Secureworks®

May 15, 2024

Dear Secureworks® stakeholder:

Fiscal 2024 highlighted how critical cybersecurity is in a world of accelerating technological change. While the pace of advancement creates compelling opportunities for organizations to grow, it also makes it challenging for governments, businesses and individuals to outpace the relentless, sophisticated adversary on their own. Attack surfaces are expanding, and threat actor dwell times are falling precipitously, now under 24 hours.

A New Paradigm Around Trust and Security

Secureworks Taegis™ XDR is the platform of choice for organizations who want to secure their data, workloads and business operations and stay ahead of the evolving threat. Taegis has been powered by advanced-AI since inception. The platform was designed to seamlessly secure the diversity and complexity of evolving customer technology environments, and to leverage our threat intelligence and automation capabilities.

Security has never been more mission critical, as we witness the early impacts of AI on threat vectors, with increasingly convincing deep fakes and savvy phishing attacks. This, and the pace of technological advancement, is creating a new paradigm around trust and security. Digitization and most aspects of our lives are now touched by technological involvement and enablement, which makes us highly vulnerable to cyber disruptions, attacks, misrepresentation, extortion, and activism, both personally and corporately. Against this threat backdrop, companies look to Secureworks to not only secure their work, but also help them navigate growing privacy and cybersecurity compliance regulations, and scale their spend on both security technology and talent at a time when fiscal prudence is top of mind and cybersecurity talent remains scarce.

Our Open without Compromise Approach to Security

The market is realizing that an open and collaborative approach to security is a must, and Secureworks is uniquely positioned to meet this market need. Our open Taegis platform future-proofs our customers, with security innovation that parallels the change in technology, pivoting and expanding with customer technology choices over time. Our open approach also provides customers with choice in how they can secure holistically across endpoint, cloud, identity and network. We designed Taegis to excel in detections across mixed environments, with the proven ability to automate sophisticated response actions. This means better, faster protection – with less noise and effort.

Taegis enables organizations to bolster their security posture with the power of Secureworks technology and security expertise. With thousands of security investigations and incident response activities each year, our platform leverages these insights to create machine-readable threat intelligence that updates our detectors every hour of every day. We continued to make significant advancements in the Taegis platform, leveraging the integration of Machine Learning and Large Language Models alongside our unique cloud architecture, to enhance the platform's security analytics and SecOps efficiency.

Our customers and partners continue to benefit from our expanding partner ecosystem. In alignment with our Partner First motion, Taegis is transparent and collaborative with critical managed service and solution providers, as well as technology alliance partners, providing flexibility and optionality around who manages detection and response activities leveraging Taegis XDR. Our unique, open without compromise approach to XDR has opened multiple go-to-market channels for Secureworks, and greater addressable market and revenue growth opportunities for our partners to deliver high margin and effective MDR.

Completing our Business Model Transformation

In Fiscal 2024, our Secureworks Taegis business continued its strong momentum. We delivered annual Taegis revenue growth of 41% and ended the year with the vast majority of our annual recurring revenue (ARR) from Taegis solutions, signaling the near completion of our transformation from a pure-play services company into a SaaS-led business. To put this growth into context, we were recognized as having the largest XDR market share by both Gartner and IDC this year. We made significant progress on profitability, achieving positive EBITDA in fourth quarter, and we accomplished this while accelerating toward the finish line of our business model transformation. This is a testament to the hard work of our teammates as we actively streamlined our cost structure while sunsetting certain non-strategic business lines. We are delivering – and remain committed to driving – sustained growth, while

improving the scale, productivity, and operational efficiencies of our business.

Innovating for Our Customers and Partners

We are fulfilling the promise that is the foundation for Taegis – bringing the T (Technology) and Aegis (Shield) together – by providing organizations with holistic coverage and a multilayered cybersecurity strategy. That is the only way organizations can outpace and outmaneuver an ever-evolving adversary. We're advancing our mission with continued integrations, new features and expanded capabilities, and scaled services powered by our Taegis platform to meet organizations where they are on their security journey. Our innovation will ensure we continue to raise the bar to prevent more, detect better, and respond faster to threats, protecting our customers from ransomware and other cyberattacks.

On behalf of the entire Secureworks team, we thank you for investing in our mission to Secure Human Progress, with Taegis defining the future of threat detection and response, driving superior long-term and sustainable growth and value creation for investors. Thank you to our customers and partners for the trust that they place in us, and I deeply appreciate our Board and teammates around the globe for their diligence, integrity and commitment to securing our customers. We look forward to our continued partnership in Fiscal 2025 and beyond.

Sincerely,

Wendy K. Thomas

Chief Executive Officer

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
Washington, D.C. 20549
FORM 10-K

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

For the fiscal year ended February 2, 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: 001-37748

Secureworks®

SecureWorks Corp.

(Exact name of registrant as specified in its charter)

Delaware	**27-0463349**
(State or other jurisdiction of incorporation or organization)	(I.R.S. Employer Identification No.)

One Concourse Parkway NE Suite 500, Atlanta, Georgia 30328
(Address of principal executive offices) (Zip Code)

Registrant's telephone number, including area code: **(404)327-6339**
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 $0.01 per share	**SCWX**	**The Nasdaq Stock Market LLC (Nasdaq Global Select Market)**

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 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, 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 ☑

As of August 4, 2023, the last business day of the registrant's most recently completed second fiscal quarter, the aggregate market value of the registrant's common stock held by non-affiliates was approximately $103.0 million (based on the closing price of $7.05 per share of Class A common stock reported on the Nasdaq Global Select Market on that date).

As of March 19, 2024, there were 88,287,001 shares of the registrant's common stock outstanding, consisting of 18,287,001 outstanding shares of Class A common stock and 70,000,000 outstanding shares of Class B common stock.

DOCUMENTS INCORPORATED BY REFERENCE

The information required by Part III of this report, to the extent not set forth herein, is incorporated by reference from the registrant's proxy statement relating to the annual meeting of stockholders in 2024. Such proxy statement will be filed with the Securities and Exchange Commission within 120 days after the end of the fiscal year to which this report relates.

TABLE OF CONTENTS

CAUTIONARY NOTE REGARDING 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 and Section 21E of the Securities Exchange Act of 1934. The words "believe," "may," "would," "could," "potentially," "anticipate," "estimate," "expect," "intend," "plan," "aim," "seek" and similar expressions that convey uncertainty regarding future events or outcomes as they relate to us or our management are intended to identify forward-looking statements. Our results could be materially different from our expectations because of various risks, including the risks discussed in this report under "Part I – Item 1A – Risk Factors" and in our other periodic and current reports filed with the Securities and Exchange Commission. Moreover, we operate in a very competitive and rapidly changing environment, and new risks emerge from time to time. All statements by us regarding our expected financial position, revenues, cash flows and other operating results, business strategy, future product and service developments, legal proceedings and similar matters are forward-looking statements. Our expectations expressed or implied in these forward-looking statements may not turn out to be correct. Any forward-looking statement speaks only as of the date as of which such statement is made, and, except as required by law, we undertake no obligation to revise or update any forward-looking statement after the date as of which such statement was made, whether to reflect changes in circumstances or our expectations, the occurrence of unanticipated events, or otherwise.

Except where the context otherwise requires or where otherwise indicated, all references in this report to "Secureworks," "we." "us," "our," and "our company" refer to SecureWorks Corp. and our subsidiaries on a consolidated basis, and all references to "Dell" refer to Dell Inc. and its subsidiaries on a consolidated basis.

Our fiscal year is the 52- or 53-week period ending on the Friday nearest January 31. Our 2024 fiscal year ended on February 2, 2024, our 2023 fiscal year ended on February 3, 2023, and our 2022 fiscal year ended on January 28, 2022. Our 2024 and 2022 fiscal years each consisted of 52 weeks. Our 2023 fiscal year consisted of 53 weeks.

Part I

Item 1. Business

Overview

We are a leading global cybersecurity provider of technology-driven solutions singularly focused on protecting our customers.

Our vision is to be the essential cybersecurity company for a digitally connected world. We believe we are the security platform of choice to deliver a holistic approach to security at scale for our customers to achieve their best security outcomes. We combine considerable experience from securing thousands of customers and processing billions of customer events, incorporate artificial intelligence and machine-learning in our security platform, and utilize actionable insights from our team of elite researchers, analysts, and consultants to create a powerful network effect that provides increasingly strong protection for our customers.

Our proprietary Taegis™ security platform utilizes an open architecture that is designed to process a wide variety of telemetry to see security threats quickly and to leverage our customers' existing investments. Our solutions collect and process vast amounts of data across the information technology, or IT, ecosystem by integrating a wide array of proprietary and third-party security products. This open-platform approach allows us to aggregate events from a wide range of endpoint, network, cloud, and business systems to increase the effectiveness of our solutions.

By aggregating and analyzing data from sources around the world, we offer solutions that enable organizations to:

- prevent security breaches,
- detect malicious activity,
- respond rapidly when a security breach occurs, and
- identify emerging threats.

We believe our security platform supports innovation and collaboration by enabling the security community to outmaneuver the adversary. Leveraging our extensive security expertise and threat intelligence, we utilize our unique insights to extend our Taegis XDR platform to defend against cyber-attacks.

The integrated approach we have pioneered enables us to deliver a broad portfolio of security solutions to organizations of varying size and complexity. We seek to provide the right level of security for each customer's particular situation, which evolves with our customers as their organizations grow and change over time. Our flexible and scalable solutions secure the evolving needs of large enterprises as well as small and medium-sized businesses and U.S. state and local government agencies with limited in-house capabilities and resources.

We offer our customers:

- software-as-a-service, or SaaS, solutions,
- managed solutions, and
- professional services, including incident response and penetration testing services.

Our solutions leverage our proprietary technologies, security operations workflows, and the extensive expertise and knowledge of the tactics, techniques, and procedures of the adversary that we have developed over more than two decades. As key elements of our strategy, we seek to:

- be the SaaS security platform of choice,
- broaden our reach with security service providers to deliver our security platform globally, and
- empower the global security community to beat the adversary at scale.

Our Competitive Strengths

We believe that the following key competitive advantages will allow us to maintain and extend our leadership position in providing technology-driven security solutions:

A Leader in Technology-Driven Security Solutions. We are a global leader in providing technology-driven security solutions and believe we have become a mission-critical partner to many of the large enterprises, small and medium-sized businesses and U.S. state and local government agencies we serve. With decades of security operations expertise, we are recognized by our customers, partners, and industry analysts as a leader in empowering effective security outcomes. We leverage this knowledge and expertise to help customers optimize their security investments and teams, and we enable our partners to build a highly effective and high margin security services business. We believe our position as a technology and market leader enhances our brand and positions our offerings as a preferred solution.

Purpose-Built, Proprietary Technology. At the core of our solutions is the proprietary Taegis software platform that collects, aggregates, correlates and analyzes hundreds of billions of daily events and data points and generates enriched security intelligence on adversary groups and global threat indicators. Our Taegis platform is designed with an open and scalable architecture optimized to deliver comprehensive answers to security challenges and allows for expanded visibility and timely detections using our telemetry normalization techniques and proprietary algorithms that, coupled with 1-click response actions, drive efficiency and faster remediation times.

Open Platform Approach. Taegis utilizes an open architecture that is designed to process a wide variety of telemetry to accelerate security threat visibility while leveraging our customers' existing investments. Our solutions collect and process vast amounts of data across the IT ecosystem by integrating a wide array of proprietary and third-party security products. We designed Taegis to address the reality and complexity of customer technology environments, including endpoint technologies from multiple vendors, deployed simultaneously across their organizations and hybrid and multi-cloud environments. This open platform approach allows us to aggregate events from a wide range of endpoint, network, cloud, and business systems to increase the effectiveness of our solutions.

Threat Intelligence. Our proprietary and purpose-built technology uses analytical models and sophisticated algorithms to generate threat intelligence. This intelligence is augmented by our Counter Threat Unit™ research team, which conducts research into adversaries, uncovers new attack techniques, analyzes emerging threats, and evaluates the risks posed to our customers. By integrating this intelligence throughout our solutions, our customers are given deeper insights and enriched context regarding the tactics, techniques, and procedures employed by those adversaries.

Breadth and Depth of Detection Capabilities. Our powerful and unique threat intelligence, which is continuously fueled by incident response engagements, penetration testing exercises, activity in our security operations centers, and by our Counter Threat Unit research team, is turned into machine-readable software that enhances our long-standing use of AI and machine learning capabilities. These capabilities allow us to deliver innovative detectors and threat context indicators, each of which is individually powerful, but they are even more powerful when working in unison for our customers and partners.

Simple, Predictable Pricing Structure. Taegis pricing is based on customer endpoint and/or asset counts, which are easily attainable and predictable by our customers. This simple pricing approach avoids unpredictable charges that make forecasting difficult and disincentivizes customers from sharing their data.

Scalable Software Platforms with Powerful Network Effects. Our security platform offers multi-tenant security capabilities to provide rapid threat detection and response with integrated proprietary orchestration and automation capabilities, a growing set of response playbooks, and access to unlimited incident response. As our customer base increases, our security platform can analyze more event data, further adding intelligence to make our security platform more effective. This in turn drives broader customer adoption and enhances the value of the solutions to both new and existing customers.

Global Customer Base. Our global customer base provides visibility into the cyber threat landscape through 3,900 customers across 73 countries. We gain real-time insights that enable us to identify, detect and respond to threats quickly and effectively.
Our global footprint and diverse customer base allow us to identify threats originating within a particular geographic area or related to a particular industry, and we proactively leverage this threat intelligence to protect our customers against those threats.

Specialist Focus and Expertise. Our company, technology and culture were built with a singular focus on protecting our customers by delivering technology-driven security solutions to outpace and outmaneuver the adversary. We believe this continued focus reinforces our differentiation from other information security vendors, including network providers, IT security product companies, and local and regional information security solutions providers.

Strong Team Culture. The fight against sophisticated and malicious cybersecurity threats is a personal one for our company, and we take great pride in helping our customers protect their critical business data and processes. We dedicate significant resources to ensure that our culture and brand reflect our singular focus on protecting our customers against the adversary.

Our Growth Strategy

Our strategy is to be the essential cybersecurity company for a digitally connected world. To pursue our strategy, we seek to:

Broaden our portfolio of software-as-a-service solutions. In fiscal 2020, we launched our first SaaS application, called Taegis XDR, an Extended Detection and Response solution. We deploy a managed version of this application called Taegis ManagedXDR, which allows Secureworks or our partners to manage the application for customers. Since fiscal 2020, we have expanded our SaaS portfolio by launching our vulnerability management application, called Taegis VDR, and our next generation anti-virus, or NGAV, add-on solution called Taegis NGAV. We intend to continue expanding our Taegis portfolio with additional internally developed or acquired SaaS solutions.

Extend our technology leadership. We intend to enhance our leading technology-driven integrated suite of solutions by adding complementary solutions that strengthen the security posture of our customers. We intend to meet this goal by continuing to invest in research and development, increasing our global threat research capabilities and hiring personnel with extensive cybersecurity expertise.

Embrace our partner ecosystem. We are continuing to embrace strategic partnerships with our channel partners, technology alliance partners, and system integrators. Our Partner First strategy is focused on further expanding our partner ecosystem to open new channels to market and enabling customers to succeed with our open platform through the delivery of comprehensive security solutions.

Expand and diversify our customer base. We intend to continue to expand and diversify our customer base, both domestically and internationally, by investing in our demand generation and marketing capabilities, investing in our Partner First strategic relationships, and pursuing opportunities across a broad range of industries. We also intend to continue increasing our geographic footprint to further enhance our deep insight into the global threat landscape and ability to deliver comprehensive threat intelligence to our customers.

Deepen our existing customer relationships. We provide scalable software-as-a-service solutions and intend to continue leveraging the strong customer relationships and high customer satisfaction from across our customer base to sell additional solutions to existing customers. We expect to continue to invest in our account management, marketing initiatives and customer success programs in seeking to achieve high customer renewal rates, help customers realize greater value from their existing solutions and encourage them to expand their use of our solutions over time.

Attract and retain top talent. Our technology leadership, brand, exclusive focus on information security, customer-first culture, and robust training and development program have enabled us to attract and retain highly skilled professionals with a passion for building a career in the information security industry. We plan to continue to invest in attracting and retaining top talent to support and enhance our information security offerings.

Our Taegis Subscription and Professional Services Offerings

We offer an integrated suite of technology-driven security solutions enabled by our Taegis security platform and team of highly skilled security experts. Our technology-driven security solutions offer an innovative approach to prevent, detect and respond to cyber-attacks. Our Taegis security platform collects, aggregates, correlates and analyzes billions of events daily from our extensive customer base by leveraging artificial intelligence and machine-learning capabilities and utilizing actionable insights provided by our team of elite researchers, analysts, and consultants to detect malicious activity and deliver security countermeasures, dynamic threat intelligence and valuable context regarding the intentions and actions of cyber adversaries. Through our Taegis security solutions, which are sold on a subscription basis, we provide global visibility and insight into malicious activity, enabling our customers to detect, respond to and effectively remediate threats quickly.

We leverage current threat intelligence and our extensive expertise and knowledge of the tactics, techniques, and procedures of the adversary, which we have developed over two decades of processing and handling events, to provide insight into how cyber-attacks are initiated and spread across our customers' networks. The Taegis security platform applies intelligence based on threat indicators continuously gathered by our Counter Threat Unit research team through in-depth analysis of the global cyber threat environment. Our Counter Threat Unit researches emerging adversaries and new attack tactics, techniques, and procedures, and it develops countermeasures to enable customers to prevent and detect potential compromises. Our ability to see more security incidents along with the applied intelligence acts as an early warning system that enables us to proactively alert customers, apply protections and respond quickly with appropriate context. The more security events we see, the more effective we become at deploying countermeasures, detections, and response actions. Our security platform is designed to be open, enabling our customers to aggregate events from a wide range of endpoint, network, cloud, and business systems.

By delivering integrated security solutions, we seek to allow organizations to:

- measurably reduce their business risk from cyber exposure;
- optimize their existing investments in security systems and controls; and
- address the shortage of personnel with cybersecurity expertise.

Customers may subscribe to our full suite of security solutions or elect to subscribe to various combinations of individual solutions. We offer solutions, including the offerings discussed below, primarily on a subscription basis with terms typically ranging from one to three years.

We began transforming our subscription business to our Taegis solutions during fiscal 2021. Customers were informed during the fourth quarter of fiscal 2022 that many of our other managed security services would no longer be available for purchase, and renewals would not extend, beyond the end of fiscal 2023. By the end of fiscal 2024, revenue from our Taegis solutions represent 87.1% of our total subscription revenue.

Taegis Subscription Solutions

Our proprietary Taegis security platform was purpose-built as a SaaS platform and serves as the core of our SaaS solutions. Our security platform leverages artificial intelligence, machine learning and actionable threat intelligence to unify detection and response across endpoint, network, cloud, and other business systems to increase the effectiveness of our security solutions, accelerate the speed of response actions, and simplify security operations.

Taegis XDR, ManagedXDR and VDR are the first in our integrated suite of technology-driven security solutions built on our Taegis security platform that we plan to release.

Extended Detection and Response. Taegis XDR collects and processes billions of events daily from a wide variety of sources through hundreds of out-of-the-box integrations. The resulting advanced security analytics created from our security platform through a network effect provided by our diverse, global customer base are further enriched by our extensive threat intelligence and understanding of the evolving global threat landscape.

- Taegis XDR analyzes activity from endpoint, network, cloud, and other business systems while reducing the number of false-positive results security professionals face. It detects advanced threats by correlating information from a variety of sources and threat intelligence feeds, integrating our knowledge and research of adversarial behaviors, and applying artificial intelligence, machine learning and other advanced analytics to provide vital context about the threat faced. Taegis XDR builds trust with users, prioritizes security alerts, and empowers security teams to focus on the most critical threats.
- Taegis XDR unifies security environments and analyzes all relevant signals in one place. Customers gain additional context so they can quickly and accurately judge the implications of each event.

- By enabling collaborative investigations with seamless hand-offs, Taegis enables customers to quickly reach conclusions with confidence. Customers can use our built-in chat feature, accessible from the user interface, during an investigation to get real-time expert help from Secureworks in less than 90 seconds.
- Our platform allows for a quick, accurate, software-driven response that gives users the ability to automate the right actions.
- Taegis XDR is a cloud-based, SaaS platform that is continuously updated with new features and updates pushed to the production environment.
- Taegis XDR includes advanced endpoint threat detection and network solutions with enhanced features such as next-generation anti-virus prevention capabilities, or NGAV. These features enable customers to consolidate spending with a single vendor, using our security platform as the centralized solution.
- The platform is designed to efficiently integrate into an organization's current security controls framework.

Managed Detection and Response. Taegis ManagedXDR, a fully-managed cybersecurity solution, combines the capabilities of the Taegis XDR platform with extensive security expertise for 24/7 protection.

- Taegis ManagedXDR leverages the knowledge and actionable insights developed from our long history of security analysis, threat research and incident response engagements to continuously enhance our threat intelligence and security analytics used to recognize malicious activity. The Taegis platform uses artificial intelligence, machine learning and other advanced analytics to discover stealthy threats and automatically prioritize the most serious threats, allowing customers to focus on the events that matter.
- Taegis ManagedXDR provides customers with access to the same intuitive interface and platform as our Secureworks analysts to collaborate in the ways customers prefer. Customers can reach our analysts directly 24/7 via live chat functionality in Taegis XDR.
- Taegis ManagedXDR includes threat hunting to proactively isolate and contain threats that evade existing security controls.
- Taegis ManagedXDR incorporates incident response support that can be deployed quickly during a critical investigation.

Customers can extend the benefits of Taegis ManagedXDR with high-value add-ons:

- Taegis ManagedXDR *Elite* solution provides a designated threat-hunting expert to perform continuous, proactive, and iterative threat hunting across endpoint, network and cloud environments with bi-weekly updates on an organization's exposure to targeted threats.
- Taegis ManagedXDR *Enhanced* solution delivers higher-touch threat analysis and orchestrated response in which enhanced security analysts swivel between the Taegis XDR platform and multiple customer systems to provide a deeper level of analysis, yielding clear business context that consolidates everything occurring in a customer's environment into one holistic picture, enabling intelligent and rapid escalation and orchestrated remediation.

Vulnerability Detection and Response. Taegis VDR simplifies vulnerability management with a risk-based approach that prioritizes the most critical threats and optimizes remediation efforts to protect what's most important. Powered by automated intelligent machine learning, VDR is a fully integrated, comprehensive solution that requires no configuration and automatically discovers endpoints, network equipment and devices, web applications and forgotten assets to scan for vulnerabilities and prioritize them. It's a self-learning system that improves autonomously with use, further reducing risk and creating more efficiency and time for your security team to focus on what matters most for your organization.

- Taegis VDR helps organizations reduce risk by simplifying security operations with a single solution to identify and respond to vulnerabilities instead of relying on multiple technologies.
- Taegis VDR identifies vulnerabilities that require remediation by deploying a machine-learning risk prioritization engine. The solution provides context to determine which vulnerabilities pose the biggest risk to each customer. The machine-learning engine will continuously learn and improve its performance as it collects data over time, leading to a more effective and efficient vulnerability management program.
- Taegis VDR features an automated approach to vulnerability management that helps an organization's staff focus on other tasks while VDR continues to scan for vulnerabilities.

Professional Services

In addition to our Taegis solutions, we offer a variety of consulting and professional services that advise customers on a broad range of security and risk-related matters, which include incident response, penetration testing and Taegis professional services to accelerate adoption of our solutions.

Incident Response

In our incident response engagements, we help customers rapidly analyze, contain, and remediate security incidents to minimize their duration and impact. In addition, our incident response services can increase customer awareness of, and interest in, our Taegis subscription solutions as we help customers develop a stronger and more comprehensive security program and posture.

Incident Readiness. Secureworks provides a wide variety of incident readiness services to help customers understand the current state, identify areas of weakness or existing compromise, and give expert guidance to enable pragmatic and risk-based improvements. Our incident management retainer offering provides 24/7/365 access to incident response experts and provides access to a variety of other proactive services where customers can conduct a tabletop exercise, understand their risk exposure within Active Directory, and engage in other services that help prepare for a cyber attack. Our deep experience in incident response investigations and security best practices forms the basis of our comprehensive incident response plan review, which is designed to assist our customers in guarding against gaps and uncertainty amid a crisis and incorporates the latest threat intelligence tailored to the customer's specific needs.

Emergency Incident Response Solutions. We seek to ensure that organizations experience minimal economic loss and operational disruption when facing a cybersecurity incident. Our team of experienced security professionals work hand-in-hand with customers to minimize the duration and impact of security incidents through incident management, technical expertise, investigative know-how, malware analysis and reverse engineering. Layered into our incident response investigations and integrated into our Taegis security platform is the threat intelligence developed by our Counter Threat Unit research team, which enriches our overall knowledge of the adversary and allows investigators to take a targeted approach and get to a faster resolution for our customers.

Threat Hunting Assessment. The Secureworks Threat Hunting Assessment is a point-in-time, 30-day comprehensive and intensive evaluation of a customer's environment to identify previously unknown compromise activity, security misconfigurations, visibility gaps, control issues, and cyber threats and risks. Our team of security experts possess decades of combined experience countering adversary tradecraft. This human intelligence, along with our proprietary hunting technology and our advanced security analytics, enables us to identify the presence of historical and active compromises entrenched within that customer's environment. This service helps a customer increase its cyber resilience with focused, tailored recommendations on security architecture, instrumentation, and controls.

Penetration Testing Services

We facilitate improvements to our customers' security posture by assessing their security capabilities, preparing employees against cyber-attacks, improving compliance, and identifying, prioritizing and resolving the vulnerabilities that pose the greatest threat.

Our team has extensive experience conducting offensive security engagements across many industries and geographic areas and under recent regulations and industry standards that impose security mandates.

Our penetration testing services provide customers with a thorough analysis of their security posture to include logical, physical, technical, and non-technical threats. These penetration testing services identify risk-generating gaps in people, process, and technology, and they help organizations construct a stronger security posture and meet compliance mandates. Our testing solutions touch nearly every aspect of offensive security, including:

- Application security
- Network security
- Adversary exercises
- Vulnerability assessments delivered using Taegis VDR
- Other customized and specialized testing services

All our offensive services simulate cyber-attacks using real-world tactics, techniques, and procedures through a blend of automated and manual attacks. Our offensive professionals also assist the Incident Response team during their investigations and provide insight on the adversary, which drives continuous improvements to the detection efficacy of the Taegis security platform.

Taegis & Other Professional Services

Taegis Professional Services. Our Taegis Professional Services assist customers by providing training, onboarding, and integration services to assist with the implementation and adoption of our Taegis XDR platform. The services include assessing the customer's environment, performing data integration activities, and providing training for customers to effectively use the Taegis security platform.

Security Residency Solutions. Our Security Residency Solutions provide customers with security consultants who serve as extended members of their staff either on-site or remotely to extend and heighten an organization's security expertise and capabilities. Residency solutions are combined with other Secureworks solutions within complex enterprise environments to enhance the value customers experience. We align with each customer's internal processes, integrate our data feeds into customer applications and dashboards, and produce customized analytics and reporting. In addition, we assist customers with handling the security events identified by our solutions.

Other Legacy Managed Security Services

Our Other Legacy Managed Security Services, which were end-of-life at the end of fiscal 2023, were only provided to customers in Japan or customers who had contracts that extended beyond fiscal 2023. These other legacy managed security services described below accounted for 10.7% and 37.8% of our total revenue in fiscal 2024 and 2023, respectively. These services included security monitoring, advanced endpoint threat detection, firewall and next-generation firewall services, managed network intrusion detection systems and log retention services.

Our Customers

As of February 2, 2024, we had approximately 3,900 customers, including approximately 2,000 Taegis and 300 managed security subscription customers, across 73 countries. We serve customers in a broad range of industries, including the financial services, manufacturing, technology, retail, insurance, utility, and healthcare sectors. No one customer represented more than 10% of our annual revenue in any of our last three fiscal years. In fiscal 2024, financial services and manufacturing customers accounted for 20% and 26%, respectively, of our revenue. No other industries accounted for 10% or more of our fiscal 2024 revenue.

The fees we charge for our solutions vary based on a number of factors, including the solutions selected, the number of customer devices covered by the selected solutions, and the level of management we provide for the solutions. Approximately 83% of our revenue is derived from subscription-based arrangements, attributable to Taegis solutions and managed security services, while approximately 17% is derived from professional services engagements. As we respond to the evolving needs of our customers, the relative mix of subscription-based solutions and professional services we provide our customers may fluctuate.

International revenue, which we define as revenue contracted through non-U.S. entities, represented approximately 37%, 34% and 33% of our revenue in fiscal 2024, fiscal 2023 and fiscal 2022, respectively. For additional information about our non-U.S. revenues and assets, see "Notes to Consolidated Financial Statements—Note 12—Selected Financial Information" in our consolidated financial statements included in this report.

Customer Success and Support

Customer success, training and support are key elements of our commitment to provide a superior customer experience and differentiated value. We have a comprehensive customer success training and support program to continuously improve the customer experience and enhance the value that our customers derive from our solutions. We provide education, training, and support on the functionality of our solutions so that our customers fully utilize their benefits, and we regularly conduct customer surveys to improve and enhance both our customer relationships and solutions portfolio. Our Taegis XDR and Taegis VDR customers receive 24/7 application support as well as an integrated chat function. Our Taegis platform has an integrated customer experience software that analyzes how customers use our applications, highlights new features available, and solicits customer feedback.

Research and Development

We believe that innovation and the timely development of new solutions are essential to meeting the needs of our customers and improving our competitive position. We plan to continue making investments in our research and development effort as we evolve and extend the capabilities of our solutions portfolio.

We focus our research and development efforts on enhancing and adding new functionality to our Taegis security platform and purpose-built technologies that are critical enablers of our solutions and services. The Taegis security platform and its capabilities follow an agile development, continuous release process with new features pushed to production environments daily, and user interface enhancements released every two weeks.

Our research and development organization is responsible for the architecture, design, development and testing of all aspects of our suite of security solutions. We have deep security, software and data science expertise and work closely with our product management, customer success and support teams and with customers to gain insights into future product development opportunities. We focus our research on identifying next-generation threats and adversaries and developing countermeasures, which are continuously applied to our security platforms and used to respond to the rapidly evolving security threat landscape. In addition to improving on our features and functionality, our research and development organization works closely with our information technology team to ensure that our security platforms are available, reliable, and stable.

Sales and Marketing

Sales and Marketing, together with our partners, drives growth by focusing on defining the Secureworks brand, increasing awareness, building a robust opportunity and revenue pipeline, and cultivating partner and customer relationships. We create customer value with our managed detection and response security solutions that are cloud native and are offered primarily on a subscription basis. We typically offer contract terms from one to three years and, as of February 2, 2024, our contracts average roughly two years in duration. We provide additional customer value through our Taegis professional services and our consulting services, which include incident response and penetration security testing services.

Partner Program

Secureworks Taegis is an XDR platform that serves as the core of the Secureworks MDR solution. The Taegis platform's architecture enables us to quickly integrate solutions and innovations from our partners, offering the best-fit security solutions to our joint Secureworks and partner customers.

Our Partner First strategy equips and enables our partners to leverage the Taegis security platform, together with Secureworks expert services, as an engine for growth. Our partners, in turn, enable Secureworks to be more flexible and fast to market, driving superior customer retention with their supplemental solution offerings and knowledge of customer needs. Our growing partner ecosystem includes cyber risk partners, solution providers, technology alliance partners, and managed security service providers, or MSSPs.

Sales Teams

Our Sales teams are committed to driving sales opportunities through our partner community and closing deals together. Our Customer Success and Account Management teams extend the value of our solutions by identifying cross-selling and upselling opportunities within our customer base and enhancing customer satisfaction. Our routes to market vary by country, by partner channel and the size of the customer organization.

Our Sales teams are a mix of inside sales and field sales professionals who are aligned with geographic regions. These sales professionals are supported by technical Sales Engineers with deep security experience, who assess customer environments and needs by delivering strong proof of value experiences, and by our partner community, which matches the best security solutions to customer needs. In fiscal 2024, approximately 77% of Secureworks revenue, and 78% of our Taegis revenue, was generated through Secureworks-sourced sales opportunities, with the remaining portion generated through partners.

Marketing Team

Our Marketing team builds our Secureworks and Taegis brands, and increases awareness for our platform and solutions, as well as generating market demand and driving pipeline growth and helping grow and maintain our competitive advantage. We develop and continuously refine company and solution messages, based on customer and buyer dialogs, and we launch new and enhanced offerings to market.

We deploy demand generation campaigns, including digital marketing and joint partner marketing programs, to engage, educate, and inspire prospects to action by creating marketing content that is relevant to buyer needs at every stage of the buying cycle. Our awareness programs yield consistent editorial coverage in widely distributed business publications and industry trade publications. Our social media programs regularly engage individual buyers and influencers with marketing and executive content, and we participate in digital marketing programs and face-to-face events to create customer and prospect awareness and action.

We frequently brief industry analysts and are a subject of analyst publications and references, building third-party validation of our company and our solutions. We also enable our sales and partner teams with sales tools, education, competitive insights, and field marketing activities to help them convert leads into customers.

Competition

The markets for our technology-driven security solutions and services are intensely competitive, and we expect competition to continue to increase in the future with the introduction of new security solutions, new technologies and new market entrants. Conditions in our market could change rapidly and significantly resulting from technological advances, partnerships, or acquisitions by our competitors. Changes in the threat and technology landscape have led to constantly evolving customer requirements for protection from security threats and adversaries.

We compete primarily against the following three types of security product and services providers, some of which operate principally in the large enterprise market and others in the market for small and medium-sized businesses:

- security providers and niche IT security products and services such as CrowdStrike, Inc., Rapid7, Inc., SentinelOne, Inc. and Arctic Wolf;
- diversified technology and telecommunications companies such as Palo Alto Networks, Inc., Microsoft, International Business Machines Corporation and AT&T Inc.; and
- small regional managed security service providers, including new market entrants, that compete in the small and medium-sized businesses market.

As the extended detection and response market continues its rapid growth, it will continue to attract new market entrants as well as existing security vendors acquiring or bundling their products more effectively.

We believe that the principal competitive factors in our market include:

- global visibility into the threat landscape;
- ability to generate actionable intelligence based on historical data and emerging threats;
- speed of innovation;
- scalability and overall performance of platform technologies;
- deep understanding of security operations best practices;
- ability of our technology to integrate with a variety of third-party products;
- ability to deliver SaaS solutions to meet specific customer needs;
- ability to attract and retain high-quality professional staff with information security expertise;
- brand awareness and reputation;
- strength of sales and marketing efforts;
- cost effectiveness;
- customer success and support; and
- breadth and richness of threat intelligence, including a history of data collection and diversity and geographic scope of customers.

We believe that we generally compete favorably with our competitors based on these factors because of the features and performance of our security offerings, the quality of our threat intelligence, the security expertise within our organization, and the ease of integration of our solutions with other technology infrastructures. However, many of our competitors, particularly in the large enterprise market, have advantages over us because of their greater brand name recognition, larger customer bases, more extensive relationships within large commercial enterprises, more mature intellectual property portfolios, and greater financial and technical resources.

Intellectual Property

Our intellectual property is an essential element of our business. To protect our intellectual property rights, we rely on a combination of patent, trademark, copyright, trade secret and other intellectual property laws as well as confidentiality, employee non-disclosure and invention assignment agreements.

Our employees and contractors involved in technology developments are required to sign agreements acknowledging that all inventions, trade secrets, works of authorship, developments, processes, and other intellectual property rights conceived or reduced to practice by them on our behalf are our property, and assigning to us any ownership that they may claim in those intellectual property rights. We maintain internal policies regarding confidentiality and disclosure. Our customer and resale contracts prohibit reverse engineering, decompiling and other similar uses of our technologies and require that our technologies be returned to us upon termination of the contract. We also require our vendors and other third parties who have access to our confidential information or proprietary technology to enter into confidentiality agreements with us.

Despite our precautions, it may be possible for third parties to obtain and use, without our consent, intellectual property that we own or otherwise have the right to use. Unauthorized use of our intellectual property by third parties, and the expenses we incur in protecting our intellectual property rights, may adversely affect our business.

Our industry is characterized by the existence of a large number of patents, which leads to frequent claims and related litigation regarding patent and other intellectual property rights. In particular, large and established companies in the IT security industry have extensive patent portfolios and are regularly involved in litigation asserting or defending against patent infringement claims. From time to time, third parties, including some of these large companies as well as non-practicing entities, may assert patent, copyright, trademark and other intellectual property rights against us, our channel partners, or our end-customers, which we are obligated to indemnify against such claims under our standard license and other agreements. Successful claims of infringement by a third party, if any, could prevent us from performing certain solutions, require us to expend time and money to develop non-infringing solutions, or force us to pay substantial damages (including, in the United States, treble damages if we are found to have willfully infringed patents), royalties or other fees.

Patents and Patent Applications

As of February 2, 2024, we owned 58 issued patents and 8 pending patent applications in the United States and six issued patents and 12 pending patent applications outside the United States. The issued patents are currently expected to expire between 2028 and 2041. Although we believe that our patents as a whole are important to our business, we are not substantially dependent on any single patent.

We do not know whether any of our patent applications will result in the issuance of a patent or whether the examination process will require us to modify or narrow our claims, as has happened in the past with respect to certain claims. Any patents that may be issued to us may not provide us with any meaningful protection or competitive advantages, or may be contested, circumvented, found unenforceable, or invalidated, and we may not be able to prevent third parties from infringing upon them.

Trademarks and Copyrights

The U.S. Patent and Trademark Office has granted us federal registrations for some of our trademarks. Federal registration of trademarks is effective for as long as we continue to use the trademarks and maintain our registrations as permitted under federal law. We also have obtained protection for some of our trademarks, and have pending applications for trademark protection, in the European Community and various countries. We may, however, be unable to obtain trademark protection for our technologies and names that we use, and the names, slogans. or logos that we use or may use may be deemed non-distinctive. Therefore, we may be unable to distinguish our solutions from those of our competitors in one or more countries.

We have entered into a trademark license agreement with Dell Inc. under which Dell Inc. has granted us a non-exclusive, royalty-free worldwide license to use the trademark "DELL," solely in the form of "SECUREWORKS-A DELL COMPANY," in connection with our business and products, services and advertising and marketing materials related to our business.

Backlog

We define backlog as the non-cancellable value of subscription-based solutions to be provided under our Taegis solutions and managed security services contracted with a customer that have not yet been provisioned or installed. Backlog is not recorded in revenue, deferred revenue or elsewhere in our consolidated financial statements until we establish a contractual right to invoice, at which point backlog is recorded as revenue or deferred revenue, as appropriate. All contractual amounts included in backlog are available to be installed with revenue recognition commencing within the coming fiscal year. As of February 2, 2024 and February 3, 2023, backlog of subscription-based solutions was approximately $1.4 million and $3.0 million, respectively. Backlog is influenced by several factors, including seasonality, the compounding effects of renewals, and the mix of solutions under contract with customers. Accordingly, we believe that fluctuations in backlog are not always a reliable indicator of future revenues.

Seasonality

As a result of the annual budget approval process of many of our customers, we have historically seen seasonal patterns in our business, with sales to new customers and additional sales to existing customers becoming greater in the second half of the year. In addition, we also experience seasonality in our gross and operating margins, with lower margins in the first half of our fiscal year as a result of greater expenditures for payroll taxes and annual sales and marketing events. This seasonality may also affect the timing of our operating cash flow.

Human Capital Resources

Employee Population

As of February 2, 2024, we employed 1,516 full-time employees. Approximately 50.1% of our employees were located in the United States and the remainder were located in 24 other countries. None of our employees in the United States are represented by a labor organization or the subject of a collective-bargaining agreement. Employees of some of our foreign subsidiaries are represented on workers' councils.

Compensation, Benefits and Well-being

We are committed to providing employees with compensation and benefits that support their physical, mental, and financial well-being. We believe our compensation program is designed to attract and reward talented individuals who possess the skills necessary to support our business objectives and assist in the achievement of our strategic goals. In addition to competitive base salaries, eligible employees can receive short-term cash incentives and long-term cash or equity awards. We also offer employees a wide array of benefits, including life and health and welfare insurance, retirement benefits, and paid time off.

We have a remote work policy for all but a small number of essential personnel. This policy is supported by a culture that includes quarterly all-hands calls celebrating our people and business, with more frequent touchpoints by leaders throughout the organization. Our approach to remote work focuses on helping our employees manage their work responsibilities in addition to focusing on their well-being, health, and safety.

Diversity and Inclusion

In the global fight to protect our customers, we believe that our future growth and innovation require respecting and celebrating our teammates, learning from each other, and creating an environment where people can be themselves. We are committed to educating our teammates, enabling inclusion, and enhancing diversity. We also seek to connect our employees across regions and provide them with opportunities to enhance cultural awareness and inclusivity, and to enable collaboration.

Communication and Engagement

We believe that our corporate culture depends on our employees' engagement and understanding of their contribution to the achievement of our strategic imperatives, vision and mission to secure human progress. In addition to prioritizing regular communications, we conduct regular employee surveys to seek feedback on what is going well and where we can focus our efforts to do more. We also have active employee resource groups, which are designed to address the need for more social and community interaction in our globally diverse workforce.

Community Involvement

We aim to give back to the communities where we live and work, and we believe that this commitment helps in our efforts to attract and retain employees. We partner with a variety of universities and inclusion-focused programs globally to promote STEM education for all. Beyond contributions of cash, we encourage employees to participate in numerous local events and engage in volunteer service throughout the year.

Corporate Information

We are a holding company that conducts operations through our wholly-owned subsidiaries. The mailing address of our principal executive offices is One Concourse Parkway NE, Suite 500, Atlanta, Georgia 30328. Our telephone number at that address is (404) 327-6339.

Secureworks was acquired by Dell, Inc. in February 2011 and completed its initial public offering, or IPO, in April 2016. Upon the closing of our IPO, Dell Technologies Inc., the ultimate parent company of Dell, Inc., owned indirectly through Dell Inc. and Dell Inc.'s subsidiaries, all shares of our outstanding Class B common stock, which as of February 2, 2024 represented approximately 81.0% of our total outstanding shares of common stock and approximately 97.7% of the combined voting power of both classes of our outstanding common stock.

Available Information

Our annual report on Form 10-K, quarterly reports on Form 10-Q, current reports on Form 8-K, amendments to these reports, and other filings made with the U.S. Securities and Exchange Commission, or SEC, whether filed or furnished pursuant to Section 13(a) and 15(d) of the Securities Exchange Act of 1934, as amended, are available free of charge on our website at www.investors.secureworks.com as soon as reasonably practicable after we electronically file or furnish them with the SEC. Information appearing on, or accessed through, our website is not a part of this report.. Our references to URLs for these websites are intended to be inactive textual references only.

Investors and others should note that we may announce material financial information to our investors using our website, SEC filings, press releases, public conference calls, and webcasts, or a combination thereof, to achieve compliance with our Regulation FD disclosure obligations. We also use these disclosure channels, our corporate website (https://www.secureworks.com) and social media to communicate with the public about our services, solutions, and other issues. It is possible that the information we make available on our investor relations website, corporate website, or social media platforms could be deemed to be material information; therefore, we encourage investors, the media, and other interested parties to review the information we make available through such means.

Information about our Executive Officers

The following table contains information with respect to our executive officers as of March 22, 2024.

Name	Age	Position
Wendy K. Thomas	52	Chief Executive Officer
Alpana Wegner	51	Chief Financial Officer
George B. Hanna	57	Chief Legal & Administrative Officer and Corporate Secretary
Stephen L. Fulton	50	President, Customer Success

Each executive officer is appointed by, and serves at the discretion of, our board of directors.

Wendy K. Thomas has served as our Chief Executive Officer since September 2021. Prior to this appointment, Ms. Thomas served in a number of critical positions at Secureworks, including as President and Chief Executive Officer from September 2021 to February 2023, as President, Customer Success from April 2020 to September 2021, as Chief Product Officer from June 2019 to April 2020, as Senior Vice President, Business and Product Strategy from March 2018 to June 2019, as Vice President, Strategic and Financial Planning from March 2017 to March 2018, and as Vice President, Financial Planning and Analysis from July 2015 to March 2017 and from June 2008 to June 2011. In addition, Ms. Thomas served as Chief Financial Officer of Bridgevine, Inc. (currently Updater Inc.), a marketing software company, from November 2013 to July 2015, and as Vice President, Financial Planning and Analysis, at First Data Corporation (currently Fiserv, Inc.), a payment processing and financial services technology company, from July 2011 to October 2013. Earlier in her career, Ms. Thomas held other positions, including multiple finance roles at BellSouth Corporation, a telecommunications company, culminating in the position of Director, Finance.

Alpana Wegner has served as our Chief Financial Officer since June 2023. Before joining us, Ms. Wegner served as Executive Vice President, Chief Financial Officer of Benefitfocus, Inc., a cloud-based benefits administration technology company, from August 2020 to May 2023. Before serving in this role, Ms. Wegner was Vice President, Corporate Controller of Benefitfocus from December 2017 to August 2020 and was General Manager of the Carrier Business Unit from April 2017 until December 2017. Ms. Wegner's previous experience includes multiple senior financial and operational roles, including service at Blackbaud, Inc., a cloud software company, as Vice President, Sales Operations from April 2016 to January 2017 and as Vice President, CFO of the Enterprise Customer Business Unit from June 2013 to April 2016. Ms. Wegner is a Certified Public Accountant.

George B. Hanna has served as our Chief Legal & Administrative Officer and Corporate Secretary since October 2015. Before joining us, Mr. Hanna was the Executive Vice President, Chief Legal & Administrative Officer for YP Holdings, one of the country's largest digital media companies, from January 2013 to October 2015. Prior to his service with YP Holdings, Mr. Hanna served in various leadership roles at Wellmark Blue Cross Blue Shield from July 2007 to January 2013, including as the Chief Executive Officer of Wellmark Health Plan of Iowa and as Executive Vice President of Sales & Marketing and Chief Legal Officer for Wellmark Blue Cross Blue Shield. Mr. Hanna previously was employed at BellSouth Corporation from February 1995 to July 2007, where he held senior legal roles including a position as Vice President & Deputy General Counsel.

Stephen L. Fulton has served as our President, Customer Success since February 2023. Prior to this appointment, Mr. Fulton served in several instrumental positions at Secureworks leading all aspects of the Taegis XDR platform vision and development, including as Senior Vice President & Chief Product Officer from September 2020 to January 2023, and as Vice President, Software Engineering from May 2017 to September 2020. Before joining us, Mr. Fulton held a number of senior leader roles at a variety of software companies, including as a Vice President at Velostrata (acquired by Google) from 2015 to 2017, as Vice President of Business Development at EMC from 2014 to 2015, and as Vice President, Corporate Development at ScaleIO (acquired by EMC) from 2013 to 2014. Mr. Fulton's previous experience also includes multiple strategy, software and business development roles as Director, Cloud Strategy at Dell from 2011 to 2013, as Vice President, New Software Development at ServiceMesh (acquired by CSC) from 2010 to 2011, as Vice President, PM and Business Development at Wanova (acquired by VMware) from 2008 to 2010, and in a business development and product management role as Senior Director, Product Management at NetQoS (acquired by CA Technologies) from 2000 to 2008.

Item 1A. Risk Factors

A description of the risks and uncertainties associated with our business and industry, our relationship with Dell and Dell Technologies, and ownership of our Class A common stock is set forth below. You should carefully consider the following risks, together with all of the other information in this report, including our consolidated financial statements and the related notes thereto. The risks and uncertainties described below are not the only ones we face. Additional risks and uncertainties that we are unaware of, or that we currently believe are not material, may also become important factors that affect us. If any of the following risks occur, our business, financial condition, operating results and prospects could be materially and adversely affected.

Risks Related to Our Business and Our Industry

We have a history of losses and may not be able to achieve or maintain profitability.

We incurred net losses of $86.0 million in fiscal 2024, $114.5 million in fiscal 2023 and $39.8 million in fiscal 2022. Failure to increase our revenue as we grow our business could prevent us from achieving profitability or maintaining profitability on a consistent basis. As we pursue our growth strategy, our operating expenses may increase as we expand and diversify our customer base and attract and retain top talent. Our strategic initiatives may be more expensive than we expect, and we may not be able to increase our revenue to offset these increased operating expenses. Our revenue growth may slow, or revenue may decline, for a number of reasons as described elsewhere in this Risk Factors section, which may lead to increased pressure on our profit margins. If we are unable to meet these risks as we encounter them, our business, financial condition and results of operations may suffer.

We must continue to enhance our existing Taegis subscription solutions and their underlying technologies, and develop or acquire new solutions and technologies, or we will lose customers and our competitive position will suffer.

Many of our customers operate in markets characterized by rapidly changing technologies, which require them to utilize a variety of hardware, software applications, operating systems, and networks. As their technologies grow more complex, we expect these customers to face new technological vulnerabilities and increasingly sophisticated methods of cyber-attack. To maintain or increase our market share, we must continue to adapt and improve our Taegis subscription solutions to respond to these evolving cyber-attacks without compromising the high service levels and security that our customers demand. Failure to predict, detect and respond effectively to the changing needs of our customers from these emerging technological advances through the timely development or enhancement of our Taegis subscription solutions could result in reputational harm, loss of customers and cause a negative impact to our business operations and financial condition.

Our future growth is dependent on our ability to continue enhancing the efficacy of the detection and response capabilities within our Taegis software-as-a-service, or SaaS, platform and increasing the interoperability of our Taegis SaaS-based platform with third-party products and services that our customers use. If our Taegis security platform is unable to successfully analyze, categorize and process the increasing number of events, and automate response capabilities, we, our customers and/or partners might fail to identify and respond to significant threat events, which could harm the business and operations of our customers and negatively affect our business reputation, financial condition, and operating results.

Our revenue growth may vary due to global economic conditions, geopolitical uncertainty, and volatile financial markets, which may have an adverse effect on our business and financial condition.

Our company operates on a global basis directly and through our channel partners, serving thousands of customers worldwide. Accordingly, our business, revenue and operating results could be impacted by declining global economic conditions, geopolitical uncertainty and volatile financial markets affecting us, our channel partners, and our existing and potential customers. Impacts of the ongoing conflict between Russia and Ukraine or between Israel and Hamas (including the risk of potential escalation or geographic expansion), and geopolitical tensions between the United States and China could result in further domestic and international regulatory changes, import and export restrictions or other effects on international trade relations, hindering our ability to grow our customer base and continue servicing our existing customers. Economic weakness and uncertainty worldwide could reduce the demand for our Taegis subscription solutions, may prolong sales cycles or cause a reduction in spending by potential customers, or could make it difficult for us to accurately forecast revenue, gross margin, cash flows, and expenses, which could negatively impact our business, financial condition, and results of operations.

We rely on personnel with extensive information security expertise, and the loss of, or our inability to attract and retain, qualified personnel in this highly competitive labor market could harm our business.

Our future success depends on our ability to identify, attract, retain, and motivate qualified personnel. We depend on continued contributions by Wendy K. Thomas, our Chief Executive Officer, and our other senior executives, who have extensive information security expertise. From time to time, there may be changes to our senior management team or other key personnel resulting from termination, departure, or retirement. The temporary or permanent loss of any of these executives or key

personnel could harm our business and distract from the responsibilities of those who must perform the responsibilities of lost executives or key employees or actively participate in the search for personnel to replace them.

We also employ experts in information security, software coding, data science and advanced mathematics to staff our Counter Threat Unit and to support and enhance our Taegis security platform. In addition, we currently employ, and seek to further employ, individuals with cybersecurity sales expertise to continue growing revenue attributable to our Taegis subscription solutions. We face intense competition, both within and outside of the cybersecurity industry, to hire and retain individuals with the requisite expertise, including from companies that have greater resources than we do. As a result of this competition, we may be unable to attract and retain suitably qualified individuals at acceptable compensation levels who have the technical, operational, sales, and/or managerial knowledge and experience to meet our needs. Any failure by us to attract and retain qualified individuals could adversely affect our competitive market position, revenue, financial condition, and results of operations.

Implementation of our plans to strategically realign and optimize our investments with our priorities may not be successful, which could adversely affect our reputation, profitability and financial condition.

On February 7, 2023, we announced a plan to accelerate our transition to a software-as-a-service business through our Taegis security platform and, during the three months ended August 4, 2023, the Company approved continued reorganization actions in alignment with the plan. Specifically, we reduced our workforce and made decisions to optimize and align our facilities and investments with our strategic priorities. These activities may not achieve our strategic priorities to optimize our operating expenses and enhance our prospects for profitable operations. Instead, we may experience additional unexpected costs that could negatively impact our cash flows from operations and liquidity in addition to employee attrition beyond the intended reductions, adverse effects on employee morale, diversion of management's attention, reputational impacts hindering our ability to attract and retain top talent in the future, and cause operational delays as a result of the loss of qualified employees. If we do not realize the anticipated benefits of our plan, our business, reputation, financial condition, and results of operations could be negatively impacted.

We face intense competition, including from larger companies, and may lack sufficient financial or other resources to maintain or improve our competitive position.

The market for our Taegis subscription solutions and other security consulting services is highly competitive, and we expect competition to intensify in the future from both established competitors and new market entrants. Increased competition may result in greater pricing pressure, reductions in profit margins, increases to sales and marketing expenses, replacement by newer or disruptive products or technologies including the increasing use of artificial intelligence within the cybersecurity industry, and risks to holding or increasing our market share.

Many of our existing and potential competitors, particularly in the large enterprise market, enjoy substantial competitive advantages because of their longer operating histories, greater brand name recognition, larger customer bases, more extensive customer relationships, greater customer support resources, broader distribution relationships, more mature intellectual property portfolios, and greater financial and technical resources. Some of our competitors also have made strategic acquisitions or entered into partnerships or other tactical relationships to offer more comprehensive cybersecurity solutions than each competitor could offer individually.

In addition, rapidly changing market conditions and significant technological advancements, partnerships, or acquisitions by our competitors, as well as continued market consolidation, may alter the market for our Taegis subscription solutions. Smaller innovative companies and large competitors making significant research and development investments could develop similar or superior products or services that compete with our Taegis security platform. Additionally, some of our larger competitors maintain broader and more diverse product and service offerings, which may lead customers to choose a competitor's bundled product or service offerings even if the competitor's security solutions have more limited functionality than our Taegis subscription solutions. These competitive pressures within our market could result in price reductions for our Taegis subscription solutions and other cybersecurity offerings, margin erosion, fewer orders, and loss of market share.

If we cannot successfully execute our go-to-market strategy by attracting new customers, retaining existing customers or increasing the annual contract values for Taegis subscription solutions, our business, results of operations and financial performance will be adversely affected.

To achieve revenue growth, we must expand our customer base, retain existing customers, and increase our annual contract values, especially as they relate to our Taegis subscription solutions. In addition to attracting large enterprise and small and medium-sized business customers, our strategy is to continue obtaining non-U.S. customers, government entity customers and customers in other industry sectors in which our competitors may have a stronger position. If we fail to attract new customers, our revenue may decline or cease to grow.

Some customers also may elect not to renew their contracts with us or negotiate to renew them on less favorable terms, resulting in our inability, on a consistent basis, to increase our annual contract values by obtaining advantageous contract

renewals. We offer Taegis subscription solutions on a subscription basis under contracts with initial terms that typically range from one to three years and, as of February 2, 2024, averaged two years in duration. Our customers have no obligation to renew their contracts after the expiration of their initial terms. Our initial contracts with customers may include amounts for hardware, installation, onboarding, and other professional services that may not recur. Further, if a customer renews a contract for a term longer than the preceding term, it may pay us greater total fees than it paid under the preceding contract; however, the average annual fee may be lower because we may offer discounted rates in exchange for longer contract terms. In any of these situations, we must sell additional solutions or enhancements to the Taegis subscription solutions to maintain the same level of annual fees from the customer but may be unable to do so. As a result, existing customers renewing on lower average annual fees or choosing not to renew their contracts with us would negatively impact our revenue, financial condition and operating results.

We generate a significant portion of our revenue from customers in the financial services industry, and changes within that industry, including new or altered compliance obligations or priorities, or an unfavorable review by the federal banking regulatory agencies could reduce demand for our Taegis subscription solutions and other cybersecurity offerings.

We derived approximately 20% of our revenue in fiscal 2024 from financial services institutions and expect to continue to derive a substantial portion of our revenue from customers in that industry. Changes in the industry, including new or altered compliance obligations or regulatory priorities, could adversely affect our revenue, profitability, and financial condition. Technology spending by financial services customers generally has fluctuated, and may continue to fluctuate, based on changing regulations, regulatory priorities and economic conditions, among other factors, including, but not limited to, restructured or reduced technology spending to improve a customer's profitability or financial risk profile or merger and acquisition activity within the financial industry, which may reduce our current and potential customer base, resulting in a smaller market for our Taegis subscription solutions.

Some of our cybersecurity offerings have been deemed to achieve mission-critical functions within our financial institution customers who are regulated by one or more member agencies of the Federal Financial Institutions Examination Council, or the FFIEC. Accordingly, we are subject to periodic examination by the member agencies of the FFIEC. An unfavorable review of our processes and business operations could result in our financial institution customers not being allowed, or not choosing, to continue using our Taegis subscription solutions, which could adversely affect our revenue, financial condition, and results of operations.

If we fail to manage our growth effectively, we may be unable to execute our business plan and maintain high levels of customer service due to operational disruptions.

As our customer base and s Taegis subscription solutions grow, the need to expand our operations may place a strain on our resources, business operations and technology infrastructure. This strain may affect our ability to maintain the quality and successful deployment of our Taegis subscription solutions, degrading customer support after deployment. Our productivity, customer-focused culture, and the quality of our Taegis subscription solutions may be negatively affected if we do not quickly and successfully integrate and train our new employees and channel partners, particularly sales and customer success personnel. In addition, adapting our information technology infrastructure to support our growth and interoperability may require substantial investment, while also investing resources to ensure we maintain and improve our procedures relating to operations, financials and managerial controls reporting. If we are unable to manage our growth, expenses, or business operations efficiently and effectively in accordance with our strategy, our financial condition, results of operations and profitability could be negatively impacted.

Failure to maintain high-quality customer service and support functions, including the quality of the services and support provided by our channel partners, could adversely affect our reputation and sales growth prospects.

Once our Taegis subscription solutions are deployed within our customers' networks, our customers depend on our knowledge and technical expertise to provide support services, including those provided by our channel partners in relation to the Taegis subscription solutions, to ensure the security of their IT systems. The potential for human error in connection with our customer service and support functions, or that of our channel partners, or the internal systems and networks that underpin our ability to provide the Taegis subscription solutions to our customers, even if promptly discovered and remediated, could disrupt customer operations, cause losses for customers, harm our internal operations, lead to regulatory fines or civil litigation, or damage our reputation. In addition, if we, or our channel partners, do not effectively assist our customers with the deployment of our Taegis subscription solutions, timely resolve post-deployment issues or provide effective ongoing support, our ability to retain existing customers, sell additional security solutions or subscriptions to existing customers could suffer and damage our reputation with potential customers. If we, or our channel partners, fail to meet the expectations of, or contractual obligations with, our existing customers, particularly larger enterprises that may require complex and sophisticated support, it may be more difficult to realize our strategy of selling higher-margin and differentiated cybersecurity offerings to those customers.

Our reputation and results of operations may be adversely affected by service level agreements with some of our customers that require us to provide them with credits for service failures or inadequacies.

We have agreements with certain customers that include commitments to providing them with our Taegis subscription solutions and other cybersecurity services at specified levels. If we are unable to meet these commitments, we may be obligated to extend service credits to those customers or the agreements may be terminated by the customer. The damages for failure to meet the service levels are specified in our service level agreements and generally are limited to the fees charged over the prior 12-month period. If disputed by the customer, however, such limits may not be upheld, and we may be required to pay damages that exceed such fees. Repeated or significant service failures or other inadequacies could adversely affect our reputation and results of operations.

Because we recognize revenue ratably over the terms of our Taegis subscription solutions contracts, decreases in sales of these solutions may not immediately be reflected in our results of operations.

The effect of significant downturns in our sales results for our Taegis subscription solutions may not be fully reflected in our results of operations in the current period, making it challenging for investors to effectively evaluate our financial performance.

In fiscal 2024, approximately 83% of our revenue was derived from subscription-based solutions, attributable to Taegis subscription solutions and other subscription-based services, while approximately 17% was derived from professional services engagements. Our subscription contracts typically range from one to three years in duration and, as of February 2, 2024, averaged two years in duration. Revenue related to these contracts is generally recognized ratably over the contract term. As a result, we derive most of our quarterly revenue from contracts we entered into during previous fiscal quarters. Declines in new or renewed contracts and any renewals made at reduced annual dollar amounts occurring in a particular quarter may not be overtly reflected in our revenue for that quarter; however, they would negatively affect revenue in future quarters. Accordingly, the effects of reduced sales or renewals at lower annual dollar amounts may not be fully reflected in our results of operations until future periods.

As of February 2, 2024, we billed approximately 65% of our recurring revenue in advance. We may not be able to adjust our cash outflows to match any decreases in cash received from prepayments if sales decline. In addition, we may be unable to further adjust our cost structure to account for the reduced revenue, which would negatively affect our earnings in future periods. Our subscription model also makes it difficult for us to increase our revenue rapidly through additional sales in any period, since revenue from new customers is recognized ratably over the applicable contract terms.

Our sales cycles are long and unpredictable, and our sales efforts require considerable time and expense, which could adversely affect our results of operations.

Sales of our Taegis subscription solutions usually require lengthy sales cycles, which are typically three to nine months, but can exceed 12 months for larger customers. We spend substantial time, effort, and resources in our sales efforts without any assurance that our efforts will generate long-term contracts. Given current macroeconomic conditions, we may experience further lengthening of sales cycles for our Taegis subscription solutions. Sales to our customers can be complex and require us to educate our customers about our technical capabilities and the use and benefits of our Taegis subscription solutions. Even if we are successful in convincing a prospective customer that the Taegis subscription solutions will increase their defenses against cybersecurity threats, the customer may decide not to, or may delay its decision to, purchase the Taegis subscription solutions for various reasons, which may include budgetary constraints, timing concerns, uncertain economic conditions, unexpected administrative interruptions, or processing and other delays, all of which are outside of our control. If organizations, especially new potential customers, do not decide to adopt our Taegis subscription solutions, our sales efforts will not be economically recognized and revenue will not grow as quickly as anticipated, or at all, which would result in harm to our business, revenue, operating results, and financial condition.

As we continue to expand the sale of our Taegis subscription solutions and other cybersecurity offerings to customers located outside the United States, our business increasingly will be susceptible to risks associated with international sales and operations.

We expect to increase our global presence through new or expanded relationships with local and regional strategic channel partnerships and potentially through acquisitions of other companies. International revenue, which we define as revenue contracted through non-U.S. entities, contributed approximately 37% of our total revenue in fiscal 2024. Operating in international markets requires significant management attention and financial resources and carries legal, regulatory and compliance risks. Our investments and use of other resources to establish operations and seek growth opportunities in other countries may not produce the expected levels of revenue or earnings. Conducting international operations subjects us to a variety of risks, including those described elsewhere in this section. Such risks could negatively affect our overall business, results of operations and financial condition.

Tax matters may materially affect our financial position and results of operations.

Changes in United States and other global tax laws have impacted and will continue to impact our effective global tax rate, which may materially affect our financial position and results of operations. Further, organizations such as the Organisation for Economic Co-operation and Development have published action plans that, if adopted by countries where we do business,

could increase our tax obligations in these countries. Because of the scale of our U.S. and international business activities, some of the applicable changes enacted or proposed, including those relating to cash movements, may increase our global effective tax rate and harm our business. For example, the Tax Cuts and Jobs Act of 2017 eliminates our ability to deduct research and development expenditures in the year incurred, requiring amortization in accordance with Internal Revenue Code Section 174. If this requirement remains effective without modification, it will materially increase our effective tax rate and reduce our operating cash flows. Further, portions of our operations are subject to a reduced tax rate or are tax free under various tax holidays, which periodically expire in whole or in part or may be terminated if certain conditions are not met. Although many of these holidays may be extended when certain conditions are met, we may not be able to meet such conditions. If the tax holidays are not extended, or if we fail to satisfy the conditions of the reduced tax rate, our effective tax rate could increase in the future.

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

Our revenue and expenses denominated in foreign currencies are subject to fluctuations due to changes in foreign currency exchange rates. Although more of our sales contracts are denominated in U.S. dollars, our strategy to grow internationally will lead to more of our sales contracts being denominated in foreign currencies and to an increase in operating expenses incurred outside the United States. Because of significant volatility in foreign currency exchange rates, which has increased in recent periods, sales contracts that are denominated, or operating expenses that are incurred, in currencies other than in the U.S. dollar may negatively impact our financial condition and operating results.

Geopolitical developments, including the ongoing conflict between Russia and Ukraine or between Israel and Hamas (including the risk of potential escalation or geographic expansion), trade tariff developments and international economic tensions between the United States and China, the strengthening of the U.S. dollar and increasing inflation could amplify the volatility of currency fluctuations and increase the real cost of our Taegis subscription solutions and other cybersecurity offerings to our customers outside the United States, which could adversely affect our non-U.S. sales and results of operations. While we do not currently use financial instruments to hedge against the risks associated with currency fluctuations, we may begin to use such instruments to partially mitigate, and increase the predictability of, the impact of fluctuations in net monetary assets denominated in foreign currencies. Any such hedges may not fully protect us against foreign currency risk.

Governmental export or import controls or international sanctions could require additional compliance obligations or may limit our ability to compete in foreign markets.

Our cybersecurity solutions and technologies incorporate encryption technology that may be exported outside the United States only if we obtain an export license or qualify for an export license exception. Following the compliance obligations to ensure the legal export of our Taegis subscription solutions, other cybersecurity offerings and their underlying technologies may create delays in introducing our Taegis subscription solutions, other cybersecurity offerings and their underlying technologies into certain international markets or prevent certain customers from utilizing our solutions and technologies throughout their global infrastructure. Such compliance obligations could hinder our ability to export our Taegis subscription solutions, other cybersecurity offerings and their underlying technologies to some countries altogether. In addition, various countries regulate the import of our Taegis subscription solutions, other cybersecurity offerings and their underlying technologies and have enacted laws that may limit our ability to distribute, and our customers' ability to implement, such solutions, offerings, and technologies within those countries. New or modified export, import, or sanctions restrictions against certain persons, entities, regions, or countries (such as those imposed on Russia in response to the ongoing military conflict between Russia and Ukraine), changes to product classification procedures, or new or altered approaches to the enforcement or scope of existing regulations, could result in delayed adoption by new customers, or decreased use by existing customers, of our Taegis subscription solutions, other cybersecurity offerings and underlying technologies, loss of sales to potential multinational customers, and decreased revenue. Additionally, if we fail to comply with applicable export and import regulations or our sanctions compliance obligations, we may be subjected to fines or other penalties or be unable to export our Taegis subscription solutions, other cybersecurity offerings and their underlying technologies into other countries.

An inability to expand our key distribution relationships could constrain the growth of our business.

We intend to continue strategically growing our business and domestic and international customer base through our channel partners, including distributors, resellers and managed security service providers. Approximately 23% of our revenue in fiscal 2024 was generated through our channel partners, which include referral agents, regional value-added resellers, trade associations, and managed security service providers. We assist these channel partners with selling our Taegis subscription solutions by providing training and other sales support, but such time, effort and expense may not result in increasing our revenue. Our channel partners may be unable to market, sell and support the Taegis subscription solutions successfully, or these partners may not be properly incentivized to sell our Taegis subscription solutions to end-users. Our inability to further develop or maintain these partnerships could reduce sales revenue of our Taegis subscription solutions. If we fail to manage our sales

channels or partnerships effectively, our ability to sell our Taegis subscription solutions may be limited, adversely affecting our revenue growth and financial condition.

Agreements with our partners generally are non-exclusive, and our partners may have more established relationships with one or more of our competitors. If our partners do not successfully market and sell our Taegis subscription solutions, if they choose to place greater emphasis on their own products or services or those offered by our competitors, if they are not properly incentivized to sell our Taegis subscription solutions, or if they fail to meet the expectations of our customers, our ability to expand our business and sell our Taegis subscription solutions may be negatively impacted. Our business also may suffer by losing a substantial number of our partners, failing to recruit additional partners, or partners reducing or delaying the sales of our Taegis subscription solutions.

Even if we do expand relationships with our channel partners, gross margins from sales made by our partners are generally lower than gross margins to us from direct sales. In addition, sales by our partners are more likely to involve collections issues than direct sales, which may contribute to periodic fluctuations in our results of operations.

Our technology alliance partnerships expose us to an array of business risks and uncertainties that could prevent us from realizing the benefits we seek from these partnerships.

We have entered, and intend to continue entering, into technology alliance partnerships with third parties in alignment with our strategic growth plans. Such relationships include technology licensing, joint technology development and integration, research cooperation, co-marketing, and sell-through arrangements. We face risks relating to these partnerships, which could inhibit us from realizing the benefits we seek. Many technology alliance partnerships require significant coordination by both parties and significant time and resource commitments by their technical staffs. In cases where we are developing integrations of our Taegis subscription solutions into a partner's products or services, the integration development process may be more challenging than anticipated, and the risk of difficulties, incompatibility and undetected programming errors or defects may be higher than introducing new products or services. In addition, any particular relationship may be temporary. If we lose a significant technology alliance partner, we may lose the expected benefit of investment into the partnership. Moreover, we could incur significant expenses developing a new strategic alliance or formulating and implementing a strategic alternative.

Real or perceived defects, errors, or vulnerabilities in our Taegis subscription solutions or real or perceived failure of our Taegis subscription solutions to prevent or detect threat actor activity could harm our reputation, cause us to lose customers and expose us to costly litigation.

Our Taegis subscription solutions are complex and may contain defects or errors that cannot be detected until after customer adoption. Such defects may cause our customers to be vulnerable to cyber-attacks, and hackers or other threat actors may misappropriate our customers' data or other assets or otherwise compromise their IT systems. Threat actors frequently change their tactics, techniques, and procedures to access or sabotage technology systems and networks, and attacks generally are not recognized until launched against a target. An advanced attack from a sophisticated threat actor could emerge that our Taegis subscription solutions are unable to detect or prevent. A security breach of a customer's proprietary information could result in significant legal and financial exposure to us, damage our reputation and cause customers to lose confidence in our Taegis subscription solutions, which may adversely affect our business.

If a customer experiences a security breach after adopting our Taegis subscription solutions, even if our Taegis subscription solutions protected the customer from data theft or provided remediation, the customer still may be disappointed with our Taegis subscription solutions and could seek alternative cybersecurity offerings from a competitor. In addition, if any customer that is known to use our Taegis subscription solutions, especially a governmental entity or publicly traded company subject to the U.S. Securities and Exchange Commission's cybersecurity disclosure requirements, is the subject of a publicized cyber-attack, that customer or other current customers may seek to replace our Taegis subscription solutions with those provided by our competitors, regardless of whether the Taegis subscription solutions protected the customer from data theft and provided remediation. Further, even if a cyber-attack were to occur through a customer's security or network devices, applications, or endpoints that we are not contractually obligated to monitor, our reputation could be damaged if there is a misperception that Secureworks monitors all the affected customer's devices, applications, and endpoints.

Any person that circumvents our security measures could misappropriate customer confidential information or other valuable property or disrupt the customer's operations. Because our Taegis subscription solutions provide and monitor information security and may protect valuable information, we still could face liability claims or claims for breach of service level agreements or product warranties. Provisions in our product agreements that limit our exposure to liability claims may not be enforceable in some circumstances or may not protect us fully against such claims and related costs. Alleviating any of these problems could require us to incur significant expense and result in interruptions to, and delays in, the delivery of our Taegis subscription solutions, which could cause us to lose existing or potential customers and damage our business and reputation.

Our inability to expand our development, use and adoption of artificial intelligence, or issues presented in our development, use and adoption of artificial intelligence, could harm our reputation, expose us to liability and cause us to lose customers.

We currently incorporate certain artificial intelligence, or AI, capabilities and large language models, or LLMs, into our Taegis subscription solutions, and we endeavor to continue researching and developing AI capabilities and LLMs within our Taegis subscription solutions. As with many innovative and disruptive technologies, AI and LLMs present risks, challenges, and unintended consequences, many of which cannot be fully appreciated currently. These risks, challenges and unintended consequences could negatively affect further adoption of AI and LLMs in our Taegis subscription solutions, impacting our ability to compete effectively within the cybersecurity industry. AI algorithms and the training methodologies for such algorithms may contain flaws, which could result in ineffective, inadequate, or inaccurate AI capabilities, or could impair customer or partner acceptance of our Taegis subscription solutions leveraging such AI capabilities. Should we develop and incorporate flawed AI capabilities within our Taegis subscription solutions, such flaws would negatively impact our brand and reputation, increase costs to develop and implement new AI capabilities, or lead to a decline in sales revenue. Such impacts would harm our business, financial condition, and results of operations.

Because AI is an emerging technology with a developing legal and regulatory landscape both in the United States and globally, incorporating AI into our Taegis subscription solutions and internal business processes could result in an increased risk of litigation and regulatory non-compliance due to changes in laws or regulations, including, but not limited to, intellectual property, privacy, or data protection. Our obligations to comply with current and future legal and regulatory obligations in the United States and worldwide could require us to incur significant costs to achieve compliance, which would negatively impact our business, financial condition and results of operations, or may hinder our ability to incorporate AI capabilities into our Taegis subscription solutions or distribute our Taegis subscription solutions in certain areas of the globe.

As we continue to develop ways to leverage AI capabilities within our internal business operations to create economic efficiencies for our business, the use of AI capabilities in our internal business operations could present risks and challenges. While we strive to use AI in an ethical and compliant manner, we may be unsuccessful in identifying and/or resolving ethical or legal issues before they arise, which could increase our legal and regulatory risks, including, but not limited to, data privacy and security, leading to the improper transmission of proprietary or sensitive information, whether or not intentional. We could fail to implement and maintain the AI tools we develop, may incur significant research and development costs without achieving the anticipated economic efficiencies we desire, and/or may fail to establish adequate AI governance processes safeguards, which could negatively impact our business, financial condition, and results of operations.

Cyber-attacks or other data security incidents that disrupt our operations or result in the breach or compromise of proprietary or confidential information about us, our workforce, customers, or other third parties could harm our business and expose us to costly regulatory enforcement and other liability.

As a well-known, publicly traded provider of cybersecurity offerings that is subject to the U.S. Securities and Exchange Commission's cybersecurity disclosure requirements, we are a high-profile target for threat actors, and our websites, networks, information systems, solutions and technologies may be selected for sabotage, disruption or misappropriation by cyber-attacks specifically designed to interrupt our business and harm our reputation. Our Taegis subscription solutions frequently involve collecting, filtering, and logging of customer information, while our business operations collect, process, store and dispose of our own human resources, intellectual property, and other information. We also rely, in certain limited capacities, on third-party data management providers and other vendors to host, accept, transmit or otherwise process electronic data in connection with our business operations and activities. Threat actors may seek to penetrate our network security or the security of our third-party service providers and misappropriate or compromise our confidential information or that of our customers or other third parties, create system disruptions or cause shutdowns. In addition, cyber-attacks are increasingly being used in geopolitical conflicts, including Russia's military action in Ukraine and between Israel and Hamas, which may result in increased risk to our customers, our third-party service providers, and our company as a leading cybersecurity solutions provider. We may experience breaches, security incidents or other compromises of our information technology systems. Further, hardware and operating system software and applications that we produce or procure from third parties may contain defects in design or manufacture that could unexpectedly lead to vulnerabilities, or provide access, to our systems and data to a threat actor. Our shift to a remote-friendly organization may also increase our vulnerability, as third-party providers' networks and employees' home networks may pose a significant network security risk.

The costs to address the foregoing security problems and vulnerabilities before or after a cyber or other security incident could be significant, regardless of whether the incident is malicious or the incident resulted from an attack on us directly or on a third-party vendor upon which we rely. Cyber-attacks could compromise or disrupt our internal systems, our Taegis subscription solutions or the systems of our customers or third-party service providers, resulting in interruptions, delays, or cessation of service that could disrupt business operations for us and our customers and that could impede our sales. Remediation efforts may not be successful or timely. Breaches of our security measures or those of our third-party service providers and the unapproved dissemination of proprietary information or sensitive or confidential data about us or our customers or other third parties could expose us, our customers or other affected third parties to a risk of loss or misuse of this information, potentially leading to regulatory enforcement actions, litigation and potential liability for us, and damaging our brand and reputation or otherwise harming our business.

Further, we are a publicly traded company, subject to disclosure obligations set forth by the U.S. Securities and Exchange Commission, or the SEC. We are required to publicly disclose a material security incident within four business days of determining that such an incident is, or is likely, material. As a provider of cybersecurity offerings, such public disclosure could have a negative impact on our brand and reputation and may adversely impact our business, results of operation, and financial condition. In addition, we may file an initial Form 8-K filing before all relevant information is determined or before such information is available. Such a filing may cause a negative impact on our brand and reputation and cause further harm to our business and financial condition even if subsequent developments indicate the incident is not as detrimental as initially reported.

Although we maintain insurance policies that may cover liabilities in certain situations in connection with a threat event or cybersecurity incident, we cannot be certain that the insurance company will cover the claim, that our insurance policy will adequately cover the liability incurred, or that such insurance will continue to be available on commercially reasonable terms. Any claim against our insurance policy, changes to the policy, or increases in premiums or deductibles could have a negative effect on our business, reputation, financial condition, or results of operation.

If our Taegis subscription solutions do not interoperate with our customers' technology infrastructure, our Taegis subscription solutions may become less competitive, and our results of operations may be harmed.

Our Taegis subscription solutions were designed to be open without compromise, effectively interoperating with each customer's existing or future technology infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products and services from multiple security and other technology vendors, and contains products and services that were added over time. As a result, when problems occur in a customer's infrastructure or network, it may be challenging to identify the sources of these problems and avoid disruptions when we update our software or patch to defend against certain vulnerabilities. Ineffective interoperability may increase the risk of a successful cyber-attack or cause a service disruption in violation of our service level agreements, each of which may increase the risk of litigation, cause reputational harm, or reduce our revenue generation.

Loss of our right or ability to use various third-party technologies could result in short-term disruptions to our business and may cause harm to our brand and reputation.

We rely on certain third-party vendors to provide technology to perform certain critical business functions, some of which are incorporated into our Taegis subscription solutions. We may seek to utilize additional third-party technologies in our Taegis subscription solutions, and we will continue to use technology to assist us as we operate our business. However, any unanticipated loss of our rights to use third-party or other technologies could result in business delays or hinder our ability to produce or deliver our Taegis subscription solutions until we identify, evaluate, and integrate equivalent technologies. If any of the technologies we license or purchase from others, or functional equivalents of these technologies, are no longer available to us or are no longer offered to us on commercially reasonable terms, then we may be required to either find another third-party vendor or develop these capabilities ourselves, which could result in increased costs to our business or cause delivery delays for Taegis subscription solutions. We also might have to limit the features available in our current or future Taegis subscription solutions and other cybersecurity offerings. If we fail to maintain or renegotiate some of our technology agreements with third parties or are unable to anticipate the loss of our rights to use such third-party technologies, we could face significant delays and diversion of resources in attempting to license and integrate other technologies with equivalent functions. Any inability to procure and implement suitable replacement technologies in a timely manner could adversely affect our business and results of operations by impeding delivery of our Taegis subscription solutions.

In addition, any errors or defects in third-party technologies or any inability to utilize third-party technologies as intended, may negatively impact our ability to perform business activities or provide our Taegis subscription solutions to customers. Such errors, defects or vulnerabilities involving third-party technologies we utilize may also require public disclosure if we determine that they would constitute a material security incident under the SEC's cybersecurity disclosure rules. Where a disclosure is required to report a security incident involving the use of third-party technologies, our brand and reputation may be negatively impacted, which could further affect our business, results of operations and financial condition. Although we take steps to implement appropriate risk management controls over such third-party technologies, any failure to appropriately assess, test and mitigate the risks associated with the implementation of third-party technologies may cause delays in our business activities or delivery of our Taegis subscription solutions to customers, which could hinder our ability to restore operations in the event of a third-party failure.

New and evolving information security, cybersecurity and data privacy laws and regulations may result in increased compliance costs, impede the development or performance of our Taegis subscription solutions, and cause us to incur monetary or other penalties.

We are currently subject, and may become further subject, to federal, state and foreign laws and regulations regarding the privacy and protection of personal data or other potentially sensitive information. These laws and regulations address a range of issues, including data privacy, cybersecurity and restrictions or technological requirements regarding the collection, use, storage, protection, retention, or transfer of data. The regulatory frameworks for data privacy and cybersecurity issues that have

been instituted around the world can vary substantially from jurisdiction to jurisdiction, are rapidly evolving and are likely to remain uncertain for the foreseeable future.

In the United States, federal, state, and local governments have enacted data privacy and cybersecurity laws (including data breach notification laws, personal data privacy laws and consumer protection laws). For example, the California Privacy Rights Act, referred to as the CPRA, which updated the California Consumer Privacy Act of 2018, referred to as the CCPA, went into effect on January 1, 2023, and imposes obligations on certain businesses, service providers, third parties and contractors. These obligations include providing specific disclosures in privacy notices and granting California residents certain rights related to their personal data. The CCPA imposes statutory fines for non-compliance (up to $7,500 per violation). Other states have proposed privacy laws with similar compliance obligations.

Internationally, most of the jurisdictions in which we operate have established their own data security and privacy legal frameworks with which we or our customers must comply. For example, in the European Economic Area, the General Data Protection Regulation, or GDPR, imposes stringent operational and governance requirements for companies that collect or process personal data of residents of the European Union and Iceland, Norway and Lichtenstein. The GDPR also provides for significant penalties for non-compliance, which can be up to four percent of annual worldwide "turnover" (a measure similar to revenues in the United States). Following the withdrawal of the United Kingdom from the European Union (i.e., Brexit), and the expiry of the Brexit transition period which ended on December 31, 2020, the European Union GDPR has been implemented in the United Kingdom, referred to as the U.K. GDPR. The U.K. GDPR sits alongside the U.K. Data Protection Act 2018, which implements certain derogations in the E.U. GDPR into English law. The requirements of the U.K. GDPR, which are (at this time) largely aligned with those under the E.U. GDPR, may lead to similar compliance and operational costs and potential fines.

Some countries are considering or have enacted legislation requiring local storage and processing of data that could increase the cost and complexity of delivering our services. In addition, under the GDPR and a growing number of other legislative and regulatory requirements globally, jurisdictions are adopting consumer, regulator and customer notification obligations and other requirements in the event of a data breach.

The costs of compliance with, and other burdens imposed by, these laws and regulations may become substantial and may limit the use and adoption of our Taegis subscription solutions in new or existing locations, require us to change our business practices, impede the performance and development of our Taegis subscription solutions, lead to significant fines, penalties or liabilities for noncompliance with such laws or regulations, including through individual or class action litigation, or result in reputational harm. We also may be subject to claims of liability or responsibility for the actions of third parties with which we interact or upon which we rely in relation to various services, including, among others, vendors, and business partners.

If we are unable to maintain and enhance our brand, our revenue and profitability could be adversely affected.

We believe that it is critical to maintain and enhance the Secureworks brand to grow our relationships with our existing and potential customers, channel partners, technology alliance partners, and employees in order to expand our revenue and profitability. However, our brand promotion activities may be unsuccessful. Successful promotion of our brand will depend on our marketing and public relations efforts, our ability to continue offering high-quality cybersecurity solutions and our ability to successfully differentiate our Taegis subscription solutions and other cybersecurity offerings from the services offered by our competitors.

We believe our association with Dell has helped us to build relationships with many of our customers because of its globally recognized brand and the favorable market perception of the quality of its products. We have entered into a trademark license agreement with Dell Inc. under which Dell Inc. has granted us a non-exclusive, royalty-free worldwide license to use the trademark "DELL," solely in the form of "SECUREWORKS-A DELL COMPANY," in connection with our business and products, services and advertising and marketing materials related to our business. Under the agreement, our use of the Dell trademark in relation to any product, service or otherwise is subject to Dell Inc.'s prior review and written approval, which may be revoked at any time. The agreement is terminable at will by either party and, if terminated, we must cease all use of the Dell trademark in connection with any product, service, or material. If we discontinue our association with Dell in the future, we may be unable to attract new customers and channel partners.

We may expand through acquisitions of other companies, which could divert our management's attention and company resources from our current business, resulting in unforeseen operating difficulties, increased costs and dilution to the ownership interests of our stockholders.

We may make strategic acquisitions of other companies in addition to organic growth. We may not realize the anticipated benefits of any acquisition we are able to complete. We could experience unforeseen operating difficulties in assimilating or integrating the businesses, technologies, services, products, personnel, or operations of acquired companies, especially if the key personnel of any acquired company choose not to work for us. To complete an acquisition, we may be required to use a substantial amount of our cash, sell or use equity securities, or incur debt to secure additional funds. If we raise additional funds

through issuances of equity or convertible debt securities, our existing stockholders could suffer significant dilution of their ownership, and any new equity securities we issue could have rights, preferences, and privileges senior to those of our Class A common stock. Any debt financing obtained by us in the future could involve restrictive covenants that would limit our capital-raising activities and operating flexibility. In addition, we may not be able to obtain additional financing on terms favorable to us or at all, which could limit our ability to engage in acquisitions or develop new products or technologies.

Earthquakes, fires, power outages, floods, terrorist attacks, geopolitical and military conflicts, public health issues, and other catastrophic events could disrupt our business and ability to serve our customers and could have a material adverse effect on our business, supply chain, results of operations or financial condition.

A significant natural disaster, such as an earthquake, a fire, a flood or a significant power outage, geopolitical conflicts, such as the ongoing military action between Russia and Ukraine or between Israel and Hamas (including the risk of potential escalation or geographic expansion), increasing tensions between the United States and China, or a widespread public health issue including a pandemic such as COVID-19, could have a material adverse effect on our business, supply chain, results of operations or financial condition. We rely on public cloud providers to sustain our operations. While these public cloud providers are capable of sustaining our operations, a failure of these public cloud providers could disrupt our ability to serve our customers for a period of time.

In addition, our ability to deliver our Taegis subscription solutions as agreed upon with our customers depends on the ability of our supply chain, manufacturing vendors or logistics providers to deliver products or perform services we have procured from them. If any natural disaster, terrorist attacks, war, geopolitical turmoil, civil unrest, or other catastrophic event, including widespread public health issues, impairs the ability of our vendors or service providers to provide timely support or disrupts our Taegis subscription solutions or other cybersecurity offerings, our ability to perform our customer engagements may suffer. Disruptions, such as those caused by COVID-19, resulted in restrictions on the ability of our employees or the employees of our customers, vendors, channel partners, or suppliers to travel, as well as closures of our facilities or the facilities of these third parties. Any expansion of hostilities into nearby countries related to the ongoing conflict between Russia and Ukraine may have a direct impact on our employees and operations in Romania as well as on the businesses of our customers, vendors and suppliers. Any restrictions or closures could affect our ability to sell our Taegis subscription solutions, develop and maintain customer relationships or render other security services, such as our consulting services, may adversely affect our ability to generate revenues or might lead to inadvertent breaches of contract by us or by our customers, channel partners, vendors or suppliers.

While we did not experience a reduction in customer demand or lengthening in sales cycles during fiscal 2024 that we believe is attributable to COVID-19, in prior fiscal periods we did experience such reductions in demand and elongated sales cycles, which could again impact our results in future periods. Pandemics such as COVID-19 are impossible to predict in terms of extent and severity; therefore, should we encounter another pandemic, we might experience curtailed customer spending, delayed or deferred purchasing decisions, elongated sales cycles, and delays in receiving customer or partner payments. These effects, individually or in the aggregate, could have a material negative impact on our business and future financial results.

Risks Related to Intellectual Property

We rely in part on patents to protect our intellectual property rights, and if our patents are ineffective in doing so, third parties may be able to use certain aspects of our proprietary technology without compensating us.

As of February 2, 2024, we owned 58 issued patents and 8 pending patent applications in the United States and six issued patents and 12 pending patent applications outside the United States. Any failure of our patents and patent strategy to adequately protect our intellectual property rights could harm our competitive position. The legal systems of some countries do not favor the aggressive enforcement of patents, and the laws of other countries may not allow us to protect our inventions with patents to the same extent as U.S. laws. Changes in patent laws, implementing regulations or the interpretation of patent laws may diminish the value of our rights. Our competitors may design around technologies we have patented, licensed, or developed. In addition, the issuance of a patent does not necessarily give us the right to practice the patented invention. Third parties may have blocking patents that could prevent us from marketing our Taegis subscription solutions and other cybersecurity offerings or practicing our own patented technology. If any of our patents is challenged, invalidated, or circumvented by third parties, and if we do not own or have exclusive rights to other enforceable patents protecting our Taegis subscription solutions or other technologies, competitors and other third parties could market products or services and use processes that incorporate aspects of our proprietary technology without compensating us, which may have an adverse effect on our business.

If we are unable to protect, maintain or enforce our non-patented intellectual property rights and proprietary information, our competitive position could be harmed, and we could be forced to incur significant expenses to enforce our rights.

Our business relies in part on non-patented intellectual property rights and proprietary information, such as trade secrets, confidential information, and know-how, all of which offer limited protection to our technology. The legal standards relating to

the validity, enforceability, and scope of protection of intellectual property rights in the information technology and software industries are highly uncertain and evolving. While we regularly enter into non-disclosure and confidentiality agreements with employees, vendors, customers, channel partners, technology alliance partners, and other third parties, these agreements may be breached or otherwise fail to prevent disclosure of our proprietary or confidential information effectively or to provide an adequate remedy in the event of such unauthorized disclosure. Our ability to police such misappropriation or infringement is uncertain, particularly in other countries. Costly and time-consuming litigation could be necessary to enforce and determine the scope of our proprietary rights, and our failure to maintain trade secret protection could adversely affect our competitive business position.

Claims by others that we infringe their proprietary technology could harm our business and financial condition.

Third parties could claim that our technologies and the processes underlying our Taegis subscription solutions infringe or otherwise violate their proprietary rights. The software and technology industries are characterized by the existence of numerous patents, copyrights, trademarks, and trade secrets, causing frequent litigation, including by non-practicing entities, based on allegations of infringement or other violations of intellectual property rights. We expect that such claims may increase as competition in the cybersecurity market further intensifies, as we introduce new cybersecurity offerings, including within our Taegis subscription solutions (including by increasing our global presence in areas where we currently do not operate) and as the overlap of our cybersecurity offerings continue to occur with our competitors.

Our use of open-source technology could require us in some circumstances to make the source code of our modifications to that technology available to the public, which could include source code of our proprietary technologies, restricting our ability to commercialize our cybersecurity offerings.

Some portions of our cybersecurity offerings and technologies incorporate open-source software licensed by its authors or by other third parties. To the extent that we use such software, we face risks relating to the scope and requirements of common open-source software licenses. Some of these open-source licenses contain requirements that we make available the source code for certain modifications or derivative works that we create based on the open-source software and that we license such modifications or derivative works under the terms of a particular open-source license or another license granting third parties certain rights of further use. If we combine our proprietary technology with open-source software in a certain manner, we could face periodic claims from third parties claiming ownership of, or demanding that we release, the open-source software or derivative works that we developed using such software, which could include our proprietary source code, or the third parties could seek to enforce the terms of the applicable open-source license.

Our ability to commercialize our cybersecurity offerings or technologies incorporating open-source software may be restricted because, among other reasons, open-source license terms may be ambiguous and could result in unanticipated or uncertain obligations regarding our cybersecurity offerings, litigation, or loss of the right to use such software or the modifications or derivative works we develop based on such software. Therefore, there is a risk that the terms of these open-source licenses will be construed in a manner that imposes unanticipated conditions or restrictions on our ability to commercialize our cybersecurity offerings utilizing such software. As a result, we may be required to seek licenses from third parties to continue offering certain cybersecurity offerings, re-engineer our technology to remove the open-source software or discontinue offering our certain cybersecurity offerings if re-engineering is not commercially reasonable.

Risks Related to Our Relationship with Dell and Dell Technologies

Our inability to favorably resolve any potential conflicts or disputes that arise between us and Dell or Dell Technologies relating to our past and ongoing relationships may adversely affect our business and prospects.

Potential conflicts or disputes may arise between us and Dell or Dell Technologies in a variety of areas relating to our past or ongoing relationships, including:

- intellectual property, tax, employee benefits, indemnification, and other matters arising from our agreements and relationship with Dell;
- employee retention and recruiting;
- business combinations involving us;
- our ability to engage in activities with certain channel, technology alliance or other marketing partners;
- sales or dispositions by Dell Technologies of all or any portion of its beneficial ownership interest in us;
- dilution in the ownership or voting interest of Dell Technologies resulting from the issuance of additional shares of Class A common stock authorized and available under the SecureWorks Corp. 2016 Long-Term Incentive Plan;
- sales of our Taegis subscription solutions and other cybersecurity offerings by Dell Technologies in accordance with our agreements with Dell or Dell Technologies;
- the nature, quality and pricing of services Dell has agreed to provide to us;

- business opportunities that may be attractive to both us and Dell;
- Dell's ability to use and sublicense patents that we have licensed to Dell under a patent license agreement; and
- product or technology developments or marketing activities that may require consent of Dell or Dell Technologies.

The resolution of any potential conflicts or disputes between us and Dell or Dell Technologies over these or other matters may be less favorable to us than the resolution we might achieve if we were dealing with an unaffiliated party.

If Dell Technologies, Dell or Dell Technologies' other affiliates, or Silver Lake or its affiliates, engage in the same or similar type of business we conduct, enter partnerships with our competitors, or take advantage of business opportunities that might be attractive to us, our ability to operate successfully and expand our business may be hampered.

Our certificate of incorporation, or charter, provides that, except as otherwise agreed in writing between us and Dell Technologies, Dell or Dell Technologies' other affiliates (other than us or our controlled affiliates), referred to as the Dell Technologies Entities, have no duty to refrain from:

- engaging in the same or similar activities or lines of business as those in which we are engaged;
- doing business with any of our customers, partners or vendors; or
- employing, or otherwise engaging or soliciting for such purpose, any of our officers, directors or employees.

In addition, under our charter, Silver Lake and its affiliates, referred to as the Silver Lake Entities, which are significant stockholders in Dell Technologies, have no duty to refrain from any of the foregoing activities except as otherwise agreed in writing between us and a Silver Lake Entity. These and other related provisions of our charter may result in the Dell Technologies Entities and the Silver Lake Entities having rights to corporate opportunities in which both we and the Dell Technologies Entities or the Silver Lake Entities have an interest, which could impede our ability to operate successfully and expand our business.

In accordance with agreements between us and Dell or Dell Technologies, we have limited capabilities to pursue opportunities to raise capital, acquire other companies, or undertake other transactions without Dell's or Dell Technologies' express consent, which may limit our ability to grow our business.

To preserve its ability to effectuate a future tax-free spin-off of our company, or certain other tax-free transactions involving us, Dell Technologies is required to maintain "control" of us within the meaning of Section 368(c) of the Internal Revenue Code, which is defined as 80% of the total voting power and 80% of all other classes of stock. In addition, to preserve its ability to consolidate with us for tax purposes, Dell Technologies generally is required to maintain 80% of the voting power and 80% of the value of our outstanding stock. We have entered into an amended and restated tax matters agreement with Dell Technologies that restricts our ability to issue any stock, issue any instrument that is convertible, exercisable or exchangeable into any of our stock or which may be deemed to be equity for tax purposes, or take any other action that would be reasonably expected to cause Dell Technologies to beneficially own stock in us that, on a fully diluted basis, does not constitute "control" within the meaning of Section 368(c) of the Internal Revenue Code or causes us to become deconsolidated with respect to the Dell Technologies affiliated group, unless we have obtained Dell's prior written consent. We also have agreed to indemnify Dell Technologies for any breach by us of the tax matters agreement. As a result, we may be prevented from raising equity capital or pursuing acquisitions or other growth initiatives that involve issuing equity securities as consideration.

Upon our deconsolidation from the Dell Technologies affiliated tax group, we may be unable to collect reimbursements or fully utilize related tax assets, and we might be obligated to pay to Dell Technologies certain previously realized or future tax benefits, which may adversely affect our results of operations and financial condition.

We may have payment obligations or be unable to collect reimbursements from Dell Technologies upon the deconsolidation of our Company since we will become ineligible for inclusion in the Dell Technologies affiliated tax group, which may have adversely effect on our cash flow and liquidity, the severity of which depends on the magnitude of such payments. On August 1, 2015, we entered into a tax matters agreement, or TMA, with Dell Technologies whereby, in general, Dell Technologies would reimburse us for any amounts by which our tax assets reduce the amount of tax liability owed by the Dell Technologies affiliated tax group. Under the TMA, as amended and restated in June 2023, upon deconsolidation, our Company will only fully utilize our income tax assets to the extent we generate sufficient income. On or about March 13, 2024, Dell's economic ownership of our Company dropped below 80%, and Dell Technologies can no longer utilize our tax assets for which we currently receive reimbursement. If we are unable to generate sufficient taxable income to fully utilize our tax assets, our operations and financial condition could be adversely affected. In addition, under the TMA, as amended and restated in June 2023, upon deconsolidation for tax purposes from the Dell Technologies affiliated tax group, we may be required to pay Dell Technologies in cash amounts for the benefits we previously realized under the TMA and for certain benefits Dell Technologies will no longer be receiving because of the allocation of taxes and tax assets upon the deconsolidation. The amounts that we may have to pay to Dell Technologies could reflect benefits that we have already realized or may relate to benefits that we will not

realize until future periods. Such payments, if significant, could materially and adversely affect our results of operations and financial condition.

Risks Related to Ownership of Our Class A Common Stock

The market price for our Class A common stock has been and is likely to continue to be volatile or may decline regardless of our operating performance.

The stock markets, and securities of companies within the technology and software industries particularly, have experienced extreme price and volume fluctuations that have affected and continue to affect the market prices of equity securities of many technology companies similarly situated to us. For many technology and software companies, the fluctuations in the stock prices have been unrelated or disproportionate to their operating performance. The economic impact and uncertainty of changes in the inflation, interest rate, and the macroeconomic and geopolitical environments, including Russia's ongoing conflict with Ukraine and the ongoing conflict between Israel and Hamas (including the risk of potential escalation or geographic expansion), have exacerbated price and volume volatility in both the overall stock markets and the market price of our Class A common stock. The market price of our Class A common stock may continue to fluctuate significantly in response to a variety factors, many of which are beyond our control, including:

- actual or anticipated changes or fluctuations in our operating results;
- the financial forecasts and guidance we may provide to the public, any changes in our forecasts or guidance, or our failure to meet the forecasts or guidance;
- reactions by financial analysts, industry analysts or investors to our press releases, other public announcements, and SEC filings;
- failure of financial analysts to maintain coverage of us, changes in financial estimates by any financial analysts who follow our company, or our failure to meet the financial estimates or the expectations of investors;
- announcements by us or our competitors of new or enhanced offerings, or new or terminated significant contracts, commercial relationships or capital commitments;
- rumors and market speculation involving us or our competitors;
- material changes in investor confidence in the market for technology stocks or the stock market in general;
- changes in industry analyst or investor perceptions of us, the benefits of our offerings and the industries in which we operate;
- periodic price and volume fluctuations in the overall stock market;
- changes in operating performance and/or stock market valuations of other technology companies generally, or those in our industry in particular;
- actual or anticipated general developments in our business or our competitors' businesses or the competitive landscape;
- litigation involving us, our industry, both, or investigations by regulators into our operations or those of our competitors;
- developments or disputes concerning our intellectual property rights or our Taegis subscription solutions or other cybersecurity offerings, or third-party proprietary rights;
- rumored, announced or completed acquisitions of businesses or technologies by us or our competitors;
- breaches of, or failures relating to, privacy, data protection or information security;
- new laws or regulations or new interpretations of existing laws or regulations applicable to our business, including, but not limited to, the SEC's finalized cybersecurity disclosure requirements;
- any major changes to the composition of our management team or our board of directors;
- general economic conditions, whether in the United States or globally, and slow growth of our markets; and
- other events or factors, including those resulting from war, pandemics, geopolitical conflict, trade embargoes, incidents of terrorism, or any responses to such events.

As long as Dell Technologies Inc. controls us, the ability of our other stockholders to influence matters requiring stockholder approval will be limited.

As of February 2, 2024, Dell Technologies owned, indirectly through Dell Inc. and Dell Inc.'s subsidiaries, all 70,000,000 outstanding shares of our Class B common stock, which represented approximately 81.0% of our total outstanding shares of common stock and approximately 97.7% of the combined voting power of both classes of our outstanding common stock.

Our other stockholders will not be able to affect the outcome of any stockholder vote in which holders of the Class B common stock are entitled to vote as long as Dell Technologies controls the majority of the voting power of our outstanding common stock. Generally, Dell Technologies can control, directly or indirectly and subject to applicable law, significant matters affecting us, including, among others, the election and removal of our directors, and determinations with respect to business

combinations, dispositions of assets or other extraordinary corporate transactions. If Dell Technologies does not provide its required affirmative vote on matters requiring stockholder approval allowing particular corporate actions when requested, we will not be able to take such action, and, as a result, our business and our results of operations may be adversely affected.

While it is not expected to occur, Dell Technologies could have interests that differ from, or conflict with, the interests of our other stockholders, and could cause us to take corporate actions even if such actions are not in the interest of our company or our other stockholders, or such actions are opposed by our other stockholders. For example, the voting control possessed by Dell Technologies could discourage or prevent a change in control of our Company even if some of our other stockholders might favor such a transaction.

We do not expect to pay any dividends on our Class A common stock for the foreseeable future.

In accordance with our current business strategy, we intend to retain the profits we make to finance the operation and continued growth of our business; therefore, we currently do not expect to pay any cash dividends on our Class A common stock for the foreseeable future. Accordingly, for investors to realize any future profit on their investments, they must rely on the sale of our Class A common stock after its value increases.

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

Our Class B common stock has ten votes per share and our Class A common stock has one vote per share. The limited ability of holders of our Class A common stock to influence matters requiring stockholder approval may adversely affect the market price of our Class A common stock.

In addition, certain stock indices, including, but not limited to, FTSE Russell and S&P Dow Jones, have adopted eligibility criteria to exclude new companies with multiple classes of common stock from being added to certain of their stock indices. Under the current criteria, our dual-class capital structure might make our Class A common stock ineligible for inclusion in certain indices, which may cause certain mutual funds, exchange-traded funds, and other investment vehicles that track certain indices may not invest in our stock. Other major stock indices might adopt similar requirements in the future. It is challenging to gauge whether the exclusion from any indices will affect the financial valuation and market price of such an excluded company. It is possible that such policies could depress the financial valuation and stock price of a public company excluded from such indices compared to other companies that do not have multi-class capital structures.

As a "controlled company" under the marketplace rules of the Nasdaq Stock Market, we may rely on exemptions from certain corporate governance requirements that provide protection to stockholders of companies that are subject to such requirements.

As of February 2, 2024, Dell Technologies beneficially owns more than 50% of the combined voting power of both classes of our outstanding shares of common stock. As a result, we are a "controlled company" under the marketplace rules of the Nasdaq Stock Market, or Nasdaq, and eligible to rely on exemptions from Nasdaq corporate governance requirements that generally obligate listed companies to maintain a board of directors having a majority of independent directors and compensation and nominating committees composed solely of independent directors. We currently rely on the exemption from the requirement to maintain a board of directors having a majority of independent directors. Although we do not currently rely on the other exemptions from Nasdaq's corporate governance requirements pertaining to the composition of compensation and nominating committees, we may decide to avail ourselves of one or more of these exemptions in the future. During any period in which we do so, investors may not have the same protections afforded to stockholders of companies that must comply with all of Nasdaq's corporate governance requirements. Our status as a controlled company could make our Class A common stock less attractive to some investors or otherwise adversely affect its trading price.

Future sales, or the perception of future sales, of a substantial number of shares of our Class A common stock could depress the trading price of our Class A common stock.

Sales of a substantial number of shares of our Class A common stock in the public market, or the perception that these sales may occur, could adversely affect the market price of the Class A common stock.

As of February 2, 2024, we have outstanding 16,392,287 shares of our Class A common stock and 70,000,000 shares of our Class B common stock. The shares of Class A common stock are freely tradeable without restriction or further registration under the Securities Act of 1933, or Securities Act, unless these shares are held by our "affiliates," as that term is defined in Rule 144 under the Securities Act, or Rule 144. As of February 2, 2024, Dell Technologies owned, indirectly through its subsidiary Dell Inc. and through Dell Inc.'s subsidiaries, no shares of our Class A common stock and all 70,000,000 outstanding shares of our Class B common stock. The shares of our Class A common stock eligible for resale by our affiliates under Rule 144, subject to the volume limitations and other requirements of Rule 144, include the 70,000,000 shares of Class A common stock issuable upon conversion of the same number of shares of our Class B common stock that are outstanding.

We have entered into a registration rights agreement with Dell Marketing L.P. (the record holder of our Class B common stock), Michael S. Dell, the Susan Lieberman Dell Separate Property Trust, MSDC Denali Investors, L.P., MSDC Denali EIV,

LLC and the Silver Lake investment funds that own Dell Technologies common stock in which we have granted them and their respective permitted transferees demand and piggyback registration rights with respect to the shares of our Class A common stock and Class B common stock held by them from time to time. Registration of those shares under the Securities Act would permit the stockholders under the registration rights agreement to sell their shares into the public market.

Our charter designates the Court of Chancery of the State of Delaware as the sole and exclusive forum for certain types of actions and proceedings that may be initiated by our stockholders, which could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or with our directors, our officers or other employees, or our majority stockholder.

Our charter provides that, unless we consent in writing to the selection of an alternative forum, the Court of Chancery of the State of Delaware will, to the fullest extent permitted by law, be the exclusive forum for:

- any derivative action or proceeding brought on our behalf;
- any action asserting a claim of breach of a fiduciary duty owed, or other wrongdoing, by any of our directors, officers or other employees, or stockholders to us or our stockholders;
- any action asserting a claim arising pursuant to any provision of the Delaware General Corporation Law or as to which the Delaware General Corporation Law confers jurisdiction on the Court of Chancery of the State of Delaware; and
- any action asserting a claim governed by the internal affairs doctrine.

Any person purchasing or otherwise acquiring any interest in shares of our capital stock is deemed to have received notice of and consented to the foregoing provisions. This choice of forum provision may limit a stockholder's ability to bring a claim in a judicial forum that it finds more favorable for disputes with us or with our directors, our officers or other employees, or our other stockholders, including our majority stockholder, which may discourage such lawsuits against us and such other persons. Alternatively, if a court were to find this choice of forum provision inapplicable to, or unenforceable in respect of, one or more of the specified types of actions or proceedings, we may incur additional costs associated with resolving such matters in other jurisdictions, which could adversely affect our business, results of operations and financial condition.

Our choice of forum provision is intended to apply to the fullest extent permitted by law to the types of actions and proceedings specified above, including, to the extent permitted by the federal securities laws, to lawsuits asserting claims under such actions and proceedings and claims under the federal securities laws. Application of the choice of forum provision may be limited in some instances by applicable law. Section 27 of the Securities Exchange Act of 1934, or Exchange Act, creates exclusive federal jurisdiction over all suits brought to enforce any duty or liability created by the Exchange Act or the rules and regulations thereunder. As a result, the choice of forum provision will not apply to actions arising under the Exchange Act or the rules and regulations thereunder. Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over suits brought to enforce any duty or liability created by the Securities Act or the rules and regulations thereunder, subject to a limited exception for certain "covered class actions." Due to current litigation, there is uncertainty as to whether a court would enforce the choice of forum provision with respect to claims under the Securities Act. Our stockholders will not be deemed, by operation of our choice of forum provision, to have waived claims arising under the federal securities laws and the rules and regulations thereunder.

We are obligated to develop and maintain proper and effective internal control over financial reporting and any failure to maintain the adequacy of our internal controls may adversely affect investor confidence in our company, potentially resulting in a negative impact on the value of our Class A common stock.

We are required, pursuant to Section 404 of the Sarbanes-Oxley Act to furnish a report by our management each year on the effectiveness of our internal control over financial reporting. We are required to also disclose significant changes made in our internal control procedures on a quarterly basis. In addition, our independent registered public accounting firm is required annually to express an opinion as to the effectiveness of our internal control over financial reporting.

During the evaluation and testing process of our internal controls, if we identify one or more material weaknesses in our internal control over financial reporting, we will be unable to assert that our internal control over financial reporting is effective. We may experience material weaknesses or significant deficiencies in our internal control over financial reporting. Any failure to maintain internal control over financial reporting could severely inhibit our ability to report accurately our financial condition or results of operations. If we are unable to conclude that our internal control over financial reporting is effective, or if our independent registered public accounting firm determines we have a material weakness in our internal control over financial reporting, investors could lose confidence in the accuracy and completeness of our financial reports, the market price of our Class A common stock could decline, and we may be subject to sanctions or investigations by the SEC or other regulatory authorities. Failure to remedy any material weakness in our internal control over financial reporting, or to implement or maintain other effective control systems required of public companies, also could restrict our future access to the capital markets.

Item 1B. Unresolved Staff Comments

None.

Item 1C. Cybersecurity

As a provider of cybersecurity offerings, we understand that threat actors are increasingly becoming more sophisticated and extremely effective at compromising information and operational technologies. As this trend continues, it is vital that we have processes in place to timely and accurately detect, mitigate, respond to, and remediate cybersecurity incidents, threats or vulnerabilities that may create a material risk to our Company, that could, if the risk occurs, materially impact our Company, including, but not limited to, our financial condition and results of operations. For additional information regarding the variety of material risks we may face, including, but not limited to, those that relate to cybersecurity, refer to "Part I – Item 1A – Risk Factors" in this report.

While our enterprise risk management program considers cybersecurity risks alongside other significant business risks, we also maintain robust cybersecurity processes, technologies, and controls to aid our efforts to identify, assess, and manage material risks posed to our Company. Annually, we conduct an information security risk assessment, and we periodically review our security architecture and assess third-party vendors that we use. We continuously monitor for security risks and vulnerabilities posed by the technological tools and people enabled processes we utilize. In addition, we employ a range of tools and services, including network and endpoint monitoring, third-party penetration testing, and periodic tabletop exercises to ensure timely discovery of, response to, and remediation of, security incidents. While we assess and monitor for security risks and vulnerabilities posed by 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 our assessment and monitoring of such third parties will prevent or mitigate the risk of any compromise or failure in the information assets they own or control.

Our internal security controls are designed to align with standards set by the National Institute of Standards and Technology, or NIST, and the International Organization for Standardization, or ISO. In addition, our security processes are assessed by the Federal Financial Institutions Examination Council, or FFIEC, due to our status as a cybersecurity provider to several financial institutions and financial services organizations. Our security processes also are tested or assessed in accordance with the Sarbanes-Oxley Act of 2002, compliance obligations under the Service Organization Control Type 2 auditing procedure, or SOC2, and applicable privacy laws, both in the United States and internationally.

Our internal security controls and our cybersecurity processes, technologies, and controls are governed by the Company's Chief Security Officer and Chief Information Security Officer, or CISO, who reports quarterly on security matters, including cybersecurity, to the Company's internal Enterprise Risk Committee. Our CISO has been with us since 2011 and has worked in cybersecurity for over 21 years. In addition, as a provider of cybersecurity offerings, we employ numerous leaders who have experience in the cybersecurity industry. All Company employees must complete required annual information security and privacy training, which are reviewed and updated annually. They also receive ongoing security awareness education through emails, presentations, and other available training materials on our intranet.

Pursuant to the Board's oversight of the Company's operational risk management, the Board has designated authority and responsibility to its Audit Committee to regularly review our processes and procedures for managing cybersecurity risks and handling cybersecurity incidents. The Audit Committee receives quarterly updates from the CISO and others from the CISO's security team regarding our security programs, including a review of cybersecurity risks, threats, and vulnerabilities. Additionally, the Board of Directors receives an annual report on the cybersecurity threat landscape from at least one senior leader.

Our Company, through the leadership of the CISO, utilizes a variety of security governance and operational processes to manage our secure use of technology, including, but not limited to, the management of risks from insiders, third-parties, security controls, vulnerabilities, threats, and incident response.

We have adopted a comprehensive cybersecurity assessment framework, which is integrated into our security team's processes to ensure cybersecurity incidents are assessed and escalated in a timely manner, so that certain leaders within our organization further investigate, respond to, and remediate, the incident. Certain members of the Company's executive leadership team will also consider potentially applicable legal and regulatory obligations and take action to mitigate brand and reputational damage. In fiscal 2024, we did not identify any cybersecurity threats or incidents that have materially affected or are reasonably likely to materially affect our business strategy, results of operations, or financial condition. However, despite our efforts, we cannot eliminate all risks from cybersecurity threats or incidents or provide assurances that we have not experienced an undetected cybersecurity incident. If a cybersecurity incident is determined to be material, in accordance with reporting requirements applicable to us, our comprehensive cybersecurity assessment framework outlines our controls and the procedures adopted to ensure timely compliance with our reporting obligations.

Item 2. Properties

As of February 2, 2024, our facilities consisted of our corporate headquarters and various other facilities housing our security operations center personnel as well as research and development, marketing and sales, administrative and IT functions. We either lease these facilities or have the right to use them pursuant to service agreements with Dell or with other third parties. As of February 2, 2024, we did not own any facilities.

Our corporate headquarters is located in Atlanta, Georgia, where we lease facilities of approximately 115,800 square feet. As of February 2, 2024, we leased or licensed additional facilities in the following locations: Providence, Rhode Island; Edinburgh, Scotland; and Bucharest, Romania. Our employees also operate out of a number of Dell facilities internationally pursuant to arrangements with Dell. For information about our facility leases, see "Notes to Consolidated Financial Statements—Note 8—Leases" in our consolidated financial statements included in this report.

In future periods, we may lease or license additional sites, either from Dell or other third parties for sales offices and other functions. We believe that suitable additional facilities will be available on commercially reasonable terms.

Item 3. Legal Proceedings

From time to time, we are a party to or otherwise subject to legal proceedings that arise in the ordinary course of our business. As of February 2, 2024, we were not subject to any material pending legal proceedings.

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 for Class A Common Stock

Our Class A common stock is listed and traded on the Nasdaq Global Select Market under the symbol "SCWX." There is no public market for our Class B common stock.

Holders

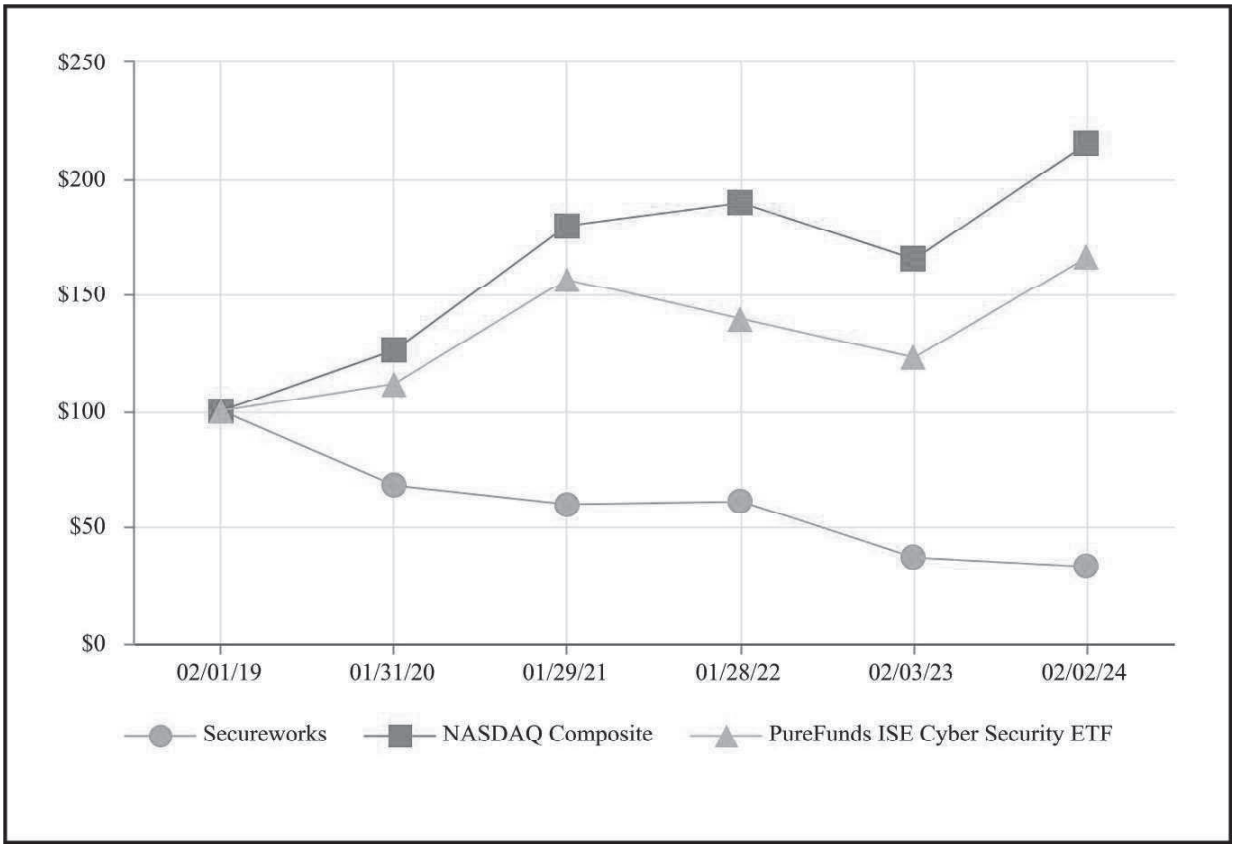
As of March 19, 2024, there were seven holders of record of our Class A common stock and one holder of record of our Class B common stock. The number of record holders of our Class A common stock does not include individuals or entities that beneficially own shares of Class A common stock, but whose shares are held of record by a broker, bank, or other nominee.

Dividends

We have not declared or paid cash dividends on our common stock. We do not anticipate declaring or paying any cash dividends on our common stock in the foreseeable future. We currently intend to retain all available funds and any future earnings to support our operations and finance the growth and development of our business. Any future determination related to our dividend policy will be made at the discretion of our board of directors and will depend upon, among other factors, our results of operations, financial condition, capital requirements, contractual restrictions, business prospects and other factors our board of directors may deem relevant.

Stock Performance Graph

The following graph compares the cumulative total return on the Class A common stock for the period from February 1, 2019 through February 2, 2024 with the total return over the same period on the Nasdaq Composite Index and the PureFunds ISE Cyber Security ETF Index. The graph assumes that $100 was invested on February 1, 2019, in the Class A common stock and in each of the foregoing indices and assumes reinvestment of dividends, if any. The comparisons in the graph are based on historical data and are not necessarily indicative of the future price performance of the Class A common stock.



	February 1, 2019	January 31, 2020	January 29, 2021	January 28, 2022	February 3, 2023	February 2, 2024
Secureworks	$ 100.00	$ 68.07	$ 59.89	$ 60.88	$ 36.85	$ 33.10
NASDAQ Composite	100.00	125.98	179.94	189.58	165.30	215.16
PureFunds ISE Cyber Security ETF	100.00	111.56	156.46	139.36	122.99	166.19

This performance graph shall not be deemed to be incorporated by reference by means of any general statement incorporating by reference this annual report on Form 10-K into any filing under the Securities Act of 1933,or Securities Act, or the Securities Exchange Act of 1934, or Exchange Act, except to the extent that Secureworks specifically incorporates such information by reference, and shall not otherwise be deemed filed under the Securities Act or the Exchange Act.

Item 6. Reserved

Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations

This management's discussion and analysis is based upon the financial statements of Secureworks which have been prepared in accordance with accounting principles generally accepted in the United States, or GAAP, and should be read in conjunction with our consolidated financial statements and related notes included in this report. In addition to historical financial information, the following discussion contains forward-looking statements that reflect our plans, estimates, beliefs, and future expectations. Our actual results could differ materially from those discussed or implied in our forward-looking statements. Factors that could cause or contribute to these differences include those discussed in "Risk Factors."

Our fiscal year is the 52- or 53-week period ending on the Friday closest to January 31. We refer to the fiscal year ending February 2, 2024 as fiscal 2024 and the fiscal years ended February 3, 2023 and January 28, 2022 as fiscal 2023 and fiscal 2022, respectively. Fiscal 2024 and fiscal 2022 each consisted of 52 weeks. Fiscal 2023 consisted of 53 weeks. Unless otherwise indicated, all changes identified for the current-period results represent comparisons to results for the prior corresponding fiscal period. For discussion and analysis related to our financial results comparing fiscal 2023 with fiscal 2022, see Part II, Item 7. Management's Discussion and Analysis of Financial Condition and Results of Operations in our Annual Report on Form 10-K for fiscal year ended February 3, 2023, which was filed with the Securities and Exchange Commission on March 23, 2023.

All percentage amounts and ratios presented in this management's discussion and analysis were calculated using the underlying data in thousands.

Except where the context otherwise requires or where otherwise indicated, (1) all references to "Secureworks" "we," "us," "our," and "our Company" in this management's discussion and analysis refer to SecureWorks Corp. and our subsidiaries on a consolidated basis, (2) all references to "Dell" refer to Dell Inc. and its subsidiaries on a consolidated basis and (3) all references to "Dell Technologies" refer to Dell Technologies Inc., the ultimate parent company of Dell Inc.

Overview

We are a leading global cybersecurity provider of technology-driven solutions singularly focused on protecting our customers.

Our vision is to be the essential cybersecurity company for a digitally connected world. We believe we are the security platform of choice to deliver a holistic approach to security at scale for our customers to achieve their best security outcomes. We combine considerable experience from securing thousands of customers, processing billions of customer events leveraging artificial intelligence and machine-learning in our security platform, and actionable insights from our team of elite researchers, analysts and consultants to create a powerful network effect that provides increasingly strong protection for our customers.

Our proprietary Taegis security platform utilizes an open architecture that is designed to process a wide variety of telemetry to see security threats quickly and leverage our customers' existing investments. Our solutions collect and process vast amounts of data across the IT ecosystem by integrating a wide array of proprietary and third-party security products. This open-platform approach allows us to aggregate events from a wide range of endpoint, network, cloud and business systems to increase the effectiveness of our solutions.

By aggregating and analyzing data from sources around the world, we offer solutions that enable organizations to:

- prevent security breaches,
- detect malicious activity,
- respond rapidly when a security breach occurs, and
- identify emerging threats.

We believe our security platform supports innovation and collaboration by enabling the security community to outmaneuver the adversary. Leveraging our extensive security expertise and threat intelligence, we utilize our unique insights to extend our Taegis XDR platform to defend against cyber-attacks.

The integrated approach we have pioneered enables us to deliver a broad portfolio of security solutions to organizations of varying size and complexity. We seek to provide the right level of security for each customer's particular situation, which evolves with our customers as their organizations grow and change over time. Our flexible and scalable solutions secure the evolving needs of large enterprises as well as small and medium-sized businesses and U.S. state and local government agencies with limited in-house capabilities and resources.

We offer our customers:

- software-as-a-service, or SaaS, solutions,
- managed solutions, and
- professional services, including incident response and penetration testing services.

Our security solutions leverage our proprietary technologies, security operations workflows, and extensive expertise and knowledge of the tactics, techniques, and procedures of the adversary that we have developed over more than two decades. As key elements of our strategy, we seek to:

- be the SaaS security platform of choice,
- broaden our reach with security service providers to deliver our security platform globally, and
- empower the global security community to beat the adversary at scale.

Taegis was purpose-built as a SaaS platform that combines the power of artificial intelligence and machine-learning capabilities with actionable security analytics and threat intelligence to unify detection and response across endpoint, network, cloud, email and other systems for better security outcomes and simpler security operations. The Taegis security platform is a core element of our SaaS solutions, which leverage workflows designed from our extensive security operations expertise and our integrated orchestration and automation capabilities to increase the speed of response actions.

We offer an integrated suite of technology-driven security solutions enabled by our Taegis security platform and team of highly skilled security experts. Our technology-driven security solutions offer an innovative approach to prevent, detect and respond to cybersecurity breaches. The platform collects, aggregates, correlates and analyzes billions of events daily from our extensive customer base utilizing sophisticated algorithms to detect malicious activity and deliver security countermeasures, dynamic intelligence and valuable context regarding the intentions and actions of cyber adversaries. Through our Taegis solutions, which are sold on a subscription basis, we provide global visibility and insight into malicious activity, enabling our customers to detect, respond to and effectively remediate threats quickly.

In addition to our Taegis solutions, we offer a variety of professional services to advise customers on a broad range of security and risk-related matters, which include incident response, penetration testing services and Taegis professional services, to accelerate adoption of our software solutions.

Reorganization and other related costs

During the fiscal year ended February 3, 2023, the Company committed to a plan to align its investments more closely with its strategic priorities to meet the expected future needs of the business by reducing the Company's workforce and implementing certain real estate-related and other cost optimization actions. Under this plan and through continued reorganization actions conducted during fiscal year ended February 2, 2024, the Company began rebalancing investments cross-functionally in alignment with the Company's current strategy and growth opportunities, such as focusing on the higher value, higher margin Taegis solutions, optimizing the Company's organizational structure to increase its scalability, and other priorities, to better position the Company for continued growth with improving operating margins over time. The Company incurred expenses of approximately $17.1 million and $15.5 million for the fiscal years ended February 2, 2024, and February 3, 2023, respectively, consisting primarily of severance and other termination benefits, real estate-related expenses, as well as other related costs. See Note 14 —"Reorganization and other related costs" for further discussion.

Key Factors Affecting Our Performance

We believe that our sustained success will depend on many factors, including the adoption of our Taegis security solutions by organizations, continued investment in our technology and threat intelligence research, our introduction of new solutions, our ability to increase sales of our solutions to new and existing customers, and our ability to attract and retain top talent. Although these areas present significant opportunities, they also present risks that we must manage to ensure we remain successful. We operate in an intensely competitive industry and face, among other competitive challenges, pricing pressures within the information security market resulting from actions taken by our larger competitors to reduce the prices of their security prevention, detection, and response solutions, as well as the prices of their managed security services. If we are unable to continue to manage our investments in an efficient manner or to effectively execute our strategies aimed to foster sustained success, our business could be adversely affected.

The key factors affecting our performance include the following:

Adoption of Technology-Driven Solution Strategy. The evolving landscape of applications, modes of communication, and IT architectures makes it increasingly challenging for organizations of all sizes to protect their critical business assets, including proprietary information, from cyber threats. New technologies heighten security risks by increasing the number of ways a threat actor can attack a target, by giving users greater access to important business networks and information and by facilitating the transfer of control of underlying applications and infrastructure to third-party vendors. An effective security strategy requires the coordinated deployment of a solution across the entire network infrastructure. Our Taegis security solutions are designed to facilitate the successful implementation of such a strategy, but continuous investment in, and adaptation of, our technology will be required as the threat landscape continues to evolve rapidly. The degree to which prospective and current customers recognize the mission-critical nature of our technology-driven information security solutions, and subsequently allocate budget dollars to our solutions, will affect our future financial results.

Investment in Our Technology and Threat Intelligence Research. Our software platforms constitute the core of our technology-driven security solutions. They provide our customers with an integrated perspective and intelligence regarding their network environments and security threats. Our software platforms are augmented by our Counter Threat Unit research team, which conducts exclusive research into threat actors, uncovers new attack techniques, analyzes emerging threats and evaluates the risks posed to our customers. Our performance is significantly dependent on the investments we expect to continue making into our research and development efforts and on our ability to remain at the forefront of threat intelligence research and adapt these software platforms to new technologies as well as to changes in existing technologies. This is an area in which we expect to continue to invest. We believe that continued investment in our Taegis subscription solutions will contribute to its long-term revenue growth, but the costs of our investment may continue to adversely affect our prospects for near-term profitability.

Introduction of New Security Solutions. Our performance is significantly dependent on our ability to continue to innovate and introduce new information security solutions, such as our Taegis solutions, that protect our customers from an expanding array of cybersecurity threats. We intend to continue to invest in security solutions innovation and leadership, including by hiring top technical talent and focusing on core technology innovation. In addition, we will continue to evaluate and utilize third-party proprietary technologies, where appropriate, for the continuous development of complementary offerings. We believe that our investment in security solutions development will increase the likelihood we will achieve long-term revenue growth, but this investment may continue to adversely affect our prospects for near-term profitability.

Investments in Expanding Our Customer Base.

Embracing our Partner Ecosystem. To support future sales, we expect to need to continue to devote resources to the development of strategic partnerships with our channel partners, technology alliance partners, and system integrators. We have made and plan to continue to make investments in both marketing and go-to-market efforts with our partners. These investments may not result in an increase in revenue or an improvement in our results of operations in the near term, although we do expect both will improve in the long term from these investments.

Deepening Our Customer Relationships. The continued growth of our business also depends in part on our ability to sell additional solutions to our existing customers. As our customers realize the benefits of the solutions they previously purchased, our portfolio of solutions provides us with a significant opportunity to expand these relationships.

Investment in Our People. The difficulty in providing effective information security is exacerbated by the highly competitive environment for identifying, hiring, and retaining qualified information security professionals. Our technology leadership, brand, exclusive focus on information security, customer-first culture, and robust training and development program have enabled us to attract and retain highly talented professionals with a passion for building a career in the information security industry. These professionals are led by a highly experienced and tenured management team with extensive IT security expertise and a record of developing successful new technologies and solutions to help protect our customers. We expect to continue to invest in attracting and retaining top talent to support and enhance our information security offerings.

Key Operating Metrics

Commencing in fiscal 2021, we began transitioning our subscription customers to our Taegis solutions from our non-strategic, lower margin other managed security subscription services. Although it has resulted in a decline in both our total customer base and total annual recurring revenue, we believe the transition of our subscription business to our Taegis solutions is resulting in a higher value and higher margin business. As of the end of fiscal 2024, the vast majority of our managed security services have reached end of life worldwide. A small number of contractual commitments will exist into the fiscal year ending January 31, 2025 as reflected in the operating metric table below.

The transition has resulted in the growth of our Taegis portfolio of technology-driven information security solutions offered to customers of all sizes and across all industries. We have achieved this organic growth by re-solutioning existing customers to our Taegis offerings, which generate more average revenue per customer, and through continued expansion in volume and breadth of the Taegis solutions we deploy. The transformation of our Taegis subscription-based model has required ongoing investment in our business, which has contributed to higher net losses. We believe these investments are critical to our long-term success, although they may continue to impact our prospects for near-term profitability.

Relevant key operating metrics are presented below as of the dates indicated and for the fiscal years then ended.

	February 2, 2024	February 3, 2023	January 28, 2022
Taegis subscription customer base	2,000	2,000	1,200
Managed security subscription customer base	300	700	2,400
Total subscription customer base	2,200	2,500	3,400
Total customer base	3,900	4,500	5,000
Taegis annual recurring revenue (in millions)	$ 284.9	$ 261.5	$ 164.7
Managed security annual recurring revenue (in millions)	12.4	58.4	224.4
Total annual recurring revenue (in millions)	$ 297.3	$ 319.9	$ 389.1
Taegis average subscription revenue per customer (in thousands)	$ 145.0	$ 132.3	$ 134.6
Managed security average subscription revenue per customer (in thousands)	$ 42.6	$ 86.9	$ 92.9
Total average subscription revenue per customer (in thousands)	$ 137.4	$ 129.1	$ 113.9
Net revenue retention rate	88 %	75 %	86 %

Taegis Subscription Customer Base and Managed Security Subscription Customer Base. We define our Taegis subscription customer base and managed security subscription customer base as the number of customers who have a subscription agreement for that respective offering as of a particular date. Some customers may have subscription agreements for both security offerings to address their current security needs.

Total Subscription Customer Base. We define our total subscription customer base as the number of unique customers who have a subscription agreement for our Taegis solutions and/or managed security services as of a particular date. We believe that growing our existing customer base and our ability to grow our average subscription revenue per customer represent significant future revenue opportunities for us.

Total Customer Base. We define total customer base as the number of customers that subscribe to our Taegis solutions and managed security services and customers that buy professional and other services from us, as of a particular date.

Total Annual Recurring Revenue. We define total annual recurring revenue as of the measurement date. Changes to recurring revenue may result from the expansion of our offerings and sales of additional solutions to our existing customers, as well as the timing of customer renewals.

Total Average Subscription Revenue Per Customer. We define total average subscription revenue per customer as the average annual revenue per customer that subscribes to either our Taegis or other managed security subscription solutions, or both, as of the measurement date. Total average subscription revenue per customer is primarily driven by the persistence of cyber threats and the results of our sales and marketing efforts to increase the awareness of our solutions. Our customer composition of both enterprise and small and medium sized businesses provides us with an opportunity to expand our professional services revenue. For fiscal 2024, fiscal 2023 and fiscal 2022, approximately 46%, 47% and 58%, respectively, of our professional services customers subscribed to our Taegis solutions or managed security services.

Net Revenue Retention Rate. Net revenue retention rate is an important measure of our success in retaining and growing revenue from our subscription-based customers. To calculate our revenue retention rate for any period, we compare the annual recurring revenue of our subscription-based customers at the beginning of the fiscal period, or base recurring revenue, to the same measure from that same cohort of customers at the end of the period, which we refer to as retained recurring revenue. By dividing the end-of-period retained recurring revenue by the base recurring revenue from the beginning of the period, we measure our success in retaining and growing installed revenue from the specific cohort of customers we served at the beginning of the period. Our calculation includes the positive revenue impacts of selling and installing additional solutions to this cohort of customers and the negative revenue impacts of customer or service attrition during the period. The calculation, however, does not include the positive impact on revenue from sales of solutions to any customers acquired during the period. Our net revenue retention rates may increase or decline from period to period as a result of various factors, including the timing of solutions installations, customer renewal rates, and changes to solution offerings.

Non-GAAP Financial Measures

We use supplemental measures of our performance, which are derived from our financial information, but which are not presented in our financial statements prepared in accordance with generally accepted accounting principles in the United States of America, referred to as GAAP. Non-GAAP financial measures presented in this management's discussion and analysis include non-GAAP cost of revenue, non-GAAP Taegis Subscription Solutions cost of revenue, non-GAAP Managed Security Services cost of revenue, non-GAAP subscription cost of revenue, non-GAAP professional services cost of revenue, non-GAAP gross profit, non-GAAP Taegis Subscription Solutions gross profit, non-GAAP Managed Security Services gross profit, non-GAAP subscription gross profit, non-GAAP professional services gross profit, non-GAAP gross margin, non-GAAP Taegis Subscription Solutions gross margin, non-GAAP Managed Security Services gross margin, non-GAAP subscription gross margin, non-GAAP professional services gross margin, non-GAAP operating expenses, non-GAAP research and development expenses, non-GAAP sales and marketing expenses, non-GAAP general and administrative expenses, non-GAAP operating income (loss), non-GAAP net income (loss), non-GAAP earnings (loss) per share and adjusted earnings before interest, taxes, depreciation and amortization, stock-based compensation and reorganization and other related charges, or adjusted EBITDA. We use non-GAAP financial measures to supplement financial information presented on a GAAP basis. We believe these non-GAAP financial measures provide useful information to help evaluate our operating results by facilitating an enhanced understanding of our operating performance and enabling more meaningful period-to-period comparisons and comparisons to our peers. Non-GAAP measures have been used as metrics used to determine variable compensation for employees.

There are limitations to the use of the non-GAAP financial measures presented in this management's discussion and analysis. Our non-GAAP financial measures may not be comparable to similarly titled measures of other companies. Other companies, including companies in our industry, may calculate non-GAAP financial measures differently than we do, limiting the usefulness of those measures for comparative purposes.

The non-GAAP financial measures we present, as defined by us, exclude the items described in the reconciliation below. As the excluded items can have a material impact on earnings, our management compensates for this limitation by relying primarily on GAAP results and using non-GAAP financial measures supplementally. The non-GAAP financial measures are not meant to be considered as indicators of performance in isolation from or as a substitute for revenue, subscription revenue, professional services revenue, Taegis Subscription Solutions revenue, Managed Security Services revenue, gross profit, subscription gross profit, professional services gross profit, Taegis Subscription Solutions gross profit, Managed Security Services gross profit, cost of revenue, subscription cost of revenue, professional services cost of revenue, Taegis Subscription Solutions cost of revenue, Managed Security Services cost of revenue, operating expense, research and development expenses, sales and marketing expenses, general and administrative expenses, gross margin, subscription gross margin, professional services gross margin, Taegis Subscription Solutions gross margin, Managed Security Services gross margin, operating income (loss), net income (loss), or earnings (loss) per share in accordance with GAAP, and the non-GAAP financial measures should be read only in conjunction with financial information presented on a GAAP basis.

Reconciliation of Non-GAAP Financial Measures

The table below presents a reconciliation of each non-GAAP financial measure to its most directly comparable GAAP financial measure. We encourage you to review the reconciliations in conjunction with the presentation of the non-GAAP financial measures for each of the periods presented. In future fiscal periods, we may exclude such items and may incur income and expenses similar to these excluded items. Accordingly, the exclusion of these items and other similar items in our non-GAAP presentation should not be interpreted as implying that these items are non-recurring, infrequent or unusual.

The following is a summary of the items excluded from the most comparable GAAP financial measures to calculate our non-GAAP financial measures:

- *Amortization of Intangible Assets.* Amortization of intangible assets consists of amortization associated with external software development costs capitalized and acquired customer relationships and technology. In connection with the acquisition of Dell by Dell Technologies in fiscal 2014 and our acquisition of Delve Laboratories Inc. in fiscal 2021, our tangible and intangible assets and liabilities associated with customer relationships and technology were accounted for and recognized at fair value on the related transaction date.
- *Stock-based Compensation Expense.* Non-cash stock-based compensation expense relates to Secureworks' equity plan. We exclude such expense when assessing the effectiveness of our operating performance since stock-based compensation does not necessarily correlate with the underlying operating performance of the business.
- *Aggregate Adjustment for Income Taxes.* The aggregate adjustment for income taxes is the estimated combined income tax effect for the adjustments mentioned above. The tax effects are determined based on the tax jurisdictions where the above items were incurred.
- *Reorganization and other related charges.* The aggregate adjustment for expenses associated with the Company's plan to align its investments more closely with its strategic priorities, as described in the "Notes to Consolidated Financial Statements—Note 14—Reorganization and Other Related Costs."

	February 2, 2024	February 3, 2023	January 28, 2022
Net revenue:			
Taegis Subscription Solutions	$ 265,298	$ 188,085	$ 85,599
Managed Security Services	39,258	175,363	323,348
Total Subscription revenue	$ 304,556	$ 363,448	$ 408,947
Professional services	61,323	100,027	126,267
Total net revenue	$ 365,879	$ 463,475	$ 535,214
GAAP Taegis Subscription Solutions cost of revenue	$ 80,737	$ 64,118	$ 31,718
Amortization of intangibles	(4,724)	(3,492)	(2,438)
Stock-based compensation expense	(835)	(277)	(22)
Non-GAAP Taegis Subscription Solutions cost of revenue	$ 75,178	$ 60,349	$ 29,258
GAAP Managed Security Services cost of revenue	$ 29,096	$ 67,436	$ 111,797
Amortization of intangibles	(9,397)	(13,641)	(13,642)
Stock-based compensation expense	(216)	(365)	(196)
Non-GAAP Managed Security Services cost of revenue	$ 19,483	$ 53,430	$ 97,959
GAAP subscription cost of revenue	$ 109,833	$ 131,554	$ 143,515
Amortization of intangibles	(14,121)	(17,133)	(16,080)
Stock-based compensation expense	(1,051)	(642)	(218)
Non-GAAP subscription cost of revenue	$ 94,661	$ 113,779	$ 127,217
GAAP professional services cost of revenue	$ 38,287	$ 59,503	$ 73,611
Stock-based compensation expense	(1,527)	(1,358)	(905)
Non-GAAP professional services cost of revenue	$ 36,760	$ 58,145	$ 72,706
GAAP gross profit	$ 217,759	$ 272,418	$ 318,088
Amortization of intangibles	14,121	17,133	16,080
Stock-based compensation expense	2,578	2,000	1,123
Non-GAAP gross profit	$ 234,458	$ 291,551	$ 335,291
GAAP research and development expenses	$ 110,996	$ 139,785	$ 122,494
Stock-based compensation expense	(12,625)	(11,589)	(7,220)
Non-GAAP research and development expenses	$ 98,371	$ 128,196	$ 115,274
GAAP sales and marketing expenses	$ 118,351	$ 163,637	$ 145,134
Stock-based compensation expense	(4,166)	(6,568)	(4,065)
Non-GAAP sales and marketing expenses	$ 114,185	$ 157,069	$ 141,069
GAAP general and administrative expenses	$ 83,233	$ 101,554	$ 102,834
Amortization of intangibles	(14,094)	(14,094)	(14,094)
Stock-based compensation expense	(15,735)	(16,698)	(18,038)
Non-GAAP general and administrative expenses	$ 53,404	$ 70,762	$ 70,702

	February 2, 2024	February 3, 2023	January 28, 2022
GAAP operating loss	$ (111,966)	$ (148,029)	$ (52,374)
Amortization of intangibles	28,216	31,228	30,174
Stock-based compensation expense	35,104	36,855	30,446
Reorganization and other related charges	17,145	15,471	—
Non-GAAP operating (loss)/income	$ (31,501)	$ (64,475)	$ 8,246
GAAP net loss	$ (86,042)	$ (114,499)	$ (39,791)
Amortization of intangibles	28,216	31,228	30,174
Stock-based compensation expense	35,104	36,855	30,446
Reorganization and other related charges	17,145	15,471	—
Aggregate adjustment for income taxes	(13,542)	(15,941)	(12,113)
Non-GAAP net (loss)/income	$ (19,119)	$ (46,886)	$ 8,716
GAAP net loss per share	$ (1.00)	$ (1.36)	$ (0.48)
Amortization of intangibles	0.33	0.37	0.36
Stock-based compensation expense	0.41	0.44	0.36
Reorganization and other related charges	0.20	0.18	—
Aggregate adjustment for income taxes	(0.16)	(0.19)	(0.14)
Non-GAAP net (loss)/earnings per share *	$ (0.22)	$ (0.56)	$ 0.11
** Sum of reconciling items may differ from total due to rounding of individual components*			
GAAP net loss	$ (86,042)	$ (114,499)	$ (39,791)
Interest and other expense/(income), net	2,554	(1,248)	3,532
Income tax benefit	(28,478)	(32,282)	(16,115)
Depreciation and amortization	31,893	36,668	40,520
Stock-based compensation expense	35,104	36,855	30,446
Reorganization and other related charges	17,145	15,471	—
Adjusted EBITDA	$ (27,824)	$ (59,035)	$ 18,592

Our Relationship with Dell and Dell Technologies

On April 27, 2016, we completed our IPO. Upon the closing of our IPO, Dell Technologies owned, indirectly through Dell Inc. and Dell Inc.'s subsidiaries, all shares of our outstanding Class B common stock, which as of February 2, 2024, represented approximately 81.0% of our total outstanding shares of common stock and approximately 97.7% of the combined voting power of both classes of our outstanding common stock. In early March 2024, Dell's economic ownership of the Company dropped below 80%. As a result, we will no longer qualify for inclusion in Dell Technologies' U.S. federal income tax return and most U.S. state jurisdictions. For more information, see "Notes to Consolidated Financial Statements—Note 11—Income and Other Taxes" in our consolidated financial statements included in this report.

As a majority-owned subsidiary of Dell, we receive from Dell various corporate services in the ordinary course of business, including finance, tax, human resources, legal, insurance, IT, procurement, and facilities related services. The costs of these services have been charged in accordance with a shared services agreement, as amended or amended and restated, in part, from time to time, that went into effect on August 1, 2015, which is the effective date of our carve-out from Dell. For more information regarding the allocated costs and related party transactions, see "Notes to Consolidated Financial Statements—Note 13—Related Party Transactions" in our consolidated financial statements included in this report.

During the periods presented in the consolidated financial statements included in this report, Secureworks did not file separate federal tax returns, as Secureworks was generally included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate-return method, modified to apply the benefits-for-loss approach. Under the benefits-for-loss approach, net operating losses or other tax attributes are characterized as realized or as realizable by Secureworks when those attributes are utilized or expected to be utilized by other members of the Dell affiliated group. For more information, see "Notes to Consolidated Financial Statements—Note 11—Income and Other Taxes" in our consolidated financial statements included in this report.

Additionally, we participate in various commercial arrangements with Dell, under which, for example, we provide information security solutions to third-party customers with whom Dell has contracted with to provide our solutions, procure hardware, software, and services from Dell, and sell our solutions through Dell in the United States and some international jurisdictions. In connection with our IPO, effective August 1, 2015, we entered into agreements with Dell that govern these commercial arrangements. In general, these agreements were initially effective for up to one to three years and include extension and cancellation options. To the extent that we choose to, or are required to, transition away from the corporate services currently provided by Dell, we may incur additional non-recurring transition costs to establish our own stand-alone corporate functions. For more information regarding the allocated costs and related party transactions, see "Notes to Consolidated Financial Statements—Note 13—Related Party Transactions" in our consolidated financial statements included in this report.

Components of Results of Operations

Revenue

We generate revenue from the sales of our subscriptions and professional services.

- *Subscription Revenue.* Subscription revenue primarily consists of subscription fees derived from our Taegis solutions and managed security services. Taegis' core offerings are the security platform, Taegis XDR, and our supplemental MDR service, ManagedXDR. Managed Security Services are subscription-based arrangements that typically include a suite of security services utilizing our legacy platform. Our subscription contracts typically range from one to three years and, as of February 2, 2024, averaged approximately two years in duration. The revenue and any related costs for these deliverables are recognized ratably over the contractual term, beginning on the date on which the tenant is made available to customers.
- *Professional Services Revenue.* Professional services revenue consists primarily of incident response solutions and security and risk consulting. Professional services engagements are typically purchased as fixed-fee and retainer-based contracts. Professional services customers typically purchase solutions pursuant to customized contracts that are shorter in duration. Revenue from these engagements is recognized under the proportional performance method of accounting. Revenue from time-and materials-based contracts is recognized as costs are incurred at amounts represented by the agreed-upon billing rates. In general, these contracts have terms of less than one year.

The fees we charge for our solutions vary based on a number of factors, including the solutions selected, the number of customer devices covered by the selected solutions, and the level of management we provide for the solutions. In fiscal 2024, approximately 83% of our revenue was derived from subscription-based arrangements, attributable to Taegis solutions and managed security services, while approximately 17% was derived from professional services engagements. As we respond to the evolving needs of our customers, the relative mix of subscription-based solutions and professional services we provide our customers may fluctuate. International revenue, which we define as revenue contracted through non-U.S. entities, represented approximately 37%, 34% and 33% of our total net revenue in fiscal 2024, fiscal 2023 and fiscal 2022, respectively. Although our international customers are located primarily in Japan, United Kingdom, Australia, and Canada, we provided our Taegis solutions or managed security services to customers across 73 countries as of February 2, 2024.

Over all of the periods presented in this report, our pricing strategy for our various offerings was relatively consistent, and accordingly did not significantly affect our revenue growth. However, we may adjust our pricing to remain competitive and support our strategic initiatives.

Cost of Revenue

Our cost of revenue consists of costs incurred to provide subscription and professional services.

- *Cost of Subscription Revenue.* Cost of subscription revenue consists primarily of personnel-related expenses associated with maintaining our platforms and delivering managed services to our subscription customers, as well as hosting costs for these platforms. Personnel-related expenses consist primarily of salaries, benefits, and performance-based compensation. Also included in cost of subscription revenue is amortization of equipment and costs associated with hardware utilized as part of providing subscription services, amortization of technology licensing fees, amortization of intangible assets, amortization of external software development costs capitalized, maintenance fees, and overhead allocations. As our business grows, the cost of subscription revenue associated with our solutions may fluctuate.
- *Cost of Professional Services Revenue.* Cost of professional services revenue consists primarily of personnel-related expenses, such as salaries, benefits, and performance-based compensation. Also included in cost of professional services revenue is fees paid to contractors who supplement or support our solutions, maintenance fees, and overhead allocations. As our business grows, the cost of professional services revenue associated with our solutions may fluctuate.

Gross Profit and Margin

Gross margin, or gross profit as a percentage of revenue, has been and will continue to be affected by a variety of factors, including the mix between our existing solutions, introduction of new solutions, personnel-related costs, and cloud hosting costs. We expect our gross margins to fluctuate depending on these factors, but we expect them to increase over time with expected growth and higher mix of Taegis subscription solutions revenue compared to managed security services and professional services revenue. As we balance achieving revenue growth with continued investment in initiatives that drive the efficiency of our business, we expect gross margin as a percentage of total revenue to continue to fluctuate from period to period.

Operating Costs and Expenses

Our operating costs and expenses consist of research and development expenses, sales and marketing expenses and general and administrative expenses.

- *Research and Development, or R&D, Expenses.* Research and development expenses include compensation and related expenses for the continued development of our solutions offerings, including a portion of costs related to our threat research team, which focuses on the identification of system vulnerabilities, data forensics, and malware analysis. R&D expenses also encompass expenses related to the development of prototypes of new solutions offerings and allocated overhead. Our customer solutions have generally been developed internally. We operate in a competitive and highly technical industry; therefore, to maintain and extend our technology leadership, we intend to continue to invest in our R&D efforts by hiring more personnel to enhance our existing security solutions and add complementary solutions.
- *Sales and Marketing, or S&M, Expenses.* Sales and marketing expenses include salaries, sales commissions and performance-based compensation benefits and related expenses for our S&M personnel, travel and entertainment, marketing and advertising programs (including lead generation), customer advocacy events, and other brand-building expenses, as well as allocated overhead.
- *General and Administrative, or G&A, Expenses.* General and administrative expenses include primarily the costs of human resources and recruiting, finance and accounting, legal support, information management and information security systems, facilities management, corporate development, and other administrative functions, and are partially offset by allocations of information technology and facilities costs to other functions.
- *Reorganization and other related charges.* Reorganization and other related charges consist primarily of severance and other termination benefits and real estate-related expenses, as described in the "Notes to Consolidated Financial Statements—Note 14—Reorganization and Other Related Costs."

Interest and Other, Net

Interest and other, net consists primarily of the effect of exchange rates on our foreign currency-denominated asset and liability balances and interest income earned on our cash and cash equivalents. All foreign currency transaction adjustments are recorded as foreign currency gains (losses) in the Consolidated Statements of Operations. To date, we have had minimal interest income.

Income Tax Expense (Benefit)

Our effective tax benefit rate was 24.9% and 22.0% for fiscal 2024 and fiscal 2023, respectively. The change in effective tax rate between the periods was primarily attributable to the impact of certain adjustments related to the vesting of stock-based compensation awards and the recognition of additional benefits relating to research and development credits.

We calculate a provision for income taxes using the asset and liability method, under which deferred tax assets and liabilities are recognized by identifying the temporary differences arising from the different treatment of items for tax and accounting purposes. We provide valuation allowances for deferred tax assets, where appropriate. We will file the current year's U.S. federal returns on a consolidated basis with Dell. According to the terms of the tax matters agreement between Dell Technologies and Secureworks that went into effect on August 1, 2015, Dell Technologies will reimburse us for any amounts by which our tax assets reduce the amount of tax liability owed by the Dell group on an unconsolidated basis.

In early March 2024, Dell's economic ownership of the Company dropped below 80%. As a result, we will no longer qualify for inclusion in Dell Technologies' U.S. federal income tax return and most U.S. state jurisdictions. Given our history of losses, a full valuation allowance will be recorded against our deferred tax assets due to our inability to file with Dell. We expect for the foreseeable future that a full valuation allowance will be recorded against our deferred tax assets until such time that we meet the more likely than not recognition criteria.

For a further discussion of income tax matters, see "Notes to Consolidated Financial Statements—Note 11—Income and Other Taxes" in our consolidated financial statements included in this report.

Results of Operations

Fiscal 2024 Compared to Fiscal 2023

The following table summarizes our key performance indicators for the fiscal years ended February 2, 2024 and February 3, 2023.

	Fiscal Years Ended					
	February 2, 2024		February 3, 2023		Change	
	$	% of Revenue	$	% of Revenue	$	%
	(in thousands, except percentages)					
Net revenue:						
Subscription	$ 304,556	83.2 %	$ 363,448	78.4 %	$ (58,892)	(16.2)%
Professional Services	61,323	16.8 %	100,027	21.6 %	(38,704)	(38.7)%
Total net revenue	$ 365,879	100.0 %	$ 463,475	100.0 %	$ (97,596)	(21.1)%
Cost of revenue:						
Subscription	$ 109,833	36.1 %	$ 131,554	36.2 %	$ (21,721)	(16.5)%
Professional Services	38,287	62.4 %	59,503	59.5 %	(21,216)	(35.7)%
Total cost of revenue	$ 148,120	40.5 %	$ 191,057	41.2 %	$ (42,937)	(22.5)%
Total gross profit	$ 217,759	59.5 %	$ 272,418	58.8 %	$ (54,659)	(20.1)%
Operating expenses:						
Research and development	$ 110,996	30.3 %	$ 139,785	30.2 %	$ (28,789)	(20.6)%
Sales and marketing	118,351	32.3 %	163,637	35.3 %	(45,286)	(27.7)%
General and administrative	83,233	22.7 %	101,554	21.9 %	(18,321)	(18.0)%
Reorganization and other related charges	17,145	4.7 %	15,471	3.3 %	1,674	10.8 %
Total operating expenses:	$ 329,725	90.1 %	$ 420,447	90.7 %	$ (90,722)	(21.6)%
Operating loss	(111,966)	(30.6)%	(148,029)	(31.9)%	36,063	(24.4)%
Net loss	$ (86,042)	(23.5)%	$ (114,499)	(24.7)%	$ 28,457	(24.9)%
Other Financial Information [(1)]						
Net revenue:						
Subscription	$ 304,556	83.2 %	$ 363,448	78.4 %	$ (58,892)	(16.2)%
Professional Services	61,323	16.8 %	100,027	21.6 %	(38,704)	(38.7)%
Total net revenue	$ 365,879	100.0 %	$ 463,475	100.0 %	$ (97,596)	(21.1)%
Non-GAAP cost of revenue:						
Non-GAAP Subscription	$ 94,661	31.1 %	113,779	31.3 %	(19,118)	(16.8)%
Non-GAAP Professional Services	36,760	59.9 %	58,145	58.1 %	(21,385)	(36.8)%
Total Non-GAAP cost of revenue	$ 131,421	35.9 %	$ 171,924	37.1 %	$ (40,503)	(23.6)%
Non-GAAP gross profit	$ 234,458	64.1 %	$ 291,551	62.9 %	$ (57,093)	(19.6)%
Non-GAAP operating expenses:						
Non-GAAP research and development	$ 98,371	26.9 %	$ 128,196	27.7 %	$ (29,825)	(23.3)%
Non-GAAP sales and marketing	114,185	31.2 %	157,069	33.9 %	(42,884)	(27.3)%
Non-GAAP general and administrative	53,404	14.6 %	70,762	15.3 %	(17,358)	(24.5)%
Non-GAAP operating expenses	$ 265,960	72.7 %	$ 356,027	76.8 %	$ (90,067)	(25.3)%
Non-GAAP operating (loss) income	(31,501)	(8.6)%	(64,475)	(13.9)%	32,974	(51.1)%
Non-GAAP net (loss) income	$ (19,119)	(5.2)%	$ (46,886)	(10.1)%	$ 27,767	(59.2)%
Adjusted EBITDA	$ (27,824)	(7.6)%	$ (59,035)	(12.7)%	$ 31,211	(52.9)%

(1) See "Non-GAAP Financial Measures" and "Reconciliation of Non-GAAP Financial Measures" for more information about these non-GAAP financial measures, including our reasons for including the measures, material limitations with respect to the usefulness of the measures, and a reconciliation of each non-GAAP financial measure to the most directly comparable GAAP financial measure. Non-GAAP financial measures as a percentage of revenue are calculated based on total net revenue, except for non-GAAP subscription cost of revenue and non-GAAP professional services cost of revenue measures, which are calculated based on subscription net revenue and professional services net revenue, respectively.

Revenue

The following table presents information regarding our net revenue for the fiscal years ended February 2, 2024 and February 3, 2023.

	Fiscal Years Ended					
	February 2, 2024		February 3, 2023		Change	
	$	% of Revenue	$	% of Revenue	$	%
	(in thousands, except percentages)					
Net revenue:						
Taegis Subscription Solutions	$ 265,298	72.5 %	$ 188,085	40.6 %	$ 77,213	41.1 %
Managed Security Services	39,258	10.7 %	175,363	37.8 %	(136,105)	(77.6)%
Total Subscription revenue	$ 304,556	83.2 %	$ 363,448	78.4 %	$ (58,892)	(16.2)%
Professional services	61,323	16.8 %	100,027	21.6 %	(38,704)	(38.7)%
Total net revenue	$ 365,879	100.0 %	$ 463,475	100.0 %	$ (97,596)	(21.1)%

Subscription Revenue. Subscription revenue decreased $58.9 million, or 16.2%, in fiscal 2024, which consisted of 52 weeks, compared to fiscal 2023, which consisted of 53 weeks. Adjusting for the additional week in fiscal 2023, subscription revenue decreased $52.4 million, or 14.4%. The revenue decrease reflected our continued focus on reducing non-strategic service offerings and prioritizing the growth of our Taegis subscription solutions, which includes reselling Taegis offerings to our current managed security services customer base.

Professional Services Revenue. Professional services revenue decreased $38.7 million, or 38.7%, in fiscal 2024, which consisted of 52 weeks, compared to fiscal 2023, which consisted of 53 weeks. Adjusting for the additional week in fiscal 2023, professional services revenue decreased $37.0 million, or 37.0%. The revenue decrease reflects our focus on reducing non-strategic professional service offerings and an overall decrease of billable hours.

Revenue for certain services provided to or on behalf of Dell under our commercial agreements with Dell totaled approximately $0.9 million and $4.6 million for fiscal 2024 and fiscal 2023, respectively. Of the revenue derived from Dell, subscription revenue represented approximately 16% and 22% for fiscal 2024 and fiscal 2023, respectively. For more information regarding the commercial agreements with Dell, see “Notes to Consolidated Financial Statements—Note 13—Related Party Transactions” in our consolidated financial statements included in this report.

We primarily generate revenue from sales in the United States. For fiscal 2024, international revenue, which we define as revenue contracted through non-U.S. entities, totaled $136.4 million, or 37% of our total revenue. For fiscal 2023, international revenue totaled $156.7 million, or 34% of our total revenue. Currently, our international customers are primarily located in Japan, United Kingdom, Australia, and Canada. We are focused on continuing to grow our international customer base in future periods.

Cost of Revenue

The following table presents information regarding our cost of revenue for the fiscal years ended February 2, 2024 and February 3, 2023.

	Fiscal Years Ended					
	February 2, 2024		February 3, 2023		Change	
	$	% of Revenue	$	% of Revenue	$	%
	(in thousands, except percentages)					
Cost of revenue:						
Taegis Subscription Solutions	$ 80,737	30.4 %	$ 64,118	34.1 %	$ 16,619	25.9 %
Managed Security Services	29,096	74.1 %	67,436	38.5 %	(38,340)	(56.9)%
Total subscription cost of revenue	$ 109,833	36.1 %	$ 131,554	36.2 %	$ (21,721)	(16.5)%
Professional Services cost of revenue	38,287	62.4 %	59,503	59.5 %	(21,216)	(35.7)%
Total cost of revenue	$ 148,120	40.5 %	$ 191,057	41.2 %	$ (42,937)	(22.5)%
Other Financial Information						
Non-GAAP cost of revenue:						
Taegis Subscription Solutions	$ 75,178	28.3 %	$ 60,349	32.1 %	$ 14,829	24.6 %
Managed Security Services	19,483	49.6 %	53,430	30.5 %	(33,947)	(63.5)%
Total non-GAAP subscription	$ 94,661	31.1 %	$ 113,779	31.3 %	$ (19,118)	(16.8)%
Non-GAAP Professional Services	36,760	59.9 %	58,145	58.1 %	(21,385)	(36.8)%
Total Non-GAAP cost of revenue[(1)]	$ 131,421	35.9 %	$ 171,924	37.1 %	$ (40,503)	(23.6)%

(1) See "Non-GAAP Financial Measures" and "Reconciliation of Non-GAAP Financial Measures" for a reconciliation of each non-GAAP financial measure to the most directly comparable GAAP financial measure.

Subscription Cost of Revenue. Subscription cost of revenue decreased $21.7 million, or 16.5%, in fiscal 2024, which consisted of 52 weeks, compared to fiscal 2023 which consisted of 53 weeks. Adjusting for the additional week in fiscal 2023, subscription cost of revenue decreased 19.4 million, or 14.7%. As a percentage of subscription revenue, subscription cost of revenue decreased 10 basis points to 36.1%. On a non-GAAP basis, subscription cost of revenue as a percentage of subscription revenue decreased 20 basis points to 31.1%. The decrease in subscription cost of revenue was primarily attributable to our focus on delivering comprehensive higher-value security solutions and driving scale and operational efficiencies associated with reducing non-strategic service offerings.

Professional Services Cost of Revenue. Professional services cost of revenue decreased $21.2 million, or 35.7%, in fiscal 2024, which consisted of 52 weeks, compared to fiscal 2023 which consisted of 53 weeks. Adjusting for the additional week in fiscal 2023, professional services cost of revenue decreased 20.2 million, or 34.0%. As a percentage of professional services revenue, professional services cost of revenue increased 290 basis points to 62.4%. On a non-GAAP basis, professional services cost of revenue as a percentage of revenue increased 180 basis points to 59.9%. The decrease in professional services cost of revenue was primarily attributable to lower employee-related expenses associated with the reduction of non-strategic professional services offerings.

Gross Profit and Gross Margin

The following table presents information regarding our gross profit and gross margin for the fiscal years ended February 2, 2024 and February 3, 2023.

	Fiscal Years Ended			
	February 2, 2024	February 3, 2023	Change	
	$	$	$	%
	(in thousands, except percentages)			
Gross Profit:				
Taegis Subscription Solutions	$ 184,561	$ 123,967	$ 60,594	48.9 %
Managed Security Services	10,162	107,927	(97,765)	(90.6)%
Total Subscription	$ 194,723	$ 231,894	$ (37,171)	(16.0)%
Professional Services	23,036	40,524	(17,488)	(43.2)%
Total Gross Profit	$ 217,759	$ 272,418	$ (54,659)	(20.1)%
Gross Margin:				
Taegis Subscription Solutions	69.6 %	65.9 %	3.7 %	
Managed Security Services	25.9 %	61.5 %	(35.6)%	
Total Subscription	63.9 %	63.8 %	0.1 %	
Professional Services	37.6 %	40.5 %	(2.9)%	
Total Gross Margin	59.5 %	58.8 %	0.7 %	
Other Financial Information				
Non-GAAP Gross Profit:				
Taegis Subscription Solutions	$ 190,120	$ 127,736	$ 62,384	48.8 %
Managed Security Services	19,775	121,933	(102,158)	(83.8)%
Non-GAAP Subscription	$ 209,895	$ 249,669	$ (39,774)	(15.9)%
Non-GAAP Professional Services	24,563	41,882	(17,319)	(41.4)%
Total Non-GAAP Gross Profit	$ 234,458	$ 291,551	$ (57,093)	(19.6)%
Non-GAAP Gross Margin:				
Taegis Subscription Solutions	71.7 %	67.9 %	3.8 %	
Managed Security Services	50.4 %	69.5 %	(19.1)%	
Non-GAAP Subscription	68.9 %	68.7 %	0.2 %	
Non-GAAP Professional Services	40.1 %	41.9 %	(1.8)%	
Total Non-GAAP Gross Margin	64.1 %	62.9 %	1.2 %	

Subscription Gross Margin. Subscription gross margin increased 0.1% in fiscal 2024. Overall, gross margin for Taegis Subscription Solutions has improved as we scale our comprehensive, higher-value offerings. The subscription gross margin continues to trail the increasing Taegis subscription solutions gross margin due to the higher costs as a percentage of revenue required to maintain and support our non-strategic Managed Security Service offerings as we complete the end-of-life transition.

Subscription gross margin on a GAAP basis includes amortization of intangible assets and stock-based compensation expense. On a non-GAAP basis, excluding these adjustments, fiscal 2024 gross margin increased 0.2%.

Professional Services Gross Margin. Professional services gross margin decreased 2.9% in fiscal 2024. We expect professional services gross margin to fluctuate due to the timing of the revenue and related expense reductions associated with the reduction of our non-strategic professional services offerings.

Professional services gross margin on a GAAP basis includes stock-based compensation expense. On a non-GAAP basis, excluding that adjustment, fiscal 2024 gross margin decreased 1.8%.

Operating Expenses

The following table presents information regarding our operating expenses during the fiscal years ended February 2, 2024 and February 3, 2023.

	Fiscal Year Ended				
	February 2, 2024			February 3, 2023	
	$	% of Revenue	% Change	$	% of Revenue
Operating expenses:					
Research and development	$ 110,996	30.3 %	(20.6)%	$ 139,785	30.2 %
Sales and marketing	118,351	32.3 %	(27.7)%	163,637	35.3 %
General and administrative	83,233	22.7 %	(18.0)%	101,554	21.9 %
Reorganization and other related charges	17,145	4.7 %	10.8%	15,471	3.3 %
Total operating expenses	$ 329,725	90.1 %	(21.6)%	$ 420,447	90.7 %
Other Financial Information					
Non-GAAP research and development	$ 98,371	26.9 %	(23.3)%	$ 128,196	27.7 %
Non-GAAP sales and marketing	114,185	31.2 %	(27.3)%	157,069	33.9 %
Non-GAAP general and administrative	53,404	14.6 %	(24.5)%	70,762	15.3 %
Total Non-GAAP operating expenses [(1)]	$ 265,960	72.7 %	(25.3)%	$ 356,027	76.8 %

(1) See "Non-GAAP Financial Measures" and "Reconciliation of Non-GAAP Financial Measures" for a reconciliation of each non-GAAP financial measure to the most directly comparable GAAP financial measure.

Research and Development Expenses. R&D expenses decreased $28.8 million, or 20.6%, in fiscal 2024. As a percentage of revenue, R&D expenses increased 10 basis points to 30.3% in fiscal 2024. As a percentage of revenue on a non-GAAP basis, R&D expenses decreased 80 basis points to 26.9%. The decrease in R&D expenses was primarily attributable to lower employee-related expenses, professional services costs, and consulting-related costs.

Sales and Marketing Expenses. S&M expenses decreased $45.3 million, or 27.7%, in fiscal 2024. As a percentage of revenue, S&M expenses decreased 300 basis points to 32.3% in fiscal 2024. On a non-GAAP basis, S&M expenses as a percentage of revenue decreased 270 basis points to 31.2%. The decrease in S&M expenses was primarily attributable to a decrease in marketing and advertising vendor costs as well as lower employee-related expenses.

General and Administrative Expenses. G&A expenses decreased $18.3 million, or 18.0%, in fiscal 2024. As a percentage of revenue, G&A expenses increased 80 basis points to 22.7% in fiscal 2024. On a non-GAAP basis, G&A expenses as a percentage of revenue decreased 70 basis points to 14.6%. The decrease in G&A expenses was primarily attributable to lower employee-related expenses, professional services costs, and consulting-related costs.

Reorganization and other related charges. During fiscal 2024, the Company incurred expenses of $17.1 million associated with its reorganization plan consisting primarily of severance and other termination benefits and real estate-related impairment, compared with $15.5 million in fiscal 2023.

Operating Loss

Our operating loss for fiscal 2024 and fiscal 2023 was $112.0 million and $148.0 million, respectively. As a percentage of revenue, our operating loss was 30.6% and 31.9% in fiscal 2024 and fiscal 2023, respectively. The decrease in our operating loss was primarily attributable to decreased operating expenses supplemented by increased gross margins as we complete our transition to higher value, higher margin Taegis solutions.

Operating loss on a GAAP basis includes amortization of intangible assets, stock-based compensation expense, and reorganization related costs. On a non-GAAP basis, excluding these adjustments, our operating loss for fiscal 2024 was $31.5 million compared to operating loss of $64.5 million in fiscal 2023 respectively.

Interest and Other, Net

Interest and other, net represented net expense of $2.6 million in fiscal 2024 compared with income of $1.2 million in fiscal 2023. The change primarily reflected the effects of foreign currency transactions and related exchange rate fluctuations.

Income Tax Expense (Benefit)

Our income tax benefit was $28.5 million, or 24.9% of our pre-tax loss, in fiscal 2024 and $32.3 million, or 22.0% of our pre-tax loss, in fiscal 2023. The changes in the effective tax benefit rate were primarily attributable to both the decrease in loss before income taxes, the impact of certain adjustments related to stock-based compensation awards, and the recognition of additional benefits relating to research and development credits.

Net Income (Loss)

Our net loss of $86.0 million decreased $28.5 million, or 24.9%, in fiscal 2024 compared to fiscal 2023. Net loss on a non-GAAP basis was $19.1 million in fiscal 2024, which represented a decrease of $27.8 million from fiscal 2023. The changes on both a GAAP and non-GAAP basis were attributable to decreased operating expenses supplemented by increased gross margins as we complete our transition to higher value, higher margin Taegis solutions.

Liquidity, Capital Commitments and Contractual Cash Obligations

Overview

As of February 2, 2024, we have $68.7 million of cash and cash equivalents. We believe that our cash and cash equivalents and access to the revolving credit facility will provide us with sufficient liquidity to meet our material cash requirements, including to fund our business and meet our obligations for at least 12 months from the filing date of this report and for the foreseeable future thereafter.

As of the balance sheet date, we have reported a deficit in working capital. This deficit in working capital represents an excess of our current liabilities over our current assets and is primarily the result of the significant balance of deferred revenue, reported as a current liability, as of the balance sheet date. We have in recent periods incurred losses from operations and operating cash outflows. Our future capital requirements will depend on many factors, including our rate of revenue growth, the timing and extent of our expansion into new markets, the timing of introductions of new functionality and enhancements to our solutions, potential acquisitions of complementary businesses and technologies, continuing market acceptance of our solutions and general economic and market conditions.

We expect our recent reorganization actions to result in significant cost savings as we complete our transition to higher value, higher margin Taegis solutions. We believe these efforts will optimize our organizational structure and increase scalability to better position us for continued growth with improving operating margins over time.

In the event that our financial results are below our expectations as a result of the factors mentioned above or other factors, we may need to take additional actions to preserve existing cash reserves. To the extent we undertake future material acquisitions, investments, or unanticipated capital or operating expenditures, we may require additional capital or incur indebtedness. In this context, we regularly evaluate opportunities to enhance our capital structure. In addition to our $50 million revolving credit facility from Dell, described below, sources of financing may include arrangements with unaffiliated third parties. The timing, term, size, and pricing of any such financing will depend on investor interest and market conditions, and there can be no assurance that we will be able to obtain any such financing on favorable terms or at all.

Selected Measures of Liquidity and Capital Resources

Our principal sources of liquidity, consisting of cash and cash equivalents, are set forth below as of the dates indicated.

	February 2, 2024	February 3, 2023
	(in thousands)	
Cash and cash equivalents	$ 68,655	$ 143,517

Revolving Credit Facility

SecureWorks, Inc., our wholly-owned subsidiary, is party to a revolving credit agreement with a wholly-owned subsidiary of Dell Inc. under which we obtained a $50 million senior unsecured revolving credit facility. Effective September 6, 2023, the revolving credit agreement was amended and restated to: (1) increase the maximum principal amount of borrowings outstanding under the revolving credit facility to $50 million, (2) remove the one-time increase of up to an additional $30 million in borrowings upon mutual agreement by the lender and borrower, (3) extend the commitment and required repayment date under the revolving credit agreement to March 23, 2026, and (4) modify the rate at which interest accrues on funds drawn against the revolving credit agreement to SOFR plus 2.00%.

Amounts under the facility may be borrowed, repaid, and reborrowed from time to time during the term of the facility. The proceeds from loans made under the facility may be used for general corporate purposes. The credit agreement contains customary representations, warranties, covenants, and events of default. The unused portion of the facility is subject to a commitment fee of 0.35%, which is due upon expiration of the facility. There was no outstanding balance under the facility as of February 2, 2024 or February 3, 2023, and we did not borrow any amounts under the facility during any period covered by this report.

The borrower will be required to repay, in full, all of the loans outstanding, including all accrued interest, and the facility will terminate upon a change of control of SecureWorks Corp. or following a transaction in which SecureWorks, Inc. ceases to be a direct or indirect wholly-owned subsidiary of SecureWorks Corp. The facility is not guaranteed by us or our subsidiaries.

For more information regarding the facility, see "Notes to Consolidated Financial Statements—Note 6—Debt" in our consolidated financial statements included in this report.

Cash Flows

The following table presents information concerning our cash flows for the fiscal years ended February 2, 2024 and February 3, 2023.

	Fiscal Year Ended	
	February 2, 2024	February 3, 2023
	(in thousands)	
Net change in cash from:		
Operating activities	$ (59,159)	$ (58,745)
Investing activities	(6,423)	(6,011)
Financing activities	(6,163)	(8,887)
Effect of exchange rate changes on cash and cash equivalents	(3,117)	(3,495)
Change in cash and cash equivalents	$ (74,862)	$ (77,138)

- *Operating Activities* — Cash used in operating activities was $59.2 million in fiscal 2024 compared to cash used in operating activities of $58.7 million in fiscal 2023. The increased use of our operating cash was primarily driven by one-time costs incurred in connection with the reorganization, partially offset by our decreased net loss as we rebalance investments cross-functionally in alignment with our current strategy and growth opportunities.
- *Investing Activities* — Cash used in investing activities totaled $6.4 million and $6.0 million in fiscal 2024 and fiscal 2023, respectively. Investing activities consisted primarily of capitalized expenses related to the continued development of our Taegis software platform and SaaS applications, which increased $1.5 million compared to fiscal 2023.
- *Financing Activities* — Cash used in financing activities was $6.2 million and $8.9 million in fiscal 2024 and fiscal 2023, respectively. The use of cash reflected employee tax withholding payments on restricted stock-based awards.

Contractual Cash Obligations

Our material cash requirements represented by contractual cash obligations as of February 2, 2024, are summarized in the following table:

	Payments Due by Fiscal Year				
(in thousands)	Less than 1 year	1-3 years	3-5 years	Thereafter	Total
Operating leases	$ 5,095	$ 8,614	$ —	$ —	$ 13,709
Purchase obligations	41,589	101,560	74	—	143,223
Total	$ 46,684	$ 110,174	$ 74	$ —	$ 156,932

For information about leases and purchase obligations, see "Notes to Consolidated Financial Statements—Note 8—Leases" and "Notes to Consolidated Financial Statements—Note 7—Commitments and Contingencies" in our consolidated financial statements included in this report.

Critical Accounting Policies and Estimates

We prepare our financial statements in conformity with GAAP, which requires certain estimates, assumptions, and judgments to be made that may affect our consolidated financial statements. Accounting policies that have a significant impact on our results are described in "Notes to Consolidated Financial Statements—Note 2—Significant Accounting Policies" in our consolidated financial statements included in this report. The accounting policies discussed in this section are those that we consider to be the most critical. We consider an accounting policy to be critical if the policy is subject to a material level of judgment and if changes in those judgments are reasonably likely to materially impact our results.

Revenue Recognition. Secureworks derives revenue primarily from subscription services and professional services. Subscription revenue is derived from (i) Taegis software-as-a-service, or SaaS, security platform and (ii) managed security services. Professional services typically include incident response and security and risk consulting solutions.

Taegis is a SaaS security software platform deployed as a subscription-based software-as-as-service, or SaaS, designed to unify detection and response across endpoint, network and cloud environments for better security outcomes and simpler security operations for our customers. Taegis' core offerings are the security platform, Taegis XDR, and our supplemental MDR service, ManagedXDR. Customers do not have the right to take possession of the software platform. Revenue for our SaaS applications is recognized on a straight-line basis over the term of the arrangement, beginning with provision of the tenant by grant of access to the software platform. Customers also have the option to purchase an add-on managed service to supplement the XDR SaaS application, referred to as our Managed Detection and Response, or as ManagedXDR, subscription service. The ManagedXDR service is identified as a distinct performance obligation that is separable from the SaaS application. While a customer must purchase and deploy the XDR software to gain utility from the ManagedXDR service, a customer may purchase and benefit from using the XDR SaaS application on its own. In order to conclude that the two promises are not separately identifiable, the interrelationship/interdependence would most likely have to be reciprocal between the two separate offerings. The nature of the ManagedXDR service is to stand ready, or deliver, an unspecified quantity of services each day during the contract term, based on customer-specific needs. The ManagedXDR service period is contractually tied to the related software application and, as a stand ready obligation, is recognized on a straight-line basis over the term of the arrangement.

Subscription-based managed security service arrangements typically include security services, up-front installation fees and maintenance, and also may include the provision of an associated hardware appliance. We use our hardware appliances in providing security services required to access our Counter Threat Platform. The arrangements that require hardware do not typically convey ownership of the appliance to the customer. Moreover, any related installation fees are non-refundable and are also incapable of being distinct within the context of the arrangement. Therefore, we have determined that these arrangements constitute a single performance obligation for which the revenue and any related costs are recognized ratably over the term of the arrangement, which reflects our performance in transferring control of the services to the customer.

Amounts that have been invoiced for the managed security service subscription arrangements and the Taegis SaaS application offerings where the relevant revenue recognition criteria have not been met will be included in deferred revenue.

Professional services consist primarily of fixed-fee and retainer-based contracts. Revenue from these engagements is recognized using an input method over the contract term.

Secureworks reports revenue net of any revenue-based taxes assessed by governmental authorities that are imposed on, and concurrently with, specific revenue-producing transactions.

We recognize revenue when all of the following criteria are met:

- ***Identification of the contract, or contracts, with a customer—***A contract with a customer exists when (i) we enter into an enforceable contract with a customer, (ii) the contract has commercial substance and the parties are committed to perform, and (iii) payment terms can be identified and collection of substantially all consideration to which we will be entitled in exchange for goods or services that will be transferred is deemed probable based on the customer's intent and ability to pay. Contracts entered into for professional services and subscription-based solutions near or at the same time are generally not combined as a single contract for accounting purposes, since neither the pricing nor the services are interrelated.
- ***Identification of the performance obligations in the contract—***Performance obligations promised in a contract are identified based on the goods or services that will be transferred to the customer that are both (i) capable of being distinct, whereby the customer can benefit from the goods or service either on its own or together with other resources that are readily available from third parties or from us, and (ii) distinct in the context of the contract, whereby the transfer of the goods or services is separately identifiable from other promises in the contract. When promised goods or services are incapable of being distinct, we account for them as a combined performance obligation. With regard to a typical contract for subscription-based managed security services, the performance obligation represents a series of distinct services that will be accounted for as a single performance obligation. For a typical contract that includes subscription-based SaaS applications, each application is generally considered to be distinct and accounted for as a separate performance obligation. In a typical professional services contract, Secureworks has a separate performance obligation associated with each service. We generally act as a principal when delivering either our subscription-based solutions or our professional services arrangement and, thus, recognize revenue on a gross basis.
- ***Determination of the transaction price—***The total transaction price is primarily fixed in nature as the consideration is tied to the specific services purchased by the customer, which constitutes a series of distinct services for delivery of the solutions over the duration of the contract for our subscription services. For professional services contracts, variable consideration exists in the form of rescheduling penalties and expense reimbursements; no estimation is required at contract inception, since variable consideration is allocated to the applicable period.
- ***Allocation of the transaction price to the performance obligations in the contract—***We allocate the transaction price to each performance obligation based on the performance obligation's standalone selling price. Standalone selling price is determined by considering all information available to us, such as historical selling prices of the performance obligation, geographic location, overall strategic pricing objective, market conditions, and internally approved pricing guidelines related to the performance obligations.
- ***Recognition of revenue when, or as, the Company satisfies performance obligation—***We recognize revenue over time on a ratable recognition basis using a time-elapsed output method to measure progress for all subscription-based performance obligations, including managed security services and SaaS applications, over the contract term. For any upgraded installation services, which we have determined represent a performance obligation separate from its subscription-based arrangements, revenue is recognized over time using hours elapsed over the service term as an appropriate method to measure progress. For the performance obligation pertaining to professional services arrangements, we recognize revenue over time using an input method based on time (hours or days) incurred to measure progress over the contract term.

Intangible Assets Including Goodwill. Identifiable intangible assets with finite lives are amortized on a straight-line basis over their estimated useful lives. Finite-lived intangible assets are reviewed for impairment on a quarterly basis, or as potential triggering events are identified. Goodwill and indefinite-lived intangible assets are tested for impairment on an annual basis in the third fiscal quarter, or sooner if an indicator of impairment exists.

We may elect to first assess qualitative factors to determine whether it is more-likely-than-not that the fair value of goodwill at the reporting unit level, as well as indefinite-lived intangible assets at the individual asset level, are less than their respective carrying amounts. We determined that we have one reporting unit.

The qualitative assessment includes our consideration of relevant events and circumstances that would affect our single reporting unit and indefinite-lived assets, including macroeconomic, industry and market conditions, our overall financial performance, and trends in the market price of our Class A common stock. If indicators of impairment exist after performing the qualitative assessment, we will perform a quantitative assessment of goodwill and indefinite-lived intangible assets. We also may choose to perform the quantitative assessment periodically even if the qualitative assessment does not require us to do so. If the carrying amount exceeds the fair value of the reporting unit determined through the quantitative analysis, an impairment charge is recognized in an amount equal to that excess.

For the annual impairment review in the third quarter of fiscal 2024, we performed a Step 0 qualitative assessment of goodwill at the reporting unit level, and the indefinite-lived intangible assets at the individual asset level. It was concluded that it was not more likely than not that the fair value of the reporting unit and indefinite-lived intangible asset was less than their respective

carrying values. Subsequently, no triggering events have transpired since our annual test that would indicate a potential impairment occurred during the period through February 2, 2024.

Impairment of long-lived assets. We evaluate all long-lived assets, other than goodwill, whenever events or circumstances change that indicate the asset's carrying value may no longer be recoverable. If impairment indicators exist, a test of recoverability is performed by comparing the sum of the estimated undiscounted future cash flows attributable to the asset's carrying value. Impairment analyses are performed at the asset group level. If the asset's carrying value is not recoverable, impairment is measured by determining the asset's fair value and recording any difference as an impairment loss. Long-lived assets subject to this policy include property, plant & equipment, intangible assets, and right-of-use assets, such as operating leases. Impairment losses of $2.9 million and $4.0 million were recognized to our right-of-use assets for the fiscal years ended February 2, 2024, and February 3, 2023, respectively. No impairment was recognized in the fiscal year ended January 28, 2022. These amounts are presented in the Consolidated Statement of Operations as reorganization and other related charges.

Stock-Based Compensation. Our compensation programs include grants under the SecureWorks Corp. 2016 Long-Term Incentive Plan and, prior to the IPO date, grants under share-based payment plans of Dell Technologies Inc., or Dell Technologies. Under the plans, we and, prior to the IPO date, Dell Technologies have granted stock options, restricted stock awards and restricted stock units. Compensation expense related to stock-based transactions is measured and recognized in the financial statements based on grant date fair value. Fair value for restricted stock awards and restricted stock units under our plan is based on the closing price of our Class A common stock as reported on the Nasdaq Global Select Market on the day of the grant. The fair value of each option award is estimated on the grant date using the Black-Scholes option-pricing model and a single option award approach. This model requires that at the date of grant we determine the fair value of the underlying Class A common stock, the expected term of the award, the expected volatility, risk-free interest rates, and expected dividend yield. The annual grant of restricted stock and restricted stock units issued during the fiscal year ended February 2, 2024 vest over an average service period of three years and approximately 17% of such awards are subject to performance conditions. Stock-based compensation expense, regarding service-based awards, is adjusted for forfeitures, and recognized using a straight-line basis over the requisite service periods of the awards, which is generally three to four years. Stock-based compensation expense, regarding performance awards, is adjusted for forfeitures and performance criteria, and recognized on a graded vesting basis. We estimate a forfeiture rate, based on an analysis of actual historical forfeitures, to calculate stock-based compensation expense.

Loss Contingencies. We are subject to the possibility of various losses arising in the ordinary course of business. We consider the likelihood of loss or impairment of an asset or the incurrence of a liability, as well as our ability to reasonably estimate the amount of loss, in determining loss contingencies. An estimated loss contingency is accrued when it is probable that an asset has been impaired or a liability has been incurred and the amount of loss can reasonably be estimated. We regularly evaluate current information available to us to determine whether such accruals should be adjusted and whether new accruals are required.

Recently Issued Accounting Pronouncements

Information about recently issued accounting pronouncements is presented in “Notes to Consolidated Financial Statements—Note 2—Significant Accounting Policies” in our consolidated financial statements included in this report.

Item 7A. Quantitative and Qualitative Disclosures About Market Risk

Our results of operations and cash flows have been and will continue to be subject to fluctuations because of changes in foreign currency exchange rates, particularly changes in exchange rates between the U.S. dollar and the Euro, the British Pound, the Romanian Leu, the Japanese Yen, the Australian Dollar, and the Canadian Dollar; the currencies of countries where we currently have our most significant international operations. Our expenses in international locations are generally denominated in the currencies of the countries in which our operations are located.

As our international operations grow, we may begin to use foreign exchange forward contracts to partially mitigate the impact of fluctuations in net monetary assets denominated in foreign currencies.

Item 8. Financial Statements and Supplementary Data

INDEX TO CONSOLIDATED FINANCIAL STATEMENTS

Report of Independent Registered Public Accounting Firm

To the Board of Directors and Stockholders of SecureWorks Corp.

Opinions on the Financial Statements and Internal Control over Financial Reporting

We have audited the accompanying consolidated statements of financial position of SecureWorks Corp. and its subsidiaries (the "Company") as of February 2, 2024 and February 3, 2023, and the related consolidated statements of operations, of comprehensive loss, of stockholders' equity and of cash flows for each of the three years in the period ended February 2, 2024, including the related notes and financial statement schedule listed in the accompanying index (collectively referred to as the "consolidated financial statements"). We also have audited the Company's internal control over financial reporting as of February 2, 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 consolidated financial statements referred to above present fairly, in all material respects, the financial position of the Company as of February 2, 2024 and February 3, 2023, and the results of its operations and its cash flows for each of the three years in the period ended February 2, 2024 in conformity with accounting principles generally accepted in the United States of America. Also in our opinion, the Company maintained, in all material respects, effective internal control over financial reporting as of February 2, 2024, based on criteria established in Internal Control - Integrated Framework (2013) issued by the COSO.

Basis for Opinions

The Company's management is responsible for these consolidated financial statements, for maintaining effective internal control over financial reporting, and for its assessment of the effectiveness of internal control over financial reporting, included in Management's Report on Internal Control Over Financial Reporting appearing under Item 9A. Our responsibility is to express opinions on the Company's consolidated financial statements and on the Company's internal control over financial reporting based on our audits. We are a public accounting firm registered with the Public Company Accounting Oversight Board (United States) (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 audits to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement, whether due to error or fraud, and whether effective internal control over financial reporting was maintained in all material respects.

Our audits of the consolidated financial statements included performing procedures to assess the risks of material misstatement of the consolidated 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 consolidated 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 consolidated financial statements. Our audit of internal control over financial reporting included obtaining an understanding of internal control over financial reporting, assessing the risk that a material weakness exists, and testing and evaluating the design and operating effectiveness of internal control based on the assessed risk. Our audits also included performing such other procedures as we considered necessary in the circumstances. We believe that our audits provide a reasonable basis for our opinions.

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 (i) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; (ii) 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 (iii) 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.

Critical Audit Matters

The critical audit matter communicated below is a matter arising from the current period audit of the consolidated financial statements that was communicated or required to be communicated to the audit committee and that (i) relates to accounts or disclosures that are material to the consolidated financial statements and (ii) involved our especially challenging, subjective, or complex judgments. The communication of critical audit matters does not alter in any way our opinion on the consolidated 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 – subscription contracts

As described in Note 2 to the consolidated financial statements, the Company recognizes revenue when all of the following criteria are met: (i) identification of the contract, or contracts, with a customer; (ii) identification of the performance obligations in the contract; (iii) determination of the transaction price; (iv) allocation of the transaction price to the performance obligations in the contract; and (v) recognition of the revenue when, or as, the Company satisfies a performance obligation. Subscription revenue is derived from (i) the Taegis software-as-a-service security platform and (ii) managed security services. The Company recognizes revenue over time on a ratable recognition basis using a time-elapsed output method to measure progress for all subscription-based performance obligations, over the contract term. As disclosed by management, judgment is applied in recognizing revenue based on determining all the aforementioned criteria have been met. For the year ended February 2, 2024, the Company's subscription revenue was $304.6 million.

The principal considerations for our determination that performing procedures relating to revenue recognition for subscription contracts is a critical audit matter are (i) the significant judgment by management in assessing whether all of the criteria have been met related to revenue recognition for subscription contracts and (ii) the significant auditor judgment, subjectivity, and effort in performing procedures and evaluating audit evidence related to management's assessment of the revenue recognition criteria.

Addressing the matter involved performing procedures and evaluating audit evidence in connection with forming our overall opinion on the consolidated financial statements. These procedures included testing the effectiveness of controls relating to the Company's revenue recognition process for subscription contracts. These procedures also included, among others (i) evaluating management's accounting policies related to the recognition of subscription revenue, (ii) testing, for a sample of contracts, management's assessment of whether all of the criteria for revenue recognition have been met based on the contractual terms and conditions and evaluating the impact of management's assessment on the completeness, accuracy, and occurrence of revenue recognized, and (iii) testing the completeness and accuracy of data provided by management.

/s/ PricewaterhouseCoopers LLP
Atlanta, Georgia
March 22, 2024

We have served as the Company's auditor since 2014.

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF FINANCIAL POSITION
(in thousands)

	February 2, 2024	February 3, 2023
ASSETS		
Current assets:		
Cash and cash equivalents	$ 68,655	$ 143,517
Accounts receivable, net	54,266	72,627
Inventories	727	620
Other current assets	14,491	17,526
Total current assets	138,139	234,290
Property and equipment, net	2,149	4,632
Goodwill	425,472	425,519
Operating lease right-of-use assets, net	5,069	9,256
Intangible assets, net	83,235	106,208
Other non-current assets	70,715	60,965
Total assets	$ 724,779	$ 840,870
LIABILITIES AND STOCKHOLDERS' EQUITY		
Current liabilities:		
Accounts payable	$ 8,974	$ 18,847
Accrued and other current liabilities	61,895	81,566
Deferred revenue	131,245	145,170
Total current liabilities	202,114	245,583
Long-term deferred revenue	5,706	11,162
Operating lease liabilities, non-current	7,803	12,141
Other non-current liabilities	7,831	14,023
Total liabilities	223,454	282,909
Commitments and contingencies (Note 7)		
Stockholders' equity:		
Preferred stock - $0.01 par value: 200,000 shares authorized; 0 shares issued	—	—
Common stock - Class A of $0.01 par value: 2,500,000 shares authorized; 16,392 and 14,749 shares issued and outstanding at February 2, 2024 and February 3, 2023, respectively	164	147
Common stock - Class B of $0.01 par value: 500,000 shares authorized; 70,000 shares issued and outstanding	700	700
Additional paid in capital	996,291	967,367
Accumulated deficit	(470,163)	(384,121)
Accumulated other comprehensive loss	(5,771)	(6,237)
Treasury stock, at cost - 1,257 and 1,257 shares, respectively	(19,896)	(19,896)
Total stockholders' equity	501,325	557,961
Total liabilities and stockholders' equity	$ 724,779	$ 840,870

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

SECUREWORKS CORP.

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

	Fiscal Year Ended		
	February 2, 2024	**February 3, 2023**	**January 28, 2022**
Net revenue:			
Subscription	$ 304,556	$ 363,448	$ 408,947
Professional services	61,323	100,027	126,267
Total net revenue	365,879	463,475	535,214
Cost of revenue:			
Subscription	109,833	131,554	143,515
Professional services	38,287	59,503	73,611
Total cost of revenue	148,120	191,057	217,126
Gross profit	217,759	272,418	318,088
Operating expenses:			
Research and development	110,996	139,785	122,494
Sales and marketing	118,351	163,637	145,134
General and administrative	83,233	101,554	102,834
Reorganization and other related charges	17,145	15,471	—
Total operating expenses	329,725	420,447	370,462
Operating loss	(111,966)	(148,029)	(52,374)
Interest and other (expense) income, net	(2,554)	1,248	(3,532)
Loss before income taxes	(114,520)	(146,781)	(55,906)
Income tax benefit	(28,478)	(32,282)	(16,115)
Net loss	$ (86,042)	$ (114,499)	$ (39,791)
Net loss per common share (basic and diluted)	$ (1.00)	$ (1.36)	$ (0.48)
Weighted-average common shares outstanding (basic and diluted)	86,049	84,389	82,916

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

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF COMPREHENSIVE LOSS

(in thousands)

	Fiscal Year Ended		
	February 2, 2024	**February 3, 2023**	**January 28, 2022**
Net loss	$ (86,042)	$ (114,499)	$ (39,791)
Foreign currency translation adjustments, net of tax	466	(3,565)	(2,012)
Comprehensive loss	$ (85,576)	$ (118,064)	$ (41,803)

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

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF CASH FLOWS

(in thousands)

	Fiscal Year Ended		
	February 2, 2024	**February 3, 2023**	**January 28, 2022**
Cash flows from operating activities:			
Net loss	$ (86,042)	$ (114,499)	(39,791)
Adjustments to reconcile net loss to net cash (used in) provided by operating activities:			
Depreciation and amortization	31,893	36,668	40,520
Amortization of right of use asset	2,024	3,800	3,846
Reorganization and other related charges	3,272	6,112	—
Amortization of costs capitalized to obtain revenue contracts	17,133	18,203	19,330
Amortization of costs capitalized to fulfill revenue contracts	3,232	4,773	5,186
Stock-based compensation expense	35,104	36,855	30,446
Income tax benefit	(28,478)	(32,282)	(16,115)
Provision for credit losses	(282)	(524)	(430)
Changes in assets and liabilities:			
Accounts receivable	17,952	11,247	20,865
Net transactions with Dell	5,708	(1,278)	(6,500)
Inventories	(107)	(115)	55
Other assets	371	24,055	(16,251)
Accounts payable	(9,685)	4,050	(1,330)
Deferred revenue	(17,151)	(16,912)	472
Operating leases, net	(4,553)	(5,465)	(5,397)
Accrued and other liabilities	(29,550)	(33,433)	(10,374)
Net cash (used in) provided by operating activities	(59,159)	(58,745)	24,532
Cash flows from investing activities:			
Capital expenditures	(1,180)	(2,307)	(2,095)
Software development costs	(5,243)	(3,704)	(6,086)
Net cash used in investing activities	(6,423)	(6,011)	(8,181)
Cash flows from financing activities:			
Proceeds from stock option exercises	—	—	4,134
Taxes paid on vested restricted shares	(6,163)	(8,887)	(12,502)
Net cash used in financing activities	(6,163)	(8,887)	(8,368)
Effect of exchange rate changes on cash and cash equivalents	(3,117)	(3,495)	(7,628)
Net (decrease) increase in cash and cash equivalents	(74,862)	(77,138)	355
Cash and cash equivalents at beginning of the period	143,517	220,655	220,300
Cash and cash equivalents at end of the period	$ 68,655	$ 143,517	$ 220,655
Supplemental Disclosures of Non-Cash Investing and Financing Activities:			
Income taxes paid	$ 594	$ 2,461	$ 2,554

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

SECUREWORKS CORP.

CONSOLIDATED STATEMENTS OF STOCKHOLDERS' EQUITY

(in thousands, except per share data)

	Common Stock - Class A		Common Stock - Class B						
	Outstanding Shares	Amount	Outstanding Shares	Amount	Additional Paid in Capital	Accumulated Deficit	Accumulated Other Comprehensive (Loss) Income	Treasury Stock	Total Stockholders' Equity
Balances, January 29, 2021	**12,450**	**$ 125**	**70,000**	**$ 700**	**$ 917,344**	**$ (229,831)**	**$ (660)**	**$ (19,896)**	**$ 667,781**
Net loss	—	—	—	—	—	(39,791)	—	—	(39,791)
Other comprehensive loss	—	—	—	—	—	—	(2,012)	—	(2,012)
Vesting of restricted stock units	1,515	15	—	—	(15)	—	—	—	—
Exercise of stock options	1,417	14	—	—	4,120	—	—	—	4,134
Grant and forfeitures of restricted stock awards	485	5	—	—	(5)	—	—	—	—
Common stock withheld as payment of taxes and cost for equity awards	(1,585)	(16)	—	—	(12,486)	—	—	—	(12,502)
Stock-based compensation	—	—	—	—	30,446	—	—	—	30,446
Balances, January 28, 2022	**14,282**	**$ 143**	**70,000**	**$ 700**	**$ 939,404**	**$ (269,622)**	**$ (2,672)**	**$ (19,896)**	**$ 648,057**
Net loss	—	—	—	—	—	(114,499)	—	—	(114,499)
Other comprehensive loss	—	—	—	—	—	—	(3,565)	—	(3,565)
Vesting of restricted stock units	1,718	17	—	—	(17)	—	—	—	—
Grant and forfeitures of restricted stock awards	(423)	(4)	—	—	4	—	—	—	—
Common stock withheld as payment of taxes and cost for equity awards	(828)	(8)	—	—	(8,879)	—	—	—	(8,887)
Stock-based compensation	—	—	—	—	36,855	—	—	—	36,855
Balances, February 3, 2023	**14,749**	**$ 147**	**70,000**	**$ 700**	**$ 967,367**	**$ (384,121)**	**$ (6,237)**	**$ (19,896)**	**$ 557,961**
Net loss	—	—	—	—	—	(86,042)	—	—	(86,042)
Other comprehensive income	—	—	—	—	—	—	466	—	466
Vesting of restricted stock units	2,455	25	—	—	(25)	—	—	—	—
Common stock withheld as payment of taxes and cost for equity awards	(812)	(8)	—	—	(6,155)	—	—	—	(6,164)
Stock-based compensation	—	—	—	—	35,104	—	—	—	35,104
Balance, February 2, 2024	**16,392**	**$ 164**	**70,000**	**$ 700**	**$ 996,291**	**$ (470,163)**	**$ (5,771)**	**$ (19,896)**	**$ 501,325**

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

NOTE 1 - DESCRIPTION OF THE BUSINESS AND BASIS OF PRESENTATION

Description of the Business

SecureWorks Corp. (individually and collectively with its consolidated subsidiaries, "Secureworks" or the "Company") is a leading global cybersecurity provider of technology-driven security solutions singularly focused on protecting the Company's customers.

On April 27, 2016, the Company completed its initial public offering ("IPO"). Upon the closing of the IPO, Dell Technologies Inc. ("Dell Technologies") owned, indirectly through Dell Inc. and Dell Inc.'s subsidiaries (Dell Inc., individually and collectively with its consolidated subsidiaries, "Dell"), all shares of the Company's outstanding Class B common stock, which as of February 2, 2024 represented approximately 81.0% of the Company's total outstanding shares of common stock and approximately 97.7% of the combined voting power of both classes of the Company's outstanding common stock.

The Company has one primary business activity, which is to provide customers with technology-driven cybersecurity solutions. The Company's chief operating decision-maker, who is the Chief Executive Officer, makes operating decisions, assesses performance, and allocates resources on a consolidated basis. There are no segment managers who are held accountable for operations and operating results below the consolidated unit level. Accordingly, Secureworks operates its business as a single reportable segment.

Basis of Presentation and Consolidation

The Company's consolidated financial statements have been prepared in accordance with accounting principles generally accepted in the United States of America ("GAAP"). Certain amounts from the prior years have been reclassified to conform to current year presentation. The preparation of financial statements in accordance with GAAP requires management to make assumptions and estimations that affect the amounts reported in the Company's financial statements and notes. The inputs into certain of the Company's assumptions and estimations considered the economic implications of the Ukraine/Russia conflict and inflation concerns on the Company's critical and significant accounting estimates. The consolidated financial statements include assets, liabilities, revenue, and expenses of all majority-owned subsidiaries. Intercompany transactions and balances are eliminated in consolidation.

For the periods presented, Dell has provided various corporate services to the Company in the ordinary course of business, including finance, tax, human resources, legal, insurance, IT, procurement, and facilities-related services. The cost of these services is charged in accordance with a shared services agreement, as amended or amended and restated, in part, from time to time, that went into effect on August 1, 2015. For more information regarding the related party transactions, see "Note 13—Related Party Transactions."

During the periods presented in the financial statements, Secureworks did not file separate federal tax returns, as the Company is generally included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate-return method, modified to apply the benefits-for-loss approach. Under this approach, net operating losses or other tax attributes are characterized as realized or as realizable by Secureworks when those attributes are utilized or expected to be utilized by other members of the Dell affiliated group. See "Note 11—Income and Other Taxes" for more information.

Revisions

The Company's historical classification of the effects of exchange rate changes on the Company's foreign denominated cash and cash equivalents balances was not presented separately as the effect of exchange rate changes on cash and cash equivalents in the Company's Consolidated Statement of Cash Flows, but rather was included as a component of net cash provided by (used in) operating activities and investing activities. The Company has revised the Consolidated Statements of Cash Flows for fiscal year 2023 and 2022 to correct these classifications. For the fiscal year ended February 3, 2023, the impact of this correction was a decrease in net cash used in operating activities of $3.9 million and an increase in net cash used for capital expenditures, as included in the total net cash used in investing activities, of $0.4 million. For the fiscal year ended January 28, 2022, the impact of this correction was an increase in net cash provided by operating activities of $7.8 million, and an increase in cash used for capital expenditures, as included in total cash used in investing activities, of $0.2 million. The corresponding amounts are now presented separately on the Consolidated Statements of Cash Flows as the effect of exchange rate changes on cash and cash equivalents for each of the periods. These revisions do not impact the Consolidated Statements of Operations, the Consolidated Statements of Comprehensive Loss, or the Consolidated Statements of Financial Position.

The Company has concluded that the effect of this revision is not material to any of our previously issued financial statements. This revision also impacts our unaudited interim Condensed Consolidated Financial Statements for each fiscal quarter during fiscal 2024. Please see Note 15 for further details related to impacts on referenced interim periods.

Fiscal Year

The Company's fiscal year is the 52- or 53-week period ending on the Friday closest to January 31. The Company refers to the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, as fiscal 2024, fiscal 2023 and fiscal 2022, respectively. Fiscal 2024 and fiscal 2022 each consisted of 52 weeks. Fiscal 2023 consisted of 53 weeks.

Use of Estimates

The preparation of financial statements in conformity with GAAP requires management to make estimates and assumptions that affect the reported amounts of assets and liabilities, the disclosure of contingent assets and liabilities at the date of the financial statements, and the reported amounts of revenue and expenses during the reporting periods. Estimates are revised as additional information becomes available. In the Consolidated Statements of Operations, estimates are used when accounting for revenue arrangements, determining the cost of revenue, allocating cost, and estimating the impact of contingencies. In the Consolidated Statements of Financial Position, estimates are used in determining the valuation and recoverability of assets, such as accounts receivables, inventories, fixed assets, capitalized software, goodwill and other identifiable intangible assets, and purchase price allocation for business combinations. Estimates are also used in determining the reported amounts of liabilities, such as taxes payable and the impact of contingencies. All estimates also impact the Consolidated Statements of Operations. Actual results could differ from these estimates due to risks and uncertainties, including uncertainty in the current economic environment due to the Ukraine/Russia conflict and impacts of inflation. The Company considered the potential impact of the current economic and geopolitical uncertainty on its estimates and assumptions and determined there was not a material impact to the Company's consolidated financial statements as of and for the fiscal year ended February 2, 2024. As the current economic environment continues to develop, many of the Company's estimates could require increased judgment and be subject to a higher degree of variability and volatility. As a result, the Company's estimates may change materially in future periods.

Liquidity

In recent periods, the Company has incurred losses from operations and operating cash outflows and, as of the Balance Sheet date, the Company has reported a deficit in working capital.

During fiscal 2024, the Company completed reorganization actions which are expected to result in significant cost savings as the Company completes a transition to higher value, higher margin Taegis solutions. These efforts are expected to optimize the organizational structure and increase scalability to better position the Company for continued growth with improving operating margins over time. In the event that the Company's financial results are below its expectations as a result of these or other factors, the Company may need to take additional actions to preserve existing cash reserves.

As of February 2, 2024, the Company held $68.7 million of cash and cash equivalents. There were no amounts drawn on the $50 million Revolving Credit Facility with Dell as of February 2, 2024. The Company believes that its cash and cash equivalents and access to the Revolving Credit Facility will provide sufficient liquidity to meet its material cash requirements, including to fund its business and meet its obligations for at least 12 months from the filing date of this report.

NOTE 2 — SIGNIFICANT ACCOUNTING POLICIES

Cash and Cash Equivalents. As of February 2, 2024 and February 3, 2023, cash and cash equivalents are comprised of cash held in bank accounts and money market funds. The cash and cash equivalents are reported at their current carrying value, which approximates fair value due to the short-term nature of these instruments. The money market funds are valued using quoted market prices and are included as Level 1 inputs. As of February 2, 2024 and February 3, 2023, the Company had $1.7 million and $16.5 million, respectively, invested in money market funds.

Accounts Receivable. Trade accounts receivable are recorded at the invoiced amount, net of allowances for credit losses. Accounts receivable are charged against the allowance for credit losses when deemed uncollectible. Management regularly reviews the adequacy of the allowance for credit losses by considering the age of each outstanding invoice, each customer's expected ability to pay, and the collection history with each customer, when applicable, to determine whether a specific allowance is appropriate. As of February 2, 2024 and February 3, 2023, the allowance for credit losses was $1.6 million and $2.4 million, respectively.

Unbilled accounts receivable included in accounts receivable, totaling $2.9 million and $4.8 million as of February 2, 2024 and February 3, 2023, respectively, relate to work that has been performed, though invoicing has not yet occurred. All of the unbilled receivables are expected to be billed and collected within the upcoming fiscal year.

Allowance for Credit Losses. The Company recognizes an allowance for losses on accounts receivable in an amount equal to the estimated probable losses, net of recoveries. The Company assesses its allowance by taking into consideration forecasts of future economic conditions, information about past events, such as its historical trend of write-offs, and customer-specific circumstances, such as bankruptcies and disputes. The expense associated with the allowance for credit losses is recognized in general and administrative expenses.

Fair Value Measurements. The Company measures fair value within the guidance of the three-level valuation hierarchy. This hierarchy is based upon the transparency of inputs to the valuation of an asset or liability as of the measurement date. The categorization of a measurement within the valuation hierarchy is based upon the lowest level of input that is significant to the fair value measurement. The carrying amounts of the Company's financial instruments, including cash equivalents, accounts receivable, accounts payable, and accrued expenses, approximate their respective fair values due to their short-term nature.

Inventories. Inventories consist of finished goods, which include hardware devices such as servers, log retention devices and appliances that are sold in connection with the Company's solutions offerings. Inventories are stated at lower of cost or net realizable value, with cost being determined on a first-in, first-out (FIFO) basis.

Prepaid Maintenance and Support Agreements. Prepaid maintenance and support agreements represent amounts paid to third-party service providers for maintenance, support, and software license agreements in connection with the Company's obligations to provide maintenance and support services. The prepaid maintenance and support agreement balance is amortized on a straight-line basis over the contract term and is primarily recognized as a component of cost of revenue. Amounts that are expected to be amortized within one year are recorded in other current assets and the remaining balance is recorded in other non-current assets.

Property and Equipment. Property and equipment are carried at depreciated cost. Depreciation is calculated using the straight-line method over the estimated economic lives of the assets, which range from two to five years. Leasehold improvements are amortized over the shorter of five years or the lease term. For the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, depreciation expense was $4.1 million, $5.9 million and $10.3 million, respectively. Gains or losses related to retirement or disposition of fixed assets are recognized in the period incurred.

Leases. The Company determines if any arrangement is, or contains, a lease at inception based on whether the Company has the right to control the asset during the contract period and other facts and circumstances. Secureworks is the lessee in a lease contract when the Company obtains the right to control the asset. Operating leases are included in the line items operating lease right-of-use assets, net; accrued and other current liabilities; and operating lease liabilities, non-current in the Consolidated Statements of Financial Position. Leases with a lease term of 12 months or less at inception are not recorded in the Consolidated Statements of Financial Position and are expensed on a straight-line basis over the lease term in the Consolidated Statements of Operations. The Company determines the lease term by assuming the exercise of renewal options that are reasonably certain. As most of the Company's leases do not provide an implicit interest rate, Secureworks uses the Company's incremental borrowing rate based on the information available at commencement date in determining the present value of future payments. When the Company's contracts contain lease and non-lease components, the Company accounts for both components as a single lease component. See "Note 8—Leases" for further discussion.

Intangible Assets Including Goodwill. Identifiable intangible assets with finite lives are amortized on a straight-line basis over their estimated useful lives. Finite-lived intangible assets are reviewed for impairment on a quarterly basis, or as potential

triggering events are identified. Goodwill and indefinite-lived intangible assets are tested for impairment on an annual basis in the third fiscal quarter, or sooner if an indicator of impairment exists.

The Company may elect to first assess qualitative factors to determine whether it is more likely than not (greater than 50% likelihood) that the fair value of the Company's goodwill at the reporting unit, as well as indefinite-lived assets at the individual asset level, are less than their respective carrying amounts. The Company has determined it has one reporting unit.

The qualitative assessment includes the Company's consideration of relevant events and circumstances that would affect the Company's single reporting unit and indefinite-lived assets, including macroeconomic, industry, and market conditions, the Company's overall financial performance, and trends in the market price of the Company's Class A common stock. If indicators of impairment exist after performing the qualitative assessment, the Company will perform a quantitative impairment assessment of goodwill and indefinite-lived assets. The Company may also choose to perform the quantitative assessment periodically even if the qualitative assessment does not require the Company to do so. For the Company's goodwill and indefinite-lived intangible assets, if the quantitative analysis determines the carrying amount exceeds the fair value at the reporting unit level or individual asset level, an impairment charge is recognized in an amount equal to that excess.

The Company performed a Step 0 qualitative assessment of goodwill at the reporting unit level, and the indefinite-lived intangible assets at the individual asset level, during its third quarter of fiscal 2024. It was concluded that it was not more likely than not that the fair value of the reporting unit and indefinite-lived intangible asset was less than their respective carrying values. The Company has determined that it has a single goodwill reporting unit, and, accordingly, assessed the goodwill carrying value at the reporting unit level. Subsequently, no events occurred through February 2, 2024 year-end that would indicate an impairment exists.

Impairment of long-lived assets. The Company evaluates all long-lived assets, other than goodwill, whenever events or circumstances change that indicate the asset's carrying value may no longer be recoverable. If impairment indicators exist, a test of recoverability is performed by comparing the sum of the estimated undiscounted future cash flows attributable to the asset's carrying value. Impairment analyses are performed at the asset group level. If the asset's carrying value is not recoverable, impairment is measured by determining the asset's fair value and recording any difference as an impairment loss. Long-lived assets subject to this policy include property, plant & equipment, definite-lived intangible assets, and Right-of-use assets. Impairment losses of $2.9 million and $4.0 million were recognized to the Company's right-of-use assets for the fiscal years ended February 2, 2024 and February 3, 2023, respectively. No impairments were recognized in the fiscal year ended January 28, 2022.

Deferred Commissions and Deferred Fulfillment Costs. The Company accounts for both costs to obtain a contract for a customer, which are defined as costs that the Company would not have incurred if the contract had not been obtained, and costs to fulfill a contract by capitalizing and systematically amortizing the assets on a basis that is consistent with the transfer to the customer of the goods or services to which the assets relate. These costs generate or enhance resources used in satisfying performance obligations that directly relate to contracts. The Company recognizes the incremental costs of obtaining contracts as an expense when incurred if the amortization period of the incremental costs of obtaining contracts that the Company otherwise would have recognized is one year or less.

The Company's customer acquisition costs are primarily attributable to sales commissions and related fringe benefits earned by the Company's sales force and such costs are considered incremental costs to obtain a contract. Sales commissions for initial contracts are deferred and amortized taking into consideration the pattern of transfer to which assets relate and may include expected renewal periods where renewal commissions are not commensurate with the initial commission period. The Company recognizes deferred commissions on a straight-line basis over the life of the customer relationship (estimated to be six years) in sales and marketing expenses. These assets are classified as non-current and included in other non-current assets in the Consolidated Statements of Financial Position. As of February 2, 2024 and February 3, 2023, the amount of deferred commissions included in other non-current assets was $41.8 million and $49.6 million, respectively.

The Company historically recognized deferred fulfillment costs related to its other managed security services in cost of revenue on a straight-line basis over the device service life estimated at four years. Consistent with the Company's end-of-life transition of its non-strategic managed security services, these deferred fulfillment costs are fully amortized as of fiscal 2024. As of February 2, 2024 and February 3, 2023, the amount of deferred fulfillment costs included in other non-current assets was $0.0 million and $3.2 million, respectively.

Foreign Currency Translation. During the periods presented, Secureworks primarily operated in the United States. For the majority of the Company's international subsidiaries, the Company has determined that the functional currency of those subsidiaries is the local currency. Accordingly, assets and liabilities for these entities are translated at current exchange rates in effect at the balance sheet date. Revenue and expenses from these international subsidiaries are translated using the monthly average exchange rates in effect for the period in which the items occur. Foreign currency translation adjustments are included as a component of accumulated other comprehensive loss, while foreign currency transaction gains and losses are recognized in the Consolidated Statements of Operations within interest and other (expense) income, net. These transaction gains (losses) totaled $(2.6) million, $0.8 million and $(3.4) million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

Revenue Recognition. Secureworks derives revenue primarily from subscription services and professional services. Subscription revenue is derived from (i) the Taegis security platform and (ii) managed security services. Professional services typically include incident response and security and risk consulting solutions.

As indicated above, the Company has one primary business activity, which is to provide customers with technology-driven information security solutions. The Company's chief operating decision maker, who is the Chief Executive Officer, makes operating decisions, assesses performance, and allocates resources on a consolidated basis. There are no segment managers who are held accountable for operations and operating results below the consolidated unit level. Accordingly, the Company is considered to be in a single reportable segment and operating unit structure.

Beginning in fiscal 2021, the Company began transitioning its subscription business to its Taegis subscription solutions from non-strategic other managed security subscription services. As part of the Company's ongoing transition, early in the fourth quarter of fiscal 2022, it informed customers that many of its other managed security subscription services would no longer be available for purchase, effective as of the beginning of fiscal 2023, as many of those services offer a natural transition to its Taegis platform. Renewals associated with many of the Company's existing other managed security subscription services were not extended beyond the end of fiscal 2023.

The following table presents revenue by service type (in thousands):

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
Net revenue:			
Taegis Subscription Solutions	$ 265,298	$ 188,085	$ 85,599
Managed Security Services	39,258	175,363	323,348
Total Subscription revenue	304,556	363,448	408,947
Professional Services	61,323	100,027	126,267
Total net revenue	$ 365,879	$ 463,475	$ 535,214

The Company's proprietary Taegis security platform was purpose-built as a subscription-based SaaS platform that combines the power of artificial intelligence and machine-learning with security analytics and threat intelligence to unify detection and response across endpoint, network, cloud, and other business systems for better security outcomes and simpler security operations.

Taegis' core offerings are the security platform, Taegis XDR, and our supplemental MDR service, ManagedXDR. Customers do not have the right to take possession of the security platform. Revenue for our Taegis SaaS solutions is recognized on a straight-line basis over the term of the arrangement, beginning with provision of the tenant by grant of access to the security platform.

The ManagedXDR service is identified as a distinct performance obligation that is separable from the XDR SaaS solution. While a customer must purchase and deploy the XDR solution to gain any utility from the ManagedXDR service, a customer can purchase and benefit from using the XDR SaaS solution on its own. In order to conclude that the two promises are not separately identifiable, the interrelationship and interdependence would most likely have to be reciprocal between the two separate offerings. The nature of the ManagedXDR service is to stand ready or deliver an unspecified quantity of services each day during the contract term, based on customer-specific needs. The ManagedXDR service period is contractually tied to the related security solution and, as a stand-ready obligation, will be recognized on a straight-line basis over the term of the arrangement.

Subscription-based managed security service arrangements typically included security services, up-front installation fees and maintenance and also may include the provision of an associated hardware appliance. The Company uses its hardware appliances in providing security services required to access the Company's legacy Counter Threat Platform. The arrangements that require hardware do not typically convey ownership of the appliance to the customer. Moreover, any related installation fees are non-refundable and incapable of being distinct within the context of the arrangement. Therefore, the Company determined that these arrangements constitute a single performance obligation for which the revenue and any related costs are recognized over the term of the arrangement ratably, which reflects the Company's performance in transferring control of the services to the customer.

Amounts that have been invoiced for the subscription-based managed security services and the Taegis subscription solutions where the relevant revenue recognition criteria have not been met will be included in deferred revenue.

Professional services consist primarily of fixed-fee and retainer-based contracts. Revenue from these engagements is recognized using an input method over the contract term.

The Company reports revenue net of any revenue-based taxes assessed by governmental authorities that are imposed on, and concurrently with, specific revenue-producing transactions.

The Company recognizes revenue when all of the following criteria are met:

- ***Identification of the contract, or contracts, with a customer***—A contract with a customer exists when (i) the Company enters into an enforceable contract with a customer, (ii) the contract has commercial substance and the parties are committed to perform, and (iii) payment terms can be identified and collection of substantially all consideration to which the Company will be entitled in exchange for goods or services that will be transferred is deemed probable based on the customer's intent and ability to pay. Contracts entered into for professional services and subscription-based solutions near or at the same time are generally not combined as a single contract for accounting purposes, since neither the pricing nor the services are interrelated.

- ***Identification of the performance obligations in the contract*—**Performance obligations promised in a contract are identified based on the goods or services that will be transferred to the customer that are both (i) capable of being distinct, whereby the customer can benefit from the goods or service either on its own or together with other resources that are readily available from third parties or from the Company, and (ii) distinct in the context of the contract, whereby the transfer of the goods or services is separately identifiable from other promises in the contract. When promised goods or services are incapable of being distinct, the Company accounts for them as a combined performance obligation. With regard to a typical contract for subscription-based managed security services, the performance obligation represents a series of distinct services that will be accounted for as a single performance obligation. For a typical contract that includes subscription-based SaaS applications, each is generally considered to be distinct and accounted for as separate performance obligations. In a typical professional services contract, Secureworks has a separate performance obligation associated with each service. The Company generally acts as a principal when delivering either the subscription-based solutions or the professional services arrangement and, thus, recognizes revenue on a gross basis.
- ***Determination of the transaction price*—**The total transaction price is primarily fixed in nature as the consideration is tied to the specific services purchased by the customer, which constitutes a series for delivery of the solutions over the duration of the contract for the Company's subscription services. For professional services contracts, variable consideration exists in the form of rescheduling penalties and expense reimbursements; no estimation is required at contract inception, since variable consideration is allocated to the applicable period.
- ***Allocation of the transaction price to the performance obligations in the contract*—**The Company allocates the transaction price to each performance obligation based on the performance obligation's standalone selling price. Standalone selling price is determined by considering all information available to the Company, such as historical selling prices of the performance obligation, geographic location, overall strategic pricing objective, market conditions and internally approved pricing guidelines related to the performance obligations.
- ***Recognition of revenue when, or as, the Company satisfies performance obligation*—**The Company recognizes revenue over time on a ratable recognition basis using a time-elapsed output method to measure progress for all subscription-based performance obligations, including managed security services and SaaS applications, over the contract term. For any upgraded installation services which the Company has determined represent a performance obligation separate from its subscription-based arrangements, revenue is recognized over time using hours elapsed over the service term as an appropriate method to measure progress. For the performance obligation pertaining to professional services arrangements, the Company recognizes revenue over time using an input method based on time (hours or days) incurred to measure progress over the contract term.

Deferred Revenue (Contract Liabilities). Deferred revenue represents amounts contractually billed to customers or payments received from customers for which revenue has not yet been recognized. Deferred revenue that is expected to be recognized as revenue within one year is recorded as short-term deferred revenue and the remaining portion is recorded as long-term deferred revenue.

The Company has determined that its contracts generally do not include a significant financing component. The primary purpose of the Company's invoicing terms is to provide customers with simplified and predictable ways of purchasing its solutions, not to receive financing from customers or to provide customers with financing. Examples of such terms include invoicing at the beginning of a subscription term with revenue recognized ratably over the contract period.

Cost of Revenue. Cost of revenue consists primarily of compensation and related expenses, including salaries, benefits and performance-based compensation for employees who provide security services to customers, including those who deliver services associated with the Taegis platform. Other expenses include depreciation of equipment and costs associated with maintenance agreements for hardware provided to customers as part of their subscription-based solutions. In addition, cost of revenue includes amortization of technology licensing fees and external software development costs capitalized, fees paid to vendors who support and enable subscription offerings, maintenance fees and overhead allocations.

Research and Development. Research and development costs are expensed as incurred. Research and development expenses include compensation and related expenses for the continued development of solutions offerings, including a portion of costs related to the threat research team, which focuses on the identification of system vulnerabilities, data forensics and malware analysis, and product management. In addition, expenses related to the development and prototype of new solutions offerings also are included in research and development costs, as well as allocated overhead. The Company's solutions offerings have generally been developed internally.

Sales and Marketing. Sales and marketing expense consists of compensation and related expenses that include salaries, benefits, and performance-based compensation (including sales commissions and related expenses for sales and marketing personnel), marketing and advertising programs, such as lead generation, customer advocacy events, other brand-building expenses and

allocated overhead. Advertising costs are expensed as incurred and were $26.2 million, $42.8 million and $25.2 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

General, and Administrative. General and administrative expense primarily includes the costs of human resources and recruiting, finance and accounting, legal support, management information systems and information security systems, facilities management, and other administrative functions, offset by allocations of information technology and facilities costs to other functions.

Reorganization and other related charges. Reorganization and other related charges consist primarily of severance and other termination benefits and real estate-related expenses, as described in "Note 14—Reorganization and Other Related Costs."

Software Development Costs. Qualifying software costs developed for internal use are capitalized when application development begins, it is probable that the project will be completed, and the software will be used as intended. In order to expedite delivery of the Company's security solutions, the application stage typically commences before the preliminary development stage is completed. Accordingly, no significant internal-use software development costs have been capitalized during any period presented.

The Company capitalizes development costs associated with software and applications to be sold, leased, or otherwise marketed after technological feasibility of the software or application is established. Under the Company's current practice of developing new software, the technological feasibility of the underlying software or application is not established until substantially all product development and testing is complete, which generally includes the development of a working model. Software development costs associated with software and applications to be sold, leased, or otherwise marketed that have been capitalized to date total approximately $5.2 million for the fiscal year ended February 2, 2024.

Income Taxes. Current income tax expense is the amount of income taxes expected to be payable for the current year. Deferred tax assets and liabilities are recorded based on the difference between the financial statement and tax basis of assets and liabilities using enacted tax rates in effect for the year in which the differences are expected to reverse. The effect on deferred tax assets and liabilities of a change in tax rates is recognized in the Consolidated Statement of Operations in the period that includes the enactment date. The Company calculates a provision for income taxes using the asset and liability method, under which deferred tax assets and liabilities are recognized by identifying the temporary differences arising from the different treatment of items for tax and accounting purposes. The Company accounts for the tax impact of including Global Intangible Low Tax Income, or GILTI, in U.S. taxable income as a period cost. The Company provides valuation allowances for deferred tax assets, where appropriate. In assessing the need for a valuation allowance, the Company considers all available evidence for each jurisdiction, including past operating results, estimates of future taxable income, and the feasibility of ongoing tax planning strategies. In the event the Company determines all or part of the net deferred tax assets are not realizable in the future, it will make an adjustment to the valuation allowance that would be charged to earnings in the period in which such determination is made.

The accounting guidance for uncertainties in income tax prescribes a comprehensive model for the financial statement recognition, measurement, presentation, and disclosure of uncertain tax positions taken or expected to be taken in income tax returns. The Company recognizes a tax benefit from an uncertain tax position in the financial statements only when it is more likely than not that the position will be sustained upon examination, including resolution of any related appeals or litigation processes, based on the technical merits and a consideration of the relevant taxing authority's administrative practices and precedents.

During the periods presented in the financial statements, the Company did not file separate federal tax returns, as the Company was generally included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate-return method, modified to apply the benefits-for-loss approach. Under the benefits-for-loss approach, net operating losses or other tax attributes are characterized as realized or as realizable by the Company when those attributes are utilized or expected to be utilized by other members of the Dell affiliated group.

Stock-Based Compensation. The Company's compensation programs include grants under the SecureWorks Corp. 2016 Long-Term Incentive Plan and, prior to the IPO date, grants under share-based payment plans of Dell Technologies. Under the plans, the Company, and prior to the IPO, Dell Technologies, have granted stock options, restricted stock awards, and restricted stock units. Compensation expense related to stock-based transactions is measured and recognized in the financial statements based on grant date fair value. Fair value for restricted stock awards and restricted stock units under the Company's plan is based on the closing price of the Company's Class A common stock as reported on the Nasdaq Global Select Market on the day of the grant. The fair value of each option award is estimated on the grant date using the Black-Scholes option-pricing model and a single option award approach. This model requires that at the date of grant the Company must determine the fair value of the underlying Class A common stock, the expected term of the award, the expected volatility, risk-free interest rates and expected dividend yield. The Company's annual grant of restricted stock and restricted stock units issued during the fiscal year ended February 2, 2024 vest over an average service period of three years and approximately 17% of such awards are subject to

performance conditions. Stock-based compensation expense with respect to service-based awards is adjusted for forfeitures and recognized using a straight-line basis over the requisite service periods of the awards, which is generally three to four years. Stock-based compensation expense with respect to performance awards is adjusted for forfeitures and performance criteria and recognized on a graded vesting basis. The Company estimates a forfeiture rate, based on an analysis of actual historical forfeitures, to calculate stock-based compensation expense.

Loss Contingencies. Secureworks is subject to the possibility of various losses arising in the ordinary course of business. An estimated loss contingency is accrued when it is probable that an asset has been impaired or a liability has been incurred and the amount of loss can be reasonably estimated. The Company regularly evaluates current information available to determine whether such accruals should be adjusted and whether new accruals are required. See "Note 7– Commitments and Contingencies" for more information about loss contingencies.

Recently Issued Accounting Pronouncements

Segment Reporting – In November 2023, the Financial Accounting Standards Board, or FASB, issued Accounting Standards Update, or ASU, No. 2023-07, Segment Reporting, which expands annual and interim disclosure requirements for reportable segments, primarily through enhanced disclosures about significant segment expenses. The updated standard is effective for our annual periods beginning in the fiscal year ending January 31, 2025 and interim periods beginning in the first quarter of fiscal 2026. Early adoption is permitted. The Company is currently evaluating the impact that the updated standard will have on its financial statement disclosures.

Income Taxes – In December 2023, the FASB issued ASU 2023-09, Income Taxes (Topic 740): Improvements to Income Tax Disclosures, which requires an entity, on an annual basis, to disclose additional income tax information, primarily related to the rate reconciliation and income taxes paid. The amendment in the ASU is intended to enhance the transparency and decision usefulness of income tax disclosures. The ASU is effective for annual periods beginning after December 15, 2024. The Company is currently evaluating the impact of the new standard.

NOTE 3 — NET LOSS PER SHARE

Net loss per share is calculated by dividing net loss for the periods presented by the respective weighted-average number of common shares outstanding, and it excludes any dilutive effects of share-based awards that may be anti-dilutive. Diluted net loss per common share is computed by giving effect to all potentially dilutive common shares, including common stock issuable upon the exercise of stock options and restricted stock units. The Company applies the two-class method to calculate earnings per share. Because the Class A common stock and the Class B common stock share the same rights in dividends and earnings, earnings per share (basic and diluted) are the same for both classes of common stock. Since losses were incurred in all periods presented, all potential common shares were determined to be anti-dilutive.

The following table sets forth the computation of net loss per common share (in thousands, except per share amounts):

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
Numerator:			
Net loss	$ (86,042)	$ (114,499)	$ (39,791)
Denominator:			
Weighted-average number of shares outstanding:			
Basic and Diluted	86,049	84,389	82,916
Net loss per common share:			
Basic and Diluted	$ (1.00)	$ (1.36)	$ (0.48)
Weighted-average anti-dilutive stock options, non-vested restricted stock and restricted stock units	8,048	6,039	5,020

NOTE 4 — CONTRACT BALANCES AND CONTRACT COSTS

Promises to provide the Company's subscription-based SaaS solutions are accounted for as separate performance obligations and managed security services are accounted for as a single performance obligation. Our subscription-based solutions have an average contract term of approximately two years as of February 2, 2024. Performance obligations related to the Company's professional services contracts are separate obligations associated with each service. Although the Company has multi-year customer relationships for various professional service solutions, the arrangement is typically structured as a separate performance obligation over the contract period and recognized over a duration of less than one year.

The deferred revenue balance does not represent the total contract value of annual or multi-year, non-cancelable subscription agreements. The Company invoices its customers based on a variety of billing schedules. During the fiscal year ended February 2, 2024, on average, 65% of the Company's recurring revenue was billed annually in advance and approximately 35% was billed on either a monthly or quarterly basis in advance. In addition, many of the Company's professional services engagements are billed in advance of service commencement. The deferred revenue balance is influenced by several factors, including seasonality, the compounding effects of renewals, invoice duration and invoice timing.

Changes to the Company's deferred revenue during the fiscal years ended February 2, 2024 and February 3, 2023 are as follows (in thousands):

	As of February 3, 2023	Upfront payments received and billings during the fiscal year ended February 2, 2024	Revenue recognized during the fiscal year ended February 2, 2024	As of February 2, 2024
Deferred revenue	$ 156,332	$ 186,931	$ (206,312)	$ 136,951

	As of January 28, 2022	Upfront payments received and billings during the fiscal year ended February 3, 2023	Revenue recognized during the fiscal year ended February 3, 2023	As of February 3, 2023
Deferred revenue	$ 176,068	$ 220,063	$ (239,799)	$ 156,332

Remaining Performance Obligation

The remaining performance obligation represents the transaction price allocated to contracted revenue that has not yet been recognized, which includes deferred revenue and non-cancellable contracts that are expected to be invoiced and recognized as revenue in future periods. The remaining performance obligation consists of two elements: (i) the value of remaining services to be provided through the contract term for customers whose services have been activated, or active; and (ii) the value of subscription-based solutions contracted with customers that have not yet been installed, or backlog. Backlog is not recorded in revenue, deferred revenue or elsewhere in the consolidated financial statements until the Company establishes a contractual right to invoice, at which point backlog is recorded as revenue or deferred revenue, as appropriate. The Company applies the practical expedient in ASC paragraph 606-10-50-14(a) and does not disclose information about remaining performance obligations that are part of a contract that has an original expected duration of one year or less.

The Company expects that the amount of backlog relative to the total value of its contracts will change from year to year due to several factors, including the amount invoiced at the beginning of the contract term, the timing and duration of the Company's customer agreements, varying invoicing cycles of agreements and changes in customer financial circumstances. Accordingly, fluctuations in backlog are not always a reliable indicator of future revenues.

As of February 2, 2024, the Company expects to recognize remaining performance obligations as follows (in thousands):

	Total	Expected to be recognized in the next 12 months	Expected to be recognized in 12-24 months	Expected to be recognized in 24-36 months	Expected to be recognized thereafter
Performance obligation - active	$ 210,659	$ 130,295	$ 61,904	$ 14,822	$ 3,638
Performance obligation - backlog	907	493	276	138	—
Total	$ 211,566	$ 130,788	$ 62,180	$ 14,960	$ 3,638

Deferred Commissions and Fulfillment Costs

The Company capitalizes a significant portion of its commission expense and related fringe benefits earned by its sales personnel. Additionally, the Company capitalizes certain costs to install and activate hardware and software used in its managed security services, primarily related to a portion of the compensation for the personnel who perform the installation activities. These deferred costs are amortized on a systematic basis that is consistent with the transfer to the customer of the goods or services to which the assets relate.

Changes in the balance of total deferred commission and total deferred fulfillment costs during the fiscal years ended February 2, 2024 and February 3, 2023 are as follows (in thousands):

	As of February 3, 2023	Amount capitalized	Amount expensed	As of February 2, 2024
Deferred commissions	$ 49,565	$ 9,383	$ (17,133)	$ 41,815
Deferred fulfillment costs	3,232	—	(3,232)	—

	As of January 28, 2022	Amount capitalized	Amount expensed	As of February 3, 2023
Deferred commissions	$ 53,978	$ 13,790	$ (18,203)	$ 49,565
Deferred fulfillment costs	7,597	408	(4,773)	3,232

As referenced in "Note 2 — Significant Accounting Policies," deferred commissions are recognized on a straight-line basis over the life of the customer relationship, which has a current estimated life of six years, while deferred fulfillment costs were recognized over the device service life estimated at four years. During the fourth quarter of fiscal 2022, Secureworks announced the end-of-sale for a number of managed security service offerings effective the first day of fiscal 2023. Additionally, renewals associated with many of these existing other managed security subscription services were not extended beyond the end of fiscal 2023. Consistent with the end-of-life transition of these non-strategic managed security services, these deferred fulfillment costs are fully amortized as of the end of fiscal 2024.

NOTE 5 — GOODWILL AND INTANGIBLE ASSETS

Goodwill relates to the acquisition of Dell by Dell Technologies and represents the excess of the purchase price attributable to Secureworks over the fair value of the assets acquired and liabilities assumed, as well as subsequent business combinations completed by the Company. Goodwill remained unchanged, totaling $425.5 million as of each of the fiscal years ended February 2, 2024 and February 3, 2023.

Goodwill and indefinite-lived intangible assets are tested for impairment on an annual basis during the third fiscal quarter of each fiscal year, or earlier if an indicator of impairment occurs. The Company completed the most recent annual impairment test in the third quarter of fiscal 2024 by performing a "Step 0" qualitative assessment of goodwill at the reporting unit level, as well as the Company's indefinite-lived trade name asset at the individual asset level. The Company has one reporting unit. The qualitative assessment includes the Company's consideration of the relevant events and circumstances that would affect the Company's single reporting unit, including macroeconomic, industry and market conditions, the Company's overall financial performance including changes to its cost structure during calendar 2023 and trends in the market price of the Company's Class A common stock. After assessing the totality of these events and circumstances, the Company determined it was not more-likely-than not that the fair value of the reporting unit and indefinite-lived intangible asset was less than their respective carrying values as of the annual impairment date. Further, no triggering events have transpired since the performance of the qualitative assessment that would indicate a potential impairment during the fiscal year ended February 2, 2024.

Intangible Assets

The Company's intangible assets at February 2, 2024 and February 3, 2023 were as follows:

	February 2, 2024			February 3, 2023		
	Gross	Accumulated Amortization	Net	Gross	Accumulated Amortization	Net
	(in thousands)					
Customer relationships	$ 189,518	$ (147,624)	$ 41,894	$ 189,518	$ (133,530)	$ 55,988
Acquired Technology	141,784	(139,042)	2,742	141,784	(128,612)	13,172
Developed Technology	17,070	(8,589)	8,481	11,827	(4,897)	6,930
Finite-lived intangible assets	348,372	(295,255)	53,117	343,129	(267,039)	76,090
Trade name	30,118	—	30,118	30,118	—	30,118
Total intangible assets	$ 378,490	$ (295,255)	$ 83,235	$ 373,247	$ (267,039)	$ 106,208

Amortization expense related to finite-lived intangible assets was approximately $28.2 million, $31.2 million and $30.2 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively. Amortization expense is included within cost of revenue and general and administrative expenses in the Consolidated Statement of Operations. There were no impairment charges related to intangible assets during the past three fiscal years.

Estimated future amortization expense of finite-lived intangible assets as of February 2, 2024 over the next five years and thereafter is as follow (in thousands):

Fiscal Years Ending	February 2, 2024
2025	$ 19,180
2026	17,914
2027	15,783
2028	240
2029	—
Thereafter	—
Total	$ 53,117

NOTE 6 — DEBT

Revolving Credit Facility

SecureWorks, Inc., a wholly-owned subsidiary of SecureWorks Corp., is party to a revolving credit agreement with a wholly-owned subsidiary of Dell Inc. under which the Company obtained a $50 million senior, unsecured revolving credit facility. Effective September 6, 2023, the Company executed an amendment to the revolving credit agreement that was effectuated on March 23, 2023. This amended agreement: (1) increased the maximum principal amount of borrowings outstanding under the revolving credit facility to $50 million, (2) removed the one-time increase of up to an additional $30 million in borrowings upon mutual agreement by lender and borrower, (3) extended the commitment and required repayment date under the revolving credit agreement to March 23, 2026, and (4) modified the rate at which interest accrues on funds drawn against the revolving credit agreement to SOFR plus 2.00%.

Amounts under the facility may be borrowed, repaid and reborrowed from time to time during the term of the facility. The proceeds from loans made under the facility may be used for general corporate purposes. The credit agreement contains customary representations, warranties, covenants, and events of default. The unused portion of the facility is subject to a commitment fee of 0.35%, which is due upon expiration of the facility. There was no outstanding balance under the credit facility as of February 2, 2024 or February 3, 2023, and there were no amounts borrowed under the credit facility during the fiscal years ended February 2, 2024 or February 3, 2023.

The borrower will be required to repay, in full, all of the loans outstanding, including all accrued interest, and the facility will terminate upon a change of control of SecureWorks Corp. or following a transaction in which SecureWorks, Inc. ceases to be a direct or indirect wholly-owned subsidiary of SecureWorks Corp. The facility is not guaranteed by SecureWorks Corp. or its subsidiaries.

NOTE 7 — COMMITMENTS AND CONTINGENCIES

Purchase Obligations —The Company had various purchase obligations at February 2, 2024 over a period of approximately four years with vendors or contractors, subject to the Company's operational needs. As of February 2, 2024, the purchase obligations (in thousands) are as follows:

Fiscal Years Ending	Payments Due For Purchase Obligations
2025	$ 41,589
2026	41,809
2027	59,751
2028	74
2029	—
2029 and beyond	—
Total	$ 143,223

Legal Contingencies — From time to time, the Company is involved in claims and legal proceedings that arise in the ordinary course of business. The Company accrues a liability when it believes that it is both probable that a liability has been incurred and that it can reasonably estimate the amount of the loss. The Company reviews the status of such matters at least quarterly and adjusts its liabilities as necessary to reflect ongoing negotiations, settlements, rulings, advice of legal counsel and other relevant information. Whether the outcome of any claim, suit, assessment, investigation, or legal proceeding, individually or collectively, could have a material adverse effect on the Company's business, financial condition, results of operations or cash flows will depend on a number of factors, including the nature, timing and amount of any associated expenses, amounts paid in settlement, damages or other remedies or consequences. To the extent new information is obtained and the Company's views on the probable outcomes of claims, suits, assessments, investigations, or legal proceedings change, changes in accrued liabilities would be recorded in the period in which such a determination is made. As of February 2, 2024, the Company does not believe that there were any such matters that, individually or in the aggregate, would have a material adverse effect on its business, financial condition, results of operations or cash flows.

Customer-based Taxation Contingencies—Various government entities, or taxing authorities, require the Company to bill its customers for the taxes they owe based on the services they purchase from the Company. The application of the rules of each taxing authority concerning which services are subject to each tax and how those services should be taxed involves the application of judgment. Taxing authorities periodically perform audits to verify compliance and include all periods that remain open under applicable statutes, which generally range from three to four years. These audits could result in significant assessments of past taxes, fines, and interest if the Company were found to be non-compliant. During the course of an audit, a taxing authority may question the Company's application of its rules in a manner that, if the Company were not successful in substantiating its position, could result in a significant financial impact to the Company. In the course of preparing its financial statements and disclosures, the Company considers whether information exists that would warrant disclosure or an accrual with respect to such a contingency.

As of February 2, 2024, the Company is under audit with various state taxing authorities in which rulings related to the taxability of certain of its services are pending. During fiscal 2024, the Company paid $7.4 million related to such matters. As of February 2, 2024, the Company had remaining an estimated liability in the amount of $1.6 million related to such matters. The Company will continue to appeal these rulings, but should the Company not prevail, it could be subject to obligations to pay additional taxes together with associated penalties and interest for the audited tax period, as well as additional taxes for periods subsequent to the tax audit period, including penalties and interest. While Dell does provide an indemnification for certain state tax issues for tax periods prior to August 1, 2015, such indemnification would not cover a material portion of the current estimated liability.

Indemnifications — In the ordinary course of business, the Company enters into contractual arrangements under which it agrees to indemnify its customers from certain losses incurred by the customer as to third-party claims relating to the services performed on behalf of the Company or for certain losses incurred by the customer as to third-party claims arising from certain events as defined within the particular contract. Such indemnification obligations may not be subject to maximum loss clauses. Historically, payments related to these indemnifications have been immaterial.

Concentrations — The Company sells solutions to customers of all sizes primarily through its sales organization, supplemented by sales through partners. During the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, the Company had no customer that represented 10% or more of its net revenue during any such fiscal year.

NOTE 8 — LEASES

The Company's leases primarily relate to office facilities that have remaining lease terms of 0.5 years to 2.9 years, inclusive of renewal or termination options that the Company is reasonably certain to exercise.

	Fiscal Year Ended	
	February 2, 2024	February 3, 2023
	(in thousands)	
Operating lease cost	$ 4,327	$ 4,628
Variable lease costs	402	560
Total lease costs	$ 4,729	$ 5,188
Supplemental cash flow information:		
Cash paid for amounts included in the measurement of operating lease liabilities	$ 5,371	$ 5,926

Weighted-average information associated with the measurement of the Company's remaining operating lease obligations is as follows:

	February 2, 2024	February 3, 2023
Weighted-average remaining lease term	2.8 years	3.6 years
Weighted-average discount rate	5.41 %	5.38 %

The following table summarizes the maturity of the Company's operating lease liabilities as of February 2, 2024 (in thousands):

Fiscal Years Ending	February 2, 2024
2025	$ 5,095
2026	4,526
2027	4,088
2028	—
2029	—
Thereafter	—
Total operating lease payments	$ 13,709
Less imputed interest	884
Total operating lease liabilities	$ 12,825

As part of its actions to rebalance investments cross-functionally in alignment with its current strategy and growth opportunities, the Company ceased use of certain corporate office space as a part of its real estate-related cost optimization actions. The right-of-use asset was assessed to be part of an asset group separate from the Company-level single asset group. Fair value of the asset was determined using a discounted cash flow methodology considering the asset's specific use to generate cash flows. In fiscal 2023, an impairment loss of $4.0 million was recorded to its right-of-use assets. During fiscal 2024, in consideration of updated facts and circumstances, the Company reassessed the discounted cash flow methodology used to derive fair value of this asset group. The Company determined the asset values were not recoverable and recorded an impairment loss of $2.9 million to its operating lease right-of-use assets. An additional $0.4 million and $0.5 million of expenses were incurred in fiscal 2024 and fiscal 2023, respectively, associated with the real estate-related cost optimization actions taken by the Company. See Note 14 —"Reorganization and other related costs" for further discussion.

NOTE 9 — STOCKHOLDERS' EQUITY

On September 26, 2018, the Company's board of directors authorized a stock repurchase program, under which the Company was authorized to repurchase up to $15 million of the Company's Class A common stock through September 30, 2019. On March 26, 2019, the board of directors expanded the repurchase program to authorize the repurchase up to an additional $15 million of the Company's Class A common stock through May 1, 2020, on which date the program terminated. No shares of Class A common stock were repurchased during the fiscal years ended February 3, 2023 and February 2, 2024.

NOTE 10 — STOCK-BASED COMPENSATION AND EMPLOYEE BENEFIT PLAN

In connection with the IPO, the Company's board of directors adopted the SecureWorks Corp. 2016 Long-Term Incentive Plan (the "2016 Plan"). The 2016 Plan became effective on April 18, 2016, and will expire on the tenth anniversary of the effective date unless the 2016 Plan is terminated earlier by the board of directors or in connection with a change in control of SecureWorks Corp. The Company has reserved 25,000,000 shares of Class A common stock for issuance pursuant to awards under the 2016 Plan. The 2016 Plan provides for the grant of options, stock appreciation rights, restricted stock, restricted stock units, deferred stock units, unrestricted stock, dividend equivalent rights, other equity-based awards, and cash bonus awards. Awards may be granted under the 2016 Plan to individuals who are employees, officers, or non-employee directors of the Company or any of its affiliates, consultants and advisors who perform services for the Company or any of its affiliates, and any other individual whose participation in the 2016 Plan is determined to be in the best interests of the Company by the compensation committee of the board of directors. The Company utilizes both authorized and unissued shares to satisfy all shares issued under the 2016 Plan. During fiscal 2024, the 2016 Plan was amended to increase the total shares of Class A common stock available for issuance by an additional 7,500,000 shares. As of February 2, 2024, there were approximately 3,887,644 shares of Class A common stock available for future grants under the 2016 Plan.

Stock Options

Under the 2016 Plan, the exercise price of each option will be determined by the compensation committee, except that the exercise price may not be less than 100% (or, for incentive stock options to any 10% stockholder, 110%) of the fair market value of a share of Class A common stock on the date on which the option is granted. The term of an option may not exceed ten years (or, for incentive stock options to any 10% stockholder, five years) from the date of grant. The compensation committee will determine the time or times at which each option may be exercised and the period of time, if any, after retirement, death, disability or termination of employment during which options may be exercised. Options may be made exercisable in installments, and the exercisability of options may be accelerated by the compensation committee.

During the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, no stock options were granted to employees or directors. The Company recognized zero, zero and $0.2 million in compensation expense for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively, for previously granted options.

The fair value of stock options is estimated as of the date of the grant using the Black-Scholes option pricing model. This model requires the input of subjective assumptions that will usually have a significant impact on the fair value estimate. The expected term was estimated using the SEC simplified method. The risk-free interest rate is the continuously compounded, term-matching, zero-coupon rate from the valuation date. The volatility is the leverage-adjusted, term-matching, historical volatility of peer firms. The dividend yield assumption is consistent with management expectations of dividend distributions based upon the Company's business plan at the date of grant.

The following table summarizes stock option activity and options outstanding and exercisable for the fiscal years ended, and as of, February 2, 2024, February 3, 2023, and January 28, 2022.

	Number of Options	Weighted-Average Exercise Price Per Share	Weighted-Average Contractual Life (years)	Weighted-Average Grant date Fair Value Per Share	Aggregate Intrinsic Value[1] (in thousands)
Balance, January 29, 2021	1,775,565	$ 14.00			
Granted	—	—			
Exercised	(1,417,105)	14.00			
Canceled, expired or forfeited	(196,535)	14.00			
Balance, January 28, 2022	161,925	$ 14.00			
Granted	—	—			
Exercised	—	14.00			
Canceled, expired or forfeited	—	14.00			
Balance, February 3, 2023	161,925	$ 14.00			
Granted	—	—			
Exercised	—	14.00			
Canceled, expired or forfeited	(15,723)	14.00			
Balance, February 2, 2024	146,202	$ 14.00	2.3	$ 6.15	$ —
Options vested and expected to vest, February 2, 2024	146,202	$ 14.00	2.3	$ 6.15	$ —
Options exercisable, February 2, 2024	146,202	$ 14.00	2.3	$ 6.15	$ —

(1) The aggregate intrinsic values represent the total pre-tax intrinsic values based on the Company's closing share price of $7.65 as reported on the Nasdaq Global Select Market on February 2, 2024, that would have been received by the option holders had all in-the-money options been exercised as of that date.

The total fair value of options vested was zero, zero and $1.1 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively. At February 2, 2024, there was no remaining unrecognized stock-based compensation expense related to stock options as all stock options outstanding are exercisable.

In connection with the acquisition of Dell by Dell Technologies in 2013, the Company's compensation programs included grants under the Dell Technologies Inc. 2013 Stock Incentive Plan, or 2013 Plan. Under the 2013 Plan, time-based and performance-based options to purchase shares of the Series C common stock of Dell Technologies were awarded to two of the Company's executive officers. Upon the closing of the Company's IPO, all unvested time-based awards were forfeited, and 32,000 vested time-based stock options remained outstanding and 400,001 performance-based options remained unvested and outstanding subject to award terms. During the fiscal year ended January 28, 2022, 10,000 options were exercised with a pre-tax intrinsic value of $1.0 million. Cash proceeds received by Dell Technologies from the exercise of these stock options were $0.1 million and the tax benefit realized was $0.2 million for the fiscal year ended January 28, 2022. As of January 28, 2022, there were no stock options outstanding.

Restricted Stock and Restricted Stock Units

Under the 2016 Plan, a restricted stock award, or RSA, is an award of shares of Class A common stock that may be subject to restrictions on transferability and other restrictions as the compensation committee determines in its sole discretion on the date of grant. The restrictions, if any, may lapse over a specified period of time or through the satisfaction of conditions, in installments or otherwise as the Company's compensation committee may determine. Unless otherwise provided in an award agreement, a grantee who receives restricted stock will have all of the rights of a stockholder as to those shares, including, without limitation, the right to vote and the right to receive dividends or distributions on the shares of Class A common stock, except that the compensation committee may require any dividends to be withheld and accumulated contingent on vesting of the underlying shares or reinvested in shares of restricted stock.

Under the 2016 Plan, a restricted stock unit, or RSU, represents the grantee's right to receive a compensation amount, based on the value of the shares of Class A common stock, if vesting criteria or other terms and conditions established by the compensation committee are met. If the vesting criteria or other terms and conditions are met, the Company may settle, subject to the terms and conditions of the applicable award agreement, restricted stock units in cash, shares of Class A common stock or a combination of the two. All award agreements currently outstanding require settlement in shares of Class A common stock.

During the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, the Company issued restricted stock awards and restricted stock units to employees at weighted-average fair values per share of $6.88, $12.88, and $19.81, respectively. The Company's annual grants of RSAs and RSUs issued during the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022 vest ratably over three years. Approximately 17%, 16%, and 26% of such awards were subject to performance conditions for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively. Of the 8.9 million RSUs outstanding on February 2, 2024, approximately 1.2 million were performance-based awards and 7.7 million were service-based awards. For the fiscal year ended February 2, 2024, approximately 279,839 shares were forfeited for the performance-based awards that were tied to results for that fiscal year.

As of February 2, 2024, unrecognized stock-based compensation expense related to restricted stock awards and restricted stock units was $37.3 million, which is expected to be recognized over the weighted-average remaining requisite period of 1.8 years.
The following table summarizes activity for restricted stock and restricted stock units for the fiscal years ended, and as of, February 2, 2024, February 3, 2023, and January 28, 2022.

	Number of Shares	Weighted-Average Grant Date Fair Value Per Share	Weighted-Average Contractual Life (years)	Aggregate Intrinsic Value[1]
				(in thousands)
Balance, January 29, 2021	4,513,093	$ 12.68		
Granted	3,119,246	19.81		
Vested	(1,894,276)	12.71		
Forfeited	(1,039,567)	16.69		
Balance, January 28, 2022	4,698,496	$ 16.52		
Granted	4,250,300	12.88		
Vested	(2,060,611)	15.93		
Forfeited	(1,600,683)	14.91		
Balance, February 3, 2023	5,287,502	$ 14.27		
Granted	8,298,794	6.88		
Vested	(2,455,762)	14.26		
Forfeited	(2,235,036)	9.06		
Balance, February 2, 2024	8,895,498	$ 8.68	1.0	$ 68,051
Restricted stock and restricted stock units expected to vest, February 2, 2024	7,808,058	$ 8.81	1.0	$ 59,732

(1) The aggregate intrinsic values represent the total pre-tax intrinsic values based on the Company's closing share price of $7.65 as reported on the Nasdaq Global Select Market on February 2, 2024, that would have been received by the restricted stock and restricted stock unit holders had all restricted stock and restricted stock units been issued as of that date.

As of February 2, 2024, restricted stock units representing approximately 8.9 million shares of Class A common stock were outstanding, with an aggregate intrinsic value of $68.1 million based on the Company's closing stock price as reported on the Nasdaq Global Select Market on February 2, 2024. The total fair value of Secureworks' restricted stock and restricted stock units that vested during the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022 was $35.0 million, $32.8 million, and $24.1 million, respectively, and the pre-tax intrinsic value was $19.0 million, $24.9 million and $29.2 million, respectively.

Stock-based Compensation Expense

The following table summarizes the classification of stock-based compensation expense related to stock options, restricted stock and restricted stock units for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022.

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
	(in thousands)		
Cost of revenue:			
Subscription	$ 1,051	$ 642	$ 218
Professional services	1,527	1,358	905
Total cost of revenue	$ 2,578	$ 2,000	$ 1,123
Research and development	12,625	11,589	7,220
Sales and marketing	4,166	6,568	4,065
General and administrative	15,735	16,698	18,038
Total stock-based compensation expense	$ 35,104	$ 36,855	$ 30,446

The tax benefit related to stock-based compensation expense was $5.1 million, $6.2 million, and $4.2 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

Long-term Incentive Cash Awards

In March 2017, the Company began granting long-term cash awards to certain employees. Generally, employees who receive the cash awards did not receive equity awards as part of the long-term incentive program. The majority of the cash awards issued prior to the fiscal year ended January 29, 2021 are subject to various performance conditions and vest in equal annual installments over a three-year period. The cash awards issued during the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022 are not subject to any performance conditions and vest in equal installments over a three-year period. For the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, the Company granted awards of approximately $0.1 million, $0.1 million, and $9.1 million, respectively, and recognized $2.0 million, $4.6 million, and $6.4 million of related compensation expense, respectively.

Employee Benefit Plan

Substantially all employees are eligible to participate in a defined contribution plan that complies with Section 401(k) of the Internal Revenue Code, or 401(k) Plan. For all presented periods, the Company matched 100% of each participant's voluntary contributions, or 401(k) employer match, subject to a maximum contribution of 6% of the participant's compensation, up to an annual limit of $7,500, and participants vest immediately in all contributions to the 401(k) Plan. For the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, total expense under this plan was $8.0 million, $9.8 million, and $10.1 million, respectively.

NOTE 11 — INCOME AND OTHER TAXES

The Company's loss before income taxes and income tax benefit (in thousands) and effective income tax rate for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022 were as follows:

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
Loss before income taxes	$ (114,520)	$ (146,781)	$ (55,906)
Income tax benefit	$ (28,478)	$ (32,282)	$ (16,115)
Effective tax rate	24.9 %	22.0 %	28.8 %

During the periods presented in the accompanying Consolidated Financial Statements, the Company did not file separate federal tax returns, as the Company generally was included in the tax grouping of other Dell entities within the respective entity's tax jurisdiction. The income tax benefit has been calculated using the separate-return method modified to apply the benefits-for-loss approach. Under the benefits-for-loss approach, net operating losses or other tax attributes are characterized as realized by the Company when those attributes are utilized by other members of the Dell affiliated group.

Effective for tax years beginning on or after January 1, 2022, the Tax Cuts and Jobs Act of 2017 eliminated the option to deduct research and development, or R&D, expenses in the year incurred and instead requires taxpayers to capitalize R&D expenses, including software development cost, and subsequently amortize such expenses over five years for R&D activities conducted in the United States and over fifteen years for R&D activities conducted outside of the United States.

The change in the Company's effective income tax rate for the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022 was primarily attributable to the impact of certain nondeductible items related to the vesting of stock-based compensation units and the recognition of additional benefits relating to the research and development credits.

Throughout the fiscal year ended February 2, 2024, the U.S. Department of the Treasury and Internal Revenue Service issued preliminary and final regulatory guidance clarifying certain provisions of the Tax Cuts and Jobs Act of 2017, and the Company anticipates additional regulatory guidance and technical clarifications to be issued. When additional guidance and technical clarifications are issued, the Company will recognize the related tax impact in the quarter in which such guidance is issued. The GILTI provisions of the Act signed into law on December 22, 2017 require the Company to include in its U.S. income tax return foreign subsidiary earnings in excess of an allowable return on the foreign subsidiary's tangible assets. The Company has elected to account for GILTI as a current period cost included in the year incurred.

A reconciliation of the Company's benefit from income taxes to the statutory U.S. federal tax rate is as follows:

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
U.S. federal statutory rate	21.0 %	21.0 %	21.0 %
Impact of foreign operations	(0.9)	(0.7)	(1.8)
State income taxes, net of federal tax benefit	4.2	2.5	4.3
Research and development credits	4.3	2.4	8.8
Nondeductible/nontaxable items	0.9	(0.7)	0.3
Stock-based compensation	(4.5)	(2.5)	(3.8)
Total	24.9 %	22.0 %	28.8 %

The benefit for income taxes consists of the following:

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
	(in thousands)		
Current:			
Federal	$ (5,808)	$ (1,904)	$ (10,076)
State/Local	(1,260)	688	(2,603)
Foreign	1,718	1,685	2,364
Current	$ (5,350)	$ 469	$ (10,315)
Deferred:			
Federal	(19,679)	(28,241)	(4,869)
State/Local	(3,767)	(4,257)	(328)
Foreign	318	(253)	(603)
Deferred	$ (23,128)	$ (32,751)	$ (5,800)
Income tax benefit	$ (28,478)	$ (32,282)	$ (16,115)

Loss before provision for income taxes consists of the following:

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
	(in thousands)		
Domestic	$ (119,265)	$ (154,426)	$ (59,541)
Foreign	4,745	7,645	3,635
Loss before income taxes	$ (114,520)	$ (146,781)	$ (55,906)

The components of the Company's net deferred tax balances are as follows:

	February 2, 2024	February 3, 2023
	(in thousands)	
Deferred tax assets:		
Deferred revenue	$ 2,897	$ 3,158
Provision for credit losses	263	523
Credit carryforwards	844	534
Loss carryforwards	6,201	5,717
Stock-based and deferred compensation	4,682	5,896
Lease right-of-use asset	2,644	3,525
Capitalized research and development	44,698	27,482
Other	4,966	3,881
Deferred tax assets	$ 67,195	$ 50,716
Valuation allowance	(8,778)	(5,824)
Deferred tax assets, net of valuation allowance	$ 58,417	$ 44,892
Deferred tax liabilities:		
Property and equipment	(140)	(325)
Purchased intangible assets	(20,643)	(25,848)
Operating and compensation related accruals	(8,509)	(10,821)
Lease liability	(626)	(1,613)
Other	(2,796)	(2,347)
Deferred tax liabilities	$ (32,714)	$ (40,954)
Net deferred tax asset (liabilities)	$ 25,703	$ 3,938

Net deferred tax balances are included in other non-current assets and other non-current liabilities in the Consolidated Statements of Financial Position.

As of February 2, 2024 and February 3, 2023, the Company had $8.8 million and $5.8 million, respectively, of deferred tax assets related to net operating loss carryforwards for state tax returns that are not included with those of other Dell entities. The change in the valuation allowance was $3.0 million and $0.3 million for the fiscal years ended February 2, 2024 and February 3, 2023, respectively. These net operating loss carryforwards began expiring in the fiscal year ended February 2, 2024. Due to the uncertainty surrounding the realization of these net operating loss carryforwards, the Company has provided valuation allowances for the full amount as of February 2, 2024 and February 3, 2023. Because the Company is included in the tax filings of certain other Dell entities, management has determined that it will be able to realize the remainder of its deferred tax assets.

When Dell's economic ownership percentage falls below 80%, the Company will become ineligible for inclusion in the Dell Technologies affiliated tax group. The Company's ability to benefit from its losses and other tax attributes may be impaired resulting from the need to file its own Federal and State tax returns without the ability to offset its losses against the profits from the parent. Currently, net consolidated deferred tax assets are approximately $25.7 million. If the Company's tax provision had been prepared using the separate-return method, the unaudited pro forma pre-tax loss, tax expense and net loss for the fiscal year ended February 2, 2024 would have been $114.5 million, $2.1 million, and $116.6 million, respectively, as a result of the recognition of a valuation allowance that would have been recorded on certain deferred tax assets, as well as certain attributes from the Tax Cuts and Jobs Act of 2017 that would be lost if not utilized by the Dell affiliated group.

In early March 2024, Dell's economic ownership of the Company dropped below 80%. As a result, the Company will no longer qualify for inclusion in Dell Technologies' U.S. federal income tax return and most U.S. state jurisdictions. Given the Company's history of losses, a full valuation allowance will be recorded against its deferred tax assets due to the inability to file with Dell. The full valuation allowance will be recorded in the period ended May 3, 2024. Currently, the net deferred tax assets in the U.S. are approximately $23.4 million. We expect for the foreseeable future that a full valuation allowance will be recorded against our deferred tax assets until such time that we meet the more likely than not recognition criteria.

As of February 2, 2024, the Company has cumulative undistributed foreign earnings that would incur some amount of local withholding and state taxes if the earnings are distributed to SecureWorks Corp., which is domiciled in the United States. The Tax Cuts and Jobs Act of 2017 fundamentally changes the U.S. approach to taxation of foreign earnings. The Company has analyzed its global working capital and cash requirements and the potential tax liabilities attributable to repatriation, and it has determined that it may repatriate certain unremitted foreign earnings that were previously deemed indefinitely reinvested. As of February 2, 2024 and February 3, 2023, the Company has recorded withholding taxes of $0.4 million and $0.1 million, respectively, related to certain unremitted foreign earnings that may be repatriated.

A reconciliation of the Company's beginning and ending amount of unrecognized tax benefits is as follows:

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
	(in thousands)		
Beginning unrecognized tax benefits	$ 6,619	$ 6,509	$ 6,148
Increases related to tax positions of the current year	146	106	107
Increases related to tax position of prior years	95	4	256
Reductions for tax positions of prior years	—	—	(2)
Ending unrecognized tax benefits	$ 6,860	$ 6,619	$ 6,509

The Company's net unrecognized tax benefits of $4.9 million, $4.5 million, and $4.2 million include amounts reflected in the table above, plus accrued interest and penalties of $0.6 million, $0.4 million, and $0.3 million as of February 2, 2024, February 3, 2023 and January 28, 2022, respectively, and a tax benefit associated with other indirect jurisdictional effects of uncertain tax positions of $2.6 million as of February 2, 2024, February 3, 2023 and January 28, 2022 are included in other non-current liabilities in the Consolidated Statements of Financial Position. The net unrecognized tax benefits, if recognized, would increase the Company's income tax benefit and effective income tax benefit rate. Interest and penalties related to income tax liabilities are included in income tax expense. The Company recorded interest and penalties of $0.2 million, $0.1 million and $0.1 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

Judgment is required in evaluating the Company's uncertain tax positions and determining the Company's provision for income taxes. The Company does not anticipate a significant change to the total amount of unrecognized tax benefits within the next twelve months.

The Company is currently under income tax audit in both domestic and foreign jurisdictions. The Company is undergoing negotiations and, in some cases, contested proceedings relating to tax matters with the taxing authorities in these jurisdictions. The Company believes that it has provided adequate reserves related to all matters contained in the tax periods open to examination. Although the Company believes it has made adequate provisions for the uncertainties relating to these audits, if the Company should experience unfavorable outcomes, such outcomes could have a material impact on its results of operations, financial position, and cash flows.

The Company takes certain non-income tax positions in the jurisdictions in which it operates and has received certain non-income tax assessments from various jurisdictions. The Company believes that a material loss in these matters is not probable and that it is not reasonably possible that a material loss exceeding amounts already accrued has been incurred. The Company believes its positions in these non-income tax litigation matters are supportable and that it ultimately will prevail. In the normal course of business, the Company's positions and conclusions related to its non-income taxes could be challenged and assessments may be made. To the extent new information is obtained and the Company's views on its positions, probable outcomes of assessments, or litigation change, changes in estimates to the Company's accrued liabilities would be recorded in the period in which such a determination is made. In the resolution process for income tax and non-income tax audits, the Company may be required to provide collateral guarantees or indemnification to regulators and tax authorities until the matter is resolved. As of February 2, 2024, the Company is under audit with various state taxing authorities in which rulings related to the taxability of certain of our services are in appeals. See "Note 7 — Commitments and Contingencies, Customer-based Taxation Contingencies" for more information about loss contingencies.

The Company is no longer subject to tax examinations for years prior to fiscal 2017.

NOTE 12 — SELECTED FINANCIAL INFORMATION

The following table provides additional information on amounts included in the Company's Consolidated Statement of Financial Position as of February 2, 2024 and February 3, 2023.

	February 2, 2024	February 3, 2023
	(in thousands)	
Accounts receivable, net:		
Gross accounts receivable	$ 55,818	$ 75,029
Allowance for credit losses	(1,552)	(2,402)
Total	$ 54,266	$ 72,627
Other current assets:		
Income tax receivable	$ 5,092	$ 4,733
Prepaid maintenance and support agreements	5,014	7,276
Prepaid other	4,385	5,517
Total	$ 14,491	$ 17,526
Property and equipment, net		
Computer equipment	$ 30,783	$ 30,108
Leasehold improvements	10,280	22,390
Other equipment	1,526	2,144
Total property and equipment	42,589	54,642
Accumulated depreciation and amortization	(40,440)	(50,010)
Total	$ 2,149	$ 4,632
Other non-current assets		
Prepaid maintenance agreements	$ 748	$ 799
Deferred tax asset	25,716	3,951
Deferred commission and fulfillment costs	41,815	52,797
Other	2,436	3,418
Total	$ 70,715	$ 60,965
Accrued and other current liabilities		
Compensation	$ 34,888	$ 50,397
Related party payable, net	4,868	1,141
Other	22,139	30,028
Total	$ 61,895	$ 81,566

The allocation between domestic and foreign net revenue is based on the location of the Company’s customers. The following tables present net revenue and property, plant and equipment allocated between the United States and international locations. The Company defines international revenue as revenue contracted through non-U.S. entities.

	Fiscal Year Ended		
	February 2, 2024	February 3, 2023	January 28, 2022
Net revenue			
United States	$ 229,454	$ 306,799	$ 359,707
Japan	36,347	31,944	32,795
International	100,078	124,732	142,712
Total	$ 365,879	$ 463,475	$ 535,214

	February 2, 2024	February 3, 2023
Property and equipment, net		
United States	$ 1,649	$ 3,945
International	500	687
Total	$ 2,149	$ 4,632

NOTE 13 — RELATED PARTY TRANSACTIONS

Allocated Expenses

For the periods presented, Dell has provided various corporate services to Secureworks in the ordinary course of business. The costs of services provided to Secureworks by Dell are governed by a shared services agreement between Secureworks and Dell Inc. The total amounts of the charges under the shared services agreement with Dell were $2.9 million, $3.8 million, and $3.8 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively. Management believes that the basis on which the expenses have been allocated is a reasonable reflection of the utilization of services provided to or the benefit received by the Company during the periods presented.

Related Party Arrangements

For the periods presented, related party transactions and activities involving Dell Inc. and its wholly-owned subsidiaries were not always consummated on terms equivalent to those that would prevail in an arm's-length transaction where conditions of competitive, free-market dealing may exist.

The Company purchases computer equipment for internal use from Dell Inc. and its subsidiaries that is capitalized within property and equipment in the Consolidated Statements of Financial Position. Purchases of computer equipment from Dell and EMC Corporation, a wholly-owned subsidiary of Dell that provides enterprise software and storage, or EMC, totaled $0.5 million, $0.9 million, and $0.7 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

EMC previously maintained a majority ownership interest in VMware, Inc., or VMware, a company that provides cloud and virtualization software and services. The Company's purchases of annual maintenance services, software licenses and hardware systems for internal use from Dell, EMC and VMware totaled $0.9 million, $1.1 million, and $1.6 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively. On November 1, 2021, Dell Technologies completed its spin-off of all shares of common stock of VMware that were beneficially owned by Dell Technologies and its subsidiaries, including EMC, to Dell Technologies' stockholders. As a result of the spin-off transaction, the businesses of VMware were separated from the remaining businesses of Dell Technologies, although Michael S. Dell, the Chairman, Chief Executive Officer and majority stockholder of Dell Technologies, continued to serve as Chairman of the Board of VMware until VMware was acquired by Broadcom Inc. on November 22, 2023.

The Company recognized revenue related to solutions provided to VMware that totaled $0.5 million, $0.6 million and $0.5 million for the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022, respectively. In October 2019, VMware acquired Carbon Black Inc., a security business with which the Company had an existing commercial relationship. Purchases by the Company of solutions from Carbon Black totaled $2.0 million, $2.9 million, and $6.2 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

The Company also recognized revenue related to solutions provided to significant beneficial owners of Secureworks common stock, which include Mr. Dell and affiliates of Mr. Dell. The revenues recognized by the Company from solutions provided to Mr. Dell, MSD Capital, L.P. (a firm founded for the purposes of managing investments of Mr. Dell and his family), DFI Resources LLC, an entity affiliated with Mr. Dell, and the Michael and Susan Dell Foundation totaled $0.2 million, $0.3 million, and $0.2 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

The Company provides solutions to certain customers whose contractual relationships have historically been with Dell rather than Secureworks, although the Company has the primary responsibility to provide the services. Effective August 1, 2015, in connection with the IPO, many of such customer contracts were transferred from Dell to the Company, forming a direct contractual relationship between the Company and the end customer. For customers whose contracts have not yet been transferred or whose contracts were subsequently originated through Dell under a reseller agreement, the Company recognized revenues of approximately $56.6 million, $65.0 million, and $61.7 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively. In addition, as of February 2, 2024, the Company had approximately $2.9 million of contingent obligations to Dell related to outstanding performance bonds for certain customer contracts which Dell issued on behalf of the Company. These contingent obligations are not recognized as liabilities on the Company's financial statements.

As the Company's customer and on behalf of certain of its own customers, Dell also purchases solutions from the Company. The Company recognized revenues from such purchases of approximately $0.9 million, $4.6 million, and $11.7 million for the fiscal years ended February 2, 2024, February 3, 2023, and January 28, 2022, respectively.

As a result of the foregoing related party arrangements, the Company has recorded the following related party balances in the Consolidated Statement of Financial Position as of February 2, 2024 and February 3, 2023:

	February 2, 2024	February 3, 2023
	(in thousands)	
Related party payable (in accrued and other current liabilities)	$ 4,868	$ 1,141
Accounts receivable from customers under reseller agreements with Dell (in accounts receivable, net)	$ 5,748	$ 5,584
Net operating loss tax sharing receivable under agreement with Dell (in other current assets)	$ 4,976	$ 3,472

NOTE 14 — REORGANIZATION AND OTHER RELATED COSTS

During the fiscal year ended February 3, 2023, the Company committed to a plan to align its investments more closely with its strategic priorities to meet the expected future needs of the business by reducing the Company's workforce and implementing certain real estate-related and other cost optimization actions. Under this plan and through continued reorganization actions conducted during fiscal year ended February 2, 2024, the Company began rebalancing investments cross-functionally in alignment with the Company's current strategy and growth opportunities, such as focusing on the higher value, higher margin Taegis solutions, optimizing the Company's organizational structure to increase its scalability, and other priorities, to better position the Company for continued growth with improving operating margins over time. The Company incurred expenses associated with the plan of approximately $17.1 million and $15.5 million for the fiscal year ended February 2, 2024 and February 3, 2023, respectively. These expenses consisted primarily of severance and other termination benefits, real estate-related expenses, and various other cost saving measures.

The following table summarizes the liability associated with these charges that is included in accrued and other current liabilities on the accompanying Consolidated Statement of Financial Position (in thousands):

	Workforce	Real estate-related	Other	Total
Balance as of January 28, 2022	$ —	$ —	$ —	$ —
Reorganization charge	7,550	4,570	3,351	15,471
Charges settled in cash	—	(90)	(325)	(415)
Charges settled in non-cash	—	(4,480)	(1,632)	(6,112)
Balance as of February 3, 2023	$ 7,550	$ —	$ 1,394	$ 8,944
Reorganization charge	13,873	3,272	—	17,145
Charges settled in cash	(15,802)	—	(1,394)	(17,196)
Charges settled in non-cash	—	(3,272)	—	(3,272)
Balance as of February 2, 2024	$ 5,621	$ —	$ —	$ 5,621

NOTE 15 — REVISION TO PREVIOUSLY ISSUED 2024 INTERIM CONDENSED CONSOLIDATED FINANCIAL STATEMENTS (UNAUDITED)

As detailed in Note 1 to the Company's Consolidated Financial Statements, the Company's historical classification of the effects of exchange rate changes on the Company's foreign denominated cash and cash equivalents balances was not presented separately as the effect of exchange rate changes on cash and cash equivalents in the Company's Consolidated Statement of Cash Flows, but rather was included as a component of net cash provided by (used in) operating activities and investing activities. This matter also impacted interim Condensed Consolidated Financial Statements of the Company and fiscal 2024 quarterly periods will also be revised in connection with our future fiscal 2025 unaudited interim Condensed Consolidated Financial Statement filings in Quarterly Reports on Form 10-Q. The Company will revise the Condensed Consolidated Statements of Cash Flows for the year-to-date periods ended May 5, 2023, August 4, 2023, and November 3, 2023 to correct the presentation of the effect of exchange rate changes on cash and cash equivalents. This revision will result in a decrease of $1.6 million, $2.6 million, and $4.6 million in net cash used in operating activities and de minimis impacts to cash flows from capital expenditures, as included in total cash used in investing activities, for the three months ended May 5, 2023, six months ended August 4, 2023, and nine months ended November 3, 2023, respectively. The corresponding amounts will be presented separately as the effect of exchange rate changes on cash and cash equivalents.

SCHEDULE II - VALUATION AND QUALIFYING ACCOUNTS

Valuation and Qualifying Accounts

Fiscal Year	Description	Balance at Beginning of Period	Charged to Income Statement	Charged to Allowance	Balance at End of Period
Trade Receivables:					
2024	Allowance for credit losses	$ 2,402	$ (282)	$ (568)	$ 1,552
2023	Allowance for credit losses	$ 3,511	$ (524)	$ (585)	$ 2,402
2022	Allowance for credit losses	$ 4,830	$ (430)	$ (889)	$ 3,511

Item 9. Changes in and Disagreements With Accountants on Accounting and Financial Disclosure

None

Item 9A. Controls and Procedures

This report includes the certifications of our Chief Executive Officer and Chief Financial Officer required by Rule 13a-14 under the Securities Exchange Act of 1934, as amended, or Exchange Act. See Exhibits 31.1 and 31.2 filed with this report. This Item 9A includes information concerning the controls and control evaluations referred to in those certifications.

Evaluation of Disclosure Controls and Procedures

Disclosure controls and procedures (as defined in Rules 13a-15(e) and 15d-15(e) under the Exchange Act) are designed to provide reasonable assurance that information required to be disclosed in reports filed or submitted under the Exchange Act is recorded, processed, summarized and reported, within the time periods specified in the SEC's rules and forms and that such information is accumulated and communicated to management, including the Chief Executive Officer and the Chief Financial Officer, as appropriate to allow timely decisions regarding required disclosure.

In connection with the preparation of this report, our management, under the supervision and with the participation of our Chief Executive Officer and our Chief Financial Officer, conducted an evaluation of the effectiveness of the design and operation of our disclosure controls and procedures as of February 2, 2024. Based on that evaluation, our Chief Executive Officer and Chief Financial Officer have concluded that our disclosure controls and procedures were effective at the reasonable assurance level as of February 2, 2024.

Management's Report on Internal Control Over Financial Reporting

Management, under the supervision of the Chief Executive Officer and the Chief Financial Officer, is responsible for establishing and maintaining adequate internal control over financial reporting. Internal control over financial reporting (as defined in Rules 13a-15(f) and 15d-15(f) under the Exchange Act) 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. Internal control over financial reporting includes those policies and procedures which (a) pertain to the maintenance of records that, in reasonable detail, accurately and fairly reflect the transactions and dispositions of assets, (b) provide reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles, (c) provide reasonable assurance that receipts and expenditures are being made only in accordance with appropriate authorization of management and the board of directors, and (d) provide reasonable assurance regarding prevention or timely detection of unauthorized acquisition, use, or disposition of assets that could have a material effect on the financial statements.

In connection with the preparation of this report, our management, under the supervision and with the participation of our Chief Executive Officer and Chief Financial Officer, conducted an evaluation of the effectiveness of our internal control over financial reporting as of February 2, 2024, based on the criteria established in *Internal Control — Integrated Framework (2013)* issued by the Committee of Sponsoring Organizations of the Treadway Commission. As a result of that evaluation, management has concluded that our internal control over financial reporting was effective as of February 2, 2024.

The effectiveness of our internal control over financial reporting as of February 2, 2024 has been audited by PricewaterhouseCoopers LLP, our independent registered public accounting firm, as stated in their report, which is included in "Item 8 — Financial Statements and Supplementary Data."

Changes in Internal Control Over Financial Reporting

There were no changes in our internal control over financial reporting identified in connection with the evaluation required by Rule 13a-15(d) and 15d-15(d) of 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.

Limitations on the Effectiveness of Controls

Our system of controls is designed to provide reasonable, not absolute, assurance regarding the reliability and integrity of accounting and financial reporting. 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 designed and operated, can provide only reasonable, not absolute, assurance that the objectives of the control system will be met. These inherent limitations include the following:

- Judgments in decision-making can be faulty, and control and process breakdowns can occur because of simple errors or mistakes.
- Controls can be circumvented by individuals, acting alone or in collusion with each other, or by management override.
- The design of any system of controls is based in part on 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 deterioration in the degree of compliance with associated policies or procedures.
- The design of a control system must reflect the fact that resources are constrained, and the benefits of controls must be considered relative to their costs.

Item 9B. Other Information

None.

Item 9C. Disclosure Regarding Foreign Jurisdictions that Prevent Inspections

Not applicable.

Part III

Item 10. Directors, Executive Officers and Corporate Governance

We have adopted a code of ethics applicable to our principal executive officer and other senior financial officers. The code of ethics, which we refer to as our Code of Ethics for Senior Financial Officers, is available on the Investors page of our website at www.secureworks.com. To the extent required by SEC rules, we intend to disclose any amendments to this code and any waiver of a provision of the code for the benefit of any senior financial officer on our website within any period that may be required under SEC rules from time to time.

See "Part I — Item 1 — Business — Information about our Executive Officers" for information about our executive officers, which is incorporated by reference in this Item 10. Other information required by this Item 10 is incorporated herein by reference to our definitive proxy statement for our 2024 annual meeting of stockholders, referred to as the "2024 proxy statement," which we will file with the SEC on or before 120 days after our 2024 fiscal year end, and which will appear in the 2024 proxy statement, including the information in the 2024 proxy statement appearing under the captions "Proposal 1 — Election of Directors" and "Delinquent Section 16(a) Reports."

The following lists the members of our board of directors and the principal occupation of each director as of the date of this report.

Wendy K. Thomas
Chief Executive Officer
SecureWorks Corp.

Michael S. Dell
Chairman and Chief Executive Officer
Dell Technologies Inc.

Kyle Paster
Managing Director
Silver Lake Partners
(private equity)

Mr. William (Bill) H. Cary
Retired Executive of General Electric Company
Former President and Chief Operating Officer of GE Capital Corp.

Pamela Daley
Retired Senior Vice President and
Senior Advisor to the Chairman
of General Electric Company

Mark J. Hawkins
Former President and Chief Financial Officer
Salesforce.com, Inc.
(software)

Yagyensh C. (Buno) Pati
Partner Centerview Capital Technology
(investments)

Item 11. Executive Compensation

Information required by this Item 11 is incorporated herein by reference to the 2024 proxy statement, including the information in the 2024 proxy statement appearing under the captions "Proposal 1 — Election of Directors — Director Compensation" and "Compensation of Executive Officers."

Item 12. Security Ownership of Certain Beneficial Owners and Management and Related Stockholder Matters

Information required by this Item 12 is incorporated herein by reference to the 2024 proxy statement, including the information in the 2024 proxy statement appearing under the captions "Equity Compensation Plan Information" and "Security Ownership of Certain Beneficial Owners and Management."

Item 13. Certain Relationships and Related Transactions, and Director Independence

Information required by this Item 13 is incorporated herein by reference to the 2024 proxy statement, including the information in the 2024 proxy statement appearing under the captions "Proposal 1—Election of Directors" and "Transactions with Related Persons."

Item 14. Principal Accountant Fees and Services

Information required by this Item 14 is incorporated herein by reference to the 2024 proxy statement, including the information in the 2024 proxy statement appearing under the caption "Proposal 2 — Ratification of Appointment of Independent Registered Public Accounting Firm."

Part IV

Item 15. Exhibits and Financial Schedules

The following documents are filed as a part of this annual report on Form 10-K:

(1) *Financial Statements*: The following financial statements are filed as a part of this report under "Part II — Item 8 Financial Statements and Supplementary Data":

Report of Independent Registered Public Accounting Firm
Consolidated Statements of Financial Position as of February 2, 2024 and February 3, 2023
Consolidated Statements of Operations for the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022
Consolidated Statements of Comprehensive Loss for the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022
Consolidated Statements of Cash Flows for the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022
Consolidated Statements of Stockholder's Equity for the fiscal years ended February 2, 2024, February 3, 2023 and January 28, 2022
Notes to Consolidated Financial Statements
Schedule II - Valuation and Qualifying Accounts

(2) *Financial Statement Schedules*: The following financial statement schedule is included following the Notes to the Consolidated Financial Statements under "Part II — Item 8 — Financial Statements and Supplementary Data":

Schedule II — Valuation and Qualifying Accounts

(3) *Exhibits*:

EXHIBIT INDEX

Exhibit No.	Description
3.1	Restated Certificate of Incorporation of SecureWorks Corp. (the "Company") (incorporated by reference to Exhibit 4.1 to the Company's Registration Statement on Form S-8 filed with the Securities and Exchange Commission (the "Commission") on April 22, 2016 (the "Form S-8")) (Registration No. 333-210866).
3.2	Amended and Restated Bylaws of SecureWorks Corp. (incorporated by reference to Exhibit 4.2 to the Form S-8) (Registration No. 333-210866).
4.1	Specimen Certificate of Class A Common Stock, $0.01 par value per share, of the Company (incorporated by reference to Exhibit 4.1 to the Company's Registration Statement on Form S-1 filed with the Commission on December 17, 2015 (the "Form S-1")) (Registration No. 333-208596).
4.2	Description of the Company's Securities Registered Pursuant to Section 12 of the Securities Exchange Act of 1934 (incorporated by reference to Exhibit 4.2 to the Company's Annual Report on Form 10-K for the fiscal year ended January 31, 2020) (Commission File No. 001-37748).
10.1	Shared Services Agreement, effective as of August 1, 2015, between Dell Inc., for itself and its subsidiaries, and the Company (formerly known as SecureWorks Holding Corporation), for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Form S-1) (Registration No. 333-208596).
10.1.1	Amendment #1 to Shared Services Agreement, dated December 8, 2015, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1.1 to the Form S-1) (Registration No. 333-208596).
10.1.2	Amendment #2 to Shared Services Agreement, dated November 8, 2017, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1.2 to the Company's Annual Report on Form 10-K for the fiscal year ended February 2, 2018) (Commission File No. 001-37748).
10.1.3	Amendment #3 to Shared Services Agreement, dated as of July 11, 2018, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 3, 2018) (Commission File No. 001-37748).
10.1.4	Amendment #4 to Shared Services Agreement, dated as of May 29, 2019, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.1.5	Amendment #5 to Shared Services Agreement, dated as of February 1, 2022, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1.5 to the Company's Annual Report on Form 10-K for the fiscal year ended January 28, 2022) (Commission File No. 001-37748).
10.1.6	Amendment #6 to Shared Services Agreement, dated September 13, 2022, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.1.6 to the Company's Annual Report on Form 10-K for the fiscal year ended February 3, 2023) (Commission File No. 001-37748).
10.1.7	Amendment #7 to the Shared Services Agreement, dated July 21, 2023, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries.
10.2	Intellectual Property Contribution Agreement, effective as of August 1, 2015, among Dell Inc., the Company and other subsidiaries of Dell Inc. party thereto (incorporated by reference to Exhibit 10.2 to the Form S-1) (Registration No. 333-208596).
10.3	Patent License Agreement, effective as of August 1, 2015, between Dell Inc., for itself and its subsidiaries, and the Company, for itself and its subsidiaries (incorporated by reference to Exhibit 10.3 to the Form S-1) (Registration No. 333-208596).
10.4	License Agreement, dated as of September 9, 2015, between Dell Inc. and the Company (incorporated by reference to Exhibit 10.4 to the Form S-1) (Registration No. 333-208596).
10.5	Tax Matters Agreement, effective as of August 1, 2015, between the Company, for itself and its subsidiaries, and Dell Technologies Inc. (formerly known as Denali Holding Inc.), for itself and its subsidiaries other than the Company (incorporated by reference to Exhibit 10.5 to the Form S-1) (Registration No. 333-208596).
10.5.1	Amendment #1 to Tax Matters Agreement, dated December 8, 2015, between the Company, for itself and its subsidiaries, and Dell Technologies Inc., for itself and its subsidiaries other than the Company (incorporated by reference to Exhibit 10.5.1 to the Form S-1) (Registration No. 333-208596).
10.5.2	Amended and Restated Tax Matters Agreement, dated as of June 6, 2023, by and among SecureWorks Corp. (the "Company"), for itself and its subsidiaries, and Dell Technologies Inc., for itself and its subsidiaries other than the Company and the Company's subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 5, 2023) (Commission File No. 001-37748)

Exhibit No.	Description
10.6	Amended and Restated Employee Matters Agreement, effective as of August 1, 2015, among Dell Technologies Inc., Dell Inc. and the Company (incorporated by reference to Exhibit 10.6 to the Form S-1) (Registration No. 333-208596).
10.7+	Security Services Customer Master Services Agreement, effective as of July 7, 2015, between SecureWorks, Inc. and Dell USA L.P., on behalf of itself, Dell Inc., and Dell Inc.'s subsidiaries (incorporated by reference to Exhibit 10.7 to the Form S-1) (Registration No. 333-208596).
10.8	Letter Agreement to Security Services Customer Master Services Agreement and Reseller Agreement, effective as of August 1, 2015, between Dell Inc. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.8 to the Form S-1) (Registration No. 333-208596).
10.8.1+	First Amendment to Security Services Customer Master Services Agreement, effective as of November 3, 2017, between Dell USA L.P. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.8.1 to the Company's Annual Report on Form 10-K for the fiscal year ended February 2, 2018) (Commission File No. 001-37748).
10.8.2+	Amendment #2 to Security Services Customer Master Services Agreement, effective as of August 18, 2022, between Dell USA L.P., for itself and its subsidiaries (excluding SecureWorks, Inc.), and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended October 28, 2022) (Commission File No. 001-37748).
10.9+	Amended and Restated Master Commercial Customer Agreement, effective as of August 1, 2015, between Dell Marketing L.P. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.9 to the Form S-1) (Registration No. 333-208596).
10.9.1+	Amendment No. 1 to Amended and Restated Master Commercial Customer Agreement, effective as of August 4, 2018, between Dell Marketing L.P. and SecureWorks, Inc. (incorporated by reference to Exhibit 10.9.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 2, 2018) (Commission File No. 001-37748).
10.9.2	Joinder of EMC Corporation to the Amended and Restated Master Commercial Customer Agreement, dated as of March 8, 2019 (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.10+	Amended and Restated Reseller Agreement, effective as of August 1, 2015, between SecureWorks, Inc., for itself and its subsidiaries, and Dell Inc., for itself and its subsidiaries other than the Company (incorporated by reference to Exhibit 10.10 to the Form S-1) (Registration No. 333-208596).
10.10.1+	Amendment No. 1 to Amended and Restated Reseller Agreement, dated as of January 23, 2019, between Dell, Inc., for itself and its subsidiaries other than SecureWorks, Inc. and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.10.1 to the Company's Annual Report on Form 10-K for the fiscal year ended February 1, 2019) (Commission File No. 001-37748).
10.10.2**	Addendum No. 1 to Amendment No. 1 to Amended and Restated Reseller Agreement, dated as of May 8, 2019, between Dell, Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.5 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended May 3, 2019) (Commission File No. 001-37748).
10.10.3**	Amendment No. 2 to Amended and Restated Reseller Agreement, dated as of May 21, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 2, 2019) (Commission File No. 001-37748).
10.10.4**	Amendment No. 3 to Amended and Restated Reseller Agreement, dated as of June 13, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 2, 2019) (Commission File No. 001-37748).
10.10.5**	Amendment No. 4 to Amended and Restated Reseller Agreement, dated as of July 30, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.3 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 2, 2019) (Commission File No. 001-37748).
10.10.6	Amendment No. 5 to Amended and Restated Reseller Agreement, dated as of October 1, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 1, 2019) (Commission File No. 001-37748).
10.10.7**	Amendment No. 6 to Amended and Restated Reseller Agreement, dated as of October 23, 2019, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.2 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended November 1, 2019) (Commission File No. 001-37748).

Exhibit No.	Description
10.10.8**	Amended and Restated Amendment No. 6 to Amended and Restated Reseller Agreement, dated as of December 3, 2020, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.10.8 to the Company's Annual Report on Form 10-K for the fiscal year ended January 29, 2021) (Commission File No. 001-37748).
10.10.9	Letter Agreement to Amended and Restated Reseller Agreement, dated as of December 30, 2021, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.10.9 to the Company's Annual Report on Form 10-K for the fiscal year ended January 28, 2022) (Commission File No. 001-37748).
10.10.10+	Amendment No. 7 to Amended and Restated Reseller Agreement, dated as of June 23, 2022, between Dell Inc., for itself and its subsidiaries other than SecureWorks, Inc., and SecureWorks, Inc., for itself and its subsidiaries (incorporated by reference to Exhibit 10.1 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended July 29, 2022) (Commission File No. 001-37748).
10.11	Registration Rights Agreement, dated as of August 3, 2015, among the Company and the Holders party thereto (incorporated by reference to Exhibit 10.22 to the Form S-1) (Registration No. 333-208596).
10.12	Registration Rights Agreement, dated as of April 27, 2016, among the Company, Dell Marketing L.P., Michael S. Dell, the Susan Lieberman Dell Separate Property Trust, MSDC Denali Investors, L.P., MSDC Denali EIV, LLC, Silver Lake Partners III, L.P., Silver Lake Technology Investors III, L.P., Silver Lake Partners IV, L.P., Silver Lake Technology Investors IV, L.P. and SLP Denali Co-Invest, L.P. (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on April 27, 2016) (Commission File No. 001-37748).
10.13	Sixth Amended and Restated Revolving Credit Agreement, dated as of March 23, 2023, between SecureWorks, Inc. and Dell USA L.P. (incorporated by reference to Exhibit 10.13 to the Company's Annual Report on Form 10-K for the fiscal year ended February 3, 2023) (Commission File No. 001-37748).
10.13.1	First Amendment to Sixth Amended and Restated Revolving Credit Agreement, dated as of September 6, 2023, between SecureWorks, Inc. and Dell USA L.P. (incorporated by reference to Exhibit 10.3 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended August 4, 2023) (Commission File No. 001-37748)
10.14	Note Purchase Agreement, dated as of June 30, 2015 and amended on July 31, 2015, among the Company, Dell Technologies Inc. and the Investors party thereto (incorporated by reference to Exhibit 10.21 to the Form S-1) (Registration No. 333-208596).
10.15	Office Lease between Teachers Concourse, LLC and SecureWorks, Inc., dated as of April 20, 2012, as amended (incorporated by reference to Exhibit 10.23 to the Form S-1) (Registration No. 333-208596).
10.16	Unconditional Guaranty of Payment and Performance, entered into on April 20, 2012, by Dell Inc. in favor of Teachers Concourse, LLC (incorporated by reference to Exhibit 10.24 to the Form S-1) (Registration No. 333-208596).
10.17	Sublease Agreement between Dell International Services SRL and SecureWorks Europe SRL, dated as of June 22, 2015, as amended (incorporated by reference to Exhibit 10.26 to the Form S-1) (Registration No. 333-208596).
10.18	Lease Deed between Dell International Services India Private Limited and SecureWorks India Private Limited, dated as of August 8, 2015 (incorporated by reference to Exhibit 10.27 to the Form S-1) (Registration No. 333-208596).
10.19*	Dell Technologies Inc. 2013 Stock Incentive Plan (as amended and restated) (incorporated by reference to Exhibit 10.8 to Dell Technologies Inc.'s Current Report on Form 8-K filed with the Commission on December 28, 2018) (Commission File No. 001-37867).
10.20*	Dell Technologies Inc. 2012 Long-Term Incentive Plan (formerly known as Dell Inc. 2012 Long-Term Incentive Plan) as amended and restated as of October 6, 2017 (incorporated by reference to Exhibit 10.4 to Dell Technologies Inc.'s Quarterly Report on Form 10-Q for the quarterly period ended November 3, 2017) (Commission File No. 001-37867).
10.21*	Form of Indemnification Agreement between the Company and each director and executive officer of the Company (incorporated by reference to Exhibit 10.20 to the Form S-1) (Registration No. 333-208596).
10.22*	SecureWorks Corp. 2016 Long-Term Incentive Plan, as amended and restated as of June 27, 2023 (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on June 27, 2023) (Commission File No. 001-37748).
10.23*	Form of Nonqualified Stock Option Agreement for Executives under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.13 to the Form S-1) (Registration No. 333-208596).
10.24*	Form of Nonqualified Stock Option Agreement for Directors under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.13.1 to Amendment No. 1 to the Form S-1 filed with the Commission on March 22, 2016) (Registration No. 333-208596).

Exhibit No.	Description
10.25††	Form of Restricted Stock Unit Agreement for Executives under SecureWorks Corp. 2016 Long-Term Incentive Plan.
10.26*	Form of Restricted Stock Unit Agreement for Non-Employee Directors under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.5 to the Company's Quarterly Report on Form 10-Q for the quarterly period ended July 30, 2021) (Commission File No. 001-37748).
10.27*	SecureWorks Corp. Amended and Restated Severance Pay Plan for Executive Employees.
10.28††	SecureWorks Corp. Amended and Restated Non-Employee Director Compensation Policy, effective March 20, 2023 (incorporated by reference to Exhibit 10.28 to the Company's Annual Report on Form 10-K for the fiscal year ended February 3, 2023) (Commission File No. 001-37748).
10.29*	SecureWorks Corp. Form of Protection of Sensitive Information, Noncompetition and Nonsolicitation Agreement (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on December 7, 2016) (Commission File No. 001-37748).
10.30*††	Form of Performance Stock Unit Agreement for Executives under the SecureWorks Corp. 2016 Long-Term Incentive Plan.
10.31*	Amended and Restated SecureWorks Corp. Incentive Bonus Plan (incorporated by reference to Exhibit 10.33 to the Company's Annual Report on Form 10-K for the fiscal year ended February 3, 2017) (Commission File No. 001-37748).
10.32*	Form of Deferred Stock Unit Agreement for Non-Employee Directors under SecureWorks Corp. 2016 Long-Term Incentive Plan (incorporated by reference to Exhibit 10.35 to the Company's Annual Report on Form 10-K for the fiscal year ended January 28, 2022) (Commission File No. 001-37748).
10.33*	Separation Agreement and Release, dated as of June 1, 2021, between SecureWorks Corp. and Michael R. Cote (incorporated by reference to Exhibit 10.1 to the Company's Current Report on Form 8-K filed with the Commission on June 3, 2021) (Commission File No. 001-37748)
10.34*††	Separation Agreement and Release, dated as of March 21, 2023, between SecureWorks Corp. and Paul M. Parrish (incorporated by reference to Exhibit 10.34 to the Company's Annual Report on Form 10-K for the fiscal year ended February 3, 2023) (Commission File No. 001-37748).
21.1††	Subsidiaries of SecureWorks Corp.
23.1††	Consent of PricewaterhouseCoopers LLP, independent registered public accounting firm of SecureWorks Corp.
31.1††	Certification of Chief Executive Officer of the Company pursuant to Rule 13a-14(a) or Rule 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 Chief Financial Officer of the Company pursuant to Rule 13a-14(a) or Rule 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†††	Certifications of Chief Executive Officer and Chief Financial Officer of the Company pursuant to Rule 13a-14(b) or Rule 15d-14(b) under the Securities Exchange Act of 1934 and 18 U.S.C. Section 1350, as adopted pursuant to Section 906 of the Sarbanes-Oxley Act of 2002.
97.1††	Excess Incentive-Based Compensation Recoupment Policy effective October 2, 2023
101 .INS††	Inline XBRL Instance Document - the instance document does not appear in the Interactive Data File because its 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 (the cover page XBRL tags are embedded within the Inline XBRL document, which is contained in Exhibit 101).

+	Certain portions of this exhibit have been omitted pursuant to a confidential treatment request. Omitted information has been filed separately with the SEC.
††	Filed with this report.
†††	Furnished with this report.
*	Management contracts or compensation plans or arrangements in which directors or executive officers participate.
**	Certain identified portions of this exhibit have been omitted in accordance with Item 601(b)(10)(iv) of Regulation S-K.

Item 16. Form 10-K Summary

None.

SIGNATURES

Pursuant to the requirements of Section 13 or 15(d) of the Securities Exchange Act of 1934, the registrant has duly caused this report to be signed on its behalf by the undersigned, thereunto duly authorized.

SecureWorks Corp.

By: /s/ Wendy K. Thomas
Wendy K. Thomas
Chief Executive Officer
(Duly Authorized Officer)

Date: March 22, 2024

Pursuant to the requirements of the Securities Exchange Act of 1934, this report has been signed below by the following persons on behalf of the registrant and in the capacities and on the dates indicated.

SIGNATURE	TITLE	DATE
/s/ Wendy K. Thomas Wendy K. Thomas	Chief Executive Officer and Director (Principal Executive Officer)	March 22, 2024
/s/ Alpana Wegner Alpana Wegner	Chief Financial Officer (Principal Financial and Accounting Officer)	March 22, 2024
/s/ Michael S. Dell Michael S. Dell	Chairman of the Board of Directors	March 22, 2024
/s/ Kyle Paster Kyle Paster	Director	March 22, 2024
/s/ Pamela Daley Pamela Daley	Director	March 22, 2024
/s/ Yagyensh C. Pati Yagyensh C. Pati	Director	March 22, 2024
/s/ Mark J. Hawkins Mark J. Hawkins	Director	March 22, 2024