated with resolving such action in other jurisdictions, which could harm our business, financial condition, and operating results.

ITEM 1B. UNRESOLVED STAFF COMMENTS

None.

ITEM 1C. CYBERSECURITY

Cybersecurity Risk Management

As part of our overall enterprise risk management program, we maintain a robust cybersecurity risk management program. The cross-functional group responsible for the cybersecurity risk management program includes members of our information security, data privacy and product security personnel, including members of our senior management team. Our cybersecurity program provides a foundation for identifying, monitoring, evaluating, and responding to cybersecurity threats and incidents, including those associated with our use of software, applications, services, and cloud infrastructure developed or provided by third-party vendors and service providers. This framework includes steps for identifying the source of a cybersecurity threat or incident, including whether such cybersecurity threat or incident is associated with a third-party vendor or service provider, assessing the severity and overall risk of a cybersecurity threat or incident, implementing cybersecurity countermeasures and mitigation or remediation strategies, and informing the relevant members of our senior management team, which informs the Audit Committee and our Board of Directors of material cybersecurity threats and incidents.

We engage third parties, including vendors and other external service providers, to support our cybersecurity and data privacy processes. For example, we regularly engage independent third parties for penetration testing and evaluation of our various security compliance standards. We also conduct internal assessments of our cybersecurity risk management program. We review and update our cybersecurity policies, standards and procedures as needed, to account for changes in the threat and operational landscapes, as well as in response to legal and regulatory developments. Further, we require mandatory training for all employees and contractors on our cybersecurity and privacy policies. We also have processes to oversee and identify risks from cybersecurity threats associated with our use of third-party service providers. To that end, we maintain a comprehensive, risk-based approach to identifying and overseeing cybersecurity risks presented by third parties, including vendors, service providers and other external users of our systems, as well as the systems of third parties that could adversely impact our business in the event of a cybersecurity incident affecting those third-party systems. In addition, we perform diligence on our vendors and prospective vendors regarding their cybersecurity posture. Although we have continued to invest in our diligence, onboarding, and monitoring capabilities over our critical third parties, including our third-party vendors and service providers, our control over the security posture of our critical third parties is limited, and there can be no assurance that we can prevent or mitigate the risk of any compromise or failure in the information assets owned or controlled by such third parties.

A cross-functional incident response team, comprised of representatives from information security, information technology, privacy and legal, is responsible for the monitoring and disposition of potential occurrences such as data breaches, intrusions, and other security incidents and implementing our detailed incident response plan. Our incident response plan includes processes and procedures for assessing potential internal and external threats, activation and notification, and post-incident recovery designed to safeguard the confidentiality, availability, and integrity of our information assets.

In fiscal 2024, and through the filing of this Annual Report on Form 10-K, cybersecurity threats, including as a result of any previous cybersecurity incidents, have not materially affected our business strategy, operating results, and/or financial condition. If we were to experience a material cybersecurity incident in the future, such an incident could potentially have a material effect, including on our business strategy, operating results, or financial condition. For more information regarding cybersecurity risks that we face and potential impacts on our business related thereto, see Part I, Item 1A, "Risk Factors" in this Annual Report on Form 10-K.

Cybersecurity Governance

Our Board of Directors has oversight responsibility for our overall enterprise risk management, and cybersecurity risk management in particular is regularly reviewed and overseen by our Audit Committee. The Audit Committee provides oversight and reviews management policies, processes, and procedures designed to identify, monitor, evaluate, and respond to cybersecurity risks to which the company is exposed. Management regularly reports to the Audit Committee regarding its process and procedures to mitigate or remediate cybersecurity risks, threats and incidents, along with monitoring activities of the cybersecurity team.

Management is responsible for day-to-day risk management activities, including identifying and assessing cybersecurity risks, establishing processes to ensure that potential cybersecurity risk exposures are monitored, implementing appropriate mitigation or remediation measures, and maintaining cybersecurity programs. Our cybersecurity programs are under the direction of our Chief Information Officer, who is a member of our executive management team and closely coordinates as needed with other senior management personnel including the Deputy Chief Information Security Officer, the Chief Product and Technology Officer and the Chief Legal Officer, who collectively possess significant experience in evaluating, managing and mitigating security and other risks, including cybersecurity risks.

ITEM 2. PROPERTIES

We are headquartered in Mountain View, California, where we occupy over 10,000 square feet of office space pursuant to a lease that expires in February 2028 subject to the terms thereof. Our headquarters was built to reflect our corporate culture, operational needs, and dedication to employee happiness. We lease additional offices in the US and around the world, including the Czech Republic, France, India, Israel, Netherlands, United Arab Emirates, and other countries. We believe that our current facilities are adequate to meet our current needs.

ITEM 3. LEGAL PROCEEDINGS

We are currently a party to, and may from time to time in the future, be involved in, various litigation matters and subject to claims that arise in the ordinary course of business, including claims asserted by third parties in the form of letters and other communications. For more information regarding legal proceedings and other claims in which we are involved, see Note 15, *Commitments and Contingencies*, to the consolidated financial statements included in Part II, Item 8 of this Annual Report on Form 10-K, and is incorporated herein by reference.

ITEM 4. MINE SAFETY DISCLOSURES

Not applicable.

PART II.

ITEM 5. MARKET FOR REGISTRANT'S COMMON EQUITY, RELATED STOCKHOLDER MATTERS AND ISSUER PURCHASES OF EQUITY SECURITIES

Market Information for Class A Common Stock

Our Class A common stock has been traded on the NYSE under the symbol "S" since June 30, 2021. Prior to that date, there was no public trading market for our common stock. Our Class B common stock is not listed or traded on any stock exchange.

Holders of Record

As of March 22, 2024, we had 116 holders of record of our Class A common stock and 52 holders of record of our Class B common stock. Because many of our shares of common stock are held in street name by brokers, institutions, and other nominees on behalf of stockholders, we are unable to estimate the total number of beneficial owners of our common stock represented by these holders of record.

Dividend Policy

We currently intend to retain all available funds and any future earnings for use in the operation and growth of our business and do not anticipate paying any dividends on our capital stock in the foreseeable future. Any future determination to declare dividends will be made at the discretion of our board of directors, subject to applicable laws, and will depend on our financial condition, results of operations, capital requirements, general business conditions, and other factors that our board of directors may deem relevant.

Securities Authorized for Issuance Under Equity Compensation Plans

The information required by this item will be included in our Proxy Statement for the 2024 Annual Meeting to be filed with the SEC within 120 days of the fiscal year ended January 31, 2024, and is incorporated herein by reference.

Unregistered Sales of Equity Securities

On February 1, 2024, we completed the acquisition of PingSafe. Under the terms of the Purchase Agreement, we acquired 100% of the outstanding shares of PingSafe for total consideration of approximately $57.5 million in cash and 2,354,607 shares of our Class A common stock, subject to customary adjustments set forth in the Purchase Agreement, to the former shareholders of PingSafe.

We believe this transaction was exempt from registration under the Securities Act in reliance on the exemptions provided by Rule 501(a) of Regulation D under the Securities Act and Rule 902(k) of Regulation S under the Securities Act.

Issuer Purchases of Equity Securities

None.

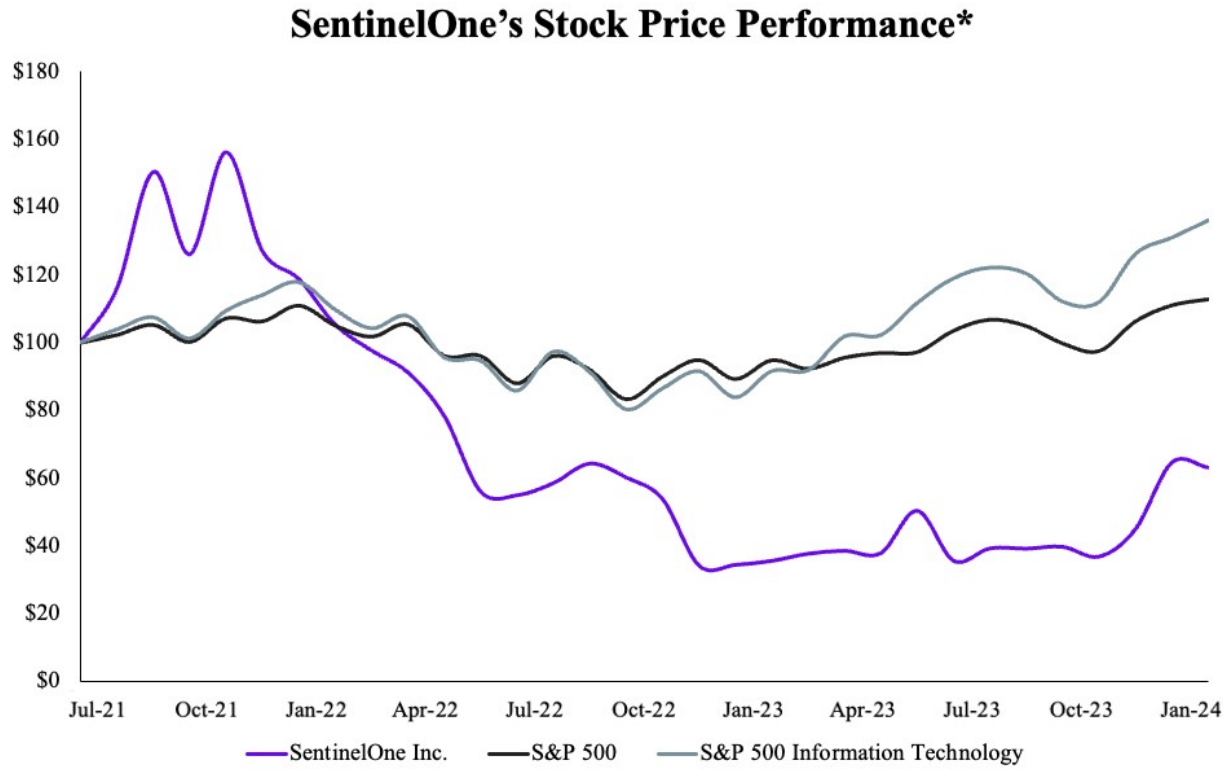
Use of Proceeds from Initial Public Offering of Common Stock and Concurrent Private Placement

None.

Stock Performance Graph

This performance graph shall not be deemed "soliciting material" or be "filed" with the SEC for purposes of Section 18 of the Exchange Act, or otherwise subject to the liability under that Section, and shall not be deemed to be incorporated by reference into any filing of SentinelOne, Inc. under the Securities Act or Exchange Act generally.

We have presented below the cumulative total return to our holders of our Class A common stock between June 30, 2021 (the date our Class A common stock commenced trading on the NYSE) through January 31, 2024 in comparison to the Standard & Poor's 500 Index and Standard & Poor Information Technology Index. All values assume a $100 initial investment and data for the Standard & Poor's 500 Index and Standard & Poor Information Technology Index assume reinvestment of dividends. Such returns are based on historical data and are not indicative of, nor intended to forecast, the future performance of our Class A common stock.



**$100 invested on 6/30/21 in SentinelOne Stock, or S&P500 Index, or S&P 500 Information Technology Index*
Copyright© 2024 Standard & Poor's, a division of S&P Global. All rights reserved.

ITEM 6. [RESERVED]

ITEM 7. MANAGEMENT'S DISCUSSION AND ANALYSIS OF FINANCIAL CONDITION AND RESULTS OF OPERATIONS

The following discussion and analysis of our financial condition and results of operations should be read in conjunction with our consolidated financial statements and related notes appearing elsewhere in this Annual Report on Form 10-K. Some of the information contained in this discussion and analysis or set forth elsewhere in this Annual Report on Form 10-K, particularly information with respect to our future results of operations or financial condition, business strategy and plans, and objectives of management for future operations, includes forward-looking statements that involve risks and uncertainties as described under the heading "Special Note About Forward-Looking Statements" in this Annual Report on Form 10-K. You should review the disclosure under the heading "Risk Factors" in this Annual Report on Form 10-K for a discussion of important factors that could cause our actual results to differ materially from those anticipated in these forward-looking statements. Our fiscal year ends on January 31, and our fiscal quarters end on April 30, July 31, October 31, and January 31. Our fiscal years ended January 31, 2024, 2023, and 2022 are referred to herein as fiscal 2024, fiscal 2023, and fiscal 2022, respectively.

Unless the context otherwise requires, all references in this report to "SentinelOne," the "Company," "we" "our" "us," or similar terms refer to SentinelOne, Inc. and its subsidiaries.

A discussion regarding our financial condition and results of operations for fiscal 2024 compared to fiscal 2023 is presented below. A discussion regarding our financial condition and results of operations for fiscal 2023 compared to fiscal 2022 can be found in "Management's Discussion and Analysis of Financial Condition and Results of Operations" in the Form 10-K for the fiscal year ended January 31, 2023 filed with the SEC on March 29, 2023.

Overview

We founded SentinelOne in 2013 with a dramatically new approach to cybersecurity.

We pioneered the world's first purpose-built AI-powered extended detection and response (XDR) platform to make cybersecurity defense truly autonomous, from the endpoint and beyond. Our Singularity Platform instantly defends against cyberattacks — performing at a faster speed, greater scale, and higher accuracy than otherwise possible from a human-powered approach.

Our Singularity Platform ingests, correlates, and queries petabytes of structured and unstructured data from a myriad of ever-expanding disparate external and internal sources in real-time. We build rich context and deliver greater visibility by constructing a dynamic representation of data across an organization. As a result, our AI models are highly accurate, actionable, and autonomous. Our distributed AI models run both locally on every endpoint and every cloud workload, as well as on our cloud platform. Our Static and vector-agnostic Behavioral AI models, which run on the endpoints themselves, provide our customers with protection even when their devices are not connected to the cloud. In the cloud, our Streaming AI detects anomalies that surface when multiple data feeds are correlated. By providing full visibility into the Storyline of every secured device across the organization through one console, our platform makes it very fast for analysts to easily search through petabytes of data to investigate incidents and proactively hunt threats. We have extended our control and visibility planes beyond the traditional endpoint to unmanaged IoT devices.

Our Singularity Platform can be flexibly deployed on the environments that our customers choose, including public, private, or hybrid clouds. Our feature parity across Windows, macOS, Linux, and Kubernetes offers best-of-breed protection, visibility, and control across today's heterogeneous IT environments. Together, these capabilities make our platform the logical choice for organizations of all sizes, industry verticals, and compliance requirements. Our platform offers true multi-tenancy, which enables some of the world's largest organizations and our managed security providers and incident response partners with an excellent management experience. Our customers realize improved cybersecurity outcomes with fewer people.

We generate substantially all of our revenue by selling subscriptions to our Singularity Platform. Our subscription tiers include Singularity Core, Singularity Control, and Singularity Complete. We also offer product bundles that include Singularity Commercial and Singularity Enterprise. Additionally, customers can extend the functionality of our platform through our subscription Singularity Modules. We generally price our subscriptions and modules on a per agent basis, and each agent generally corresponds with an endpoint, server, virtual machine, or container.

Our subscription contracts typically range from one to three years. We recognize subscription revenue ratably over the term of a contract. Most of our contracts are for terms representing annual increments, therefore contracts generally come up for renewal in the same period in subsequent years. The timing of large multi-year enterprise contracts can create some variability in subscription order levels between periods, though the impact to our revenue in any particular period is limited as a result of ratable revenue recognition.

Our go-to-market strategy is focused on acquiring new customers and driving expanded usage of our platform by existing customers. Our sales organization is comprised of our enterprise sales, inside sales and customer solutions engineering teams. It leverages our global network of independent software vendors (ISVs), alliance partners, and channel partners for prospect access. Additionally, our sales teams work closely with our customers, channel partners, and alliance partners to drive adoption of our platform, and our software solutions are fulfilled

through our channel partners. Our channel partners include some of the world's largest resellers and distributors, managed service providers (MSPs), managed security service providers (MSSPs), managed detection and response providers (MDRs), original equipment manufacturers (OEMs), and incident response (IR) firms. Once customers experience the benefits of our platform, they often upgrade their subscriptions to benefit from the full range of our extended detection and response (XDR), IT, and security operations capabilities. Additionally, many of our customers adopt Singularity Modules over time to extend the functionality of our platform and increase their coverage footprint. The combination of platform upgrades and extended modules drives our powerful land-and-expand motion.

Our Singularity Platform is used globally by organizations of all sizes across a broad range of industries. We had 1,133 customers with annualized recurring revenue (ARR) of $100,000 or more as of January 31, 2024, up from 872 customers with ARR of $100,000 or more as of January 31, 2023. We define ARR as the annualized revenue run rate of our subscription and consumption and usage-based agreements at the end of a reporting period, assuming contracts are renewed on their existing terms for customers that are under contracts with us. As of January 31, 2024 and 2023, no single end customer accounted for more than 3% of our ARR. Our revenue outside of the US represented 36% and 35% for fiscal 2024 and 2023, respectively, illustrating the global nature of our solutions.

We have grown rapidly since our inception. Our revenue was $621.2 million, $422.2 million, and $204.8 million for fiscal 2024, 2023, and 2022, respectively, representing year-over-year growth of 47% and 106%, respectively. During this period, we continued to invest in growing our business to capitalize on our market opportunity. As a result, our net loss for fiscal 2024, 2023, and 2022 was $338.7 million, $378.7 million, and $271.1 million, respectively.

Impact of Global Macroeconomic and Geopolitical Conditions

Our overall performance depends in part on worldwide economic and geopolitical conditions and their impact on customer behavior. Worsening economic conditions, including inflation, interest rate volatility, slower growth, potential recession, fluctuations in foreign exchange rates, actual or perceived instability in the global banking industry, potential uncertainty with respect to the federal debt ceiling and budget and potential government shutdowns related thereto, and other changes in economic conditions, and the impact of natural or man-made global events, including wars and other regional geopolitical armed conflict, such as the conflicts in the Middle East, Ukraine and tensions between China and Taiwan, may result in decreased sales productivity and growth and adversely affect our results of operations and financial performance. As a result of the current macroeconomic environment, we have recently experienced certain impacts on our business, including a decline in usage and consumption patterns from certain customers, especially larger enterprise customers, longer sales cycles, and deal downsizing by new customers and of renewals by existing customers, especially larger enterprises.

We intend to continue to monitor global macroeconomic conditions closely and may determine to take certain financial or operational actions in response to such conditions to the extent our business begins to be adversely impacted. For example, in June 2023, we announced a restructuring plan (the Plan) designed to improve operational efficiencies and operating costs and better align our workforce and operations with current business needs, priorities, and near-term growth expectations. The actions associated with the Plan are expected to be fully complete by the end of fiscal 2025, subject to finalizing the disposition of certain office space. We incurred approximately $7.4 million in charges in connection with the Plan in fiscal 2024, consisting of severance payments and employee benefits, impairment charges related to excess facilities and inventory write-offs, offset partially by savings related to the reversal on stock-based compensation expense.

We maintain an office in Tel Aviv, Israel and had approximately 13% of our personnel in Israel as of January 31, 2024. We are closely monitoring the unfolding events of the armed conflict in the Middle East which began in October 2023. While this conflict is still evolving, to date, the conflict has not had an adverse impact on our business and results of operations. However, if the conflict continues to worsen or intensify, any business interruptions or spillover effects could adversely affect our business and operations.

We are unable to predict the full impact that macroeconomic or other geopolitical factors will have on our future results of operations, liquidity and financial condition due to numerous uncertainties, including the actions that may

be taken by government authorities across the US or other countries, changes in central bank policies and interest rates, rates of inflation, potential uncertainty with respect to the federal debt ceiling and budget and potential, government shutdowns related thereto, regional geopolitical conflicts, the impact to our customers, partners, and suppliers, and other factors described in the section titled "Risk Factors" in this Annual Report on Form 10-K.

Key Business Metrics and Non-GAAP Financial Measures

We monitor the following key metrics and non-GAAP financial measures to help us evaluate our business, identify trends affecting our business, formulate business plans, and make strategic decisions.

Revenue

We discuss revenue below under "Components of Our Results of Operations."

	Year Ended January 31,		
	2024	2023	2022
	(in thousands)		
Revenue	$ 621,154	$ 422,179	$ 204,799

Non-GAAP operating loss

In addition to our results determined in accordance with GAAP, we use non-GAAP operating loss as part of our overall assessment of our performance, including the preparation of our annual operating budget and quarterly forecasts, to evaluate the effectiveness of our business strategies, and to communicate with our board of directors concerning our financial performance. We believe that non-GAAP operating loss provides our management and investors consistency and comparability with our past financial performance and facilitates period-to-period comparisons of operations, as this measure excludes, among other expenses, expenses that we do not consider to be indicative of our overall operating performance. Non-GAAP operating loss is calculated as GAAP operating loss adjusted to exclude amortization of acquired intangible assets, acquisition-related compensation, restructuring charges, stock-based compensation expense, and payroll tax related to stock-based compensation.

Non-GAAP operating loss has limitations as an analytical tool, and should not be considered in isolation or as a substitute for financial information presented in accordance with GAAP, including GAAP operating loss. Other companies, including companies in our industry, may calculate similarly titled non-GAAP measures, including non-GAAP operating loss, differently or may use other measures to evaluate their performance, all of which could reduce the usefulness of our non-GAAP financial measures as tools for comparison. As a result, our non-GAAP operating loss is presented for supplemental informational purposes only.

	Year Ended January 31,		
	2024	2023	2022
	(in thousands)		
Non-GAAP operating loss	$ (118,225)	$ (208,861)	$ (174,588)

A reconciliation of non-GAAP operating loss to GAAP operating loss, the most directly comparable financial measure calculated and presented in accordance with U.S. GAAP, is provided below:

	Year Ended January 31,		
	2024	2023	2022
	(in thousands)		
GAAP operating loss	$ (378,416)	$ (402,576)	$ (267,232)
Stock-based compensation expense	216,870	164,466	87,889
Employer payroll tax on employee stock transactions	3,429	2,235	1,783
Amortization of acquired intangible assets	28,363	22,645	2,972
Acquisition-related compensation	3,043	4,369	—
Inventory write-offs due to restructuring	720	—	—
Other restructuring charges	7,766	—	—
Non-GAAP operating loss	$ (118,225)	$ (208,861)	$ (174,588)

Annualized Recurring Revenue (ARR)

We believe that ARR is a key operating metric to measure our business because it is driven by our ability to acquire new subscription and consumption and usage-based customers and to maintain and expand our relationship with existing customers. ARR represents the annualized revenue run rate of our subscription and consumption and usage-based agreements at the end of a reporting period, assuming contracts are renewed on their existing terms for customers that are under contracts with us. ARR is an operational metric and is not a non-GAAP metric. ARR is not a forecast of future revenue, which can be impacted by contract start and end dates, usage, renewal rates, and other contractual terms.

	As of January 31,		
	2024	2023	2022
	(in thousands)		
Annualized recurring revenue	$ 724,404	$ 521,652	$ 277,954

*ARR as of January 31, 2023 and 2022 reflect the one-time ARR adjustment of approximately 5% made in the first quarter of fiscal 2024.

ARR grew 39% year-over-year to $724.4 million for fiscal 2024, primarily due to high growth in the number of new customers purchasing our subscriptions and to additional purchases by existing customers.

As a result of the decline in usage and consumption in the first quarter of fiscal 2024, we changed our methodology of calculating ARR for consumption and usage-based agreements to reflect committed contract values as opposed to based on consumption and usage. By making this change, we expect future ARR and revenue growth to be more closely aligned. It should also reduce volatility in ARR compared to the prior methodology where usage and consumption changes could have a magnified impact on ARR. In addition, as part of our quarter-end review of ARR in connection with the preparation of our condensed consolidated financial statements for the quarter ended April 30, 2023, we discovered some historical upsell and renewal recording inaccuracies relating to ARR on certain contracts, which we have corrected. As a result of the change in methodology and correction of historical inaccuracies, we made a one-time adjustment to ARR of $27 million or approximately 5% of total ARR, which we reflected in our total ARR as of January 31, 2023. ARR for the prior periods in fiscal 2023 and 2022 presented above have been adjusted based on the same percentage adjustment rate identified in the first quarter of fiscal 2024. This adjustment to ARR did not impact historical total bookings or revenue.

Customers with ARR of $100,000 or More

We believe that our ability to increase the number of customers with ARR of $100,000 or more is an indicator of our market penetration and strategic demand for our platform. We define a customer as an entity that has an active subscription for access to our platform. We count MSPs, MSSPs, MDRs, and OEMs, who may purchase our products on behalf of multiple companies, as a single customer. We do not count our reseller or distributor channel partners as customers.

	As of January 31,		
	2024	2023	2022
	(in thousands)		
Customers with ARR of $100,000 or more	1,133	872	500

*Customers with ARR of $100,000 or more as of January 31, 2023 and 2022 reflect the one-time ARR adjustment of approximately 5% made in the first quarter of fiscal 2024.

Customers with ARR of $100,000 or more grew 30% year-over-year to 1,133 for fiscal 2024, primarily due to growth in the ARR of existing customers from additional purchases and to growth in the average size of purchases by new customers. Based on the adjustments to ARR described above, customers with ARR of $100,000 or more for the prior periods presented above have been adjusted accordingly.

Dollar-Based Net Retention Rate (NRR)

We believe that our ability to retain and expand our revenue generated from our existing customers is an indicator of the long-term value of our customer relationships and our potential future business opportunities. NRR measures the percentage change in our ARR derived from our customer base at a point in time. To calculate NRR, we first determine Prior Period ARR, which is ARR from the population of our customers as of 12 months prior to the end of a particular reporting period. We then calculate Net Retention ARR, which represents the total ARR at the end of a particular reporting period from the same set of customers that is used to determine Prior Period ARR. Net Retention ARR includes any expansion, and is net of contraction and attrition associated with that set of customers. NRR represents the quotient obtained by dividing Net Retention ARR by Prior Period ARR.

	As of January 31,		
	2024	2023	2022
Dollar-based net retention rate	114 %	132 %	129 %

Our NRR of 114% was driven by existing customers adoption of additional endpoint licenses and adjacent platform solutions. A larger portion of our business mix was driven by new customers in 2024, which will open doors for platform adoption over time. We see significant long-term expansion potential based on high customer retention rates, expanding product categories, and early-stage adoption from our installed base.

Components of Our Results of Operations

Revenue

We generate substantially all of our revenue from subscriptions to our Singularity Platform. Customers can extend the functionality of their subscription to our platform by subscribing to additional Singularity Modules. Subscriptions provide access to hosted software. The nature of our promise to the customer under the subscription is to provide protection for the duration of the contractual term and as such is considered as a series of distinct services. Our arrangements may include fixed consideration, variable consideration, or a combination of the two. Fixed consideration is recognized over the term of the arrangement or longer if the fixed consideration relates to a material right. Variable consideration in these arrangements is typically a function of transaction volume or another usage-based measure. Depending upon the structure of a particular arrangement, we i) allocate the variable amount to each distinct service period within the series and recognize revenue as each distinct service period is performed (i.e. direct allocation), ii) estimate total variable consideration at contract inception (giving consideration to any constraints that may apply and updating the estimates as new information becomes available) and recognizes the total transaction price over the period to which it relates, or iii) apply the ‘right to invoice’ practical expedient and recognize revenue based on the amount invoiced to the customer during the period. Premium support and maintenance and other Singularity Modules are distinct from subscriptions and are recognized ratably over the term as the performance obligations are satisfied.

We invoice our customers upfront upon signing for the entire term of the contract, periodically, or in arrears. Most of our subscription contracts have a term of one to three years.

Cost of Revenue

Cost of revenue consists primarily of third-party cloud infrastructure expenses incurred in connection with the hosting and maintenance of our platform. Cost of revenue also consists of personnel-related costs associated with our customer support and services organization, including salaries, benefits, bonuses, and stock-based compensation, amortization of acquired intangible assets, amortization of capitalized internal-use software, software and subscription services used by our customer support and services team, inventory-related costs, and allocated overhead costs.

Our third-party cloud infrastructure costs are driven primarily by the number of customers, the number of endpoints per customer, the number of modules, and the incremental costs for storing additional data collected for such cloud modules. We plan to continue to invest in our platform infrastructure and additional resources in our customer support and services organization as we grow our business. The level and timing of investment in these areas could affect our cost of revenue from period to period.

Operating Expenses

Our operating expenses consist of research and development, sales and marketing, and general and administrative expenses. Personnel-related expenses are the most significant component of operating expenses and consist of salaries, benefits, bonuses, stock-based compensation, and sales commissions. Operating expenses also include allocated facilities and IT overhead costs.

Research and Development

Research and development expenses consist primarily of employee salaries, benefits, bonuses, and stock-based compensation. Research and development expenses also include consulting fees, software and subscription services, and third-party cloud infrastructure expenses incurred in developing our platform and modules.

We expect research and development expenses to increase in absolute dollars as we continue to increase investments in our existing products and services. However, we anticipate research and development expenses to decrease as a percentage of our total revenue over time, although our research and development expenses may fluctuate as a percentage of our total revenue from period to period depending on the timing of these expenses. In addition, research and development expenses that qualify as internal-use software are capitalized, the amount of which may fluctuate significantly from period to period.

Sales and Marketing

Sales and marketing expenses consist primarily of employee salaries, commissions, benefits, bonuses, stock-based compensation, travel and entertainment related expenses, advertising, branding and marketing events, promotions, amortization of acquired customer relationships, and software and subscription services. Sales and marketing expenses also include sales commissions paid to our sales force and referral fees paid to independent third parties that are incremental to obtain a subscription contract. Such costs are capitalized and amortized over an estimated period of benefit of four years, and any such expenses paid for the renewal of a subscription are capitalized and amortized over the average contractual term of the renewal.

We expect sales and marketing expenses to increase in absolute dollars as we continue to make significant investments in our sales and marketing organization to drive additional revenue, further penetrate the market, and expand our global customer base, but to decrease as a percentage of our revenue over time.

General and Administrative

General and administrative expenses consist primarily of salaries, benefits, bonuses, stock-based compensation, and other expenses for our executive, finance, legal, people team, and facilities organizations. General and

administrative expenses also include external legal, accounting, other consulting, and professional services fees, software and subscription services, and other corporate expenses.

We expect to continue to incur additional expenses as a result of operating as a public company, including costs to comply with the rules and regulations applicable to companies listed on a national securities exchange, costs related to compliance and reporting obligations, and increased expenses for insurance, investor relations, and professional services. We expect that our general and administrative expenses will increase in absolute dollars as our business grows but will decrease as a percentage of our revenue over time.

Restructuring

Restructuring charges, related to the Plan, consist primarily of charges related to severance payments, employee benefits, stock-based compensation, and impairment charges related to excess facilities. The actions associated with the Plan are expected to be fully complete by the end of fiscal 2025, subject to finalizing the disposition of certain office space.

Interest Income, Interest Expense, and Other Income (Expense), Net

Interest income consists primarily of interest earned on our cash equivalents and investments.

Interest expense consists primarily of the amortization of the discount related to the Attivo indemnity escrow liability.

Other income (expense), net consists primarily of foreign currency transaction gains and losses and gains and losses on strategic investments.

Provision for (Benefit From) Income Taxes

Provision for (benefit from) income taxes consists primarily of income taxes in certain foreign and state jurisdictions in which we conduct business, and a one-time benefit from the release of valuation allowance as a result of the Attivo acquisition during fiscal 2023. In connection with our global consolidated losses, we maintain a full valuation allowance against our US and Israel deferred tax assets because we have concluded that it is more likely than not that the deferred tax assets will not be realized.

Results of Operations

The following table sets forth our results of operations for the periods presented:

	Year Ended January 31,		
	2024	2023	2022
	(in thousands)		
Revenue	$ 621,154	$ 422,179	$ 204,799
Cost of revenue[(1)]	179,281	144,177	81,677
Gross profit	441,873	278,002	123,122
Operating expenses:			
Research and development[(1)]	218,176	207,008	136,274
Sales and marketing[(1)]	397,160	310,848	160,576
General and administrative[(1)]	198,247	162,722	93,504
Restructuring[(1)]	6,706	—	—
Total operating expenses	820,289	680,578	390,354
Loss from operations	(378,416)	(402,576)	(267,232)
Interest income	45,880	21,408	202
Interest expense	(1,216)	(1,830)	(787)
Other income (expense), net	918	(1,293)	(2,280)
Loss before income taxes	(332,834)	(384,291)	(270,097)
Provision for (benefit from) income taxes	5,859	(5,613)	1,004
Net loss	$ (338,693)	$ (378,678)	$ (271,101)

(1) Includes stock-based compensation expense as follows:

	Year Ended January 31,		
	2024	2023	2022
	(in thousands)		
Cost of revenue	$ 17,187	$ 10,093	$ 3,618
Research and development	61,055	51,771	35,358
Sales and marketing	55,798	40,115	15,460
General and administrative	83,890	62,487	33,453
Restructuring	(1,060)	—	—
Total stock-based compensation expense	$ 216,870	$ 164,466	$ 87,889

The following table sets forth the components of our consolidated statements of operations as a percentage of revenue for each of the periods presented:

	Year Ended January 31,		
	2024	2023	2022
	(as a percentage of total revenue)		
Revenue	100%	100%	100%
Cost of revenue	29	34	40
Gross profit	71	66	60
Operating expenses:			
Research and development	35	49	67
Sales and marketing	64	74	78
General and administrative	32	39	46
Restructuring	1	—	—
Total operating expenses	132	161	191
Loss from operations	(61)	(95)	(130)
Interest income	7	5	—
Interest expense	—	—	—
Other income (expense), net	—	—	(1)
Loss before income taxes	(54)	(91)	(132)
Provision (benefit) for income taxes	1	(1)	—
Net loss	(55)%	(90)%	(132)%

Note: Certain figures may not sum due to rounding.

Comparison of the Years Ended January 31, 2024 and 2023

Revenue

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Revenue	$ 621,154	$ 422,179	$ 198,975	47 %

Revenue increased by $199.0 million, or 47%, from $422.2 million for fiscal 2023 to $621.2 million for fiscal 2024, primarily due to a combination of sales to new customers and sales of additional endpoints and modules to existing customers.

Cost of Revenue, Gross Profit, and Gross Margin

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Cost of revenue	$ 179,281	$ 144,177	$ 35,104	24 %
Gross profit	$ 441,873	$ 278,002	$ 163,871	59 %
Gross margin	71%	66%		

Cost of revenue increased by $35.1 million from $144.2 million for fiscal 2023 to $179.3 million for fiscal 2024, primarily due to a $23.9 million increase in allocated customer support costs which were mostly personnel-related expenses, a $4.4 million increase in amortization of acquired intangible assets in connection with the Attivo acquisition, $3.0 million increase in amortization of capitalized internal use-software due to the continued investment in our platform, and $2.2 million increase in cloud hosting usage charges to support our expanding business. Gross margin increased from 66% for fiscal 2023 to 71% for fiscal 2024, primarily due to revenue growth from existing and new customers outpacing growth in cost of revenue.

Research and Development

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Research and development expenses	$ 218,176	$ 207,008	$ 11,168	5 %

Research and development expenses increased from $207.0 million in fiscal 2023 to $218.2 million in fiscal 2024, primarily due to an increase in personnel-related expenses of $29.1 million, including an increase of $9.3 million related to stock-based compensation expense as a result of increased headcount, partially offset by a decrease of $14.2 million incurred in the prior year as a result of the migration of Scalyr into our platform.

Sales and Marketing

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Sales and marketing expenses	$ 397,160	$ 310,848	$ 86,312	28 %

Sales and marketing expenses increased from $310.8 million in fiscal 2023 to $397.2 million in fiscal 2024, primarily due to an increase in personnel-related expenses of $56.9 million, including an increase of $15.7 million in stock-based compensation expense as a result of increased headcount and increase of $7.0 million in commission expense. In addition, there were increases in marketing expenses of $14.5 million due to overall business growth and further investment in marketing activities, and increases in allocated overhead costs of $5.4 million.

General and Administrative

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
General and administrative expenses	$ 198,247	$ 162,722	$ 35,525	22 %

General and administrative expenses increased from $162.7 million in fiscal 2023 to $198.2 million in fiscal 2024, primarily due to an increase in personnel-related expenses of $33.5 million, including an increase of $21.4 million in stock-based compensation expense as a result of increased headcount, and $9.7 million increase in litigation expenses due to settlements made during the period, partially offset by a $4.8 million decrease in office related expenditures.

Restructuring

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Restructuring	$ 6,706	$ —	$ 6,706	n/a

Restructuring charges increased by $6.7 million due to activities undertaken pursuant to the Plan. This included severance and employee benefit charges of $5.4 million and impairment charges related to excess facilities of $2.4 million, partially offset by stock-based compensation savings of $1.1 million due to decreased headcount.

Interest Income, Interest Expense, and Other Income (Expense), Net

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Interest income	$ 45,880	$ 21,408	$ 24,472	114 %
Interest expense	$ (1,216)	$ (1,830)	$ 614	(34)%
Other income (expense), net	$ 918	$ (1,293)	$ 2,211	(171)%

Interest income increased $24.5 million as a result of higher interest rates on investments. Interest expense decreased due to the amortization of the discount related to Attivo indemnity escrow liability through July 2023. The change in other income (expense), net is primarily due to gains and losses on strategic investments, partially offset by net foreign currency exchange fluctuations.

Provision for (Benefit from) Income Taxes

	Year Ended January 31,		Change	
	2024	2023	$	%
	(dollars in thousands)			
Provision for (benefit from) income taxes	$ 5,859	$ (5,613)	$ 11,472	(204)%

The provision for income taxes increased in fiscal 2024, compared to fiscal 2023, primarily as a result of the increase in foreign taxes related to operations in international subsidiaries and a one-time tax benefit from the application of our deferred assets with a full valuation allowance to net deferred tax liability of Attivo acquired intangibles recorded in fiscal 2023.

In connection with the acquisition of Attivo, which closed in May 2022, we recorded a net deferred tax liability primarily attributable to identifiable acquired intangibles. This net deferred tax liability is considered an additional source of income to support the realizability of our deferred tax asset, and as a result we released a portion of the valuation allowance and recorded a one-time discrete tax benefit of $9.7 million in fiscal 2023.

Liquidity and Capital Resources

In July 2021, upon completion of our IPO and the concurrent private placement, we received net proceeds of $1.4 billion, after deducting underwriters' discounts and commissions and estimated offering expenses of $81.6 million. We did not pay any underwriting discounts or commissions with respect to shares that were sold in the private placement.

We have financed operations primarily through proceeds received from sales of equity securities, payments received from our customers, and borrowings under a now-terminated loan and security agreement, and we have generated operating losses, as reflected in our accumulated deficit of $1.3 billion and $1.0 billion as of January 31, 2024 and 2023, respectively. We expect these and other operating losses to continue for the foreseeable future. We also expect to incur significant research and development, sales and marketing, and general and administrative expenses over the next several years in connection with the continued development and expansion of our business. As of January 31, 2024 and 2023, our principal source of liquidity was cash, cash equivalents, and investments of $1.1 billion and $1.2 billion, respectively.

In the short term, we believe that our existing cash, cash equivalents, and investments will be sufficient to support working capital and capital expenditure requirements for at least the next 12 months. In the long term beyond the next 12 months, our future capital requirements will depend on many factors, including global

macroeconomic conditions, our revenue growth rate, the timing and the amount of cash received from customers, the expansion of sales and marketing activities, the timing and extent of spending to support research and development efforts, the price at which we are able to purchase third-party cloud infrastructure, expenses associated with our international expansion, the introduction of platform enhancements, and the continuing market adoption of our platform. We have, and in the future, we may enter into arrangements to acquire or invest in complementary businesses, products, and technologies. We may be required to seek additional equity or debt financing. In the event that we require additional financing, we may not be able to raise such financing on terms acceptable to us or at all. If we are unable to raise additional capital or generate cash flows necessary to expand our operations and invest in continued innovation, we may not be able to compete successfully, which would harm our business, operating results, and financial condition.

We hold our cash, cash equivalents, and investments with a diverse group of banking partners. However, any instability in the US or global banking system or relating to the federal budget may impact liquidity both in the short term and long term and may result in adverse impacts to our or our customers' business, including in our customers' ability to pay for our platform.

The following table shows a summary of our cash flows for the periods presented:

	Years Ended January 31,		
	2024	2023	2022
	(in thousands)		
Net cash used in operating activities	$ (68,374)	$ (193,287)	$ (95,588)
Net cash provided by (used in) investing activities	$ 140,590	$ (1,312,666)	$ (19,743)
Net cash provided by financing activities	$ 47,464	$ 36,308	$ 1,387,124

Operating Activities

Our largest source of operating cash is payments received from our customers. Our primary uses of cash from operating activities are for personnel-related expenses, sales and marketing expenses, third-party cloud infrastructure expenses, and overhead expenses. We have generated negative cash flows from operating activities and have supplemented working capital through net proceeds from the sale of equity securities.

Cash used in operating activities primarily consists of our net loss adjusted for certain non-cash items, including stock-based compensation expense, depreciation and amortization, amortization of deferred contract acquisition costs, and changes in operating assets and liabilities during each period.

Cash used in operating activities during fiscal 2024 was $68.4 million, primarily consisting of our net loss of $338.7 million, and $20.2 million used in net changes to our operating assets and liabilities, partially offset by non-cash items of $290.5 million. The main drivers of the changes in operating assets and liabilities were a $81.0 million increase in deferred contract acquisition costs, a $61.9 million increase in accounts receivable due to timing of cash received from customers, and a $4.5 million decrease in accounts payable. These amounts were partially offset by a $19.1 million increase in accrued payroll and benefits and a $108.2 million increase in deferred revenue resulting primarily from increased subscription contracts.

Cash used in operating activities during fiscal 2023 was $193.3 million, primarily consisting of our net loss of $378.7 million, and $35.4 million used in net changes to our operating assets and liabilities, partially offset by non-cash items of $220.8 million. The main drivers of the changes in operating assets and liabilities were a $61.3 million increase in deferred contract acquisition costs, a $44.4 million increase in accounts receivable due to timing of cash received from customers, a $14.5 million increase in prepaid expenses and other assets primarily due to annual insurance renewal and prepaid sponsorship costs, and a $7.2 million decrease in accrued payroll and benefits. These amounts were partially offset by a $92.5 million increase in deferred revenue resulting primarily from increased subscription contracts.

Investing Activities

Cash provided by investing activities during fiscal 2024 was $140.6 million, consisting of $639.2 million of investment sales and maturities, partially offset by $466.3 million of investment purchases, $14.0 million of capitalized internal-use software costs, $13.6 million of net cash paid for the KSG acquisition, $3.5 million for purchases of intangible assets, and $1.3 million of purchases of property and equipment to support additional office facilities.

Cash used in investing activities during fiscal 2023 was $1.3 billion, consisting of $1.9 billion of investment purchases, $281.0 million of net cash paid for the Attivo acquisition, $13.5 million of capitalized internal-use software costs, and $5.0 million of purchases of property and equipment to support additional office facilities, partially offset by $925.2 million of investment maturities.

Financing Activities

Cash provided by financing activities during fiscal 2024 was $47.5 million, consisting of $28.3 million of proceeds from the exercise of employee stock options and $19.1 million of proceeds from the issuance of common stock under our 2021 Employee Stock Purchase Plan.

Cash provided by financing activities during fiscal 2023 was $36.3 million, consisting of $19.2 million of proceeds from the issuance of common stock under our 2021 Employee Stock Purchase Plan, $17.3 million of proceeds from the exercise of stock options, partially offset by $0.2 million of payments of deferred offering costs.

Contractual Obligations and Commitments

Our operating lease obligations as of January 31, 2024 were approximately $25.2 million, with $5.6 million expected to be paid within 12 months and the remainder thereafter. Our operating leases are related to leased office space with expirations through 2029. See Note 8, *Leases*, to the consolidated financial statements included in Part II, Item 8, Financial Statements and Supplementary Data.

Our purchase obligations as of January 31, 2024 were approximately $808.1 million, with $109.1 million expected to be paid within 12 months and the remainder thereafter.

Off-Balance Sheet Arrangements

We did not have during the periods presented, and we do not currently have, any off-balance sheet financing arrangements or any relationships with unconsolidated entities or financial partnerships, such as structured finance or special purpose entities, that were established for the purpose of facilitating off-balance sheet arrangements or other contractually narrow or limited purposes.

Critical Accounting Policies and Estimates

Our consolidated financial statements are prepared in accordance with generally accepted accounting principles (GAAP) in the US. The preparation of consolidated financial statements requires us to make estimates and assumptions that affect the reported amounts of assets, liabilities, revenue, expenses, and related disclosures. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, and we evaluate our estimates and assumptions on an ongoing basis. Actual results could differ significantly from the estimates made by management. To the extent that there are differences between our estimates and actual results, our future financial statement presentation, financial condition, operating results, and cash flows will be affected.

The critical accounting policies requiring estimates, assumptions, and judgments that we believe have the most significant impact on our consolidated financial statements are described below.

Revenue Recognition

We recognize revenue in accordance with Accounting Standards Codification (ASC) Topic 606, *Revenue from Contracts with Customers*.

We consider the terms and conditions of contracts with customers and our customary business practices in identifying contracts. We determine we have a contract with a customer when the contract is approved, the payment terms for the services can be identified, each party's rights regarding the services to be transferred can be identified, the contract has commercial substance, and we have determined that the customer has the ability and intent to pay. We apply judgment in determining the customer's ability and intent to pay, which is based on a variety of factors, including the customer's historical payment experience or, in the case of a new customer, credit and financial information pertaining to such customer.

Our contracts with customers may contain multiple performance obligations, which are accounted for separately if they are capable of being distinct and are distinct in the context of the contract. Contracts that contain multiple performance obligations require an allocation of the transaction price to each performance obligation based on relative standalone selling price. Certain sales arrangements may include variable consideration, which is recorded as part of the transaction price if, in our judgment, it is probable that no significant future reversal of cumulative revenue under the contract will occur.

Business Combinations

We account for our acquisitions using the acquisition method of accounting. We allocate the fair value of purchase consideration to the tangible and intangible assets acquired, and liabilities assumed, based on their estimated fair values. The excess of the fair value of purchase consideration over the values of these identifiable assets and liabilities is recorded as goodwill. When determining the fair value of assets acquired and liabilities assumed, management makes significant estimates and assumptions, especially with respect to intangible assets. Significant estimates in valuing certain identifiable assets include, but are not limited to, the selection of valuation methodologies, forecasted revenue, discount rates, and useful lives. Management's estimates of fair value are based upon assumptions believed to be reasonable, but which are inherently uncertain and unpredictable and, as a result, actual results may differ from estimates.

Recently Issued Accounting Pronouncements

See Note 2, *Summary of Significant Accounting Policies*, to the consolidated financial statements included elsewhere in this Annual Report on Form 10-K for more information regarding recently issued accounting pronouncements.

ITEM 7A. QUANTITATIVE AND QUALITATIVE DISCLOSURES ABOUT MARKET RISK

We are exposed to market risk in the ordinary course of our business. Market risk represents the risk of loss that may impact our financial condition due to adverse changes in financial market prices and rates. Our market risk exposure is primarily the result of fluctuations in interest rates and foreign currency exchange rates.

Interest Rate Risk

As of January 31, 2024, we had $1.1 billion of cash, cash equivalents, and investments, which consist of money market funds, certificates of deposit, commercial paper, corporate notes and bonds and US government securities. We also had $65.4 million of restricted cash as of January 31, 2024 primarily due to Attivo indemnity escrow liability, and to a lesser extent, outstanding letters of credit established in connection with lease agreements for our facilities. Our cash, cash equivalents, and investments are held for working capital purposes. We do not enter into investments for trading or speculative purposes. The effect of a hypothetical 100 basis point change in interest rates would result in a $4.9 million change in the fair market value of our investment portfolio as of January 31, 2024.

Foreign Currency Exchange Risk

To date, primarily all of our sales contracts have been denominated in U.S. dollars, therefore our revenue is not subject to foreign currency risk. Operating expenses within the U.S. are primarily denominated in U.S. dollars, while operating expenses incurred outside the U.S. are primarily denominated in each country's respective local currency. Our operating results and cash flows are, therefore, subject to fluctuations due to changes in foreign currency exchange rates. Foreign currency transaction gains and losses are recorded in other income (expense), net in the consolidated statements of operations. As the impact of foreign currency exchange rates has not been material to our historical operating results, we have not entered into derivative or hedging transactions, but we may do so in the future if our exposure to foreign currency becomes more significant. A hypothetical 10% adverse change in the US dollar against other currencies would have resulted in an increase in operating loss of approximately $7.4 million and $9.7 million for fiscal 2024 and 2023, respectively. The hypothetical impact in fiscal 2022 would not have been material.

ITEM 8. FINANCIAL STATEMENTS AND SUPPLEMENTARY DATA

INDEX TO CONSOLIDATED FINANCIAL STATEMENTS

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the stockholders and the Board of Directors of SentinelOne, Inc.

Opinion on the Financial Statements

We have audited the accompanying consolidated balance sheets of SentinelOne, Inc. and subsidiaries (the "Company") as of January 31, 2024 and 2023, the related consolidated statements of operations, comprehensive loss, redeemable convertible preferred stock and stockholders' equity (deficit), and cash flows, for each of the three years in the period ended January 31, 2024, and the related notes (collectively referred to as the "financial statements"). In our opinion, the financial statements present fairly, in all material respects, the financial position of the Company as of January 31, 2024 and 2023, and the results of its operations and its cash flows for each of the three years in the period ended January 31, 2024, in conformity with accounting principles generally accepted in the United States of America.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the Company's internal control over financial reporting as of January 31, 2024, based on criteria established in *Internal Control — Integrated Framework (2013)* issued by the Committee of Sponsoring Organizations of the Treadway Commission and our report dated March 27, 2024, expressed an unqualified opinion on the Company's internal control over financial reporting.

Basis for Opinion

These financial statements are the responsibility of the Company's management. Our responsibility is to express an opinion on the Company's financial statements based on our audits. We are a public accounting firm registered with the PCAOB and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audits in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether due to error or fraud. Our audits included performing procedures to assess the risks of material misstatement of the financial statements, whether due to error or fraud, and performing procedures that respond to those risks. Such procedures included examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements. Our audits also included evaluating the accounting principles used and significant estimates made by management, as well as evaluating the overall presentation of the financial statements. We believe that our audits provide a reasonable basis for our opinion.

Critical Audit Matters

The critical audit matter communicated below is a matter arising from the current-period audit of the financial statements that was communicated or required to be communicated to the audit committee and that (1) relates to accounts or disclosures that are material to the financial statements and (2) involved our especially challenging, subjective, or complex judgments. The communication of critical audit matters does not alter in any way our opinion on the financial statements, taken as a whole, and we are not, by communicating the critical audit matter below, providing a separate opinion on the critical audit matter or on the accounts or disclosures to which it relates.

Revenue Recognition — Refer to Notes 2 and 3 to the financial statements

Critical Audit Matter Description

The Company generates substantially all its revenue from subscriptions to its Singularity Platform. This includes subscription, premium support and maintenance and other Singularity Modules, which are distinct performance obligations and are recognized (i) ratably over the subscription term as the performance obligations are satisfied, (ii) based on transaction volume or (iii) based on certain usage-based measures. To determine the amount and pattern of revenue recognition, management identifies and evaluates the relevant contractual terms in its customer contracts based on its accounting policy (collectively "contract terms and conditions").

Given the significance of the proper identification and evaluation of contract terms and conditions to the amount and pattern of revenue recognition, performing audit procedures to evaluate whether management properly identified the relevant contract terms and conditions that impact the amount and pattern of revenue recognition required a high degree of auditor judgment and an increased extent of effort.

How the Critical Audit Matter Was Addressed in the Audit

Our audit procedures related to the evaluation of management's identification of the relevant contract terms and conditions that impact the amount and pattern of revenue recognition included the following, among others:

- We assessed management's significant accounting policies related to revenue recognition for compliance with Accounting Standards Codification (ASC) 606, Revenue from Contracts with Customers.
- We selected a sample of recorded revenue transactions and contracts entered during the year and performed the following procedures:
  - Obtained and read customer source documents and the contract, including master agreements and related amendments, to evaluate if relevant contract terms and conditions have been appropriately identified by management.
  - Evaluated the appropriateness of management's determination of the impact of those terms and conditions on the amount and pattern of revenue recognition.

/s/ DELOITTE & TOUCHE LLP

San Jose, California
March 27, 2024

We have served as the Company's auditor since 2018.

SENTINELONE, INC.

CONSOLIDATED BALANCE SHEETS
(in thousands, except share data)

	January 31,	
	2024	2023
Assets		
Current assets:		
Cash and cash equivalents	$ 256,651	$ 137,941
Short-term investments	669,305	485,584
Accounts receivable, net	214,322	151,492
Deferred contract acquisition costs, current	54,158	37,904
Prepaid expenses and other current assets	102,895	101,812
Total current assets	1,297,331	914,733
Property and equipment, net	48,817	38,741
Operating lease right-of-use assets	18,474	23,564
Long-term investments	204,798	535,422
Deferred contract acquisition costs, non-current	71,640	55,536
Intangible assets, net	122,903	145,093
Goodwill	549,411	540,308
Other assets	8,033	5,516
Total assets	$ 2,321,407	$ 2,258,913
Liabilities and Stockholders' Equity		
Current liabilities:		
Accounts payable	$ 6,759	$ 11,214
Accrued liabilities	104,671	100,015
Accrued payroll and benefits	74,345	54,955
Operating lease liabilities, current	4,689	3,895
Deferred revenue, current	399,603	303,200
Total current liabilities	590,067	473,279
Deferred revenue, non-current	114,930	103,062
Operating lease liabilities, non-current	18,239	23,079
Other liabilities	4,128	2,788
Total liabilities	727,364	602,208
Commitments and contingencies (Note 15)		
Stockholders' equity:		
Preferred stock; $0.0001 par value; 50,000,000 shares authorized as of January 31, 2024 and 2023, and no shares issued and outstanding as of January 31, 2024 and 2023	—	—
Class A common stock; $0.0001 par value; 1,500,000,000 shares authorized as of January 31, 2024 and 2023; 269,780,805 and 222,951,206 shares issued and outstanding as of January 31, 2024 and 2023, respectively	27	21
Class B common stock; $0.0001 par value; 300,000,000 shares authorized as of January 31, 2024 and 2023; 34,910,917 and 63,812,651 shares issued and outstanding as of January 31, 2024 and 2023, respectively	3	8
Additional paid-in capital	2,934,607	2,663,394
Accumulated other comprehensive loss	(1,550)	(6,367)
Accumulated deficit	(1,339,044)	(1,000,351)
Total stockholders' equity	1,594,043	1,656,705
Total liabilities and stockholders' equity	$ 2,321,407	$ 2,258,913

SENTINELONE, INC.

CONSOLIDATED BALANCE SHEETS
(in thousands, except share data)

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF OPERATIONS
(in thousands, except share and per share data)

	Year Ended January 31,		
	2024	2023	2022
Revenue	$ 621,154	$ 422,179	$ 204,799
Cost of revenue	179,281	144,177	81,677
Gross profit	441,873	278,002	123,122
Operating expenses:			
Research and development	218,176	207,008	136,274
Sales and marketing	397,160	310,848	160,576
General and administrative	198,247	162,722	93,504
Restructuring (Note 11)	6,706	—	—
Total operating expenses	820,289	680,578	390,354
Loss from operations	(378,416)	(402,576)	(267,232)
Interest income	45,880	21,408	202
Interest expense	(1,216)	(1,830)	(787)
Other income (expense), net	918	(1,293)	(2,280)
Loss before income taxes	(332,834)	(384,291)	(270,097)
Provision for (benefit from) income taxes	5,859	(5,613)	1,004
Net loss	$ (338,693)	$ (378,678)	$ (271,101)
Net loss per share attributable to Class A and Class B common stockholders, basic and diluted	$ (1.15)	$ (1.36)	$ (1.56)
Weighted-average shares used in computing net loss per share attributable to Class A and Class B common stockholders, basic and diluted	294,923,536	277,802,861	174,051,203

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF COMPREHENSIVE LOSS
(in thousands)

	Year Ended January 31,		
	2024	2023	2022
Net loss	$ (338,693)	$ (378,678)	$ (271,101)
Other comprehensive income (loss):			
Changes in unrealized gains (losses) on investments	4,817	(6,821)	—
Foreign currency translation adjustments	—	—	289
Total comprehensive loss	$ (333,876)	$ (385,499)	$ (270,812)

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF REDEEMABLE CONVERTIBLE PREFERRED STOCK AND STOCKHOLDERS' EQUITY (DEFICIT)
(in thousands, except share data)

	Redeemable Convertible Preferred Stock		Class A and Class B Common Stock		Additional Paid-In Capital	Accumulated Other Comprehensive Income (Loss)	Accumulated Deficit	Total Stockholders' Equity (Deficit)
	Shares	Amount	Shares	Amount				
Balances as of January 31, 2021	167,058,113	$ 621,139	39,242,316	$ 2	$ 29,869	$ 165	$ (350,572)	$ (320,536)
Conversion of redeemable convertible preferred stock to common stock upon initial public offering	(167,058,113)	(621,139)	169,787,200	10	621,129	—	—	621,139
Issuance of common stock upon initial public offering and private placements, net of underwriting discounts and commissions	—	—	41,678,568	4	1,380,956	—	—	1,380,960
Issuance of common stock upon exercise of options	—	—	9,793,331	10	14,611	—	—	14,621
Issuance of common stock upon exercise of warrants	—	—	940,953	—	—	—	—	—
Vesting of restricted stock units	—	—	15,218	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	—	—	381,716	—	11,356	—	—	11,356
Vesting of early exercised options	—	—	—	—	572	—	—	572
Issuance of common stock and awards assumed in connection with acquisition	—	—	7,277,214	1	120,319	—	—	120,320
Issuance of restricted stock awards	—	—	1,315,099	—	—	—	—	—
Stock-based compensation	—	—	—	—	92,668	—	—	92,668
Issuance of restricted stock for services provided	—	—	20,000	—	500	—	—	500
Foreign currency translation adjustments	—	—	—	—	—	289	—	289
Net loss	—	—	—	—	—	—	(271,101)	(271,101)
Balances as of January 31, 2022	—	$ —	270,451,615	$ 27	$ 2,271,980	$ 454	$ (621,673)	$ 1,650,788
Issuance of common stock upon exercise of options	—	—	7,650,525	1	17,334	—	—	17,335
Vesting of restricted stock units	—	—	1,303,854	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	—	—	1,335,183	—	19,159	—	—	19,159
Cancellation of holdback shares	—	—	(9,551)	—	—	—	—	—
Vesting of early exercised options	—	—	—	—	103	—	—	103
Issuance of common stock in connection with acquisition	—	—	6,032,231	1	186,332	—	—	186,333
Stock-based compensation	—	—	—	—	168,486	—	—	168,486
Other comprehensive loss	—	—	—	—	—	(6,821)	—	(6,821)
Net loss	—	—	—	—	—	—	(378,678)	(378,678)
Balance as of January 31, 2023	—	$ —	286,763,857	$ 29	$ 2,663,394	$ (6,367)	$ (1,000,351)	$ 1,656,705
Issuance of common stock upon exercise of options	—	—	10,298,114	1	28,317	—	—	28,318

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF REDEEMABLE CONVERTIBLE PREFERRED STOCK AND STOCKHOLDERS' EQUITY (DEFICIT)
(in thousands, except share data)

Vesting of restricted stock units	—	—	6,021,877	—	—	—	—	—
Issuance of common stock under employee stock purchase plan	—	—	1,607,874	—	19,147	—	—	19,147
Vesting of early exercised options	—	—	—	—	186	—	—	186
Stock-based compensation	—	—	—	—	223,563	—	—	223,563
Other comprehensive income	—	—	—	—	—	4,817	—	4,817
Net loss	—	—	—	—	—	—	(338,693)	(338,693)
Balance as of January 31, 2024	—	$ —	304,691,722	$ 30	$ 2,934,607	$ (1,550)	$ (1,339,044)	$ 1,594,043

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

	Year Ended January 31,		
	2024	2023	2022
CASH FLOW FROM OPERATING ACTIVITIES:			
Net loss	$ (338,693)	$ (378,678)	$ (271,101)
Adjustments to reconcile net loss to net cash used in operating activities:			
Depreciation and amortization	38,912	29,721	7,909
Amortization of deferred contract acquisition costs	48,682	36,417	21,670
Non-cash operating lease costs	4,020	3,559	2,862
Stock-based compensation expense	216,870	164,466	87,889
Accretion of discounts, and amortization of premiums on investments, net	(19,943)	(12,217)	—
Net gain on strategic investments	(2,703)	—	—
Other	4,637	(1,187)	(456)
Changes in operating assets and liabilities, net of effects of acquisitions			
Accounts receivable	(61,949)	(44,442)	(59,082)
Prepaid expenses and other current assets	(1,207)	(14,499)	(7,319)
Deferred contract acquisition costs	(81,039)	(61,289)	(53,565)
Accounts payable	(4,499)	3,670	(2,076)
Accrued liabilities	4,271	4,976	18,080
Accrued payroll and benefits	19,140	(7,205)	41,462
Operating lease liabilities	(4,410)	(5,320)	(3,139)
Deferred revenue	108,197	92,496	115,142
Other liabilities	1,340	(3,755)	6,136
Net cash used in operating activities	(68,374)	(193,287)	(95,588)
CASH FLOW FROM INVESTING ACTIVITIES:			
Purchases of property and equipment	(1,304)	(4,953)	(3,653)
Purchases of intangible assets	(3,505)	(407)	(802)
Capitalization of internal-use software	(13,956)	(13,452)	(5,839)
Purchases of investments	(466,253)	(1,938,007)	(6,000)
Sales and maturities of investments	639,193	925,185	—
Cash paid for acquisitions, net of cash and restricted cash acquired	(13,585)	(281,032)	(3,449)
Net cash provided by (used in) investing activities	140,590	(1,312,666)	(19,743)
CASH FLOW FROM FINANCING ACTIVITIES:			
Payments of deferred offering costs	—	(186)	(7,416)
Repayment of debt	—	—	(20,000)
Proceeds from exercise of stock options	28,317	17,335	14,622
Proceeds from issuance of common stock under the employee stock purchase plan	19,147	19,159	11,356
Proceeds from initial public offering and private placement, net of underwriting discounts and commissions	—	—	1,388,562
Net cash provided by financing activities	47,464	36,308	1,387,124
EFFECT OF EXCHANGE RATE CHANGES ON CASH AND CASH EQUIVALENTS	—	—	1,146
NET CHANGE IN CASH, CASH EQUIVALENTS, AND RESTRICTED CASH	119,680	(1,469,645)	1,272,939
CASH, CASH EQUIVALENTS, AND RESTRICTED CASH–Beginning of period	202,406	1,672,051	399,112
CASH, CASH EQUIVALENTS, AND RESTRICTED CASH–End of period	$ 322,086	$ 202,406	$ 1,672,051
SUPPLEMENTAL DISCLOSURE OF CASH FLOW INFORMATION:			
Interest paid	$ 7	$ 17	$ 409
Income taxes paid, net of refunds	$ 5,111	$ 500	$ 583
SUPPLEMENTAL DISCLOSURE OF NON-CASH INVESTING AND FINANCING ACTIVITIES:			
Stock-based compensation capitalized as internal-use software	$ 6,693	$ 4,020	$ 4,779
Property and equipment purchased but not yet paid	$ 98	$ 203	$ 913
Vesting of early exercised stock options	$ 186	$ 103	$ 575
Deferred offering costs accrued but not yet paid	$ —	$ —	$ 186

SENTINELONE, INC.

CONSOLIDATED STATEMENTS OF CASH FLOWS
(in thousands)

Issuance of common stock and assumed equity awards in connection with acquisitions	$ —	$ 186,332	$ 120,319
Conversion of redeemable convertible preferred stock to common stock upon initial public offering	$ —	$ —	$ 621,139

The accompanying notes are an integral part of these consolidated financial statements.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

1. ORGANIZATION AND DESCRIPTION OF BUSINESS

Business

SentinelOne, Inc. (SentinelOne, the Company, we, our, or us) was incorporated in January 2013 in the State of Delaware. We are a cybersecurity provider that delivers an artificial intelligence-powered platform to enable autonomous cybersecurity defense. Our headquarters is located in Mountain View, California with various other global office locations.

2. SUMMARY OF SIGNIFICANT ACCOUNTING POLICIES

Basis of Presentation

The consolidated financial statements have been prepared in accordance with generally accepted accounting principles (GAAP) in the United States (US). The consolidated financial statements include the accounts of SentinelOne and our wholly-owned subsidiaries. All intercompany balances and transactions have been eliminated in consolidation.

Fiscal Year

Our fiscal year ends on January 31. References to fiscal 2024, 2023 and 2022 refer to the fiscal years ended January 31, 2024, January 31, 2023 and January 31, 2022, respectively.

Use of Estimates

The preparation of the consolidated financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. These estimates include, but are not limited to, stock-based compensation, the period of benefit for deferred contract acquisition costs, useful lives of long-lived assets and intangibles, the valuation of intangibles acquired as part of a business combination, and accounting for income taxes. Actual results could differ from those estimates.

Segment and Geographic Information

We have a single operating and reportable segment. Our chief operating decision maker (CODM) is our Chief Executive Officer. The CODM reviews financial information presented on a consolidated basis for purposes of making operating decisions, allocating resources, and assessing financial performance. For information regarding our revenue and long-lived assets by geography, see Note 3, *Revenue and Contract Balances*, and Note 14, *Geographic Information*, respectively.

Foreign Currency

During fiscal 2022, we changed the functional currency of certain subsidiaries from their respective local currency to the US dollar. The change in functional currency is due to increased exposure to the US dollar as a result of a change in facts and circumstances in the primary economic environment in which these subsidiaries operate. The effects of the change in functional currency were not significant to our consolidated financial statements.

Subsequent to the change, our reporting currency and the functional currency of our foreign subsidiaries is the US dollar. Foreign currency transaction gains and losses are recorded in other income (expense), net in the consolidated statements of operations and were not material for any periods presented.

Revenue Recognition

We recognize revenue in accordance with Accounting Standards Codification (ASC) Topic 606, *Revenue from Contracts with Customers*.

Revenue is recognized when a customer obtains control of promised services. The amount of revenue recognized reflects the consideration that we expect to be entitled to receive in exchange for the subscriptions and services. We apply the following five-step approach to recognize revenue:

(i) **Identification of the Contract, or Contracts, with the Customer**—We determine that we have a contract with a customer when the contract is approved, the payment terms for the services can be identified, each party's rights regarding the services to be transferred can be identified, the customer has the ability and intent to pay, and the contract has commercial substance. We apply judgment in determining the customer's ability and intent to pay, which is based on a variety of factors, including the customer's historical payment experience or, in the case of a new customer, credit and financial information of the customer.

We sell through our indirect relationships with our channel partners or direct relationships with end customers through our internal sales force. Apart from certain sales arrangements where channel partners are determined to be our customers, we have concluded that the end customer is our customer.

(ii) **Identification of the Performance Obligations in the Contract**—Performance obligations in a contract are identified based on the services that will be transferred to a customer that are both capable of being distinct, where the customer can benefit from the service either on its own or together with other resources that are readily available to the customer, and are distinct in the context of the contract, whereby the transfer of the services is separately identifiable from other promises in the contract. To the extent a contract includes multiple promised services, we apply judgment to determine whether promised services are capable of being distinct and distinct in the context of the contract. If these criteria are not met, the promised services are accounted for as a combined performance obligation.

We have concluded that our contracts with customers do not contain warranties that give rise to a separate performance obligation.

(iii) **Determination of the Transaction Price**—The transaction price is the amount of consideration we expect to be entitled from a customer in exchange for providing the subscriptions and services. Variable consideration is included in the transaction price if, in our judgment, it is probable that no significant future reversal of cumulative revenue under the contract will occur.

Some of our end customers are entitled to receive service level commitment credits, in which we may be contractually obligated to provide partial refunds, and in rare instances, each representing a form of variable consideration. We have historically not experienced any significant incidents affecting the defined guarantees of performance levels or service response affecting the defined guarantees of performance levels or service response rates, and accordingly, estimated refunds related to service level commitment credits in the consolidated financial statements were not material during fiscal 2024, 2023 and 2022.

None of our contracts contain a significant financing component. The transaction price excludes amounts collected on behalf of third parties, such as sales taxes.

(iv) **Allocation of the Transaction Price to the Performance Obligations in the Contract**—If the contract contains a single performance obligation, the entire transaction price is allocated to the single performance obligation. Contracts that contain multiple performance obligations require an allocation of the transaction price to each performance obligation based on relative standalone selling price (SSP). Certain arrangements include variable consideration that is typically a function of transaction volume or another usage-based measure. Depending upon the structure of a particular arrangement, we may allocate the variable amount to each distinct service period within the series (i.e. direct allocation).

(v) **Recognition of Revenue when, or as, Performance Obligations are Satisfied**—Revenue is recognized when control of the related performance obligation is transferred to the customer in an

amount that reflects the consideration expected to be received in exchange for the subscriptions or services.

We generate substantially all of our revenue from subscriptions to our Singularity Platform. Our Singularity Platform delivers artificial intelligence-powered threat prevention, detection, and response capabilities, enabling an automatic protection against a full spectrum of cyber threats. We built our Singularity Platform to be deployed as a cloud service or in private and hybrid clouds. Customers can extend the functionality of their subscription to our platform by subscribing to additional Singularity Modules. The nature of our promise to the customer under the subscription is to stand ready to provide protection for the duration of the contractual term. As a result, we recognize revenue for these performance obligations ratably over the contractual term. Premium support and maintenance and other Singularity Modules are distinct from subscriptions and are recognized ratably over the term as the performance obligations are satisfied.

Certain arrangements include variable consideration related either to transaction volume or another usage-based measure. Depending upon the structure of a particular arrangement, we i) recognize revenue as each distinct service period is performed, ii) recognize the estimate of variable consideration ratably over the period to which it relates, or iii) apply the 'right to invoice' practical expedient and recognize revenue based on the amount invoiced to the customer during the period.

We generally invoice our customers upfront upon signing for the entire term of the contract, periodically, or in arrears. Most of our subscription contracts have a term of one to three years. Our payment terms typically range between 30 to 45 days. The invoiced amounts are treated as deferred revenue on the consolidated balance sheets and are recognized ratably over the term of the contract beginning on the date the customer is given access to our platform. Our contracts are generally non-cancelable over the contractual term.

Contracts with Multiple Performance Obligations

Our contracts with customers may contain multiple promised services consisting of subscriptions to our Singularity Platform, premium support and maintenance, and other Singularity Modules that are distinct and accounted for separately. The transaction price is allocated to separate performance obligations on a relative SSP basis. Our best evidence for SSP is the price we charge for the subscription or service when we sell it separately in similar circumstances to similar customers. In instances where performance obligations do not have observable standalone sales, we utilize available information that may include, but is not limited to, product groupings or applying the expected cost-plus margin approach to estimate the price we would charge if the service was sold separately.

Cost of Revenue

Cost of revenue consists primarily of third-party cloud infrastructure expenses incurred in connection with the hosting and maintenance of our platform, personnel-related costs associated with our customer support and services organization, including salaries, benefits, bonuses, and stock-based compensation, amortization of intangible assets, amortization of capitalized internal-use software, software and subscription services used by our customer support and services team, and allocated overhead costs.

Research and Development

Research and development costs are expensed as incurred, unless they qualify for recognition as capitalized internal-use software. Research and development expenses consist primarily of personnel-related costs, including salaries, benefits, bonuses, and stock-based compensation, consulting fees, software and subscription services, third-party cloud infrastructure expenses incurred in developing our platform and modules, and allocated overhead costs.

Advertising Expenses

Advertising costs are expensed as incurred and included in sales and marketing expenses in the consolidated statements of operations. Advertising expenses were $18.5 million, $12.3 million, and $8.4 million for fiscal 2024, 2023 and 2022, respectively.

Stock-Based Compensation

We account for stock-based awards issued to employees, directors, and non-employee consultants based on the fair value of the awards at grant date. The fair value of stock option awards granted and rights to purchase shares under our employee stock purchase plan (ESPP) are generally estimated using the Black-Scholes option pricing model. Stock-based compensation expense for awards with only service-based vesting conditions is recognized on a straight-line basis over the requisite service period of the awards. Forfeitures are accounted for in the period in which they occur.

We granted certain awards that have both service-based vesting conditions and performance-based vesting conditions. For these awards, we recognize stock-based compensation expense on a graded basis over the total requisite service period for each separately vesting portion of performance tranches where it is probable that the performance-based vesting conditions will be achieved.

We also granted stock option awards with service-based, performance-based, and market-based vesting conditions to our Chief Executive Officer and Chief Financial Officer. For these awards, stock-based compensation expense is recognized using the accelerated attribution method over the requisite implied service period when it is probable the performance-based vesting condition will be achieved.

Income Taxes

We are subject to income taxes in the US and other foreign jurisdictions.

We utilize the asset and liability method of accounting for income taxes whereby deferred tax assets and liabilities are determined based on differences between financial reporting and tax bases of assets and liabilities, as well as from net operating loss carryforwards, and are measured using the enacted tax rates and laws that will be in effect when the differences are expected to reverse.

A valuation allowance is established if, based upon the available evidence, it is more likely than not that some or all of the deferred tax assets will not be realized. We consider all available evidence, both positive and negative, including historical levels of income, expectations, and risks associated with estimates of future taxable income in assessing the need for a valuation allowance.

We recognize income tax benefits from uncertain tax positions only if we believe that it is more likely than not that the tax position will be sustained upon examination by the taxing authorities based on the technical merits of the position. We recognize penalties and accrued interest related to unrecognized tax benefits as income tax expense, in the consolidated statements of operations.

Net Loss per Share Attributable to Common Stockholders

We compute basic and diluted net loss per share attributable to common stockholders using the two-class method required for participating securities. We consider our redeemable convertible preferred stock, restricted common stock, and shares issued upon the early exercise of stock options subject to repurchase to be participating securities. Under the two-class method, net loss is not allocated to redeemable convertible preferred stock, restricted common stock, and early exercised stock options as the holders do not have a contractual obligation to share in our losses.

Cash, Cash Equivalents, and Restricted Cash

We consider all highly liquid investments purchased with an original maturity of three months or less at the time of purchase to be cash equivalents. Cash equivalents may consist of amounts invested in money market funds and certificates of deposit. Restricted cash consists of indemnity escrow funds related to acquisitions and collateralized letters of credit established in connection with lease agreements for our office facilities. Restricted cash, current and non-current, are included within prepaid expenses and other current assets and other assets, respectively, on our consolidated balance sheets.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

The following table provides a reconciliation of cash, cash equivalents, and restricted cash to the total of these amounts shown in the consolidated statements of cash flows (in thousands):

	As of January 31,	
	2024	2023
Cash and cash equivalents	$ 256,651	$ 137,941
Restricted cash, current	61,264	61,264
Restricted cash, non-current	4,171	3,201
	$ 322,086	$ 202,406

Investments

We determine the appropriate classification of our investments at the time of purchase and reevaluate such determination at each balance sheet date. Investments not considered cash equivalents, and with maturities of one year or less from the consolidated balance sheet date, are classified as short-term investments. Investments with maturities greater than one year from the consolidated balance sheet date are classified as long-term investments. We classify our investments as available-for-sale securities. Our investments are recorded at fair value with unrealized gains and losses, if any, reported in accumulated other comprehensive income (loss). When evaluating whether an investment's unrealized losses are related to credit factors, we review factors such as the extent to which fair value is below its cost basis, any changes to the credit rating of the security, adverse conditions specifically related to the security, changes in market interest rates and our intent to sell, or whether it is more likely than not we will be required to sell, before recovery of cost basis. We invest in highly rated securities with a weighted average maturity of 18 months or less. In addition, our investment policy limits the amount of our credit exposure to any one issuer and requires investments to be investment grade, with the primary objective of preserving capital and maintaining liquidity. Fair values were determined for each individual security in the investment portfolio.

We did not identify any credit losses on investments as of January 31, 2024 and 2023. Realized gains and losses on the sale of investments are determined on a specific identification method and are recorded in other income (expense), net in the consolidated statements of operations. Realized gains and losses on the sale of investments during fiscal 2024, 2023 and 2022 were not significant.

Strategic Investments

Our strategic investments consist of non-marketable equity and debt investments in privately held companies. We elect to apply the measurement alternative and record non-marketable equity investments at cost, less any impairment, plus or minus observable price changes in orderly transactions for identical or similar investments of the same issuer. Non-marketable debt securities are recorded at cost, less any impairment, plus or minus observable price changes in orderly transactions for identical or similar investments of the same issuer.

Strategic investments are included within long-term investments on our consolidated balance sheets and adjustments to their carrying amounts are recorded in other income (expense), net in the consolidated statements of operations. During fiscal 2024, the Company recognized impairment charges of $0.8 million and realized gains of $3.5 million on its non-marketable strategic investments. Impairment charges and realized gains on strategic investments were recognized in other income (expense), net in the consolidated statements of operations. There were no material events or circumstances impacting the carrying amount of our strategic investments during fiscal 2023 and 2022.

Fair Value of Financial Instruments

Fair value is defined as the exchange price that would be received for an asset or an exit price paid to transfer a liability in the principal or most advantageous market for the asset or liability in an orderly transaction between market participants on the measurement date. The carrying amounts reported on the consolidated balance sheets for accounts receivable, accounts payable, accrued liabilities, and accrued payroll and benefits approximate their respective fair values due to their short-term nature.

Concentrations of Credit Risk

Financial instruments that potentially subject us to concentrations of credit risk consist primarily of cash and cash equivalents, restricted cash, investments, and accounts receivable. We maintain our cash, cash equivalents, restricted cash, and investments with high-credit-quality financial institutions mainly in the US and Israel. We have not experienced any credit losses relating to our cash, cash equivalents, restricted cash, and investments. For accounts receivable, we are exposed to credit risk in the event of nonpayment by customers to the extent of the amounts recorded on the consolidated balance sheets. We perform periodic credit evaluations of our customers and generally do not require collateral.

Channel partners that represented 10% or more of accounts receivable, net for the periods presented were as follows:

	As of January 31,	
	2024	2023
Channel partner A	26 %	20 %
Channel partner B	12 %	*
Channel partner C	10 %	*

* Less than 10%

There were no end customers that represented 10% or more of accounts receivable as of January 31, 2024 or 2023.

The only channel partner that represented 10% or more of our total revenue for the periods presented was as follows:

	Year Ended January 31,		
	2024	2023	2022
Channel partner A	19 %	18 %	18 %

There were no end customers that represented 10% or more of total revenue for fiscal 2024, 2023 and 2022.

Accounts Receivable

Accounts receivable are recorded at invoiced amounts and are non-interest bearing. We have a well-established collection history from our channel partners and end customers. We periodically evaluate the collectability of our accounts receivable and provide an allowance for doubtful accounts as necessary, based on the age of the receivable, expected payment ability, and collection experience. The allowance for doubtful accounts balance was $0.7 million and $0.8 million as of January 31, 2024 and 2023, respectively.

Deferred Contract Acquisition Costs

We capitalize sales commissions and associated payroll taxes, and certain incentives (such as referral fees) paid to partners, that are incremental to obtaining a customer contract, which are recorded as deferred contract acquisition costs on the consolidated balance sheets. Sales commissions for the renewal of a contract are not considered commensurate with commissions paid for the initial contracts, given the substantive difference in commission rates in proportion to their respective contract values. Commissions paid, including certain incentives paid to partners, on a new contract are amortized on a straight-line basis over an estimated period of benefit of four years, while commissions paid on renewal contracts are amortized over the average contractual term of the renewal. We determine the estimated period of benefit based on both quantitative and qualitative factors, including the duration of our relationships with customers and the estimated useful life of our technology. Amortization of deferred contract acquisition costs is included in sales and marketing expenses in the consolidated statements of operations.

We periodically review these deferred contract acquisition costs to determine whether events or changes in circumstances have occurred that could impact the period of benefit. We did not recognize any impairment of deferred contract acquisition costs during fiscal 2024, 2023 and 2022.

Property and Equipment

Property and equipment are stated at cost, net of accumulated depreciation and amortization. Depreciation and amortization are calculated using the straight-line method over the estimated useful lives of the assets as follows:

	Estimated Useful Life
Office furniture and equipment	5 years
Computers, software, and electronic equipment	3 years
Capitalized internal-use software	4 years
Leasehold improvements	Shorter of useful life or remaining term of lease

Costs for maintenance and repairs are expensed as incurred.

Capitalized Internal-Use Software

We capitalize certain internal-use software development costs related to our cloud platform. Costs incurred in the preliminary stages of development and post-development are expensed as incurred. Internal and external costs incurred during the development phase, if direct, are capitalized until the software is substantially complete and ready for our intended use. We also capitalize costs related to specific upgrades and enhancements when it is probable the expenditures will result in additional functionality. Maintenance and training costs are expensed as incurred. Capitalized internal-use software is included in property and equipment and is amortized to cost of revenue on a straight-line basis over its expected useful life.

Impairment of Long-Lived Assets (Including Goodwill and Intangible Assets)

Long-lived assets, including intangible assets with finite lives, are reviewed for impairment when events or changes in circumstances indicate that the carrying amount of assets may not be recoverable. Recoverability of assets is measured by a comparison of the carrying amount of an asset to the future undiscounted cash flows expected to be generated by the asset. If such assets are considered to be impaired, the impairment to be recognized is measured by the amount by which the carrying amount of the assets exceeds the fair value of the asset group. In fiscal 2024, we recorded a $2.4 million impairment loss related to our excess facilities. No impairment loss was recorded during fiscal 2023 and 2022.

Goodwill is not amortized but tested for impairment at least annually in the fourth quarter, or more frequently if events or changes in circumstances indicate that impairment may exist. The impairment test consists of a qualitative assessment to determine if the quantitative assessment is required. Goodwill impairment is recognized when the quantitative assessment results in the carrying value of the reporting unit exceeding its fair value, net of related income tax effect, in which case an impairment charge is recorded to goodwill to the extent the carrying value exceeds the fair value, limited to the amount of goodwill. We did not recognize any impairment of goodwill during fiscal 2024, 2023 and 2022.

Business Combinations

We account for our acquisitions using the acquisition method of accounting. We allocate the fair value of purchase consideration to the tangible and intangible assets acquired, and liabilities assumed, based on their estimated fair values. The excess of the fair value of purchase consideration over the values of these identifiable assets and liabilities is recorded as goodwill. When determining the fair value of assets acquired and liabilities assumed, management makes significant estimates and assumptions, especially with respect to intangible assets. Significant estimates in valuing certain identifiable assets include, but are not limited to, the selection of valuation methodologies, forecasted revenue, discount rates, and useful lives. Management's estimates of fair value are based upon assumptions believed to be reasonable, but which are inherently uncertain and unpredictable and, as a result, actual results may differ from estimates. Acquisition costs, such as legal and consulting fees, are expensed as incurred and are included in general and administrative expenses in the consolidated statements of operations. During the measurement period, which is up to one year from the acquisition date, we may record adjustments to the assets acquired and liabilities assumed, with the corresponding offset to goodwill. Upon the conclusion of the measurement period, any subsequent adjustments are recorded in the consolidated statements of operations. See Note 4, *Acquisitions*, for additional information regarding our acquisitions.

Leases

In accordance with ASC Topic 842, *Leases*, we determine if an arrangement is or contains a lease at inception by evaluating various factors, including if the contract conveys the right to control the use of an identified asset for a period of time in exchange for consideration and other facts and circumstances. Operating lease right-of-use (ROU) assets and operating lease liabilities are recognized on the consolidated balance sheets at the lease commencement date based on the present value of lease payments over the lease term, which is the non-cancelable period stated in the contract adjusted for any options to extend or terminate the lease when it is reasonably certain that we will exercise that option.

Lease payments consist of the fixed payments under the arrangement, less any lease incentives, such as tenant improvement allowances. Variable costs, comprised of maintenance and utilities based on actual usage, are not included in the measurement of operating lease ROU assets and operating lease liabilities and are expensed when the event determining the amount of variable consideration to be paid occurs. When the implicit rate of the leases is not determinable, we use an incremental borrowing rate based on the information available at the lease commencement date in determining the present value of lease payments. Lease cost for lease payments is recognized on a straight-line basis over the lease term.

We account for lease components and non-lease components as a single lease component. In addition, we do not recognize operating lease ROU assets and operating lease liabilities for leases with lease terms of 12 months or less.

In addition, we sublease certain of our unoccupied facilities to third parties. We recognize sublease income on a straight-line basis over the sublease term.

We did not have any material finance leases during fiscal 2024, 2023 and 2022.

Recently Issued Accounting Pronouncements Not Yet Adopted

In November 2023, the Financial Accounting Standards Board (FASB) issued Accounting Standards Update (ASU) No. 2023-07, *Improvements to Reportable Segment Disclosures* (Topic 280). This ASU updates reportable segment disclosure requirements by requiring disclosures of significant reportable segment expenses that are regularly provided to the CODM and included within each reported measure of a segment's profit or loss. This ASU also requires disclosure of the title and position of the individual identified as the CODM and an explanation of how the CODM uses the reported measures of a segment's profit or loss in assessing segment performance and deciding how to allocate resources. The ASU is effective for annual periods beginning after December 15, 2023, and interim periods within fiscal years beginning after December 15, 2024. Adoption of the ASU should be applied retrospectively to all prior periods presented in the financial statements. Early adoption is also permitted. This ASU

will likely result in us including the additional required disclosures when adopted. We are currently evaluating the provisions of this ASU.

In December 2023, the FASB issued ASU No. 2023-09, *Improvements to Income Tax Disclosures* (Topic 740). The ASU requires disaggregated information about a reporting entity's effective tax rate reconciliation as well as additional information on income taxes paid. The ASU is effective on a prospective basis for annual periods beginning after December 15, 2024. Early adoption is also permitted for annual financial statements that have not yet been issued or made available for issuance. This ASU will result in the required additional disclosures being included in our consolidated financial statements, once adopted.

3. REVENUE AND CONTRACT BALANCES

Disaggregation of Revenue

The following table summarizes revenue by geography based on the shipping address of end customers who have contracted to use our platform for the periods presented (in thousands, except percentages):

	Year Ended January 31,					
	2024		2023		2022	
	Amount	% of Revenue	Amount	% of Revenue	Amount	% of Revenue
US	$ 397,885	64 %	$ 276,443	65 %	$ 140,034	68 %
International	223,269	36	145,736	35	64,765	32
Total	$ 621,154	100 %	$ 422,179	100 %	$ 204,799	100 %

No single country other than the US represented 10% or more of our revenue during fiscal 2024, 2023 and 2022.

Substantially all of our sales are fulfilled through channel partners, including distributors, resellers, managed security service providers, and others.

Contract Balances

Contract assets consist of unbilled accounts receivable, which arise when a right to consideration for our performance under the customer contract occurs before invoicing the customer. The amount of unbilled accounts receivable included within accounts receivable, net on the consolidated balance sheets was $3.8 million and $1.5 million as of January 31, 2024 and 2023, respectively.

Contract liabilities consist of deferred revenue, which represents invoices billed in advance of performance under a contract. Deferred revenue is recognized as revenue over the contractual period. The deferred revenue balance was $514.5 million and $406.3 million as of January 31, 2024 and 2023, respectively. We recognized revenue of $305.7 million, $195.9 million and $95.5 million for fiscal 2024, 2023 and 2022, respectively, that was included in the corresponding contract liability balance at the beginning of the period.

Remaining Performance Obligations

Our contracts with customers typically range from one to three years. Revenue allocated to remaining performance obligations represents non-cancelable contract revenue that has not yet been recognized, which includes deferred revenue and amounts that will be invoiced in future periods.

For consumption and usage-based agreements with non-cancelable commitments, remaining performance obligations are determined based on the ratable recognition of the remaining commitment over the remaining contract term. The amount and timing of revenue recognition are generally dependent on customers' future consumption, which is inherently variable at the customers' discretion.

As of January 31, 2024, our remaining performance obligations were $896.2 million, of which we expect to recognize 87% as revenue over the next 24 months, with the remainder to be recognized thereafter.

Capitalized contract costs were $125.8 million and $93.4 million as of January 31, 2024 and 2023, respectively. Amortization expense of contract costs was $48.7 million, $36.4 million, and $21.7 million for fiscal 2024, 2023 and 2022, respectively. We periodically review deferred contract acquisition costs to determine whether events or changes in circumstances have occurred that could impact the period of benefit. We did not recognize any impairment of deferred contract acquisition costs during fiscal 2024, 2023 and 2022.

4. ACQUISITIONS

KSG

On November 8, 2023, we completed our acquisition of Krebs Stamos Group LLC (KSG), a Washington D.C.-based privately held strategic advisory group. The purchase price of $13.9 million for all of the outstanding membership interests of KSG consisted of all cash and has been accounted for as a business combination in accordance with ASC Topic 805, *Business Combinations*.

We recorded $4.8 million of net identifiable assets in our consolidated balance sheet as of the KSG acquisition date, of which $3.2 million was related to intangible assets. The excess of the purchase price over the fair value of net identifiable assets acquired has been assigned to goodwill in the amount of $9.1 million. The goodwill in this transaction is primarily attributable to expected operational synergies and the assembled workforce. The goodwill is expected to be deductible for tax purposes. Intangible assets consist of customer relationships, which will be amortized to sales and marketing expense on a straight-line basis over the estimated useful life of four years. The results of operations of KSG have been included in the consolidated financial statements from the date of acquisition, and would not have had a material impact on our combined results of operation if the acquisition had occurred on February 1, 2022. The estimates and assumptions regarding the fair value of certain tangible assets acquired and liabilities assumed, the valuation of intangible assets acquired, income taxes, and goodwill are subject to change as we obtain additional information during the measurement period, which usually lasts for up to one year from the acquisition date.

In connection with the acquisition, we also granted PSUs under our 2021 Equity Incentive Plan. For further details, refer to Note 10, *Stock-Based Compensation*. As the shares are subject to post-acquisition employment, we are accounting for them as post-acquisition compensation expense.

Attivo

On May 3, 2022, we acquired 100% of the issued and outstanding equity securities of Attivo Networks, Inc. (Attivo), an identity security and lateral movement protection company (the Attivo acquisition). Attivo expands our coverage of critical attack surfaces. Identity is an adjacent security solution that complements our core endpoint solution. The Attivo acquisition closed on May 3, 2022 and has been accounted for as a business combination in accordance with ASC Topic 805, *Business Combinations*.

We had post-combination expense with a fair value of $32.9 million that was not included in the total purchase consideration, which is comprised of 307,396 shares of restricted common stock with an aggregate fair value of $10.0 million, and 378,828 assumed options with an aggregate fair value of $11.5 million. Restricted common stock and assumed options will be recognized as stock-based compensation expense. In addition, in connection with the acquisition, certain employees who were promised compensation related to their previous employment agreements will be paid $11.4 million in cash based on continued employment which will be recognized on a straight-line basis as acquisition-related compensation costs. All post-combination expense is expected to be recognized through May 2026. Post-combination compensation expense is subject to adjustment based on continuing service obligations to us of certain stockholders of Attivo.

In connection with the Attivo acquisition, we also granted RSUs and PSUs under our 2021 Equity Incentive Plan. For further details, refer to Note 10, *Stock-Based Compensation*.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

The following table presents the allocation of purchase consideration recorded on our consolidated balance sheet as of the acquisition date (in thousands):

	Amount
Consideration:	
Cash	$ 348,917
Common Stock (6,032,231 shares)[1]	185,885
Fair value of total consideration transferred	$ 534,802
Cash and cash equivalents	$ 8,836
Accounts receivable	4,867
Prepaid expense and other current assets	3,880
Operating lease right-of-use assets	260
Intangible assets	151,900
Accrued liabilities	(4,270)
Accrued payroll and benefits	(1,113)
Operating lease liabilities	(259)
Deferred revenue	(51,746)
Other liabilities	(2,357)
Deferred tax liability	(7,310)
Total identifiable net assets	102,688
Goodwill	432,114
Total purchase consideration	$ 534,802

[1] Consideration calculated using the fair value of our common stock

The valuation of intangible assets acquired are included in Note 7, *Intangible Assets*.

The excess of the purchase price over the fair value of net tangible and intangible assets acquired has been assigned to goodwill. Goodwill represents the future benefits resulting from the Attivo acquisition that will enhance the value of our product for both new and existing customers and strengthen our competitive position. Goodwill is not deductible for tax purposes.

We incurred $5.5 million of transaction expenses in connection with the Attivo acquisition during fiscal 2023. $3.2 million of these costs were recorded as general and administrative expenses in our consolidated statements of operations, with the remainder allocated to purchase price consideration. No transaction expenses in connection with the acquisition were recorded during fiscal 2024.

The following unaudited supplemental pro forma financial information is provided for informational purposes only and summarizes our combined results of operations as if the acquisition occurred on February 1, 2021 (in thousands):

	Year Ended January 31,	
	2023	2022
Revenue	$ 429,683	$ 235,321
Net loss	$ (393,773)	$ (326,829)

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

The unaudited supplemental pro forma results reflect certain adjustments for the amortization of acquired intangible assets, recognition of stock-based compensation, acquisition-related transaction expenses, and acquisition-related compensation costs. Such pro forma amounts are not necessarily indicative of the results that actually would have occurred had the acquisition been completed on the date indicated, nor is it indicative of our future operating results.

Scalyr

On February 6, 2021, we executed a merger agreement to acquire 100% of the issued and outstanding equity securities of Scalyr, Inc. (Scalyr), a leading cloud-native, cloud-scale data analytics platform. This Scalyr acquisition allows us to advance our data ingestion, search, and retention capabilities. The Scalyr acquisition closed on February 9, 2021. The aggregate consideration transferred was $125.3 million, of which $5.0 million was paid in cash, $106.2 million was comprised of 7,277,214 shares of common stock, and $14.1 million was comprised of assumed options to purchase 2,138,347 shares of common stock. As part of the merger agreement, we entered into non-compete agreements with the founder and the co-founder of Scalyr with a term of three years and a fair value of $0.7 million. The fair value of the non-compete agreements was excluded from the purchase consideration and the net assets acquired, resulting in purchase consideration of $124.6 million.

The assets acquired and liabilities assumed in connection with the acquisition were recorded at their fair value on the date of acquisition as follows (in thousands):

	Amount
Cash and cash equivalents	$ 699
Accounts receivable	3,665
Restricted cash	444
Prepaid expense	277
Intangible assets	17,150
Goodwill	108,193
Accounts payable	(412)
Deferred revenue	(5,041)
Other liabilities	(347)
Total purchase consideration	$ 124,628

The valuation of intangible assets acquired are included in Note 7, *Intangible Assets*.

The excess of the purchase price over the fair value of net tangible and intangible assets acquired has been assigned to goodwill. Goodwill represents the future benefits as a result of the acquisition that will enhance our product available to both new and existing customers and increase our competitive position. Goodwill is not deductible for tax purposes.

As part of the consideration transferred, we withheld 1,317,079 shares of our common stock with a fair value of $14.59 per share at the time of grant (Holdback Shares) and $0.4 million of cash related to certain obligations, including indemnification for potential breach of general representations and warranties of the sellers. The Holdback Shares and cash are expected to be released 18 months from the acquisition closing date, subject to claims for any obligations.

In connection with the acquisition, we granted 1,315,099 shares of restricted common stock that vest over a period of two years contingent on continued employment, for which stock-based compensation expense was recognized ratably over the vesting period.

There was no other contingent consideration or cash consideration expected to be paid out subsequent to the acquisition. The results of operations of Scalyr have been included in our consolidated financial statements from the date of acquisition.

We incurred $1.4 million of transaction costs in connection with the acquisition during fiscal 2022. These costs were recorded as general and administrative expenses in the consolidated statements of operations.

The following unaudited pro forma financial information summarizes the results of operations of SentinelOne and Scalyr as if the acquisition occurred on February 1, 2020 (in thousands):

	Year Ended January 31, 2022
Revenue	$ 204,874
Net loss	$ (262,145)

The pro forma results reflect certain adjustments for the amortization of acquired intangible assets, adjustments to revenue resulting from the fair value adjustment to deferred revenue, recognition of stock-based compensation, and acquisition-related costs. Such pro forma amounts are not necessarily indicative of the results that actually would have occurred had the acquisition been completed on the date indicated, nor is it indicative of our future operating results.

5. FAIR VALUE MEASUREMENTS

We measure fair value based on a three-level hierarchy, maximizing the use of observable inputs, where available, and minimizing the use of unobservable inputs, as follows:

Level 1: Assets and liabilities whose values are based on observable inputs such as quoted (unadjusted) prices in active markets for identical assets or liabilities.

Level 2: Assets and liabilities whose values are based on inputs from quoted prices for similar assets and liabilities in active markets or inputs that are observable for the asset or liability, either directly or indirectly through market corroboration, for substantially the full term of the asset or liability.

Level 3: Assets and liabilities whose values are based on unobservable inputs that are supported by little or no market activity and that are significant to the overall fair value measurement.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

The following table summarizes information about our cash, cash equivalents, and investments by investment category for the periods presented (in thousands):

	As of January 31, 2024				
	Fair Value Level	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value
Assets					
Cash and cash equivalents:					
Cash		$ 43,925	$ —	$ —	$ 43,925
Money market funds	Level 1	204,481	—	—	204,481
Certificates of deposit	Level 2	8,245	—	—	8,245
Total cash and cash equivalents		$ 256,651	$ —	$ —	$ 256,651
Short-term investments:					
US Treasury securities	Level 1	$ 234,776	$ —	$ (1,053)	$ 233,723
Corporate notes and bonds	Level 2	279,248	12	(1,068)	278,192
US agency securities	Level 2	157,873	18	(501)	157,390
Total short-term investments		$ 671,897	$ 30	$ (2,622)	$ 669,305
Long-term investments:					
US Treasury securities	Level 1	$ 27,175	$ 121	$ —	$ 27,296
Corporate notes and bonds	Level 2	69,970	279	(67)	70,182
US agency securities	Level 2	90,924	303	(48)	91,179
Total long-term investments		$ 188,069	$ 703	$ (115)	$ 188,657
Total assets measured at fair value		$ 1,116,617	$ 733	$ (2,737)	$ 1,114,613

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

	As of January 31, 2023				
	Fair Value Level	Amortized Cost	Gross Unrealized Gains	Gross Unrealized Losses	Estimated Fair Value
Assets					
Cash and cash equivalents:					
Cash		$ 35,055	$ —	$ —	$ 35,055
Money market funds	Level 1	102,886	—	—	102,886
Total cash and cash equivalents		$ 137,941	$ —	$ —	$ 137,941
Short-term investments:					
US Treasury securities	Level 1	$ 144,392	$ 1	$ (501)	$ 143,892
Commercial paper	Level 2	230,305	30	(667)	229,668
Corporate notes and bonds	Level 2	38,443	15	(148)	38,310
US agency securities	Level 2	74,060	3	(349)	73,714
Total short-term investments		$ 487,200	$ 49	$ (1,665)	$ 485,584
Long-term investments:					
US Treasury securities	Level 1	$ 192,337	$ —	$ (2,460)	$ 189,877
Corporate notes and bonds	Level 2	233,946	178	(2,029)	232,095
US agency securities	Level 2	101,844	27	(921)	100,950
Total long-term investments		$ 528,127	$ 205	$ (5,410)	$ 522,922
Total assets measured at fair value		$ 1,153,268	$ 254	$ (7,075)	$ 1,146,447

There were no transfers between the levels of the fair value hierarchy during fiscal 2024, 2023 and 2022. As of January 31, 2024, all of our investments will mature within two years.

As of January 31, 2024, we determined that the declines in the market value of our investment portfolio were not driven by credit related factors. During the years ended January 31, 2024 and 2023, we did not recognize any losses on our investments due to credit related factors. As of January 31, 2024, we had $2.1 million in continuous unrealized loss positions for more than twelve months on securities with a total fair value of $437.2 million.

The tables above do not include the Company's strategic investments in non-marketable debt and equity securities, which are recorded at cost, less any impairment, plus or minus observable price changes in orderly transactions for identical or similar investments of the same issuer (measurement alternative) and were $16.1 million and $12.5 million as of January 31, 2024 and 2023, respectively.

During the year ended January 31, 2024, the Company recognized impairment charges on its non-marketable strategic investments of $0.8 million. During the year ended January 31, 2024, the Company recognized realized gains of $3.5 million on its non-marketable strategic investments. Impairment charges and realized gains on strategic investments were recognized in other income (expense), net. The fair value was estimated on a non-recurring basis based on Level 3 inputs.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

6. PROPERTY AND EQUIPMENT, NET

Property and equipment, net consisted of the following (in thousands):

	As of January 31,	
	2024	2023
Office furniture and fixtures	$ 2,078	$ 2,110
Computers, software, and equipment	4,999	4,603
Capitalized internal-use software	54,325	34,753
Leasehold improvements	12,551	13,188
Construction in progress	21	3
Total property and equipment	73,974	54,657
Less: Accumulated depreciation and amortization	(25,157)	(15,916)
Total property and equipment, net	$ 48,817	$ 38,741

We capitalized internal-use software costs of $20.7 million, $17.5 million and $10.6 million during fiscal 2024, 2023 and 2022, respectively.

Depreciation and amortization expense related to property and equipment was $10.0 million, $6.7 million and $4.6 million for fiscal 2024, 2023 and 2022, respectively, including amortization expense related to capitalized internal-use software of $7.1 million, $4.1 million and $2.1 million for fiscal 2024, 2023 and 2022, respectively.

7. INTANGIBLE ASSETS

Intangible assets, net as of January 31, 2024 and 2023 consisted of the following (in thousands):

	As of January 31,	
	2024	2023
Developed technology	$ 78,700	$ 78,700
Customer relationships	82,300	79,100
Backlog	11,100	11,100
Non-compete agreements	650	650
Trademarks	150	150
Patents	5,016	1,501
Total finite-lived intangible assets	177,916	171,201
Less: accumulated amortization	(55,268)	(26,363)
Total finite-lived intangible assets, net	$ 122,648	$ 144,838
Indefinite-lived intangible assets - domain names	255	255
Total intangible assets, net	$ 122,903	$ 145,093

Amortization expense of intangible assets was $28.9 million, $23.0 million, and $3.3 million for fiscal 2024, 2023, and 2022, respectively.

As of January 31, 2024, estimated future amortization expense is as follows (in thousands):

Fiscal Year Ending January 31,	
2025	$ 25,412
2026	23,975
2027	23,975
2028	14,215
2029	8,373
Thereafter	26,698
Total	$ 122,648

8. LEASES

We have entered into real estate operating lease agreements with various expiration dates through 2029, some of which include options to extend the leases for up to seven years, and some of which include options to terminate the leases. Our lease terms include options to extend the lease if they are reasonably certain of being exercised. Our operating lease arrangements do not contain any restrictive covenants or residual value guarantees.

Supplemental cash flow information related to our operating leases for fiscal 2024, 2023, and 2022 as well as the weighted-average remaining lease term and weighted-average discount rate as of January 31, 2024 and 2023 were as follows:

	Year Ended January 31,		
	2024	2023	2022
Supplemental Cash Flow Information			
Cash paid for amount included in the measurement of operating lease liabilities	$ 4,987	$ 5,266	$ 4,596
Operating lease ROU assets obtained in exchange for operating lease liabilities	$ 616	$ 3,224	$ 8,558

	As of January 31,	
	2024	2023
Lease Term and Discount Rate		
Weighted-average remaining lease term (years)	4.53	5.55
Weighted-average discount rate	4.2 %	4.2 %

The components of lease costs, net of sublease income, consisted of the following (in thousands):

	Year Ended January 31,		
	2024	2023	2022
Operating lease costs	$ 4,855	$ 4,905	$ 4,027
Short-term lease costs	19	771	2,248
Variable lease costs	1,323	1,886	1,124
Sublease income	(941)	(700)	(563)
Total lease costs	$ 5,256	$ 6,862	$ 6,836

The maturities of our operating lease liabilities as of January 31, 2024 were as follows (in thousands):

Fiscal Year Ending January 31,	Amount
2025	$ 5,565
2026	5,684
2027	5,571
2028	5,574
2029	2,687
Thereafter	155
Total operating lease payments	$ 25,236
Less: Imputed interest	(2,308)
Present value of operating lease liabilities	$ 22,928

9. COMMON STOCK

We have two classes of common stock: Class A common stock and Class B common stock. In connection with our IPO, we amended and restated our certificate of incorporation and authorized 1,500,000,000 shares of Class A common stock and 300,000,000 shares of Class B common stock. The shares of Class A common stock and Class B common stock are identical, except with respect to voting rights. Each share of Class A common stock is entitled to one vote. Each share of Class B common stock is entitled to twenty votes. Class A and Class B common stock each have a par value of $0.0001 per share, and are referred to collectively as our common stock throughout the notes to the consolidated financial statements, unless otherwise noted. Holders of common stock are entitled to receive any dividends as may be declared from time to time by the board of directors.

Shares of Class B common stock may be converted to Class A common stock at any time at the option of the stockholder. Shares of Class B common stock automatically convert to Class A common stock at the earlier of: (i) the date specified by a vote of the holders of 66 2/3% of the then outstanding shares of Class B common stock, (ii) seven years from the date of our prospectus filed with the SEC pursuant to Rule 424(b)(4) under the Securities Act (Final Prospectus), or June 29, 2028, (iii) the first date following the completion of our IPO on which the number of shares of outstanding Class B common stock (such calculations shall include shares of Class B common stock subject to outstanding stock options) held by Tomer Weingarten, including certain permitted entities that Mr. Weingarten controls, is less than 25% of the number of shares of outstanding Class B common stock (such calculation shall include shares of Class B common stock subject to outstanding stock options) that Mr. Weingarten originally held as of the date of our Final Prospectus, (iv) the date fixed by our board of directors, following the first date following the completion of our IPO when Mr. Weingarten is no longer providing services to us as an officer, employee, consultant or member of our board of directors, (v) the date fixed by our board of directors following the date on which, if applicable, Mr. Weingarten is terminated for cause, as defined in our restated certificate of incorporation, and (vi) the date that is 12 months after the death or disability, as defined in our restated certificate of incorporation, of Mr. Weingarten.

Our common stock reserved for future issuance on an as-converted basis as of January 31, 2024 and 2023 were as follows:

	As of January 31,	
	2024	2023
Stock options outstanding	21,159,850	32,446,814
RSUs and PSUs outstanding	27,406,457	14,409,166
ESPP reserved for future issuance	9,303,700	8,043,936
2021 Plan available for future grants	36,450,021	40,175,515
Total shares of common stock reserved	94,320,028	95,075,431

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

10. STOCK-BASED COMPENSATION

Stock-Based Compensation Expense

The components of stock-based compensation expense recognized in the consolidated statements of operations consisted of the following (in thousands):

	Year Ended January 31,	
	2024	2023
Cost of revenue	$ 17,187	$ 10,093
Research and development	61,055	51,771
Sales and marketing	55,798	40,115
General and administrative	83,890	62,487
Restructuring	(1,060)	—
Total	$ 216,870	$ 164,466

2021 Equity Incentive Plan

In May 2021, our board of directors and in June 2021, our stockholders approved our 2021 Equity Incentive Plan (2021 Plan) as a successor to our 2013 Equity Incentive Plan (2013 Plan) and 2011 Stock Incentive Plan (2011 Plan) with the purpose of granting stock-based awards to employees, directors, officers and consultants, including stock options, restricted stock awards, restricted stock units (RSUs), and performance stock units (PSUs). A total of 35,281,596 shares of Class A common stock were initially available for issuance under the 2021 Plan. Our compensation committee administers the 2021 Plan. The number of shares of our Class A common stock available for issuance under the 2021 Plan is subject to an annual increase on the first day of each fiscal year beginning on February 1, 2022, equal to the lesser of: (i) five percent (5%) of the aggregate number of outstanding shares of all classes of our common stock as of the last day of the immediately preceding fiscal year or (ii) such other amount as our board of directors may determine.

The 2013 Plan and 2011 Plan (together, the Prior Plans) were terminated in June 2021, in connection with the adoption of our 2021 Plan, and stock-based awards are no longer granted under the Prior Plans. However, the Prior Plans will continue to govern the terms and conditions of the outstanding awards previously granted thereunder. Any shares underlying stock options that are expired, canceled, forfeited or repurchased under the Prior Plans will be automatically transferred to the 2021 Plan and be available for issuance as Class A common stock.

Restricted Stock Units and Performance Stock Units

A summary of our RSU and PSU activity is as follows:

	Number of Shares	Weighted-Average Grant Date Fair Value
Outstanding as of January 31, 2023	14,409,166	$ 27.37
Granted	22,822,240	17.17
Released	(6,021,877)	25.15
Forfeited	(3,803,072)	22.17
Outstanding as of January 31, 2024	27,406,457	$ 20.08

As of January 31, 2024, we had unrecognized stock-based compensation expense related to unvested RSUs of $482.6 million that is expected to be recognized on a straight-line basis over a weighted-average period of 2.95 years.

As of January 31, 2024, we had unrecognized stock-based compensation expense related to unvested PSUs of $3.8 million that is expected to be recognized on a straight-line basis over a weighted-average period of 2.13 years.

During fiscal 2024, we granted PSUs covering 1,133,455 shares of Class A common stock at target to certain executives subject to service-based and performance-based vesting conditions. As of January 31, 2024, the financial performance metrics have not been achieved. As such, we have not recorded any stock-based compensation expense and have no unrecognized stock-based compensation expense related to these PSUs.

In November 2023, we granted 312,686 PSUs with a grant date fair value of $5.4 million subject to service-based and performance-based vesting conditions to retain the services of certain former KSG employees. These PSUs will vest 100% upon the achievement of certain financial performance and integration milestone events, subject to the employees' continued service to us from the grant date through the milestone events or target dates. For further details, refer to Note 4, *Acquisitions*.

Stock Option Information

A summary of our stock option activity is as follows:

	Number of Options	Weighted-Average Exercise Price	Weighted-Average Remaining Contractual Term (in years)	Aggregate Intrinsic Value (in thousands)
Outstanding as of January 31, 2023	32,446,814	$ 4.71	6.52	$ 337,214
Granted	—	—		
Exercised	(10,298,114)	2.75		
Forfeited	(988,850)	5.60		
Outstanding as of January 31, 2024	21,159,850	$ 5.63	6.25	$ 447,989
Expected to vest as of January 31, 2024	21,159,850	$ 5.63	6.25	$ 447,989
Vested and exercisable as of January 31, 2024	15,633,560	$ 4.51	5.96	$ 348,522

There were no options granted during fiscal 2024 and 2023. The weighted-average grant-date fair value of options granted during fiscal 2022 was $13.14 per share.

The aggregate intrinsic value is the difference between the exercise price and the estimated fair value of the underlying common stock. The aggregate intrinsic value of options exercised during fiscal 2024, 2023 and 2022 was $170.1 million, $173.0 million and $333.7 million, respectively.

As of January 31, 2024, we had unrecognized stock-based compensation expense related to unvested options of $51.8 million that is expected to be recognized on a straight-line basis over a weighted-average period of 1.85 years.

Milestone Options

In March 2021, we granted 1,404,605 options to purchase shares of common stock subject to service-based, performance-based, and market-based vesting conditions to our Chief Executive Officer and Chief Financial Officer under the 2013 Plan. These stock options will vest 100% upon the occurrence of i) our IPO (the performance-based vesting condition), which was completed in June 2021, and ii) the achievement of a certain market capitalization target (the market-based vesting condition), subject to the executive's continued service to us from the grant date through the milestone event. As of January 31, 2024, the market capitalization target has not yet been achieved, and therefore, these milestone options remain unvested. For these options, we used a Monte Carlo simulation to determine the fair value at the grant date and the implied service period.

We recorded stock-based compensation expense related to these milestone options of $3.6 million, $3.6 million, and $3.1 million during fiscal 2024, 2023, and 2022, respectively. As of January 31, 2024, we had unrecognized stock-based compensation expense related to unvested milestone options of $9.1 million, that is expected to be recognized over the remaining implied service period of 2.6 years.

Restricted Common Stock

In connection with the Attivo acquisition, we issued restricted Class A common stock to Attivo's employees. We recorded stock-based compensation expense related to these restricted shares in connection with the Attivo acquisition of $0.7 million and $1.0 million during fiscal 2024 and 2023, respectively. As of January 31, 2024, we had unrecognized stock-based compensation expense related to this unvested restricted common stock of $0.3 million.

In connection with the Scalyr acquisition, we granted 1,315,099 shares of restricted common stock. We recorded stock-based compensation expense related to restricted common stock in connection with the Scalyr acquisition of $0.2 million, $8.5 million, and $10.9 million during fiscal 2024, 2023, and 2022, respectively. As of January 31, 2024, this restricted common stock has fully vested.

Employee Stock Purchase Plan (ESPP)

In May 2021, our board of directors, and in June 2021, our stockholders approved our ESPP, which became effective on the date of effectiveness of our Final Prospectus, or June 29, 2021. The ESPP initially reserved and authorized the issuance of up to a total of 7,056,319 shares of common stock to eligible employees. The number of shares reserved for issuance and sale under the ESPP will automatically increase on the first day of each fiscal year, starting on February 1, 2022 for the first ten calendar years after the first offering date, in an amount equal to (i) 1% of the aggregate number of outstanding shares of all class our common stock on the last day of the immediately preceding fiscal year, or (ii) such other amount as the administrator of the ESPP may determine. The ESPP generally provides for six-month offering periods beginning January 6 and July 6 of each year, with each offering period consisting of single six-month purchase periods, except for the initial offering period which began on July 1, 2021, and ended on July 5, 2023. On each purchase date, eligible employees will purchase the shares at a price per share equal to 85% of the lesser of i) the fair market value of our common stock as of the beginning of the offering period or ii) the fair market value of our common stock on the purchase date, as defined in the ESPP, except for the initial offering period that had a 24-month look back to the IPO price of $35.

The following table summarizes the assumptions used in estimating the fair value of employee stock purchase rights using the Black-Scholes option pricing model for the periods presented:

	Year Ended January 31,	
	2024	2023
Expected term (in years)	0.5	0.5 - 1.0
Expected volatility	55% - 85%	72% - 96%
Risk-free interest rate	5.2% - 5.5%	2.6% - 4.8%
Dividend yield	— %	— %

We recognized stock-based compensation expense related to ESPP of $11.7 million, $12.7 million, and $5.5 million during fiscal 2024, 2023, and 2022, respectively.

Modifications

During fiscal 2024 and 2023, certain members of our management team converted to non-employee consultants or to positions that no longer provide substantive service to the Company (Management Transitions). The Management Transitions have been accounted for as modifications, under which, the exercise period of certain vested awards has been extended and a certain number of unvested awards will vest through the end of the agreements entered into in connection with the Management Transitions.

During fiscal 2024 and 2023, we recognized an incremental charge of $6.2 million and $4.5 million, respectively, related to the Management Transitions.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

11. RESTRUCTURING

In June 2023, we announced a restructuring plan (the Plan) as a result of a review of current strategic priorities, resource allocation, and cost reduction intended to reduce operating costs, improve operating margins and continue advancing our ongoing commitment to profitable growth. The Plan includes a reduction of our workforce by approximately 5%, or approximately 100 full-time employees. We incurred approximately $7.4 million in charges in connection with the Plan in fiscal 2024, which consists of $5.4 million in charges related to severance payments and employee benefits, $2.4 million of impairment charges related to excess facilities, $0.7 million related to inventory write-offs, offset partially by $1.1 million in savings related to the reversal of certain stock-based compensation expense. Note that the charges related to inventory write-offs are recognized as cost of sales and not restructuring operating expenses in our consolidated financial statements of operations. These costs were paid as of January 31, 2024. The actions associated with the Plan are expected to be fully complete by the end of fiscal 2025, subject to finalizing the disposition of certain office space.

12. INCOME TAXES

Our loss before provision for income taxes for fiscal 2024, 2023 and 2022 consisted of the following (in thousands):

	Year Ended January 31,		
	2024	2023	2022
Domestic	$ (406,151)	$ (432,235)	$ (274,270)
Foreign	73,317	47,944	4,173
Loss before provision for income taxes	$ (332,834)	$ (384,291)	$ (270,097)

The components of provision for income taxes for fiscal 2024, 2023 and 2022 consisted of the following (in thousands):

	Year Ended January 31,		
	2024	2023	2022
Current:			
State	$ 150	$ 53	$ 82
Foreign	5,168	3,661	1,011
Total current	5,318	3,714	1,093
Deferred:			
Federal	—	(6,754)	—
State	—	(2,913)	—
Foreign	541	340	(89)
Total deferred	541	(9,327)	(89)
Total provision for income taxes	$ 5,859	$ (5,613)	$ 1,004

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

A reconciliation of the expected provision for (benefit from) income taxes at the statutory federal income tax rate to our recorded provision for income taxes consisted of the following (in thousands):

	Year Ended January 31,		
	2024	2023	2022
Benefit from income taxes at US federal statutory rate	$ (69,895)	$ (80,701)	$ (56,720)
State taxes, net of federal benefit	150	53	82
Foreign tax rate differential	23,179	10,140	(1,297)
Stock-based compensation	12,367	2,734	(23,442)
Non-deductible expenses	1,390	1,780	322
Research and development credits	(2,251)	(688)	(20)
Change in valuation allowance	40,525	60,145	81,739
Other	394	924	340
Total provision for (benefit from) income taxes	$ 5,859	$ (5,613)	$ 1,004

Significant components of our net deferred tax assets and liabilities as of January 31, 2024 and 2023 consisted of the following (in thousands):

	As of January 31,	
	2024	2023
Deferred tax assets:		
Net operating loss carryforwards	$ 226,971	$ 228,400
Research and development expenses	106,257	72,432
Deferred revenue	36,199	25,643
Accruals and reserves	9,265	6,215
Operating lease liabilities	7,492	9,139
Stock-based compensation	14,300	17,528
Other	7,111	2,622
Gross deferred tax assets	407,595	361,979
Valuation allowance	(340,951)	(291,751)
Total deferred tax assets	66,644	70,228
Deferred tax liabilities:		
Acquired intangibles, property and equipment	(28,652)	(37,170)
Deferred contract acquisition costs	(30,423)	(22,868)
Operating lease right-of-use assets	(6,582)	(8,162)
Other	(1,782)	(2,279)
Total deferred tax liabilities	(67,439)	(70,479)
Net deferred tax assets (liabilities)	$ (795)	$ (251)

Based upon available objective evidence, we believe it is more likely than not that the US and Israel net deferred tax assets will not be fully realizable. Accordingly, we have established a valuation allowance for the US and Israel gross deferred tax assets. As of January 31, 2024 and 2023, we had a valuation allowance of $341.0 million and $291.8 million, respectively, against our deferred tax assets. During fiscal 2024 and 2023, total valuation allowance increased by $49.2 million and $72.8 million, respectively, primarily due to additional net operating losses.

SENTINELONE, INC.

NOTES TO CONSOLIDATED FINANCIAL STATEMENTS

As of January 31, 2024, we had federal net operating loss carryforwards of $721.2 million, which will begin to expire in 2031, and state net operating loss carryforwards of $390.6 million, which will begin to expire in 2025. We also had foreign net operating loss carryforwards of $202.8 million, which do not expire.

In addition, we had federal research and development credit carryforwards of $5.9 million, which will begin to expire in 2037, and state research and development credit carryforwards of $2.9 million, which do not expire.

Federal and state tax laws impose substantial restrictions on the utilization of the net operating loss carryforwards and tax credit carryforwards in the event of an ownership change as defined in Section 382 of the Internal Revenue Code of 1986, as amended. Accordingly, our ability to utilize these carryforwards may be limited as a result of such ownership change. Such a limitation could result in the expiration of carryforwards before they are utilized. The carryforwards are currently subject to a valuation allowance.

Foreign withholding taxes have not been provided for the cumulative undistributed earnings of certain foreign subsidiaries of us as of January 31, 2024 and 2023 due to our intention to permanently reinvest such earnings. Determination of the amount of unrecognized deferred tax liability related to these earnings is not practicable.

We file income tax returns in the US federal jurisdiction and various state and foreign jurisdictions. Our tax years generally remain open and subject to examination by federal, state, or foreign tax authorities. We are currently under examination by the Israel Tax Authorities for the 2017 through 2021 tax years. We are not currently under audit in any other tax jurisdictions.

The changes in the gross amount of unrecognized tax benefits consisted of the following (in thousands):

	As of January 31,		
	2024	2023	2022
Balance at beginning of year	$ 1,013	$ 566	$ 534
Gross increases for tax positions of current year	1,027	447	32
Gross increases for tax positions of prior year	157	—	—
Balance at end of year	$ 2,197	$ 1,013	$ 566

We recognize interests and penalties related to income tax matters as a component of income tax expense. We do not anticipate that its total unrecognized tax benefits will significantly change during the next 12 months.

13. NET LOSS PER SHARE ATTRIBUTABLE TO COMMON STOCKHOLDERS

Basic and diluted net loss per share attributable to common stockholders is computed in conformity with the two-class method required for participating securities. Basic net loss per share is computed by dividing net loss attributable to common stockholders by the weighted-average number of shares of common stock outstanding during the period. Diluted net loss per share is computed by giving effect to all potentially dilutive common stock equivalents to the extent they are dilutive. For purposes of this calculation, stock options, restricted common stock, RSUs, PSUs, shares purchased pursuant to our ESPP, and early exercised stock options are considered to be common stock equivalents but have been excluded from the calculation of diluted net loss per share attributable to common stockholders as their effect is anti-dilutive for all periods presented.

The rights, including the liquidation and dividend rights, of the holders of Class A and Class B common stock are identical, except with respect to voting, conversion, and transfer rights. As the liquidation and dividend rights are identical, the undistributed earnings are allocated on a proportionate basis to each class of common stock and the

resulting basic and diluted net loss per share attributable to common stockholders are, therefore, the same for both Class A and Class B common stock on both an individual and combined basis.

Basic and diluted net loss per share attributable to common stockholders was as follows (in thousands, except share and per share data):

	Year Ended January 31,		
	2024	2023	2022
Numerator:			
Net loss attributable to Class A and Class B common stockholders	$ (338,693)	$ (378,678)	$ (271,101)
Denominator:			
Weighted-average shares used in computing net loss per share attributable to Class A and Class B common stockholders, basic and diluted	294,923,536	277,802,861	174,051,203
Net loss per share attributable to Class A and Class B common stockholders, basic and diluted	$ (1.15)	$ (1.36)	$ (1.56)

The following potentially dilutive securities were excluded from the computation of diluted net loss per share attributable to common stockholders because their inclusion would have been anti-dilutive:

	As of January 31,		
	2024	2023	2022
Stock options	21,159,850	32,446,814	42,422,473
RSUs and PSUs	27,406,457	14,409,166	1,770,304
ESPP	107,924	134,469	52,381
Shares subject to repurchase	16,543	178,308	20,091
Restricted common stock	10,621	451,444	1,142,496
Contingently issuable shares	—	—	1,317,089
Total	48,701,395	47,620,201	46,724,834

14. GEOGRAPHIC INFORMATION

Long-lived assets, consisting of property and equipment, net, and operating lease right-of-use assets, by geography were as follows (in thousands):

	As of January 31,	
	2024	2023
US	$ 40,067	$ 27,990
Israel	21,806	27,625
Rest of world	5,418	6,690
Total	$ 67,291	$ 62,305

Revenue by geography is presented in Note 3, *Revenue and Contract Balances*.

15. COMMITMENTS AND CONTINGENCIES

Legal Contingencies

From time to time, we may be a party to various legal proceedings and subject to claims in the ordinary course of business.

Securities Litigation

On June 6, 2023, a securities class action was filed against the Company, its Chief Executive Officer and its Chief Financial Officer, in the Northern District of California, captioned *Johansson v. SentinelOne, Inc., Case No. 4:23-cv-02786*. The suit is brought on behalf of an alleged class of stockholders who purchased or acquired shares of the Company's Class A common stock between June 1, 2022 and June 1, 2023. The complaint alleges that defendants made false or misleading statements about the Company's business, operations and prospects, including its annual recurring revenues and internal controls, and purports to assert claims under Sections 10(b) and 20(a) of the Securities Exchange Act of 1934, as amended. A substantially similar suit was filed on June 16, 2023 in the same court against the same defendants asserting the same claims, captioned *Nyren v. SentinelOne, Inc., Case No. 4:23-cv-02982*. On October 4, 2023, the court issued an order consolidating both cases under the caption *In re SentinelOne, Inc. Securities Litigation Case No. 4:23-cv-02786* and appointing a lead plaintiff. Lead plaintiff filed an amended complaint on December 18, 2023. Defendants moved to dismiss the amended complaint on February 16, 2024. We believe the case is without merit and intend to defend the suit vigorously.

Fortis Litigation

In September 2023, Fortis Advisors LLC (Fortis), in its capacity as the representative for the stockholders of Attivo, filed an action against the Company in Delaware Chancery Court asserting claims arising out of the Attivo Acquisition. The case is captioned *Fortis Advisors LLC v. SentinelOne, Inc., Case No. 2023-0946-VLM*.

In June 2023, the Company sent a letter to Fortis seeking indemnification for certain claims, including for breaches by Attivo of its representations and warranties in the merger agreement. Fortis is now seeking a declaratory judgment that the Company is not entitled to indemnification for the claims it has asserted, and that Fortis should recover the funds held in escrow. Fortis also alleges that the Company breached its representations and warranties in the merger agreement because its SEC filings allegedly contained materially false or misleading statements about the Company's annual recurring revenues. The Company believes Fortis' claims are without merit and intends to defend the suit vigorously. On November 3, 2023, the Company filed its answer to Fortis' complaint. On the same day, the Company filed counterclaims against Fortis, in its capacity as the representative of the stockholders of Attivo, based on Attivo's breach of several of its representations, warranties and covenants in the merger agreement. The Company's counterclaims seek an order directing Fortis to comply with its contractual obligations to release funds set aside to indemnify the Company for its losses and any additional damages in excess of the indemnity fund.

Derivative Litigation

On January 10, 2024, a shareholder derivative complaint was filed, naming the Company's Board of Directors, its Chief Executive Officer and its Chief Financial Officer as defendants, and the Company as nominal defendant. The action was filed in the United States District Court, District of Delaware, and is captioned Stochevski v. Weingarten, et al., Case No. 4:24-cv-00024. The complaint alleges that the director and officer defendants breached their fiduciary duties by making or failing to correct false or misleading statements about the Company's business, operations and prospects, including its annual recurring revenues and internal controls.

We believe that there are no other pending or threatened legal proceedings that are likely to have a material adverse effect on our consolidated financial statements.

Warranties and Indemnification

Our services are generally warranted to deliver and operate in a manner consistent with general industry standards that are reasonably applicable and materially conform with our documentation under normal use and circumstances. Our contracts generally include certain provisions for indemnifying customers against liabilities if our products or services infringe a third party's intellectual property rights.

We also offer a limited warranty to certain customers, subject to certain conditions, to cover certain costs incurred by the customer in case of a cybersecurity breach. We have a cybersecurity liability policy that may cover

our customers' actual damages. We have not incurred any material costs related to such obligations and have not accrued any liabilities related to such obligations in the consolidated balance sheets as of January 31, 2024 and 2023.

In addition, we also indemnify certain of our directors and executive officers against certain liabilities that may arise while they are serving in good faith in their company capacities. We maintain director and officer liability insurance coverage that would generally enable us to recover a portion of any future amounts paid.

16. EMPLOYEE BENEFIT PLAN

Our US employees participate in a 401(k) defined contribution plan sponsored by us. Contributions to the plan are discretionary. We made $2.6 million and $2.8 million in matching contributions for fiscal 2024 and 2023, respectively. There were no matching contributions for fiscal 2022.

Israeli Severance Pay

Israeli labor law generally requires payment of severance pay upon dismissal of an employee or upon termination of employment in certain other circumstances. Pursuant to Section 14 of the Severance Compensation Act, 1963 (Section 14), all of our employees in Israel are entitled to monthly deposits made in their name with insurance companies, at a rate of 8.33% of their monthly salary.

These payments release us from any future severance payment obligation with respect to these employees; as such, any liability for severance pay due to these employees and the deposits under Section 14 are not recorded as an asset on our consolidated balance sheets. For fiscal 2024, 2023, and 2022, we recorded $3.5 million, $3.9 million, and $3.7 million, respectively, in severance expenses related to these employees.

17. SUBSEQUENT EVENTS

On February 1, 2024, we completed the acquisition of PingSafe Pte. Ltd. (PingSafe) to provide customers better automation across their entire cloud footprint. We acquired 100% of the shares of PingSafe for total consideration of approximately $57.5 million in cash and 2,354,607 shares of our Class A common stock, subject to customary adjustments set forth in the purchase agreement.

On February 1, 2024, we acquired 100% of the issued and outstanding equity securities of Stride Security Ltd. (Stride), a security automation company. The aggregate consideration for the Stride acquisition is approximately $7.5 million in cash, subject to customary adjustments. In addition, approximately $7.5 million will be earned over three years, subject to continued employment.

The PingSafe and Stride acquisitions will be accounted for as business combinations in accordance with ASC Topic 805, *Business Combinations* and, accordingly, the total purchase price will be allocated to the tangible and intangible assets acquired and the liabilities assumed based on their respective fair values on the date of acquisition. We are currently working on the preliminary purchase price allocations and expect them to be completed in the first quarter of fiscal 2025.

ITEM 9. CHANGES IN AND DISAGREEMENTS WITH ACCOUNTANTS ON ACCOUNTING AND FINANCIAL DISCLOSURES

None.

ITEM 9A. CONTROLS AND PROCEDURES

Evaluation of Disclosure Controls and Procedures

Our management, with the participation of our Chief Executive Officer and Chief Financial Officer, has evaluated the effectiveness of our disclosure controls and procedures as of January 31, 2024. The term "disclosure controls and procedures," as defined in Rules 13a-15(e) and 15d-15(e) under the Exchange Act, means controls and other procedures of a company that are designed to ensure that information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is recorded, processed, summarized, and reported within the time periods specified in the SEC's rules and forms. Disclosure controls and procedures include, without limitation, controls and procedures designed to ensure that information required to be disclosed by a company in the reports that it files or submits under the Exchange Act is accumulated and communicated to the company's management, including its principal executive and principal financial officers, or persons performing similar functions, as appropriate to allow timely decisions regarding required disclosure. In designing and evaluating our disclosure controls and procedures, our management recognizes that disclosure controls and procedures, no matter how well conceived and operated, can provide only reasonable assurance that the objectives of the disclosure controls and procedures are met. Based on such evaluation, our Chief Executive Officer and Chief Financial Officer concluded that, as of January 31, 2024, our disclosure controls and procedures were effective at the reasonable assurance level.

Changes in Internal Control Over Financial Reporting

There were no changes in our internal control over financial reporting (as defined in Rules 13a-15(f) and 15d-15(f) under the Exchange Act) that occurred during the period covered by this Annual Report on Form 10-K that has materially affected, or is reasonably likely to materially affect, our internal control over financial reporting.

Inherent Limitations on Effectiveness of Controls

Our management, including our Chief Executive Officer and Chief Financial Officer, believes that our disclosure controls and procedures and internal control over financial reporting are designed to provide reasonable assurance of achieving their objectives and are effective at the reasonable assurance level. However, management does not expect that our disclosure controls and procedures or our internal control over financial reporting will

prevent or detect all errors and all fraud. A control system, no matter how well conceived and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system are met. Because of the inherent limitations in all control systems, no evaluation of controls can provide absolute assurance that all control issues and instances of fraud, if any, within the company have been detected. The design of any system of controls also is based in part upon certain assumptions about the likelihood of future events, and there can be no assurance that any design will succeed in achieving its stated goals under all potential future conditions. Over time, controls may become inadequate because of changes in conditions, or the degree of compliance with the policies or procedures may deteriorate. Because of the inherent limitations in a cost-effective control system, misstatements due to error or fraud may occur and not be detected.

Management's Report on Internal Control over Financial Reporting

Our management is responsible for establishing and maintaining adequate internal control over financial reporting, as such term is defined in Exchange Act Rules 13a-15(f) and 15d-15(f). Our management conducted an evaluation of the effectiveness of our internal control over financial reporting as of January 31, 2024, based on the criteria established in Internal Control - Integrated Framework (2013) issued by the Committee of Sponsoring Organizations of the Treadway Commission. Based on the results of its evaluation, management concluded that our internal control over financial reporting was effective as of January 31, 2024. The effectiveness of our internal control over financial reporting as of January 31, 2024, has been audited by Deloitte and Touche LLP, an independent registered public accounting firm, as stated in its report which is included in Part II, Item 8 of this Annual Report.

REPORT OF INDEPENDENT REGISTERED PUBLIC ACCOUNTING FIRM

To the stockholders and the Board of Directors of SentinelOne, Inc.

Opinion on Internal Control over Financial Reporting

We have audited the internal control over financial reporting of SentinelOne, Inc. and subsidiaries (the "Company") as of January 31, 2024, based on criteria established in *Internal Control — Integrated Framework (2013)* issued by the Committee of Sponsoring Organizations of the Treadway Commission (COSO). In our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of January 31, 2024, based on criteria established in *Internal Control — Integrated Framework (2013)* issued by COSO.

We have also audited, in accordance with the standards of the Public Company Accounting Oversight Board (United States) (PCAOB), the consolidated financial statements as of and for the year ended January 31, 2024, of the Company and our report dated March 27, 2024, expressed an unqualified opinion on those financial statements.

Basis for Opinion

The Company's management is responsible for maintaining effective internal control over financial reporting and for its assessment of the effectiveness of internal control over financial reporting, included in the accompanying Management's Report on Internal Control over Financial Reporting. Our responsibility is to express an opinion on the Company's internal control over financial reporting based on our audit. We are a public accounting firm registered with the PCAOB and are required to be independent with respect to the Company in accordance with the U.S. federal securities laws and the applicable rules and regulations of the Securities and Exchange Commission and the PCAOB.

We conducted our audit in accordance with the standards of the PCAOB. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether effective internal control over financial reporting was maintained in all material respects. Our audit included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, testing and evaluating the design and operating effectiveness of internal control based on the assessed risk, and performing such other procedures as we considered necessary in the circumstances. We believe that our audit provides a reasonable basis for our opinion.

Definition and Limitations of Internal Control over Financial Reporting

A company's internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles. A company's internal control over financial reporting includes those policies and procedures that (1) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (2) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, and that receipts and expenditures of the company are being made only in accordance with authorizations of management and directors of the company; and (3) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of the company's assets that could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent or detect misstatements. Also, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with the policies or procedures may deteriorate.

/s/ DELOITTE & TOUCHE LLP

San Jose, California
March 27, 2024

ITEM 9B. OTHER INFORMATION

Our directors and Section 16 officers (as defined in Rule 16a-1(f) under the Exchange Act) are generally only permitted to trade in our securities pursuant to a prearranged trading plan intended to satisfy the affirmative defense of Rule 10b5-1(c) under the Exchange Act (a Rule 10b5-1 Plan). During the fourth quarter of fiscal 2024, one of our Section 16 officers adopted a new Rule 10b5-1 Plan. The Weingarten Plan (as defined below) was entered into during an open trading window in accordance with our Insider Trading Policy.

On January 11, 2024, Tomer Weingarten, our President, Chief Executive Officer and Chairman of the Board of Directors, adopted a Rule 10b5-1 Plan (the Weingarten Plan) providing for the potential sale of shares of Class A common stock owned by Mr. Weingarten, including 64,744 shares of Class A common stock and 2,126,368 shares underlying vested stock options for Class B common stock so long as the market price of our Class A common stock is higher than certain minimum threshold prices specified in the Weingarten Plan between an estimated start date of May 9, 2024 and April 24, 2025. Additionally, the Weingarten Plan provides for the potential sale of shares of Class A common stock to be received upon vesting and settlement of certain outstanding restricted stock units, net of any shares withheld by the Company to satisfy applicable tax obligations. The number of shares to be withheld, and therefore the exact number of shares to be sold pursuant to the Weingarten Plan, can only be determined upon the occurrence of the future vesting events. The Weingarten Plan is scheduled to expire on April 30, 2025.

ITEM 9C. DISCLOSURE REGARDING FOREIGN JURISDICTIONS THAT PREVENT INSPECTIONS

Not applicable.

PART III.

ITEM 10. DIRECTORS, EXECUTIVE OFFICERS AND CORPORATE GOVERNANCE

The information required by this Item (other than the information set forth in the next paragraph) will be included in our definitive Proxy Statement for our 2024 annual meeting of stockholders, which will be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2024, and is incorporated herein by reference.

We maintain a Code of Business Conduct and Ethics (Code of Ethics), applicable to all employees, including all directors and executive officers. Our Code of Ethics is published on our Investor Relations website at investors.sentinelone.com under "Governance." We intend to satisfy the disclosure requirement under Item 5.05 of Form 8-K regarding amendments to, or waiver from, a provision of the Code of Ethics by posting such information on the website address and location specified above.

ITEM 11. EXECUTIVE COMPENSATION

The information required by this Item will be included in our Proxy Statement to be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2024, and is incorporated herein by reference.

ITEM 12. SECURITY OWNERSHIP OF CERTAIN BENEFICIAL OWNERS AND MANAGEMENT AND RELATED STOCKHOLDER MATTERS

The information required by this Item will be included in our Proxy Statement to be filed with the SEC within 120 days after the end of our fiscal year ended January 31, 2024, and is incorporated herein by reference.

ITEM 13. CERTAIN RELATIONSHIPS AND RELATED TRANSACTIONS, AND DIRECTOR INDEPENDENCE

The information required by this Item will be included in our Proxy Statement to be filed with the SEC, within 120 days after the end of our fiscal year ended January 31, 2024, and is incorporated herein by reference.

ITEM 14. PRINCIPAL ACCOUNTANT FEES AND SERVICES

The information required by this Item will be included in our Proxy Statement to be filed with the SEC, within 120 days after the end of our fiscal year ended January 31, 2024, and is incorporated herein by reference.

PART IV.

ITEM 15. EXHIBITS AND FINANCIAL STATEMENT SCHEDULES

(a) Financial Statements.

See Index to Consolidated Financial Statements in Item 8 of this Annual Report on Form 10-K.

(b) Financial Statement Schedule.

All financial statement schedules are omitted because the information required to be set forth therein is not applicable or is shown in the consolidated financial statements or the notes thereto.

(c) Exhibits.

The exhibits listed below are filed as part of this Annual Report on Form 10-K or are incorporated herein by reference, in each case as indicated below.

Exhibit Number	Description of Document	Form	File No.	Exhibit	Filing Date
3.1	Restated Certificate of Incorporation of SentinelOne, Inc.	10-K	001-40531	3.1	April 7, 2022
3.2	Amended and Restated Bylaws of SentinelOne, Inc.	8-K	001-40531	3.1	December 13, 2022
4.1	Form of Class A Common Stock certificate of SentinelOne, Inc.	S-1/A	333-256761	4.1	June 21, 2021
4.2	Description of Registrant's securities.	10-K	001-40531	4.2	April 7, 2022
4.3	Amended and Restated Investors' Rights Agreement among SentinelOne, Inc. and certain holders of capital stock, dated October 28, 2020.	S-1	333-256761	4.2	June 3, 2021
10.1	Form of Indemnification Agreement between SentinelOne, Inc. and each of its directors and executive officers.	S-1	333-256761	10.1	June 3, 2021
10.2†	SentinelOne, Inc. 2021 Equity Incentive Plan and related form agreements.	S-1	333-256761	10.4	June 3, 2021
10.3†	SentinelOne, Inc. 2021 Employee Stock Purchase Plan and related form agreements.	S-1/A	333-256761	10.5	June 21, 2021
10.4†	Confirmatory Employment Letter between SentinelOne, Inc. and Tomer Weingarten, dated May 28, 2021.	S-1/A	333-256761	10.7	June 21, 2021
10.5†	Confirmatory Employment Letter between SentinelOne, Inc. and David Bernhardt, dated May 28, 2021.	S-1/A	333-256761	10.8	June 21, 2021
10.6†	Confirmatory Employment Letter between SentinelOne, Inc. and Ric Smith, dated May 28, 2021.	10-K	001-40531	10.7	April 7, 2022
10.7†	Offer of Employment and Change in Control and Severance Agreement between SentinelOne, Inc. and Keenan Conder, effective June 24, 2021.	10-K	001-40531	10.8	April 7, 2022
10.8†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and Tomer Weingarten, dated May 28, 2021.	S-1/A	333-256761	10.11	June 21, 2021

10.9†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and David Bernhardt, dated May 28, 2021.	S-1/A	333-256761	10.12	June 21, 2021
10.10†	Change in Control and Severance Agreement by and between SentinelOne, Inc. and Ric Smith.	10-K	001-40531	10.12	April 7, 2022
10.11†	Offer of Employment and Change in Control and Severance Agreement between SentinelOne, Inc. and Narayanan 'Vats' Srivatsan, effective February 26, 2022.	10-K	001-40531	10.13	March 29, 2023
10.12†	SentinelOne Global Corporate Cash Bonus Plan as amended effective August 1, 2022.	10-Q	001-40531	10.3	June 1, 2023
10.13†	2021 Equity Incentive Plan Global Notice of Restricted Stock Unit Award, as amended.	10-Q	001-40531	10.1	December 5, 2023
10.14	Office Lease, by and between SIC-Mountain Bay Plaza, LLC and SentinelOne, Inc. and Silicon Valley Bank dated as of June 9, 2020, as amended.	S-1	333-256761	10.7	June 3, 2021
10.15†	2021 Equity Incentive Plan Global Notice of Performance Stock Unit Award				
21.1	List of Subsidiaries of SentinelOne, Inc.				
23.1	Consent of Deloitte & Touche LLP, independent registered public accounting firm.				
24.1	Power of Attorney (included in signature pages hereto).				
31.1	Certification of Principal Executive Officer Pursuant to Rules 13a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as Adopted Pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.				
31.2	Certification of Principal Financial Officer Pursuant to Rules 13a-14(a) and 15d-14(a) under the Securities Exchange Act of 1934, as Adopted Pursuant to Section 302 of the Sarbanes-Oxley Act of 2002.				
32.1*	Certification of Chief Executive Officer and Chief Financial Officer pursuant to 18 U.S.C. Section 1350, as adopted pursuant to section 906 of the Sarbanes-Oxley Act of 2002.				
97.1	SentinelOne, Inc. Compensation Recovery Policy				
101.INS	Inline XBRL Instance Document--the instance document does not appear in the Interactive Data File because XBRL tags are embedded within the Inline XBRL document.				
101.SCH	Inline XBRL Taxonomy Extension Schema Document.				

101.CAL	Inline XBRL Taxonomy Extension Calculation Linkbase Document.
101.DEF	Inline XBRL Taxonomy Extension Definition Linkbase Document.
101.LAB	Inline XBRL Taxonomy Extension Label Linkbase Document.
101.PRE	Inline XBRL Taxonomy Extension Presentation Linkbase Document.
104	Cover Page Interactive Data File (formatted as inline XBRL and contained in Exhibit 101).

---

* The certifications furnished in Exhibits 32.1 hereto are deemed to accompany this Annual Report on Form 10-K and will not be deemed "filed" for purposes of Section 18 of the Exchange Act, or otherwise subject to the liability of that section, nor shall they be deemed incorporated by reference into any filing under the Securities Act or the Exchange Act.

† Indicates management contract or compensatory plan.

ITEM 16. FORM 10-K SUMMARY

None.

SIGNATURES

Pursuant to the requirements of the Securities Exchange Act of 1934, as amended, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized, in Mountain View, California on the 27th day of March, 2024.

SENTINELONE, INC.

By: /s/ Tomer Weingarten
Tomer Weingarten
Chairman of the Board of Directors, President and Chief Executive Officer
(*Principal Executive Officer)*

POWER OF ATTORNEY

KNOW ALL THESE PERSONS BY THESE PRESENTS, that each person whose signature appears below constitutes and appoints Tomer Weingarten and David Bernhardt, and each of them, as his or her true and lawful attorney-in-fact and agent, with full power of substitution and resubstitution, for him or her and in his or her name, place and stead, in any and all capacities, to sign any and all amendments to this Annual Report on Form 10-K, and to file the same, with all exhibits thereto, and other documents in connection therewith, with the Securities and Exchange Commission, granting unto said attorneys-in-fact and agents, and each of them, full power and authority to do and perform each and every act and thing requisite and necessary to be done in connection therewith, as fully to all intents and purposes as he or she might or could do in person, hereby ratifying and confirming all that said attorneys-in-fact and agents, or any of them, or their, his or her substitutes, may lawfully do or cause to be done by virtue thereof.

Pursuant to the requirements of the Exchange Act of 1934, as amended, this Annual Report on Form 10-K has been signed by the following persons in the capacities and on the dates indicated.

Signature	Title	Date
/s/ Tomer Weingarten Tomer Weingarten	Chairman of the Board of Directors, President, and Chief Executive Officer (Principal Executive Officer)	March 27, 2024
/s/ David Bernhardt David Bernhardt	Chief Financial Officer (Principal Financial Officer)	March 27, 2024
/s/ Robin Tomasello Robin Tomasello	Chief Accounting Officer (Principal Accounting Officer)	March 27, 2024
/s/ Charlene T. Begley Charlene T. Begley	Director	March 27, 2024
/s/ Aaron Hughes Aaron Hughes	Director	March 27, 2024
/s/ Mark S. Peek Mark S. Peek	Director	March 27, 2024
/s/ Ana Pinczuk Ana Pinczuk	Director	March 27, 2024

/s/ Daniel Scheinman Daniel Scheinman	Director	March 27, 2024
/s/ Teddie Wardi Teddie Wardi	Director	March 27, 2024

SentinelOne

Contact Us

investors@sentinelone.com

sentinelone.com

About SentinelOne

SentinelOne (NYSE:S) is pioneering autonomous cybersecurity to prevent, detect, and respond to cyber attacks faster and with higher accuracy than ever before. Our Singularity XDR platform protects and empowers leading global enterprises with real-time visibility into attack surfaces, cross-platform correlation, and AI-powered response. Achieve more capability with less complexity.