Risk Factors Comparison 2024-03-22 to 2023-03-23 Form: 10-K

Legend: **New Text** ~~Removed Text~~ Unchanged Text Moved Text Section

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 ~~and $ 21~~. ~~9 million in fiscal 2021. Any failure~~ **Failure** to increase our revenue as we grow our business could prevent us from achieving **profitability** or maintaining profitability on a consistent basis ~~or at all~~. As we pursue our growth strategy, ~~we expect~~ our operating expenses **may** ~~to continue to~~ 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 ~~support~~ **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 ~~in~~ **to** ~~response~~ **respond** to these evolving cyber- attacks without compromising the high service levels and security **that** ~~demanded by~~ our customers **demand** . **Failure** ~~If we fail~~ to predict, detect and respond effectively to the changing needs of our customers **from these** ~~in light of~~ emerging technological ~~trends necessitating~~ **advances through the** timely development or enhancement of our ~~products and features~~ **Taegis subscription solutions could result in reputational harm** , ~~we will lose~~ **loss of** customers and **cause a negative impact to** our business ~~will suffer~~ **operations and financial condition** . Our future growth ~~also~~ **is** ~~depends~~ **dependent** on our ability to continue enhancing the efficacy of the detection and response capabilities ~~of~~ **within** our Taegis software **- as- a- service, or SaaS,** platform and increasing the **interoperability of our Taegis SaaS- based** platform ~~'s interoperability~~ with third- party products and services **that** ~~adopted by~~ our customers **use** . If our Taegis ~~software~~ **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 ~~events as~~ **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** ~~the current~~ economic conditions, geopolitical uncertainty **,** and volatile financial ~~market~~ **markets** , which may have an adverse effect on our business and financial condition. **Our** ~~As a~~ company ~~, we operate~~ **operates** on a global basis **directly and through our channel partners** , serving thousands of customers **worldwide** ~~throughout the world~~ . Accordingly, our business, revenue and operating results ~~are~~ **could be** impacted by **declining** global economic conditions, geopolitical uncertainty and volatile financial markets ~~that affect~~ **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** ~~, which may~~ result in further domestic and international regulatory changes, import and export restrictions or other effects on international trade relations, ~~may hinder~~ **hindering** our ability to grow our customer base and continue servicing our existing customers. ~~Continued disruption or~~ **Economic weakness and** uncertainty **worldwide could reduce** ~~in economic and market conditions, including the continued failure of banks and other~~ -- **the** ~~financial institutions globally~~ **demand for our Taegis subscription solutions** , ~~also~~ may prolong sales cycles ~~,~~ **or** cause **a** reduction in spending by potential customers, or ~~slow the adoption of new cybersecurity technologies~~ **could make it difficult for us to accurately forecast revenue, gross margin, cash flows, and expenses** , which ~~may~~ **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 ~~the~~ continued contributions ~~of~~ **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 ~~operating~~ 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 ~~software~~ **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 ~~software~~ **security** platform ~~. In connection~~ **and, during the three months ended August 4, 2023, the Company approved continued reorganization actions in alignment** with ~~this~~ **the** plan **. Specifically** , we reduced our workforce and made decisions to optimize and align our facilities and investments with our strategic priorities. ~~This plan~~ **These activities** may not **achieve** ~~succeed in reducing~~ our ~~overhead costs,~~ **strategic priorities to** ~~optimizing~~ **optimize** our operating expenses ~~,~~ and ~~enhancing~~ **enhance** our prospects for profitable operations. ~~We may instead~~ **Instead , we may** experience additional unexpected costs ~~and~~ **that could** ~~negative~~ **negatively** ~~impacts~~ **impact** ~~on~~ 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 ~~that may hinder~~ **hindering** our ability to attract and retain top talent in the future, and **cause operational** delays ~~in operations~~ **as a** ~~resulting~~ **result** ~~from~~ **of** the loss of qualified employees. If we do not realize the ~~expected~~ **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 ~~software~~ **subscription** solutions ~~, managed security services~~ 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 ~~could~~ **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. ~~In addition, some~~ **Some** of our competitors **also** have made **strategic** acquisitions or entered into partnerships or other ~~strategic~~ **tactical** relationships ~~with one another~~ 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 ~~software~~ **subscription** solutions. **Smaller innovative** ~~Start- up~~ companies ~~that innovate~~ and large competitors **making** ~~that make~~ significant research and development investments ~~may~~ **could** develop similar or superior products or services that compete with our Taegis ~~software~~ **security** platform. Additionally, some of our larger competitors ~~have~~ **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 ~~solution~~ **solutions** ~~has~~ **have** more limited functionality than our ~~security~~ **Taegis subscription** ~~solution~~ **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 ~~are unable~~ **cannot successfully execute our go-** to **- market strategy by** ~~attract~~ **attracting** new customers, ~~retain~~ **retaining** existing customers or ~~increase~~ **increasing** ~~our~~ **the** annual contract values **for Taegis subscription solutions** , our ~~revenue growth~~ **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 ~~additional~~ large enterprise and small and medium- sized business customers, our strategy is to continue ~~to obtain~~ **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, ~~as a result~~ **resulting in our inability** ~~of which we may not be able~~ , on a consistent basis, to increase our annual contract values by obtaining advantageous contract renewals. We offer Taegis ~~software~~ **subscription** solutions ~~and managed security services~~ on a subscription basis under contracts with initial terms that typically range from one to three years and, as of February ~~3~~ **2** , ~~2023~~ **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** ~~but may pay a lower~~ average annual fee ~~,~~ **may be lower** because we ~~generally~~ **may** offer discounted rates in ~~connection with~~ **exchange for** longer contract terms. In any of these situations, we **must** ~~would need to~~ sell additional solutions or enhancements to the Taegis ~~software~~ **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 ~~have a negative~~ **negatively** impact ~~on~~ 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 ~~2023~~ **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, ~~such as decisions by customers~~ **including, but not limited** to **,** ~~reduce or restructure~~ **restructured** ~~their~~ **or reduced** technology spending to improve **a customer' s** profitability or ~~mitigate~~ **financial** risk **profile or** ~~. Further, mergers~~ **merger** ~~or consolidations of~~ **and acquisition activity within the** financial ~~institutions could~~ **industry, which may** reduce our current and potential customer base, resulting in a smaller market for our ~~security~~ **Taegis subscription** solutions. Some of our ~~solutions~~ **cybersecurity offerings** have been deemed to ~~be~~ **achieve** mission- critical functions ~~of~~ **within** our financial institution customers ~~that~~ **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 ~~software~~ **s Taegis subscription** solutions ~~offerings continue to~~ grow, ~~we plan~~ **the need** to ~~further~~ expand our operations **may** ~~, which could~~ 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 ~~software~~ **Taegis subscription** solutions, **degrading customer** ~~successfully deploy our software solutions,~~ support ~~our customers~~ after deployment ~~, and preserve our customer- centric culture~~ . 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 ~~account management~~ **customer success** personnel ~~, quickly and effectively~~ . In addition, ~~we may need~~ **adapting our information technology infrastructure** to ~~make~~ **support our growth and interoperability may require** substantial ~~investments~~ **investment** ~~to adapt our IT infrastructure to support our growth and interoperability~~ , while **also investing resources to ensure we** ~~maintaining~~ --- **maintain and improve** ~~or~~ **our** ~~improving our~~ **procedures relating to** ~~operational~~ **operations** , ~~financial~~ **financials** and managerial controls reporting ~~procedures~~ . 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 ~~adversely affected~~ **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 ~~and~~ growth prospects. Once our **Taegis subscription** solutions are deployed within our customers' networks, our customers depend on our **knowledge and** technical ~~and other~~ **expertise to provide** support services, including those provided by our channel partners in relation to the Taegis ~~software~~ **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 ~~or ,~~ 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 ~~to~~ **with the** ~~deploy~~ **deployment of** our ~~software~~ **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 ~~could be damaged~~ . If we, or our channel partners, fail to meet the ~~requirements~~ **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 ~~solutions~~ **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 ~~some~~ **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 ~~could face terminations of~~ the ~~service~~ agreements **may be terminated by the customer** . **The** ~~Damages~~ **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 ~~previous~~ **prior** 12 **-** ~~months~~ **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 ~~and managed security services~~ 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** ~~and marketing acceptance of~~ our **Taegis subscription** solutions may not be fully reflected in our results of operations in the current period, making it **challenging** ~~more difficult~~ for investors to **effectively** evaluate our financial performance. In fiscal ~~2023~~ **2024** , approximately ~~78~~ **83** % of our revenue was derived from subscription- based solutions, attributable to Taegis **subscription** solutions and ~~managed security~~ **other subscription- based** services ~~contracts~~ , while approximately ~~22~~ **17** % was derived from professional services engagements. Our subscription contracts typically range from one to three years in duration and, as of February ~~3~~ **2** , ~~2023~~ **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. ~~A decline~~ **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 any significant manner~~ in our revenue for that quarter ~~but~~ **; however, they** would negatively affect revenue in future quarters. Accordingly, the ~~effect~~ **effects** of ~~significant downturns in contracts~~ **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 ~~3~~ **2** , ~~2023~~ **2024** , we billed approximately ~~63~~ **65** % of

our recurring revenue in advance. We may not be able to adjust our **cash** outflows ~~of cash~~ 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 ~~reflect~~ **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, ~~as~~ **since** revenue from new customers **is** ~~must be~~ recognized **ratably** over the applicable contract ~~term~~ **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. ~~If we do not realize the sales we expect from potential customers, our revenue and results of operations could be adversely affected.~~ Sales of our ~~security~~ **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 ~~the~~ current macroeconomic conditions, we may experience further lengthening of sales cycles for our ~~security~~ **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 ~~software platform~~ **subscription solutions** will increase their defenses against cybersecurity threats, the customer may decide not to, or may delay its decision to, purchase the Taegis ~~software platform~~ **subscription solutions** for various reasons, which may include budgetary constraints, timing concerns, ~~unexpected administrative, processing and other delays, or~~ 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 ~~software platform~~ **subscription solutions** , our sales **efforts will not be economically recognized and revenue** will not grow as quickly as anticipated, or at all, ~~and~~ **which would result in harm to** our business **, revenue** , operating results **,** and financial condition ~~would be harmed. We spend substantial time, effort and resources in our sales efforts without any assurance that our efforts will generate long- term contracts~~ . As we continue to expand **the** ~~sales~~ **sale** of our ~~information security~~ **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 ~~internationally~~ through new or expanded relationships with local and regional strategic ~~and~~ channel partnerships and potentially through acquisitions of other companies. International revenue, which we define as revenue contracted through non- U. S. entities, contributed approximately ~~34~~ **37** % of our total revenue in fiscal ~~2023~~ **2024** . ~~Our relative lack of experience in operating~~ **Operating** ~~our business outside the United States increases the risk that any international expansion efforts will not be successful. In addition, operating~~ in international markets requires significant management attention ~~,~~ **and** financial resources ~~,~~ and **carries** legal **, regulatory and compliance** risks. ~~The~~ **Our** ~~investment~~ **investments** and ~~additional~~ **use of other** resources ~~required~~ to establish operations and ~~manage~~ **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 ~~international business and 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 ~~in the United States, the European Union and around the globe~~ have impacted and will continue to impact our effective ~~worldwide~~ **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, ~~many~~ **some** of ~~these~~ -- **the applicable changes** enacted ~~and~~ **or** proposed ~~changes to the taxation of our activities~~ , including **those relating to** cash movements, ~~could~~ **may** increase our ~~worldwide~~ **global** effective tax rate and harm our business. **For example** ~~Beginning in our fiscal year 2023~~ , the Tax Cuts and Jobs Act of 2017 eliminates ~~the option~~ **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** ~~is not repealed or otherwise modified~~ , it will materially increase our effective tax rate and reduce our operating cash flows. ~~Additionally~~ **Further** , portions of our operations are subject to a reduced tax rate or are **tax** free ~~of tax~~ under various tax holidays ~~that~~ **, which periodically** expire in whole or in part ~~from time to time,~~ 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 ~~subscriptions~~ **other cybersecurity offerings** to our customers outside the United States, which could adversely affect our non- U. S. sales and results of operations. ~~Although~~ **While** we do not currently **use financial instruments to** hedge against the risks associated with currency fluctuations, we may begin to use **such instruments** ~~foreign exchange forward contracts~~ 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** ~~be ineffective to~~ protect

us ~~fully~~ against foreign currency risk. ~~The imposition of new governmental~~ **Governmental** export or import controls or ~~of~~ international sanctions could require ~~us to comply with~~ additional compliance obligations or **may** limit our ability to compete in foreign markets ~~. 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 technologies into other countries~~ . 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~~ **compliance obligations to ensure** ~~with applicable regulatory requirements regarding~~ the **legal** export of our **Taegis subscription** solutions **, other cybersecurity offerings** and **their underlying** technologies may create delays in ~~the introduction~~ -- **introducing** ~~of~~ our **Taegis subscription** solutions **, other cybersecurity offerings** and **their underlying** technologies ~~in~~ **into certain** international markets ~~,~~ **or** prevent ~~our~~ **certain** customers ~~with international operations~~ from utilizing our solutions and technologies throughout their global ~~systems, or~~ **infrastructure. Such compliance obligations could** hinder ~~the~~ **our ability to** export ~~of~~ our **Taegis subscription** solutions **, other cybersecurity offerings** and **their underlying** technologies to some countries altogether. In addition, various countries regulate the import of our ~~appliance- based~~ **Taegis subscription solutions, other cybersecurity offerings and their underlying** technologies and have enacted laws that ~~could~~ **may** limit our ability to distribute, and our customers' ability to implement, ~~our~~ **such solutions, offerings, and** technologies ~~in~~ **within** those countries. New **or modified** export, import, or sanctions restrictions against certain persons, entities, regions, or countries (such as those imposed on Russia ~~and otherwise~~ in response to the ongoing military conflict between Russia and Ukraine), changes to product classification ~~processes~~ **procedures** , or new ~~legislation~~ or ~~shifting~~ **altered** approaches ~~in~~ **to** the enforcement or scope of existing regulations, could result in **delayed adoption by new customers, or** decreased use ~~of our solutions and technologies~~ by existing customers ~~with international operations~~ **, of our Taegis subscription solutions, other cybersecurity offerings and underlying technologies** , loss of sales to potential **multinational** customers ~~with international operations~~ , 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 ~~18~~ **23** % of our revenue in fiscal ~~2023~~ **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 ~~software~~ **subscription** solutions by providing training and other sales support, but such time, effort and ~~costs~~ **expense** may not result in ~~increased~~ **increasing our** revenue ~~for us~~ . Our channel partners may be unable to market, sell and support the Taegis ~~software~~ **subscription** solutions successfully, or these partners may not be properly incentivized to sell our Taegis ~~software~~ **subscription** solutions to end- ~~customers~~ **users** . Our inability to ~~maintain or~~ further develop ~~relationships with our~~ - **or maintain these** ~~current and prospective distribution partners~~ **partnerships** could reduce sales **revenue** of our **Taegis subscription** solutions. If we fail to ~~effectively~~ manage our sales channels or ~~channel partners~~ **partnerships effectively** , our ability to sell our Taegis ~~software~~ **subscription** solutions may be limited, adversely affecting our revenue growth and financial condition. ~~Our agreements~~ **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 ~~effectively~~ **successfully** market and sell our ~~software~~ **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 ~~software~~ **our Taegis subscription** solutions, or if they fail to meet the ~~needs~~ **expectations** of **our** customers ~~utilizing~~ **,** our ~~software~~ **ability to expand our business and sell our Taegis subscription** solutions ~~, our ability to expand our business and sell our solutions~~ may be ~~adversely affected~~ **negatively impacted** . Our business also may suffer **by losing** ~~from the loss of~~ a substantial number of our partners, **failing** ~~the failure~~ to recruit additional partners, ~~any~~ **or partners** ~~reduction~~ -- **reducing** or ~~delay~~ **delaying** ~~in~~ the sales of our **Taegis subscription** solutions ~~by our partners, or conflicts between sales by our partners and our direct sales and marketing activities~~ . Even if we do expand relationships with our channel partners, ~~our results will reflect that the~~ gross margins ~~to us~~ from sales **made** by our partners **are** generally ~~are~~ 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** ~~to involve collectability concerns and~~ may contribute to periodic fluctuations in our results of operations. Our technology alliance partnerships expose us to ~~a range~~ **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 ~~to enter~~ **entering** , into technology alliance partnerships with third parties ~~to support~~ **in alignment with** our ~~future~~ **strategic** growth plans. Such relationships include technology licensing, joint technology development and integration, research cooperation, co- marketing **,** and sell- through arrangements. We face ~~a number of~~ risks relating to ~~our~~ **these partnerships, which could inhibit us from realizing the benefits we seek. Many** technology alliance partnerships ~~that could prevent us from fully realizing the benefits we seek from these partnerships. Technology alliance partnerships can~~ require significant coordination ~~between the~~ **by both** ~~partners~~ -- **parties** and ~~a~~ significant ~~commitment of~~ time and ~~resources~~ -- **resource commitments** by their technical staffs. In cases where we ~~wish to~~ **are developing** ~~integrate~~ **integrations of our Taegis subscription solutions into** a partner' s products or services ~~into our solutions~~ , the integration **development** process may be more ~~difficult~~ **challenging** than ~~we anticipate~~ **anticipated** , and the risk of difficulties, incompatibility and undetected programming errors or defects may be higher than ~~with the introduction~~ -- **introducing** ~~of~~ new products or services. In addition, any particular relationship may **be temporary** ~~not continue for any specific period of time~~ . If we lose a significant technology alliance partner, we **may lose the expected benefit of investment into the partnership. Moreover, we** could ~~lose the benefit of our investment of time, money and resources in the relationship. Moreover, we could be required to~~ incur significant expenses ~~to develop~~ **developing** a new strategic alliance or ~~to formulate~~ **formulating** and ~~implement~~ **implementing** ~~an~~ **a strategic**

alternative ~~plan to pursue the opportunity that we targeted with the former partner~~ . 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 ~~a security breach~~ **threat actor activity** could harm our reputation, cause us to lose customers and expose us to costly litigation. Our ~~software~~ **Taegis subscription** solutions are complex and may contain defects or errors that ~~are undetectable~~ **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. ~~Because~~ **Threat actors frequently change** ~~the~~ **their tactics,** techniques ~~used~~ **, and procedures** to access or sabotage ~~IT~~ **technology** systems and networks **,** ~~change frequently~~ and **attacks** generally are not recognized until launched against a target ~~,~~ ~~an~~ **. 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 ~~to~~ our reputation and ~~a~~ **cause customers to** ~~loss~~ **lose** ~~of~~ confidence in our ~~security~~ **Taegis subscription** solutions, which ~~could~~ **may** adversely affect our business. If **a** ~~any of our customers~~ **customer** experiences **a** ~~an IT~~ 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 ~~could~~ **still may** be disappointed with our **Taegis subscription** solutions and could seek ~~alternatives~~ **alternative** ~~to our solutions~~ **cybersecurity offerings from a competitor** . In addition, if any ~~enterprise~~ **customer that is known to use** ~~or~~ **our Taegis subscription solutions, especially a** ~~government~~ **governmental** entity **or** publicly ~~known~~ **traded company subject** to ~~use our solutions~~ **the U. S. Securities and Exchange Commission' s cybersecurity disclosure requirements,** is the subject of a publicized cyber- attack, ~~some of~~ **that customer** ~~our~~ **or** other current customers ~~could~~ **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** ~~our reputation could be damaged~~ 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 ~~perception~~ **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 ~~service~~ **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** ~~expenditures by us~~ 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 ~~solutions provider~~ **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 ~~enterprise~~ **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. ~~Criminals, terrorists, or other threat~~ **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 ~~cause~~ **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 ~~, criminal or terrorist~~ . ~~The~~ **Our** shift to ~~work~~ **a remote** - **friendly organization** ~~from- home arrangements~~ 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** ~~incidents~~ **incident is malicious or the incident** ~~result~~ **resulted** from an attack on us directly or on **a** third- party ~~vendors~~ **vendor** upon which we rely. Cyber- attacks could compromise **or disrupt** our internal systems ~~and products~~ **, 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, ~~resulting in~~ **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 ~~coverage~~ will adequately cover the liability incurred, or that ~~the~~ **such** insurance ~~policy~~ 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' ~~IT~~ **technology** infrastructure, our **Taegis subscription** solutions may become less competitive **,** and our results of operations may be harmed. Our **Taegis subscription** solutions ~~must~~ **were designed to be open without compromise,** effectively ~~interoperate~~ **interoperating** with each customer' s existing or future ~~IT~~ **technology** infrastructure, which often has different specifications, utilizes multiple protocol standards, deploys products and services from multiple **security and other technology** vendors **,** and contains ~~multiple generations of~~ products and services that **were** ~~have been~~ added over time. As a result, when problems occur in a **customer' s infrastructure or** network, it may be ~~difficult~~ **challenging** to identify the sources of these problems and avoid disruptions when we ~~provide~~ **update our** software ~~updates~~ or ~~patches~~ -- **patch** to defend against ~~particular~~ **certain** vulnerabilities. Ineffective ~~interoperation could~~ **interoperability may** increase the risk of a successful cyber- attack ~~and~~ **or cause a service disruption in** ~~violations~~ **violation** of our service level agreements, **each of** which ~~would require us to provide service credits that would~~ **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. ~~Any~~ **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 ~~would~~ **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** ~~in the delivery of our~~ 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 ~~contemplated~~ **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 ~~may~~ **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** ~~impediments to~~ the development or performance of our ~~offerings~~ **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 ~~worldwide~~ **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 ~~offerings~~ **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 ~~not able~~ **unable** to maintain and enhance our brand, our revenue and profitability could be adversely affected. We believe that **it is critical to** ~~maintaining~~ **---maintain** and ~~enhancing~~ **enhance** the Secureworks brand ~~is critical~~ to **grow** our relationships with our existing and potential customers, channel partners **, technology alliance partners,** and employees ~~and~~ **in order** to **expand** our revenue ~~growth~~ and profitability. ~~Our~~ **However, our** brand promotion activities ~~, however,~~ may ~~not~~ be ~~successful~~ **unsuccessful** . ~~Any successful~~ **Successful** promotion of our brand will depend on our marketing and public relations efforts, our ability to continue ~~to offer~~ **offering** high- quality ~~information security~~ **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** ~~Dell' s~~ 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 ~~connection with~~ **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 ~~upon any such termination~~ in connection with any product, service **,** or material. If we discontinue our association with Dell in the future, ~~our ability~~ **we may be unable** to attract new customers ~~may suffer~~ **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, ~~which may result~~ **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** ~~supplement our internal~~ 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 ~~will~~ **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 ~~services~~ offerings, our ability to perform our customer engagements may suffer. Disruptions ~~resulting from~~ **, such as those caused by** COVID- 19 ~~included~~ **, 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, ~~could~~ **may** adversely affect our ability to generate revenues or ~~could~~ **might** lead to inadvertent breaches of contract by us or by our customers, **channel partners,** vendors or suppliers. **While** ~~During fiscal 2023,~~ we **did not** ~~experienced~~ **experience** a ~~limited~~ reduction in customer demand ~~and~~ **or** lengthening ~~of~~ **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 ~~may also~~ **could again** impact our results in future periods. **Pandemics such as** ~~Although we are unable to predict the extent and severity of all future impacts of~~ COVID- 19 **are impossible to predict in terms of extent and severity; therefore** , ~~the~~ **should we encounter another** pandemic **, we** might ~~further~~ **experience** ~~curtail~~ **curtailed** customer spending, ~~lead to~~ delayed or deferred purchasing decisions, ~~lengthen~~ **elongated** sales cycles **,** and ~~result in~~ 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 ~~3~~ **2** , ~~2023~~ **2024** , we owned ~~56~~ **58** issued patents and ~~10~~ **8** pending patent applications in the United States and ~~four~~ **six** issued patents and ~~eight~~ **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 ~~required~~ **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 ~~only~~ 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** ~~industry~~ **industries** are highly uncertain and evolving. ~~Although~~ **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 ~~that~~ **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** ~~a large number of~~ patents, copyrights, trademarks **,** and trade secrets ~~and by~~ **, 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 ~~information security~~ **cybersecurity** market **further** ~~continues to intensify~~ **intensifies** , as we introduce new **cybersecurity offerings, including within our Taegis subscription** solutions (including **by increasing our global presence** in ~~geographic~~ areas where we currently do not operate) ~~,~~ and as **the** ~~business- model or service overlaps~~ **overlap** ~~between~~ **of our cybersecurity offerings continue to occur with** our competitors ~~and us continue to occur~~ . Our use of open **-** source technology could require us in some circumstances to make ~~available~~ **the** source code of our modifications to that technology **available to the public** , which could include source code of our proprietary technologies, ~~and may restrict~~ **restricting** our ability to commercialize our ~~solutions~~ **cybersecurity offerings** . Some **portions** of our ~~solutions~~ **cybersecurity offerings** and technologies incorporate **open- source** software licensed by its authors or **by** other third parties ~~under open source licenses~~ . To the extent that we use **such** ~~open source~~ software, we face risks ~~arising from~~ **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 ~~may~~ **could** face periodic claims from third parties claiming ownership **of** , or demanding **that we** release, ~~of~~ the open **-** source software or derivative works that we developed using such software, which could include our proprietary source code, or ~~otherwise seeking~~ **the third parties could seek** to enforce the terms of the applicable open **-** source license. Our ability to commercialize ~~solutions~~ **our cybersecurity offerings** or technologies incorporating open **-** source software may be restricted because, among other reasons, open **-** source license terms may be ambiguous and ~~may~~ **could** result in unanticipated or uncertain obligations regarding our ~~solutions~~ **cybersecurity offerings** , litigation **,** or loss of the right to use ~~this~~ **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 ~~solutions~~ **cybersecurity offerings utilizing such software** . As a result, we ~~could~~ **may** be required to seek licenses from third parties to continue offering ~~our solutions~~ **certain cybersecurity offerings** , re- engineer our technology **to remove the open- source software** or discontinue offering our ~~solutions~~ **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** ~~with respect~~ 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 ~~and us~~ in a ~~number~~ **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 ~~and us~~ ; • Dell' s ability to use and sublicense patents that we have licensed to Dell under a patent license agreement; and • product or technology ~~development~~ **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 ~~could~~ **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 ~~might~~ **could** impede our ability to operate successfully and expand our business. ~~To preserve~~ **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 ~~conduct a tax- free distribution of the shares of our Class B common stock that it beneficially owns and its ability to consolidate with us for tax purposes, we may be~~

~~prevented from pursuing opportunities to raise capital, acquire other companies or undertake other transactions, which could hurt 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 ~~each~~ **all other class classes** of ~~nonvoting~~ 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 ~~a~~ **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 ~~to cause~~ **causes** ~~a deconsolidation of~~ us ~~for tax purposes~~ **to become deconsolidated** with respect to the Dell Technologies ~~consolidated~~ **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 ~~companies in~~ **and software industries** ~~particular~~ **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** ~~Stock prices of~~ many technology **and software** companies **, the fluctuations in the stock prices** have **been** ~~fluctuated in a manner~~ unrelated or disproportionate to ~~the~~ **their** operating performance ~~of those companies. In particular, stock prices of companies with significant operating losses have recently declined significantly, and in many instances more significantly than stock prices of companies with operating profits~~ . The economic impact and uncertainty of changes in the inflation, interest **rate,** and **the** macroeconomic **and geopolitical** environments ~~and~~ **, 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 ~~this~~ **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 ~~numerous~~ **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 ~~or financial analyst~~ **analysts** or ~~investor~~ **investors** ~~reaction~~ to our press releases, other public announcements, and SEC filings **;** • failure of ~~industry or~~ financial analysts to maintain coverage of us, changes in financial estimates by any **financial** analysts who follow our company, or our failure to meet ~~these~~ -- **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 ~~other companies in~~ our ~~industry~~ **competitors** ; • **material changes in** ~~a gain or loss of~~ 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 ~~from time to time~~ ; • 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 ~~generally~~ ; • 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 ~~in~~ **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 ~~those~~ **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 ~~3~~ **2** , ~~2023~~ **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 ~~82~~ **81** . ~~6~~ **0** % of our total outstanding shares of common stock and approximately 97. ~~9~~ **7** % of the combined voting power of both classes of our outstanding common stock. **Our** ~~So long as Dell Technologies controls the majority of the voting power 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 ~~is~~ **controls the majority of the voting power of our outstanding common stock.** ~~generally~~ **Generally** ~~able to~~ **, 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 ~~any~~ **its** required affirmative vote on matters requiring stockholder approval allowing ~~us to take~~ particular corporate actions when requested, we will not be able to take such ~~actions~~ **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 ~~the~~ **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 ~~' voting control~~ could discourage or prevent a change in control of our ~~company~~ **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. ~~We~~ **In accordance with our current business strategy, we** intend to retain ~~any earnings~~ **the profits we make** to finance the operation and ~~expansion~~ **continued growth** of our business **; therefore** , ~~and~~ **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** ~~sales~~ **sale** of our Class A common stock after **its value increases** ~~price appreciation, which may never occur, as the only way to realize any future gains on their investment~~ . 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** ~~makes~~ **make** our Class A common stock ineligible for inclusion in **certain** ~~any of these~~ indices ~~and~~ , ~~as a result,~~ **which may cause certain** mutual funds, exchange- traded funds **,** and other investment vehicles that track ~~these~~ **certain** indices ~~will~~ **may** not invest in our stock. Other major stock indices might adopt similar requirements in the future. It is **challenging to gauge whether the** ~~unclear what effect, if any,~~ exclusion from any indices will **affect** ~~have on~~ the **financial** ~~valuations~~ **valuation and market price** of **such an excluded** ~~the affected publicly- traded companies~~ **company** . It is possible that such policies could depress the **financial** ~~valuations~~ **valuation and stock price** of **a** public ~~companies~~ **company** excluded from such indices compared to ~~those of~~ 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 ~~3~~ **2** , ~~2023~~ **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 ~~3~~ **2** , ~~2023~~ **2024** , we have outstanding ~~14~~ **16** , ~~748~~ **392** , ~~810~~ **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 ~~3~~ **2** , ~~2023~~ **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~~ **there** is uncertainty ~~, particularly in light of current litigation,~~ 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 ~~and~~ , ~~as~~ **potentially resulting in** a ~~result,~~ **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 ~~could~~ **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. **30**