**Risk Factors Comparison 2025-02-24 to 2024-02-28 Form: 10-K**

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

Our operations and financial results are subject to significant risks and uncertainties including those described below. You should carefully consider the risks and uncertainties described below, in addition to other information contained in this Annual Report on Form 10- K, including our consolidated financial statements and related notes. 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 adversely affect our business. If any of the following risks or others not specified below materialize, our business, financial condition and results of operations could be materially and adversely affected. Selected Risks Affecting Our Business Our business is subject to a number of risks of which you should be aware before making a decision to invest in our common stock. These risks are more fully described in this " Risk Factors " section, including the following: • We have a history of losses and may not achieve or maintain profitability in the future. • We face intense competition. If we do not continue to innovate and offer solutions that address the dynamic cybersecurity landscape, we may not remain competitive. • We may not be able to sustain our revenue growth rate in the future. • We may not be able to **continue to** scale our business quickly enough to meet our customers' growing needs. • Our brand, reputation and ability to attract, retain and serve our customers are dependent in part upon the reliability and accuracy of our data, solutions, infrastructure and those of third parties upon which we rely. If our information technology systems or data, or those of third parties upon which we rely, are or were compromised, or if our solutions fail to detect vulnerabilities or incorrectly detect vulnerabilities, or if they contain undetected errors or defects, we could experience adverse consequences, including but not limited to regulatory investigations or actions; litigation; fines and penalties; disruptions of our business operations; reputational harm; loss of revenue or profits; loss of customers or sales; and other adverse consequences. • **We have incorporated and may in the future further incorporate generative and other types of AI processes, algorithms, and technologies into certain of our products and services. This technology is new and developing, and may generate output that is inaccurate or flawed or may not achieve market acceptance, which could result in operational, financial, regulatory, and reputational harm and other adverse consequences to our business. •** Our future quarterly results of operations are likely to fluctuate significantly due to a wide range of factors, which makes our future results difficult to predict. • Our business and results of operations depend substantially on our customers renewing their subscriptions with us and expanding the number of IT assets or IP addresses under their subscriptions. Any decline in our customer renewals, terminations or failure to convince our customers to expand their use of **our** subscription offerings would harm our business, results of operations, and financial condition. • We rely on third parties to maintain and operate certain elements of our network infrastructure. • We are subject to stringent and changing laws, regulations, rules, contractual obligations, policies, and other obligations related to data privacy and security. Our failure or perceived failure to comply with such obligations could lead to regulatory investigations or actions; litigation; fines and penalties; disruptions of our business operations; reputational harm; loss of revenue or profits; loss of customers or sales; and other adverse business consequences. • We rely on our third- party channel partner network of distributors and resellers to generate a substantial amount of our revenue. • We rely on the performance of highly skilled personnel, including senior management and our engineering, professional services, sales and technology professionals, and our ability to increase our customer base will depend to a significant extent on our ability to expand our sales and marketing operations. Risks Related to Our Business and Industry We have historically incurred net losses, including net losses of $ ~~78~~ **36** . 3 million, $ **78. 3 million and $** 92. 2 million ~~and $ 46. 7 million~~ in **2024,** 2023 ~~,~~ **and** 2022 ~~and 2021~~ , respectively. At December 31, ~~2023~~ **2024** , we had an accumulated deficit of $ ~~825~~ **861** . ~~0~~ **3** million. Because the market for our offerings is highly competitive and rapidly evolving and these solutions have not yet reached widespread adoption, it is difficult for us to predict our future results of operations. While we have experienced significant revenue growth in recent periods, we are not certain whether or when we will obtain a high enough volume of sales of our offerings to sustain or increase our growth or achieve or maintain profitability in the future. We also expect our costs to increase in future periods, which could negatively affect our future operating results if our revenue does not increase at a greater rate. In particular, we expect to continue to expend substantial financial and other resources on: • public cloud infrastructure and computing costs; • research and development related to our offerings, including investments in our research and development team; • sales and marketing, including a significant expansion of our sales organization, both domestically and internationally; • continued international expansion of our business; and • general and administrative expense. These investments may not result in increased revenue or growth in our business. If we are unable to increase our revenue at a rate sufficient to offset the expected increase in our costs, our business, financial position and results of operations will be harmed and we may not be able to achieve or maintain profitability over the long term. Additionally, we may encounter unforeseen operating expenses, difficulties, complications, delays and other unknown factors that may result in losses in future periods. If our revenue growth does not meet our expectations in future periods, our financial performance may be harmed, and we may not achieve or maintain profitability in the future. The market for cybersecurity solutions is fragmented, intensely competitive and constantly evolving. We compete with a range of established and emerging cybersecurity software and services vendors, as well as homegrown solutions. With the introduction of new technologies and market entrants, we expect the competitive environment to remain intense going forward. Our competitors include: vulnerability management and assessment vendors, including Qualys and Rapid7; diversified security software and services vendors; endpoint security vendors with nascent vulnerability assessment capabilities, including CrowdStrike; public cloud vendors and companies, such as Palo Alto Networks and Wiz, that offer solutions for cloud security (private, public and hybrid cloud); and providers of point solutions

that compete with some of the features present in our solutions. We also compete against internally- developed efforts that often use open source solutions. Some of our actual and potential competitors have significant advantages over us, such as longer operating histories, significantly greater financial, technical, marketing or other resources, stronger brand and business user recognition, larger intellectual property portfolios, government certifications and broader global distribution and presence. In addition, our industry is evolving rapidly and is becoming increasingly competitive. Companies that are larger and more established than us are focusing on cybersecurity and could directly compete with us. For example, Microsoft has a vulnerability management offering and has continued to acquire security solutions for their cybersecurity platform. Smaller companies could also launch new products and services that we do not offer and that could gain market acceptance quickly. In addition, some of our larger competitors have substantially broader product offerings and can bundle competing products and services with other software offerings which customers may choose even if individual products have more limited functionality than our solutions. These competitors may also offer their products at a lower price, which could increase pricing pressure on our offerings and cause the average sales price for our offerings to decline. These larger competitors are also often better positioned to withstand any significant reduction in capital spending, and will therefore not be as susceptible to economic downturns. One component of our enterprise platform involves assessing Cyber Exposure in a public cloud environment. We are dependent upon the providers to allow our solutions to access their cloud offerings. If one or more cloud providers elected to offer exclusively their own cloud security product or otherwise eliminate the ability of our solutions to access their cloud on behalf of our customers, our business and financial results could be harmed. Additionally, the cybersecurity market is characterized by very rapid technological advances, changes in customer requirements, frequent new product introductions and enhancements and evolving industry standards. Our success depends on continued innovation to provide features that make our solutions responsive to the cybersecurity landscape, including the shift to employees working from home or in hybrid environments and the increasing adoption by organizations of cloud or hybrid cloud architectures. Developing new solutions and product enhancements is uncertain, expensive and time- consuming, and there is no assurance that such activities will result in significant cost savings, revenue or other expected benefits. If we spend significant time and effort on research and development and are unable to generate an adequate return on our investment, our business and results of operations may be materially and adversely affected. Further, we may not be able to successfully anticipate or adapt to changing technology or customer requirements or the dynamic threat landscape on a timely basis, or at all, which would impair our ability to execute on our business strategy. Our competitors may be able to respond more quickly and effectively than we can to new or changing opportunities, technologies, standards or customer requirements or new or evolving attacks by, or indicators of compromise that identify, cyber bad actors. Furthermore, our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources and products and services offerings in the markets we address. In addition, current or potential competitors may be acquired by third parties with greater available resources, which may enable them to adapt more quickly to new technologies and customer needs, devote greater resources to the promotion or sale of their products and services, initiate or withstand substantial price competition, take advantage of other opportunities more readily or develop and expand their product and service offerings more quickly than we do. For all of these reasons, we may not be able to compete successfully against our current or future competitors. From ~~2022 to~~ 2023 **to 2024** , our revenue grew from $ ~~683~~ **798** . ~~2~~ **7** million to $ ~~798~~ **900** . ~~7~~ **0** million, representing year over year growth of ~~17~~ **13** %. This growth was primarily from an increase in subscription revenue. Although we have experienced rapid growth historically and currently have high customer renewal rates, we may not continue to grow as rapidly in the future due to a decline in our renewal rates, failure to attract new customers or other factors. Any success that we may experience in the future will depend in large part on our ability to, among other things: • maintain and expand our customer base; • increase revenue from existing customers through increased or broader use of our offerings within their organizations; • improve the performance and capabilities of our offerings through research and development or the integration of acquired products and capabilities; • continue to develop and expand our enterprise platform; • maintain or increase the rate at which customers purchase and renew subscriptions to our enterprise platform offerings; • continue to successfully expand our business domestically and internationally; and • successfully compete with other companies. If we are unable to maintain consistent revenue or revenue growth, including as a result of macroeconomic conditions, our stock price could be volatile, and it may be difficult to achieve and maintain profitability. You should not rely on our revenue for any prior quarterly or annual periods as any indication of our future revenue or revenue growth. We may be unable to rapidly and efficiently adjust our cost structure in response to significant revenue declines, which could adversely affect our operating results. Our subscription offerings are term- based and a majority of our subscription contracts are for one year in duration. In order for us to maintain or improve our results of operations, it is important that a high percentage of our customers renew their subscriptions with us when the existing subscription term expires, and renew on the same or more favorable terms. Our customers have no obligation to renew their subscriptions, and we may not be able to accurately predict customer renewal rates. In addition, the growth of our business depends in part on our customers expanding their use of subscription offerings and related services. Historically, some of our customers have elected not to renew their subscriptions with us for a variety of reasons, including as a result of changes in their strategic IT priorities, budgets, costs and, in some instances, due to competing solutions. Our retention rate may also decline or fluctuate if our existing customers choose to reduce or delay technology spending in response to economic conditions, including those resulting from exchange rate fluctuations relative to the U. S. dollar that make our products more expensive to existing customers, high rates of inflation and interest rates or concerns of an economic recession in the United States or other major markets, that could lead to decreased spending, as well as a result of a number of other factors, including our customers' satisfaction or dissatisfaction with our software, the increase in the contract value of subscription and support contracts from new customers, the effectiveness of our customer support services, our pricing, the prices of competing products or services, mergers and acquisitions affecting our customer base, global economic conditions, and the other risk factors described in this Annual Report on Form 10- K. We cannot assure you that customers will maintain

their agreements with us, renew subscriptions or increase their usage of our software. If our customers do not maintain or renew their subscriptions or renew on less favorable terms, or if we are unable to expand our customers' use of our software, our business, results of operations, and financial condition may be harmed. We recognize substantially all of our revenue ratably over the term of our subscriptions and, to a lesser extent, perpetual licenses ratably over an expected period of benefit and, as a result, downturns in sales may not be immediately reflected in our operating results. We recognize substantially all of our revenue ratably over the terms of our subscriptions with customers, which generally occurs over a one- year period and, for our perpetual licenses, over a five- year expected period of benefit. As a result, a substantial portion of the revenue that we report in each period will be derived from the recognition of deferred revenue relating to agreements entered into during previous periods. Consequently, a decline in new sales or renewals in any one period, including as a result of macroeconomic conditions, may not be immediately reflected in our revenue results for that period. This decline, however, would negatively affect our revenue in future periods. Accordingly, the effect of significant downturns in sales and market acceptance of our solutions and potential changes in our rate of renewals may not be fully reflected in our results of operations until future periods. This also makes it difficult for us to rapidly increase our revenue growth through additional sales in any period, as revenue from new customers generally will be recognized over the term of the applicable agreement. **We may not be able to continue scaling our business quickly enough to meet our customers' growing needs.** As usage of our enterprise platform grows, and as customers expand in size or expand the number of IT assets or IP addresses under their subscriptions, we may need to devote additional resources to improving our technology architecture, integrating with third- party systems and maintaining infrastructure performance. In addition, we will need to appropriately scale our sales and marketing headcount, as well as grow our third- party channel partner network, to serve our growing customer base. If we are unable to scale our business appropriately, it could reduce the attractiveness of our solutions to customers, resulting in decreased sales to new customers, lower renewal rates by existing customers or the issuance of service credits or requested refunds, each of which could hurt our revenue growth and our reputation. Even if we are able to upgrade our systems and expand our personnel, any such expansion will be expensive and complex, requiring management time and attention. We could also face inefficiencies or operational failures as a result of our efforts to scale our infrastructure. Moreover, there are inherent risks associated with upgrading, improving and expanding our information technology systems. We cannot be sure that the expansion and improvements to our infrastructure and systems will be fully or effectively implemented on a timely basis, if at all. These efforts may reduce revenue and our margins and adversely impact our financial results. If our enterprise platform offerings do not interoperate with our customers' network and security infrastructure, including remote devices, or with third- party products, websites or services, our results of operations may be harmed. Our enterprise platform offerings must interoperate with our customers' existing network and security infrastructure, including remote devices. These complex systems are developed, delivered and maintained by the customer, their employees and a myriad of vendors and service providers. As a result, the components of our customers' infrastructure, including remote devices, have different specifications, rapidly evolve, utilize multiple protocol standards, include multiple versions and generations of products and may be highly customized. We must be able to interoperate and provide our security offerings to customers with highly complex and customized networks, including remote devices, which requires careful planning and execution between our customers, our customer support teams and our channel partners. Further, when new or updated elements of our customers' infrastructure, new usage trends, such as remote and hybrid work, or new industry standards or protocols are introduced, we may have to update or enhance our cloud platform and our other solutions to allow us to continue to provide service to customers. Our competitors or other vendors may refuse to work with us to allow their products to interoperate with our solutions, which could make it difficult for our cloud platform to function properly in customer networks that include these third- party products. We may not deliver or maintain interoperability quickly or cost- effectively, or at all. These efforts require capital investment and engineering resources. If we fail to maintain compatibility of our cloud platform and our other solutions with our customers' network and security infrastructures, including for remote devices, our customers may not be able to fully utilize our solutions, and we may, among other consequences, lose or fail to increase our market share and experience reduced demand for our services, which would materially harm our business, operating results and financial condition. Our brand, reputation and ability to attract, retain and serve our customers are dependent in part upon the reliability and accuracy of our data, solutions, infrastructure and those of third parties upon which we rely. If our information technology systems or data, or those of third parties upon which we rely, are or were compromised **or disrupted** , or if our solutions fail to detect vulnerabilities or incorrectly detect vulnerabilities, or if they contain undetected errors or defects, we could experience adverse consequences. In the ordinary course of our business, we collect, store, use, transmit, disclose or otherwise process proprietary, confidential, and sensitive information, including personal data, intellectual property, and trade secrets. We sell cybersecurity products and, as a result, may be at increased risk of being a target of cyberattacks designed to penetrate our platform or internal systems, to compromise our data, alter or modify our source code, or to otherwise impede the performance of our products. Threats to information systems and data come from a variety of sources. In addition to computer " hackers, " threat actors, personnel (such as through theft or misuse **, or other insider threat listed below** )," hacktivists," organized criminal threat actors, sophisticated nation- states and nation- state- supported actors now engage and are expected to continue to engage in cyber- attacks. Nation- state actors and nation- state- supported actors may engage in such attacks for geopolitical reasons and in conjunction with military conflicts and defense activities, including the ongoing conflict between Ukraine and Russia, the ongoing conflict in the Middle East, and rising tensions between China and Taiwan. During times of war and other major conflicts, we, third parties upon which we may rely, and our customers may be vulnerable to a heightened risk of these threats, including retaliatory cyber- attacks that could materially disrupt our systems and operations, supply chain, and ability to produce, sell and distribute our goods and services. We, our customers, and the third parties upon which we rely are subject to a variety of evolving threats, which are prevalent, continue to rise, and increasingly difficult to detect. These threats include but are not limited to: social- engineering attacks (including through deep fakes, which may be increasingly more difficult to

identify as fake, and phishing attacks); credential harvesting; malicious code (such as viruses and worms); malware (including as a result of advanced persistent threat intrusions); denial- of- service attacks, credential stuffing; **insider threats (including due to** personnel misconduct ~~or~~ **,** error **or malicious activity)** ; ransomware attacks; supply- chain attacks; software bugs; server malfunctions; software or hardware failures; loss of data or other information technology assets; adware; telecommunications failures; attacks enhanced or facilitated by artificial intelligence and other similar threats. In particular, ransomware attacks, including those from organized criminal threat actors, nation- states and nation- state supported actors, are becoming increasingly prevalent and severe and can lead to significant interruptions, delays, or outages in our operations, loss of data, loss of income, significant extra expenses to restore data or systems, reputational loss and the diversion of funds. To alleviate the financial, operational and reputational impact of a ransomware attack, it may be ~~necessary~~ **prudent** to make extortion payments, but we may be unable to do so if, for example, applicable laws prohibit such payments. Additionally, we are incorporated into the supply chain of a large number of companies worldwide and, as a result, if our solutions are compromised, a significant number or, in some instances, all of our customers and their data could be simultaneously affected. The potential liability and associated consequences we could suffer as a result of such a large- scale event could be catastrophic and result in irreparable harm. ~~The increased prevalence of remote~~ **Remote** work and use of remote devices has increased risks to our information technology systems and data, as more of our ~~employees~~ **personnel** utilize network connections, computers and devices outside of our premises or network, including working at home, while in transit and in public locations. ~~Furthermore, future~~ **Future** or past business transactions, such as acquisitions or integrations, could expose us to additional cybersecurity risks and vulnerabilities, as our systems could be negatively affected by vulnerabilities present in acquired or integrated entities' systems and technologies. Furthermore, we may discover security issues that were not identified during due diligence of such acquired or integrated entities, and it may be difficult to integrate other companies into our information technology environment and security program. We rely on third **-** party service providers and technologies to operate critical business systems, including processing confidential and sensitive information, including, without limitation, cloud- based infrastructure, data center facilities, encryption and authentication technology, employee email and other functions. We also rely on third- party service providers to provide other products, services, or otherwise **, to** operate our business **and elements of our infrastructure, including endpoints** . Our ability to monitor these third parties' information security practices is limited, and these third parties may not have adequate information security measures in place. **Additionally, software errors or vulnerabilities in these third- party technologies could result in significant disruptions to our information technology systems, leading to downtime, data loss, or compromised data integrity.** If our third- party service providers **or partners** experience a security incident or other interruption **or cause an extended outage or disruption to our systems** , we could experience adverse consequences. It is possible that our customers and potential customers would hold us accountable for any security incident affecting our third- party service providers' **or partners' infrastructure or other interruption caused by our third- party service providers or partners that impacts our** infrastructure. We may incur significant liability from those customers and from other third parties with respect to any such incident. Because our agreements with certain third- party service providers, such as ~~Amazon Web Services, or~~ AWS **and Snowflake** , limit their liability for damages, we may not be able to recover a material portion of our liabilities to our customers and third parties arising from issues with such third- party service providers, such as AWS **and Snowflake** , in the event of an incident affecting the third parties' systems. Moreover, while we may be entitled to damages from ~~other~~ third- party service providers if they fail to satisfy their privacy or security- related obligations to us **or if they cause a disruption in our infrastructure** , any award may be insufficient to cover our damages, or we may be unable to recover such reward. In addition, supply- chain attacks have increased in frequency and severity ~~,~~ and ~~we~~ **there have been high- profile incidents of third- party service providers causing widespread disruptions in their customers' infrastructures due to errors in their SaaS offerings, such as the Windows outage caused by a flawed CrowdStrike software update that occurred in July 2024. We** cannot guarantee that third parties' infrastructure in our supply chain or our third- party partners' supply chains have not been compromised **or** ~~. While we have implemented security measures designed to protect against security incidents, there can be no assurance~~ that ~~these measures will be effective~~ **errors by our third- party service providers won' t cause disruptions in our infrastructure** . We have experienced, and may in the future experience, disruptions, outages ~~and~~ **,** other performance problems **and security threats** due to a variety of factors, including infrastructure changes, deliberate or unintentional human ~~or~~ **actions (including by third parties),** software **defects and configuration** errors, capacity constraints, fraud or security incidents. **We** ~~Moreover, we~~ take steps designed to detect, mitigate and remediate vulnerabilities **and defects and configuration errors** in our information technology systems (such as our hardware and software, including that of third parties upon which we rely) and in our software applications, products and services. We may not, however, be able to detect and remediate all such vulnerabilities **, defects or configuration errors** on a timely basis. For example, we have identified certain vulnerabilities in our information systems and software applications, and we take steps designed to mitigate the risks associated with known vulnerabilities. Despite our efforts, there can be no assurance that these vulnerability **, defect and configuration error** mitigation measures will be **completely** effective. Further, we may experience delays in developing and deploying remedial measures and patches designed to address any such identified vulnerabilities **, defects or configuration errors. Additionally, as part of our business operations, employees and authorized personnel, or insiders, access our systems, applications, and data, including through the use of mobile devices, including personally- owned devices. Our business may be adversely affected if insiders cause cybersecurity incidents such as data breaches, intellectual property theft, ransom demands, or operational disruptions. We take steps designed to detect and mitigate insider threats, however, despite our efforts, there can be no assurance that these efforts will be completely effective and we have expended significant resources to prevent, detect and investigate such threats. Additionally, our ability to implement and enforce security measures on employee- owned mobile devices is more limited, which increases the risk of cybersecurity threats** . Any of these or similar threats could cause a security incident or other interruption that can result in

unauthorized, unlawful, or accidental acquisition, modification, destruction, loss, alteration, encryption, disclosure of, or access to our proprietary, confidential, and sensitive information or our information technology systems, or those of the third parties upon whom we rely. **For example, we have been the target of unsuccessful phishing attempts in the past and we expect such attempts will continue in the future.** A security incident or other interruption could disrupt our ability (and that of third parties upon whom we rely) to provide our solutions. **In some instances, we or our third- party service providers may not be able to identify the cause or causes of these security incidents or performance problems within an acceptable period of time. If our solutions are unavailable or if our customers are unable to access features of our solutions within a reasonable amount of time or at all, our business could be adversely affected. In addition, if we or any of the third- party providers we use were to experience or cause a significant or prolonged outage or security incident, our business could be adversely affected.** We may expend significant resources or modify our business activities to try to protect against **or recover from** security incidents. Certain data privacy and security obligations may require us to implement and maintain specific security measures, industry- standard or reasonable security measures to protect our information technology systems and proprietary, confidential, and sensitive information, including personal data. Data protection requirements may also require us **or we may voluntarily choose** to notify relevant stakeholders of security incidents, including affected individuals, partners, collaborators, customers, regulators, law enforcement agencies and others **, or take other actions, such as providing credit monitoring and identity theft protection services** . Such disclosures ~~are~~ **and related actions can be** costly, and the disclosures or failure to comply with such **applicable** requirements could lead to adverse consequences. Additionally, even if we have issued or otherwise made patches or information for vulnerabilities in our software applications, products or services, our customers may be unwilling or unable to deploy such patches and use such information effectively and in a timely manner. Vulnerabilities could be exploited and result in a security incident. If we, our customers, or a third party upon which we rely, experience **or cause** a security incident or other interruption, or are perceived to have experienced **or caused** a security incident or other interruption, we may experience **material** adverse consequences, such as government enforcement actions (for example, investigations, fines, penalties, audits, and inspections); additional reporting obligations and / or oversight; restrictions on processing information (including personal data); litigation (including class claims); indemnification obligations; negative publicity; reputational harm; monetary fund diversions; interruptions of our operations (including availability of data); financial loss (including by issuing credits to our customers); diversion of management attention; and other similar harm. Security incidents **or other disruptions** and attendant **material** consequences may cause customers to stop using our solutions (including by not renewing their purchases of our solutions), deter new customers from using our solutions, and negatively impact our ability to grow and operate our business. There can be no assurance that any limitations or exclusions of liabilities in our contracts would be enforceable or adequate or would otherwise protect us from liabilities or damages if we fail to comply with data protection requirements related to information security or security incidents. We cannot be sure that our insurance coverage will be adequate or otherwise protect us from or adequately mitigate liabilities or damages with respect to claims, costs, expenses, litigation, fines, penalties, business loss, data loss, regulatory actions or other impacts arising out of security incidents. In addition, we face unique risks as a SaaS company ~~, particularly in light~~ **that sells products and services that involve protecting the information systems** of our **customers** ~~business model~~ . If our solutions fail to detect vulnerabilities in our customers' cybersecurity infrastructure, including for remote devices, or if our solutions fail to identify new and increasingly complex methods of cyberattacks, our business may suffer and our customers' businesses may be damaged, including by interrupting their networking traffic or operational technology environments **. Furthermore, a security incident could heighten the impact of these material adverse consequences because of the nature of our business and expectations of our customers** . There is no guarantee that our solutions will detect all vulnerabilities or threats in our customers' systems, especially in light of the rapidly changing security landscape to which we must respond. Additionally, our solutions may falsely detect vulnerabilities or threats that do not actually exist. For example, our solutions rely on information provided by an active community of users who contribute information about new exploits, attacks and vulnerabilities. If the information from these third parties is inaccurate, the potential for false indications of vulnerabilities or threats increases. These false positives, while typical in the industry, may impair the perceived reliability of our offerings. Additionally, our business depends upon the appropriate and successful implementation of our product by our customers. If our customers fail to use our solutions according to our specifications, our customers may suffer a security incident on their own systems or other adverse consequences. Even if such an incident is unrelated to our security practices, it could result in our incurring significant economic and operational costs in investigating, remediating, and implementing additional measures to further protect our customers from their own vulnerabilities. The reliability and continuous availability of our solutions is critical to our success. We have experienced errors or defects in the past in connection with the release of new solutions and product upgrades, and we expect that these errors or defects will be found from time to time in the future in new or enhanced solutions after commercial release. **For example, on December 31, 2024, we identified Nessus agents versions 10. 8. 0 and 10. 8. 1 going offline under certain conditions which impacted the availability of our Vulnerability Management and Security Center solutions for certain customers. Upon discovery of the incident, we developed and released a version 10. 8. 2 of our Nessus agent on January 2, 2025, which enabled affected customers to resolve the issue. Although the financial impacts of this incident have not been significant, similar incidents in the future could result in costs associated with service- level credits and loss of customer trust, which could have a material adverse effect on our business and financial performance.** In addition, we use third parties to assist in the development of our products and these third parties could be a source of errors or defects. Some defects may cause our solutions to be vulnerable to attacks, cause them to fail to detect vulnerabilities, or temporarily interrupt customers' networking traffic or operational technology environments, any of which may damage our customers' business and could hurt our reputation. As a result of any of the risks associated with our SaaS business, we may experience **material** adverse consequences. We may also be subject to liability claims for damages related to errors or defects in our solutions **. We have**

**incorporated and may in the future further incorporate AI features in certain of our products and services, including ExposureAI and Tenable AI Assistant. The use of generative AI processes at scale is relatively new, and may lead to challenges, concerns and risks, including various privacy and security risks that are significant or that we may not be able to predict, especially if our use of these technologies in our products and services becomes more important to our operations over time. The technologies underpinning these features are in the early stages of commercial use and exist in an emerging regulatory environment, which presents regulatory, litigation, ethical, reputational, operational and financial risks. AI in our products and services may be difficult to deploy successfully due to operational issues inherent to the nature of such technologies, including the development, maintenance and operation of deep learning datasets. Additionally, if we do not have adequate rights to utilize the data or other materials and content that our AI technologies depend on, we may face legal consequences for violating applicable laws, third- party intellectual property, privacy or other rights, or contracts to which we are a party. Uncertainty in the legal regulatory regime relating to AI and emerging ethical issues surrounding the use of AI may require significant resources to modify and maintain business practices to comply with U. S. and non- U. S. laws, the nature of which cannot be determined at this time. Existing laws and regulations may apply to us or our suppliers, vendors, partners and customers in new ways, and new laws and regulations may be instituted. Many U. S. and international governmental bodies and regulators have proposed, enacted or are in the process of developing, new regulations related to the use of AI and machine learning technologies. For example, the European Union authorities recently adopted a legal framework on AI regulation, the Artificial Intelligence Act, which applies beyond the European Union' s borders and establishes obligations for AI providers and those deploying AI systems. Other jurisdictions may adopt similar or potentially more restrictive laws, which may render the use of such technologies challenging. The final form of these may impose obligations related to our development, offering and use of AI technologies and expose us to increased risk of regulatory enforcement and litigation. Any sensitive information (including confidential, competitive, proprietary, or personal data) that we input into a third- party generative AI platform could be leaked or disclosed to others, including if sensitive information is used to train the third parties' AI model. Additionally, where an AI model ingests personal data and makes connections using such data, those technologies may reveal other personal or sensitive information generated by the model. Our AI technology features may also generate output that is misleading, insecure, inaccurate, harmful or otherwise flawed. Our customers or others may rely on or use such misleading, insecure, harmful or otherwise flawed content to their detriment, which may harm our brand, reputation, business or customers, cause competitive harm or expose us to legal liability. For example, AI algorithms use machine learning and predictive analytics which may be insufficient or of poor quality and reflect inherent biases and could lead to flawed, biased, and inaccurate results. Deficient or inaccurate recommendations, forecasts, or analyses that generative AI applications assist in producing could lead to customer rejection or skepticism of our products, affect our reputation or brand, and negatively affect our financial results. Further, unauthorized use or misuse of AI by our employees or others may result in disclosure of confidential company and customer data, reputational harm, privacy law violations and legal liability. Our use of generative AI may also lead to novel and urgent cybersecurity risks, including related to personal data, which may adversely affect our operations and reputation** . Our revenue and results of operations have historically varied from period to period, and we expect that they will continue to do so as a result of a number of factors, many of which are outside of our control, including: • the level of demand for our solutions; • the introduction of new products and product enhancements by existing competitors or new entrants into our market, and changes in pricing for solutions offered by us or our competitors; • the rate of renewal of subscriptions, and extent of expansion of assets under such subscriptions, with existing customers; • the mix of customers licensing our products on a subscription basis as compared to a perpetual license; • large customers failing to renew their subscriptions; • the size, timing and terms of our subscription agreements with new customers; • our ability to interoperate our solutions with our customers' network and security infrastructure, including remote devices; • the timing and growth of our business, in particular through our hiring of new employees and international expansion; • network outages, security breaches, technical difficulties or interruptions with our solutions (including security breaches by our service providers or vendors); • changes in the growth rate of the markets in which we compete; • the length of the license term, amount prepaid and other material terms of subscriptions to our solutions sold during a period; • customers delaying purchasing decisions in anticipation of new developments or enhancements by us or our competitors or otherwise; • changes in customers' budgets; • seasonal variations related to sales and marketing and other activities, such as expenses related to our customers; • our ability to increase, retain and incentivize the channel partners that market and sell our solutions; • our ability to integrate our solutions with our ecosystem partners' technology; • our ability to integrate any future acquisitions of businesses; • our brand and reputation; • the timing of our adoption of new or revised accounting pronouncements applicable to public companies and the impact on our results of operations; • our ability to control costs, including our operating expenses, such as personnel costs, third- party cloud infrastructure costs and facilities costs; • our ability to hire, train and maintain our direct sales force; • unforeseen litigation and intellectual property infringement; • fluctuations in our effective tax rate; • general economic and political conditions, both domestically and internationally, as well as economic conditions specifically affecting industries in which our customers operate; and • other events or factors, including those resulting from public health crises such as pandemics or similar outbreaks, war, incidents of terrorism or responses to these events, or an economic recession in the United States or other major markets. Any one of these or other factors discussed elsewhere in this Annual Report on Form 10- K, or the cumulative effect of some of these factors, may result in fluctuations in our revenue and operating results, meaning that quarter- to- quarter comparisons of our revenue, results of operations and cash flows may not necessarily be indicative of our future performance and may cause us to miss our guidance and analyst expectations and may cause our stock price to decline. In addition, we have historically experienced seasonality in entering into agreements with customers. We typically enter into a significantly higher percentage of agreements with new customers, as well

as renewal agreements with existing customers, in the third and fourth quarters. The increase in customer agreements in the third quarter is primarily attributable to U. S. government and related agencies, and the increase in the fourth quarter is primarily attributable to large enterprise account buying patterns typical in the software industry. We expect that seasonality will continue to affect our operating results in the future and may reduce our ability to predict cash flow and optimize the timing of our operating expenses. We must maintain and enhance our brand. We believe that developing and maintaining widespread awareness of our brand in a cost- effective manner is critical to achieving widespread acceptance of our enterprise platform and attracting new customers. Brand promotion activities may not generate customer awareness or increase revenue and, even if they do, any increase in revenue may not offset the expenses we incur in maintaining and promoting our brand. If we fail to successfully promote and maintain our brand, or incur substantial expenses, we may fail to attract or retain customers necessary to realize a sufficient return on our brand- building efforts, or to achieve the widespread brand awareness that is critical for broad customer adoption of our solutions. We utilize data centers located in North America, Europe and Asia to operate and maintain certain elements of our own network infrastructure. Some elements of this complex system are operated by third parties that we do not control and that could require significant time to replace. We expect this dependence on third parties to continue. For example, Tenable One is hosted on ~~Amazon Web Services, or~~ AWS ~~,~~ which provides us with computing and storage capacity. Interruptions in our systems or the third- party systems on which we rely, particularly AWS, whether due to system failures, computer viruses or cyber threats, physical or electronic break- ins or other factors, could affect the security or availability of our solutions, network infrastructure and website. Our existing data center facilities and third- party hosting providers have no obligations to renew their agreements with us on commercially reasonable terms or at all, and certain of the agreements governing these relationships may be terminated by either party with notice or access to hosting services may be restricted by the provider at any time, with no or limited notice. For example, our agreement with AWS allows AWS to terminate the agreement with two years' written notice and allows AWS, under certain circumstances, to temporarily restrict access to hosting services provided by AWS without prior notice. Although we expect that we could receive similar services from other third parties, if any of our arrangements with third parties, including AWS, are terminated, we could experience interruptions on our platform and in our ability to make our platform available to customers, as well as downtime, delays and additional expenses in arranging alternative cloud infrastructure services. Organizations may be reluctant to purchase our enterprise platform offerings that are cloud- based due to the actual or perceived vulnerability of cloud solutions. Some organizations, including those in the defense industry and highly regulated industries such as healthcare and financial services, have historically been reluctant to use cloud- based solutions for cybersecurity because they have concerns regarding the risks associated with the reliability or security of the technology delivery model associated with these solutions. If we or other software companies with cloud- based offerings experience security incidents, breaches of customer data, disruptions in service delivery or other problems, the market for cloud- based solutions as a whole may be negatively impacted, which in turn would negatively impact our revenue and our growth prospects. Our sales cycle is long and unpredictable. The timing of sales of our offerings is difficult to forecast because of the length and unpredictability of our sales cycle, particularly with large enterprises and with respect to certain of our solutions. We sell our solutions primarily to IT departments that are managing a growing set of user and compliance demands, which has increased the complexity of customer requirements to be met and confirmed during the sales cycle and prolonged our sales cycle. Our average sales cycle with an enterprise customer is approximately four months, although unfavorable macroeconomic conditions and the extent to which we continue to enter into larger deals, could result in longer average sales cycles. Further, the length of time that potential customers devote to their testing and evaluation, contract negotiation and budgeting processes varies significantly, depending on the size of the organization and nature of the product or service under consideration. Macroeconomic uncertainty, including foreign exchange rates, inflation, disruptions in access to bank deposits or lending commitments due to bank failures and uncertainty about economic stability, and concerns about economic recessions in the United States or other major markets, have and could continue to impact the budgets and purchasing decisions and processes of certain of our customers and prospective customers, some of whom have added additional controls on expenditures and require additional internal approvals of expenditures, even if relatively small in dollar amount, all of which could lengthen our average sales cycle. In addition, we might devote substantial time and effort to a particular unsuccessful sales effort, and as a result, we could lose other sales opportunities or incur expenses that are not offset by an increase in revenue, which could harm our business. We are subject to stringent and changing laws, regulations, rules, contractual obligations, policies, and other obligations related to data privacy and security. Our failure, or perceived failure to comply with such obligations ~~,~~ could lead to regulatory investigations or actions; litigation; fines and penalties; disruptions of our business operations; reputational harm; loss of revenue or profits; loss of customers or sales; and other adverse business consequences. In the ordinary course of our business, we collect, receive, store, process, generate, use, transfer, disclose, make accessible, protect, secure, dispose of, transmit, and share (collectively, " process ") personal data and other sensitive information, including proprietary and confidential business information, trade secrets, intellectual property, and sensitive third-party information. Our data processing activities subject us to numerous data privacy and security obligations, such as various laws, rules, regulations, guidance, industry standards, external and internal privacy and security policies, contracts, and other obligations that govern the processing of personal data by us and on our behalf. In the United States, federal, state, and local governments have enacted numerous data privacy security laws, including data breach notification laws, data privacy laws, consumer protection laws (e. g., Section 5 of the Federal Trade Commission Act), and other similar laws (e. g., wiretapping laws). ~~In the past few years, numerous~~ **Numerous** U. S. states ~~— including California, Virginia, Colorado, Connecticut, and Utah —~~ have enacted comprehensive privacy laws that impose certain obligations on covered businesses, including providing specific disclosures in privacy notices and affording residents with certain rights concerning their personal data. As applicable, such rights may include the right to access, correct, or delete certain personal data, and to opt- out of certain data processing activities, such as targeted advertising, profiling, and automated decision- making. The exercise of these rights may impact our

business and ability to provide our products and services. Certain states also impose stricter requirements for processing certain personal data, including sensitive information, such as conducting data privacy impact assessments. These state laws allow for statutory fines for noncompliance. For example, the California Consumer Privacy Act of 2018, as amended by the California Privacy Rights Act of 2020, ~~CPRA~~ or collectively, the CCPA, imposes obligations on covered businesses to provide specific disclosures in privacy notices and honor requests of California residents to exercise certain rights related to their personal data. The CCPA applies to personal data of **consumers,** business representatives and employees **who are California residents** and provides for fines for noncompliance (up to $ 7, 500 per intentional ~~violation~~ **violations** ~~)~~. Further, the ~~CPRA' s recent amendments expanded the~~ CCPA **allows private litigants affected** ~~' s requirements, including~~ by **certain** ~~adding a new right for individuals to correct their personal~~ data **breaches** ~~and by establishing a new regulatory agency~~ to **recover significant statutory damages** ~~implement and enforce the law, which could increase the risk of an enforcement action~~. Similar laws have been passed or are being considered in several other states, as well as at the federal and local levels, and we expect more states to pass similar laws in the future. These developments may further complicate compliance efforts and may increase legal risk and compliance costs for us, the third parties ~~upon~~ **with** whom we ~~rely~~ **work**, and our customers **. Our employees and personnel use generative AI technologies to perform their work, and the disclosure and use of personal data in generative AI technologies is subject to various privacy laws and other privacy obligations. Governments have passed and are likely to pass additional laws regulating generative AI. Our use of this technology could result in additional compliance costs, regulatory investigations and actions, and lawsuits. If we are unable to use generative AI, it could make our business less efficient and result in competitive disadvantages**. Additionally, under various privacy laws and other obligations, we may be required to provide certain notices and obtain consents to process certain types of personal data. For example, some of our data processing practices may be challenged including in relation to our use of chatbot and session replay providers **. These practices may be subject to increased challenges by class action plaintiffs**. Our inability or failure to obtain consent for these practices could result in adverse consequences. Outside the United States, an increasing number of laws, regulations, and industry standards govern data privacy and security. For example, the European Union' s General Data Protection Regulation, or EU GDPR, and the United Kingdom' s GDPR, or UK GDPR, impose strict requirements for processing the personal data of individuals. Violations of these obligations carry significant potential consequences. For example, under the EU GDPR, government regulators may impose temporary or definitive bans on processing, as well as fines of up to € 20 million or 4 % of the annual global revenue, whichever is greater **. In addition, new EU and UK regulations or legislative actions regarding data privacy and security (together with applicable industry standards) may be proposed or enacted, such as the EU' s Digital Operational Resilience Act and its second Network and Information Security Directive, which may increase our costs of doing business, and non- compliance with such laws and regulations, as applicable to us, may lead to significant administrative fines**. We have an internal data privacy function that oversees and supervises our compliance with ~~European~~ **data privacy laws, including EU** and UK data protection regulations but, despite our efforts, we may fail, or be perceived to have failed, to comply. Canada' s Personal Information Protection and Electronic Documents Act, or PIPEDA, and various related provincial laws, Canada' s Anti- Spam Legislation, or CASL, and Brazil' s General Data Protection Law (Law No. 13, 709 / 2018), or Lei Geral de Proteção de Dados Pessaois, or LGPD, may apply to our operations. The LGPD broadly regulates processing personal data of individuals in Brazil and imposes compliance obligations and penalties comparable to those of the EU GDPR. Additionally, we also target customers in Asia and may be subject to new and emerging data privacy regimes in Asia, including China' s Personal Information Protection Law, Japan' s Act on the Protection of Personal Information, and Singapore' s Personal Data Protection Act. In addition, we may be unable to transfer personal data from Europe and other jurisdictions to the United States or other countries due to data localization requirements or limitations on cross- border data flows. Europe and other jurisdictions have enacted laws requiring data to be localized or limiting the transfer of personal data to other countries. In particular, the European Economic Area, or EEA, and the United Kingdom, or UK, have significantly restricted the transfer of personal data to the United States and other countries whose privacy laws it believes are inadequate. Other jurisdictions may adopt **or have already adopted** similarly stringent ~~interpretations of their~~ data localization and cross- border data transfer laws. Although there are currently various mechanisms that may be used to transfer personal data from the EEA and UK to the United States in compliance with law, such as the EEA standard contractual clauses, the UK' s International Data Transfer Agreement / Addendum, and the EU- U. S. Data Privacy Framework and the UK extension thereto (which allows for transfers to relevant U. S.- based organizations who self- certify compliance and participate in the Framework), these mechanisms are subject to legal challenges, and there is no assurance that we can satisfy or rely on these measures to lawfully transfer personal data to the United States. If there is no lawful manner for us to transfer personal data from the EEA, the UK, or other jurisdictions to the United States, or if the requirements for a legally- compliant transfer are too onerous, we could face significant adverse consequences, including the interruption or degradation of our operations, the need to relocate part of or all of our business or data processing activities to other jurisdictions at significant expense, increased exposure to regulatory actions, substantial fines and penalties, the inability to transfer data and work with partners, vendors and other third parties, and injunctions against our processing or transferring of personal data necessary to operate our business. Additionally, companies that transfer personal data out of the EEA and UK to other jurisdictions, particularly to the United States, are subject to increased scrutiny from regulators, individual litigants, and activist groups. For example, some European regulators have significantly restricted some companies from transferring certain personal data out of Europe for allegedly violating the GDPR' s cross- border data transfer limitations. In addition to data privacy and security laws, we are contractually subject to industry standards adopted by industry groups and may become subject to such obligations in the future. Furthermore, we are bound by other contractual obligations relating to data privacy and security, and our efforts to comply with such obligations may not be successful. For example, certain privacy laws, such as the GDPR and the CCPA, require our customers to impose specific contractual restrictions on their service providers. Additionally, some of our customer contracts require us to host personal data

locally. We have published privacy policies, marketing materials **, whitepapers,** and other statements, such ~~as~~ **statements related to** compliance with certain certifications or self- regulatory principles, ~~regarding~~ **concerning** data privacy ~~and~~ **,** security **, and artificial intelligence** . ~~If~~ **Regulators in the United States are increasingly scrutinizing these statements, and if** these policies, materials or statements are found to be deficient, lacking in transparency, deceptive, unfair **, misleading** , or misrepresentative of our practices, we may be subject to investigation, enforcement actions by regulators, or other adverse consequences. Our obligations related to data privacy and security (and customers' data privacy expectations) are quickly becoming increasingly stringent, and creating uncertainty. Additionally, these obligations may be subject to differing applications and interpretations, which may be inconsistent or in conflict among jurisdictions. Preparing for and complying with these obligations requires us to devote significant resources. These obligations may necessitate changes to our services, information technologies, systems, and practices and to those of any third parties that process personal data on our behalf. Existing and proposed laws and regulations can be costly to comply with, can delay or impede the development or adoption of our products and services and require significant management time and attention. Although we endeavor to comply with all data privacy and security obligations, we may at times fail (or be perceived to have failed) to do so. Moreover, despite our efforts, our personnel or third parties upon which we rely may fail to comply with such obligations, which could negatively impact our business operations and compliance posture. If we or the third parties upon which we rely fail, or are perceived to have failed, to address or comply with applicable data privacy and security obligations, we could face significant consequences. These consequences include, but are not limited to: government enforcement actions (such as investigations, fines, penalties, audits, inspections, and similar actions); litigation (including class- action related claims) and mass arbitration demands; additional reporting requirements and / or oversight; bans on processing personal data; and orders to destroy or not use personal data. In particular, plaintiffs have become increasingly more active in bringing privacy- related claims against companies, including class claims and mass arbitration demands. Some of these claims allow for the recovery of statutory damages on a per violation basis, and, if viable, carry the potential for significant statutory damages, depending on the volume of data and the number of violations. Any of these events could have a material adverse effect on our reputation, business, or financial condition, including but not limited to: interruptions or stoppages in our business operations, inability to process personal data or operate in certain jurisdictions; limited ability to develop or commercialize our products; expenditure of time and resources to defend any claim or inquiry; reputational harm; loss of customers; reduction in the use of our products; or revision or restricting of our operations. Our success is dependent in part upon establishing and maintaining relationships with a variety of channel partners that we utilize to extend our geographic reach and market penetration. We **typically** use a two- tiered, **channel** ~~indirect fulfillment~~ model whereby we sell our products and services to our distributors, ~~which~~ **who** in turn sell to our resellers, ~~which~~ **who** then sell to our end users, ~~which~~ **who** we call customers. We anticipate that we will continue to rely on this two- tiered sales model in order to help facilitate sales of our offerings as part of larger purchases in the United States and to grow our business internationally. In **2024,** 2023 ~~,~~ **and** 2022 ~~and 2021~~ , we derived **94 %,** 93 % ~~,~~ **and** 92 % ~~and 92 %~~ , respectively, of our revenue from **sales** ~~subscriptions and perpetual licenses sold~~ through channel partners, and the percentage of revenue derived from channel partners may continue to increase in future periods. Ingram Micro, Inc., a distributor, accounted for **34 %,** 36 % ~~,~~ **and** 38 % ~~and 39 %~~ of our revenue in **2024,** 2023 ~~,~~ **and** 2022 ~~and 2021~~ , respectively, and ~~32~~ **29** % of our accounts receivable at December 31, ~~2023~~ **2024** and ~~36~~ **32** % at December 31, ~~2022~~ **2023** . Our agreements with our channel partners, including our agreement with Ingram Micro, are non- exclusive and do not prohibit them from working with our competitors or offering competing solutions, and some of our channel partners may have more established relationships with our competitors. Similarly, our channel partners have no obligations to renew their agreements with us on commercially reasonable terms or at all, and certain of the agreements governing these relationships may be terminated by either party at any time, with no or limited notice. For example, our agreement with Ingram Micro allows Ingram Micro to terminate the agreement in their discretion upon 30 days' written notice to us. If our channel partners choose to place greater emphasis on products of their own or those offered by our competitors or **as** a result of an acquisition, competitive factors or other reasons do not continue to market and sell our solutions in an effective manner or at all, our ability to grow our business and sell our solutions, particularly in key international markets, may be adversely affected. In addition, our failure to recruit additional channel partners, or any reduction or delay in their sales of our solutions and professional services, including as a result of economic uncertainty **, legal or regulatory actions, such as government investigations or law enforcement activities, impacting their business** , or conflicts between channel sales and our direct sales and marketing activities may harm our results of operations. Finally, even if we are successful, our relationships with channel partners may not result in greater customer usage of our solutions and professional services or increased revenue. A portion of our revenue is generated from subscriptions and perpetual licenses sold to domestic governmental entities, foreign governmental entities and other heavily regulated organizations, which are subject to a number of challenges and risks. A portion of our revenue is generated from subscriptions and perpetual licenses sold to governmental entities in the United States. Additionally, many of our current and prospective customers, such as those in the financial services, energy, insurance and healthcare industries, are highly regulated and may be required to comply with more stringent regulations in connection with subscribing to and implementing our enterprise platform. Selling licenses to these entities can be highly competitive, expensive and time- consuming, often requiring significant upfront time and expense without any assurance that we will successfully complete a sale. Governmental demand and payment for our enterprise platform may also be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our enterprise platform. In addition, governmental entities have the authority to terminate contracts at any time for the convenience of the government, which creates risk regarding revenue anticipated under our existing government contracts. Further, governmental and highly regulated entities often require contract terms that differ from our standard customer arrangements, including terms that can lead to those customers obtaining broader rights in our solutions than would be expected under a standard commercial contract and terms that can allow for early termination. The U. S. government will be able to

terminate any of its contracts with us either for its convenience or if we default by failing to perform in accordance with the contract schedule and terms. Termination for convenience provisions would generally enable us to recover only our costs incurred or committed, settlement expenses, and profit on the work completed prior to termination. Termination for default provisions do not permit these recoveries and would make us liable for excess costs incurred by the U. S. government in procuring undelivered items from another source. Contracts with governmental and highly regulated entities may also include preferential pricing terms. In the United States, federal government agencies may promulgate regulations, and the President may issue executive orders, requiring federal contractors to adhere to different or additional requirements after a contract is signed. If we do not meet applicable requirements of law or contract, we could be subject to significant liability from our customers or regulators. Even if we do meet these requirements, the additional costs associated with providing our enterprise platform to government and highly regulated customers could harm our operating results. Moreover, changes in the underlying statutory and regulatory conditions that affect these types of customers could harm our ability to efficiently provide them access to our enterprise platform and to grow or maintain our customer base. In addition, engaging in sales activities to foreign governments introduces additional compliance risks, including risks specific to anti- bribery regulations, including the U. S. Foreign Corrupt Practices Act of 1977, as amended, or the FCPA, the U. K. Bribery Act 2010 and other similar statutory requirements prohibiting bribery and corruption in the jurisdictions in which we operate. Further, in some jurisdictions we may be required to obtain government certifications, which may be costly to maintain and, if we lost such certifications in the future or if such certification requirements changed, would restrict our ability to sell to government entities until we have attained such certifications. Some of our revenue is derived from contracts with U. S. government entities, as well as subcontracts with higher-tier contractors **and customers who receive government funding** . As a result, we are subject to federal contracting regulations, including the Federal Acquisition Regulation, or the FAR. Under the FAR, certain types of contracts require pricing that is based on estimated direct and indirect costs, which are subject to change **. The new U. S. presidential administration' s commitment to reduce government spending, may impact availability of funding for U. S. government customers, generally, as well as eliminate departments and / or personnel who rely on our products which could adversely affect our business and financial performance** . In connection with our U. S. government contracts, we may be subject to government audits and review of our policies, procedures, and internal controls for compliance with contract terms, procurement regulations, and applicable laws. In certain circumstances, if we do not comply with the terms of a contract or with regulations or statutes, we could be subject to contract termination or downward contract price adjustments or refund obligations, could be assessed civil or criminal penalties, or could be debarred or suspended from obtaining future government contracts for a specified period of time. Any such termination, adjustment, sanction, debarment or suspension could have an adverse effect on our business. **Moreover, as a U. S. government contractor, we maintain plans to ensure compliance with nondiscrimination and regulatory requirements for qualified employees on the basis of gender, race, disability and veteran status. Consequently, we may be subject to executive orders and regulatory changes affecting various aspects of our operations, including compliance with nondiscrimination plans. Any required elimination or modification of such plans in response to new executive orders could pose challenges in hiring or retaining employees and may lead to other adverse operational impacts. Failure to comply with these requirements could expose us to administrative, civil, or criminal liabilities, including fines, penalties, repayments or suspension or debarment from eligibility from future U. S. government contracts. Further, as a U. S. government contractor, we are subject to an increased risk of investigations, criminal prosecution, civil fraud, whistleblower lawsuits and other legal actions and liabilities as compared to solely private sector commercial companies.** In the course of providing our solutions and professional services to governmental entities, our employees and those of our channel partners may be exposed to sensitive government information. Any failure by us or our channel partners to safeguard and maintain the confidentiality of such information could subject us to liability and reputational harm, which could materially and adversely affect our results of operations and financial performance. Our pricing model subjects us to various challenges that could make it difficult for us to derive expected value from our customers and we may need to reduce our prices or change our pricing model to remain competitive. Subscriptions and perpetual licenses to our enterprise platform are generally priced based on the number of IP addresses or total IT assets that can be monitored. We expect that we may need to change our pricing from time to time. As competitors introduce new products that compete with ours or reduce their prices, we may be unable to attract new customers or retain existing customers based on our historical pricing. We also must determine the appropriate price to enable us to compete effectively internationally. Moreover, mid- to large- size enterprises may demand substantial price discounts as part of the negotiation of sales contracts and, as the amount of IT assets or IP addresses within our customers' organization grows, we may face additional pressure from our customers regarding our pricing. As a result, we may be required or choose to reduce our prices or change our pricing model, which could adversely affect our business, revenue, operating margins and financial condition. Further, our subscription agreements and perpetual licenses generally provide that we can audit our customers' use of our offerings to ensure compliance with the terms of such agreement or license and monitor an increase in IT assets and IP addresses being monitored. However, a customer may resist or refuse to allow us to audit their usage, in which case we may have to pursue legal recourse to enforce our rights under the agreement or license, which would require us to spend money, distract management and potentially adversely affect our relationship with our customers and users. If our enterprise platform offerings do not achieve sufficient market acceptance, our results of operations and competitive position will suffer. We spend substantial amounts of time and money to research and develop and enhance our enterprise platform offerings to meet our customers' rapidly evolving demands. In addition, we invest in efforts to continue to add capabilities to our existing products and enable the continued detection of new network vulnerabilities. We typically incur expenses and expend resources upfront to market, promote and sell our new and enhanced offerings. Therefore, when we develop and introduce new or enhanced offerings, they must achieve high levels of market acceptance in order to justify the amount of our investment in developing and bringing them to market, and if these new or

enhanced offerings do not garner widespread market adoption and implementation, our operating results and competitive position could suffer. Further, we may make enhancements to our offerings that our customers do not like, find useful or agree with. We may also discontinue certain features, begin to charge for certain features that are currently free or increase fees for any of our features or usage of our offerings. Our new offerings or enhancements and changes to our existing offerings could fail to attain sufficient market acceptance for many reasons, including: • failure to predict market demand accurately, including changes in demand as a result of macroeconomic trends, in terms of functionality and to supply offerings that meets this demand in a timely fashion; • defects, errors or failures; • negative publicity about their performance or effectiveness; • delays in releasing our new offerings or enhancements to our existing offerings to the market; • introduction or anticipated introduction of competing products by our competitors; • poor business conditions for our customers, including as a result of difficult macroeconomic conditions, causing them to delay or forgo IT purchases; and • reluctance of customers to purchase cloud- based offerings. If our new or enhanced offerings do not achieve adequate acceptance in the market, our competitive position will be impaired, and our revenue will be diminished. The adverse effect on our operating results may be particularly acute because of the significant research, development, marketing, sales and other expenses we will have incurred in connection with the new or enhanced offerings. Our strategy of offering and deploying our solutions in the cloud, on- premises environments or using a hybrid approach causes us to incur increased expenses and may pose challenges to our business. We offer and sell our enterprise platform for use in the cloud, on- premises environments or using a hybrid approach using the customer' s own infrastructure. Our cloud offering enables our customers to eliminate the burden of provisioning and maintaining infrastructure and to scale their usage of our solutions quickly, while our on- premises offering allows for the customer' s complete control over data security and software infrastructure. Historically, our solutions were developed in the context of the on- premises offering, and we have less operating experience offering and selling subscriptions to our solutions via our cloud offering. Although a substantial majority of our revenue has historically been generated from customers using our solutions on an on- premises basis, our customers are increasingly adopting our cloud offering. We expect that our customers will continue to move to our cloud offering and that it will become more central to our distribution model ~~. We expect our gross profit to increase in absolute dollars and our gross margin to decrease to the extent that revenue from our cloud- based subscriptions increases as a percentage of revenue, although our gross margin could fluctuate from period to period~~ . To support both on- premises environments and cloud instances of our product, our support team must be trained on and learn multiple environments in which our solution is deployed, which is more expensive than supporting only a cloud offering. Moreover, we must engineer our software for an on-premises environment, cloud offering and hybrid installation, which we expect will cause us additional research and development expense that may impact our operating results. As more of our customers transition to the cloud, we may be subject to additional competitive pressures, which may harm our business. We are directing a significant portion of our financial and operating resources to implement a robust and secure cloud offering for our customers, but even if we continue to make these investments, we may be unsuccessful in growing or implementing our cloud offering in a way that competes successfully against our current and future competitors and our business, results of operations and financial condition could be harmed. Our customers' increased usage of our cloud- based offerings requires us to continually improve our computer network and infrastructure to avoid service interruptions or slower system performance. As usage of our cloud- based offerings grows and as customers use them for more complicated applications, increased assets and with increased data requirements, we will need to devote additional resources to improving our platform architecture and our infrastructure in order to maintain the performance of our cloud offering. Any failure or delays in our computer network and infrastructure systems could cause service interruptions or slower system performance. If sustained or repeated, these performance issues could reduce the attractiveness of our enterprise platform to customers. These performance issues could result in lost customer opportunities and lower renewal rates, any of which could hurt our revenue growth, customer loyalty and reputation. A component of our growth strategy is dependent on our continued international expansion, which adds complexity to our operations. We market and sell our solutions and professional services throughout the world and have personnel in many parts of the world. International operations generated **46 % and** 45 % ~~and 44 %~~ of our revenue in **2024 and** 2023 ~~and 2022~~ , respectively. Our growth strategy is dependent, in part, on our continued international expansion. We expect to conduct a significant amount of our business with organizations that are located outside the United States, particularly in Europe and Asia. We cannot assure that our expansion efforts into international markets will be successful in creating further demand for our solutions and professional services outside of the United States or in effectively selling our solutions and professional services in the international markets that we enter. Our current international operations and future initiatives will involve a variety of risks, including: • increased management, infrastructure and legal costs associated with having international operations; • reliance on channel partners; • trade and foreign exchange restrictions, including potential changes in trade relations arising from policy initiatives; • volatility of foreign exchange rates; • economic or political instability in foreign markets, including instability related to the United Kingdom' s recent exit from the European Union and the corresponding impact on its ongoing legal, political, and economic relationship with the European Union and heightened levels of inflation; • greater difficulty in enforcing contracts, accounts receivable collection and longer collection periods; • changes in regulatory requirements, including, but not limited to data privacy, data protection and data security regulations; • difficulties and costs of staffing, managing and potentially reorganizing foreign operations, including increased employee recruitment, training and retention costs related to global employment turnover trends and inflationary pressures in the labor market; • the uncertainty and limitation of protection for intellectual property rights in some countries; • costs of compliance with foreign laws and regulations and the risks and costs of non- compliance with such laws and regulations; • differing labor regulations in foreign jurisdictions where labor laws are generally more advantageous to employees, including deemed hourly wage and overtime regulations in these locations; • costs of compliance with U. S. laws and regulations for foreign operations, including the FCPA, import and export control laws, tariffs **imposed by the United States or other governments on our solutions** , trade barriers, economic sanctions and other regulatory or contractual limitations on our ability

to sell or provide our solutions in certain foreign markets, and the risks and costs of non- compliance; • requirements to comply with foreign privacy, data protection and information security laws and regulations and the risks and costs of noncompliance; • heightened risks of unfair or corrupt business practices in certain geographies and of improper or fraudulent sales arrangements that may impact financial results and result in restatements of, and irregularities in, financial statements; • the potential for political unrest, public health crises such as pandemics or similar outbreaks, acts of terrorism, hostilities or war, including the conflict between Ukraine and Russia, the ongoing conflict in the Middle East and increasing tensions between China and Taiwan; • management communication and integration problems resulting from cultural differences and geographic dispersion; • costs associated with language localization of our solutions; and • costs of compliance with multiple and possibly overlapping tax structures and regimes. Our business, including the sales of our solutions and professional services by us and our channel partners, may be subject to foreign governmental regulations, which vary substantially from country to country and change from time to time. Our failure, or the failure by our channel partners, to comply with these regulations could adversely affect our business. Further, in many foreign countries it is common for others to engage in business practices that are prohibited by our internal policies and procedures or U. S. regulations applicable to us. Although we have implemented policies and procedures designed to comply with these laws and policies, there can be no assurance that our employees, contractors, channel partners and agents have complied, or will comply, with these laws and policies. Violations of laws or key control policies by our employees, contractors, channel partners or agents could result in delays in revenue recognition, financial reporting misstatements, fines, penalties or the prohibition of the importation or exportation of our solutions and could have a material adverse effect on our business and results of operations. If we are unable to successfully manage the challenges of international expansion and operations, our business and operating results could be adversely affected. We believe our success has depended, and continues to depend, on the efforts and talents of our senior management team and our highly skilled team members, including our sales personnel, professional services personnel and software engineers. We do not maintain key person insurance on any of our executive officers or key employees. Our senior management and key employees are employed on an at- will basis, which means that they could terminate their employment with us at any time. The loss of any of our senior management or key employees **, including the recent passing of our former CEO, Mr. Yoran,** could adversely affect our ability to execute our business plan, and we may not be able to find adequate replacements. We cannot ensure that we will be able to retain the services of any members of our senior management or other key employees **. As previously announced, our Board of Directors is conducting a process to identify a new Chief Executive Officer for our company, including internal and external candidates. Although we intend to navigate this transition effectively, the uncertainty during the transition period may interrupt operations, impact relationships with partners and customers and increase the risks of employee departures, which may also result in the loss of institutional or technical knowledge, all of which may adversely affect our business** . Our ability to successfully pursue our growth strategy also depends on our ability to attract, motivate and retain our personnel. Competition for well- qualified employees in all aspects of our business is intense. The move by companies to offer a remote or hybrid work environment may increase competition for such employees outside of our traditional office locations. In addition, employee turnover rates in the broader global economy and inflationary pressures in the labor market have increased and may continue to be elevated, which has led, and could continue to lead to increased recruiting, training and retention costs. If we do not succeed in attracting well- qualified employees, retaining and motivating existing employees or maintaining our corporate culture in a hybrid or remote work environment, our business would be adversely affected. In addition, our ability to increase our customer base and achieve broader market acceptance of our Cyber Exposure solutions will depend to a significant extent on our ability to expand our sales force and our third- party channel partner network of distributors and resellers, both domestically and internationally. We may not be successful in attracting and retaining talented sales personnel or strategic partners, and any new sales personnel or strategic partners may not be able to achieve productivity in a reasonable period of time or at all. We also plan to dedicate significant resources to sales and marketing programs, including through electronic marketing campaigns and, when deemed safe to do so, trade event sponsorship and participation. All of these efforts will require us to invest significant financial and other resources and our business will be harmed if our efforts do not generate a correspondingly significant increase in revenue. We must offer high- quality support. Our customers rely on our personnel for support of our enterprise platform. High- quality support is important for the renewal of our agreements with existing customers and to our existing customers expanding the number of IP addresses or IT assets under their subscriptions. The importance of high- quality support will increase as we expand our business and pursue new customers. If we do not help our customers quickly resolve issues and provide effective ongoing support, our ability to sell new software to existing and new customers would suffer and our reputation with existing or potential customers would be harmed. Our growth depends in part on the success of our strategic relationships with third parties. In order to grow our business, we anticipate that we will continue to depend on relationships with strategic partners to provide broader customer coverage and solution delivery capabilities. We depend on partnerships with market leading technology companies to maintain and expand our exposure management ecosystem by integrating third party data into our platform. Identifying partners, and negotiating and documenting relationships with them, requires significant time and resources. Our agreements with our strategic partners generally are non- exclusive and do not prohibit them from working with our competitors or offering competing solutions. Our competitors may be effective in providing incentives to third parties to favor their products or services or to prevent or reduce subscriptions to our services. If our partners choose to place greater emphasis on products of their own or those offered by our competitors or do not effectively market and sell our product, our ability to grow our business and sell software and professional services may be adversely affected. In addition, acquisitions of our partners by our competitors could result in a decrease in the number of our current and potential customers, as our partners may no longer facilitate the adoption of our solutions by potential customers. We also license third- party threat data that is used in our solutions in order to deliver our offerings. In the future, this data may not be available to us on commercially reasonable terms, or at all. Any loss of the right to use any of this data could result in delays in

the provisioning of our offerings until equivalent data is either developed by us, or, if available, is identified, obtained and integrated, which could harm our business. If we are unsuccessful in establishing or maintaining our relationships with third parties, our ability to compete in the marketplace or to grow our revenue could be impaired and our operating results may suffer. Even if we are successful, we cannot assure you that these relationships will result in increased customer usage of our solutions or increased revenue. Recent and future acquisitions could disrupt our business and adversely affect our business operations and financial results. We have acquired products, technologies and businesses from other parties, such as our **acquisition of Vulcan Cyber Ltd., or Vulcan Cyber, which we announced in January 2025, our June 2024 acquisition of Eureka Security, Inc., or Eureka, and our** October 2023 acquisition of **Ermetic, Ltd., or** Ermetic, and we expect to expand our current business by acquiring additional businesses or technologies in the future. Acquisitions involve many risks, including the following: • an acquisition may negatively affect our financial results because it may require us to incur charges or assume substantial debt or other liabilities, may cause adverse tax consequences or unfavorable accounting treatment, may expose us to claims and disputes by third parties, including intellectual property claims and disputes, or may not generate sufficient financial return to offset additional costs and expenses related to the acquisition; • we may encounter difficulties or unforeseen expenditures in integrating the business, technologies, products, personnel or operations of any company that we acquire, particularly if key personnel of the acquired company decide not to work for us; • an acquisition may disrupt our ongoing business, divert resources, increase our expenses and distract our management; • an acquisition may result in a delay or reduction of customer purchases for both us and the company acquired due to customer uncertainty about continuity and effectiveness of service from either company; • we may encounter difficulties in, or may be unable to, successfully sell any acquired solutions; • an acquisition may involve the entry into geographic or business markets in which we have little or no prior experience or where competitors have stronger market positions; • our use of cash to pay for an acquisition would limit other potential uses for our cash; • the issuance of additional stock in connection with an acquisition could result in substantial dilution to our existing stockholders; and • if we incur debt to fund such acquisition, such debt may subject us to material restrictions on our ability to conduct our business as well as financial maintenance covenants. Acquired businesses have had, and may in the future have, a less mature cybersecurity program than our own. While we take steps designed to ensure our data and system security protection measures cover the acquired business, there may be cybersecurity risks and vulnerabilities arising from those acquired or integrated entities' systems, technologies and services, that could also impact our existing systems, technologies and services and increase our cybersecurity risks. The occurrence of any of these risks could have a material adverse effect on our business operations and financial results. In addition, we may only be able to conduct limited due diligence on an acquired company' s operations. Following an acquisition, we may be subject to unforeseen liabilities arising from an acquired company' s past or present operations and these liabilities may be greater than the warranty and indemnity limitations that we negotiate. Any unforeseen liability that is greater than these warranty and indemnity limitations could have a negative impact on our financial condition. In addition, **Vulcan Cyber, Eureka and** Ermetic **and other companies we have acquired** principally ~~operates~~ **operate** in Israel and the ~~recent~~ **Regional** conflict **in** ~~there~~ -- **the Middle East** may also have the effect of heightening the risks identified above. We are subject to risks associated with our investments in private companies, including partial or complete loss of invested capital, and significant changes in the fair value of this portfolio could adversely impact our financial results. We have invested, and may continue to invest, in private companies where we do not have the ability to exercise significant influence over results. Investments in private companies are inherently risky. The companies in which we invest are early stage private companies focused on cybersecurity innovation, and such companies may still be developing technologies or products with limited cash to support the development, marketing and sales of their technologies or products. These companies may have no or limited revenues, may not be or ever become profitable, may not be able to secure additional private financing to fund their operations, or their technologies, services, or products may not be successfully developed or introduced to the market. If any company in which we invest fails, we could lose all or part of our investment in that company. In addition, if we determine that any of our investments in such companies have experienced a decline in value, we will recognize an expense to adjust the carrying value to its estimated fair value. For example, in 2023 we recognized $ 5. 6 million of impairment loss related to ~~related to~~ our investments. Negative changes in the estimated fair value of our investments in private companies could have an adverse effect on our results of operations and financial condition. Furthermore, our ability to liquidate an investment in a private company will typically depend on a liquidity event, such as a private equity financing, a public offering or acquisition, as no public market currently exists for such securities. We may not be able to dispose of these investments on favorable terms or at all. We may require additional capital to support business growth, and this capital might not be available on acceptable terms, if at all. We expect that our existing cash and cash equivalents will be sufficient to meet our anticipated cash needs for working capital and capital expenditures for at least the next 12 months and the foreseeable future. However, we intend to continue to make investments to support our business growth and may require additional funds to respond to business challenges, including the need to develop new features or enhance our product, improve our operating infrastructure or acquire complementary businesses and technologies. Accordingly, we may need to engage in equity or debt financings to secure additional funds. If we raise additional funds through future issuances of equity or convertible debt securities, our existing stockholders could suffer significant dilution, and any new equity securities we issue could have rights, preferences and privileges superior to those of holders of our common stock. Our current ~~loan~~ **Credit** ~~agreement~~ **Agreement** includes, and we expect that any future agreements governing our indebtedness will include, restrictive covenants relating to our capital raising activities and other financial and operational matters, which may make it more difficult for us to obtain additional capital and to pursue business opportunities, including potential acquisitions. We may not be able to obtain additional financing on terms favorable to us, if at all. Weakness and volatility in the capital markets and the economy in general could limit our access to capital markets and increase our costs of borrowing. If we are unable to obtain adequate financing or financing on terms satisfactory to us when we require it, our ability to continue to support our business growth and to respond to business challenges could be significantly

impaired, and our business may be adversely affected. If we do not generate sufficient cash flows, we may be unable to service all of our indebtedness. To service our indebtedness, we will require a significant amount of cash. Our ability to generate cash, make scheduled payments or to refinance our debt obligations depends on our successful financial and operating performance, which may be affected by a range of economic, competitive and business factors, many of which are outside of our control and some of which are described elsewhere in the " Risk Factors " section of this report. If our cash flows and capital resources are insufficient to fund our debt service obligations, or to repay ~~the~~ **our outstanding senior secured credit facility, or** ~~term~~ **Term** ~~loan~~ **Loan ,** when it matures, we may have to undertake alternative financing plans, such as refinancing or restructuring our debt, selling assets or operations, reducing or delaying capital investments, or seeking to raise additional capital. We may not be able to refinance our debt, or any refinancing of our debt could be at higher interest rates and may require us to comply with more restrictive covenants that could further restrict our business operations. Our ability to implement successfully any such alternative financing plans will depend on a range of factors, including general economic conditions, the level of activity in capital markets generally, and the terms of our various debt instruments then in effect. Covenants under our Credit Agreement may restrict our business and operations in many ways, and if we do not effectively manage our covenants, our financial conditions and results of operations could be adversely affected. Our Credit Agreement imposes various covenants that limit our ability and / or our restricted subsidiaries' ability to, among other things: • pay dividends or distributions, repurchase equity, prepay, redeem or repurchase certain debt, and make certain investments; • incur additional debt and issue certain preferred stock; • provide guarantees in respect of obligations of other persons; • incur liens on assets; • engage in certain asset sales, including capital stock of our subsidiaries; • merge, consolidate with, or sell all or substantially all our assets to another person; • enter into transactions with affiliates; • enter into agreements that restrict distributions from our subsidiaries; • designate subsidiaries as unrestricted subsidiaries; and • prohibit certain restrictions on the ability of restricted subsidiaries to pay dividends or make other payments to us. These covenants may: • limit our ability to borrow additional funds for working capital, capital expenditures, acquisitions, or other general business purposes; • limit our ability to use our cash flow or obtain additional financing for future working capital, capital expenditures, acquisitions, or other general business purposes; • require us to use a substantial portion of our cash flow from operations to make debt service payments; • limit our flexibility to plan for, or react to, changes in our business and industry; • place us at a competitive disadvantage compared to less leveraged competitors; and • increase our vulnerability to the impact of adverse economic and industry conditions. If we are unable to successfully manage the limitations and decreased flexibility on our business due to our significant debt obligations, we may not be able to capitalize on strategic opportunities or grow our business to the extent we would be able to without these limitations. Our failure to comply with any of the covenants could result in a default under the Credit Agreement, which could permit the administrative agent or the lenders to cause the administrative agent to declare all or part of any of our outstanding senior secured term loans or revolving loans to be immediately due and payable or to exercise any remedies provided to the administrative agent, including, proceeding against the collateral granted to secure our obligations under the Credit Agreement. An event of default under the Credit Agreement could also lead to a default under the terms of certain of our other agreements. Any such event of default or any exercise of rights and remedies by our creditors could seriously harm our business. Our variable rate debt subjects us to interest rate risk that could cause our debt service obligations to increase significantly. The indebtedness under our Credit Agreement is at variable rates of interest, which exposes us to interest rate risk. ~~Reference rates used to determine the applicable interest rates for our variable rate debt began to rise significantly in the second half of fiscal year 2022 and continued into fiscal year 2023.~~ If interest rates ~~continue to~~ increase, the debt service obligations on such indebtedness **would** ~~will continue to~~ increase even if the amount borrowed remains the same, and our net income and cash flows, including cash available for servicing our indebtedness, ~~will~~ **would** correspondingly decrease. In addition, as a result of an amendment to our Credit Agreement, certain of the variable rate indebtedness extended to us uses the Secured Overnight Financing Rate, or SOFR, as a benchmark for establishing the interest rate. While we will continue to use SOFR, other factors may impact SOFR including factors causing SOFR to cease to exist, new methods of calculating SOFR to be established, or the use of an alternative reference rate (s). These consequences are not entirely predictable and could have an adverse impact on our financing costs, returns on investments, valuation of derivative contracts and our financial results. The nature of our business requires the application of complex accounting rules and regulations and public reporting and corporate governance requirements. If there are significant changes in current principles, financial reporting standards, interpretations or public reporting and corporate governance requirements, or if our estimates or judgments relating to our critical accounting policies or reporting or governance requirements prove to be incorrect, we may experience unexpected financial reporting fluctuations or increased compliance costs and strain on our resources and our results of operations could be adversely affected. The accounting rules and regulations that we must comply with are complex and subject to interpretation by the Financial Accounting Standards Board, the SEC, and various bodies formed to promulgate and interpret appropriate accounting principles. In addition, many companies' accounting disclosures are being subjected to heightened scrutiny by regulators and the public. Further, the accounting rules and regulations are continually changing in ways that could impact our financial statements. The preparation of financial statements in conformity with generally accepted accounting principles in the United States, or U. S. GAAP, requires management to make estimates and assumptions that affect the amounts reported in the consolidated financial statements and accompanying notes. We base our estimates on historical experience and on various other assumptions that we believe to be reasonable under the circumstances, as provided in the section of this report titled " Management' s Discussion and Analysis of Financial Condition and Results of Operations. " Significant assumptions and estimates used in preparing our consolidated financial statements include the determination of the estimated economic life of perpetual licenses for revenue recognition, the estimated period of benefit for deferred commissions, useful lives of long- lived assets, the valuation of stock- based compensation, the incremental borrowing rate for operating leases, and the valuation of deferred tax assets. Our results of operations may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our results of

operations to fall below the expectations of securities analysts and investors, resulting in a decline in the trading price of our common stock. As a public company, we are also subject to the reporting and corporate governance requirements of the Exchange Act, the listing requirements of the Nasdaq Stock Market and other applicable securities rules and regulations, including the Sarbanes- Oxley Act and the Dodd- Frank Wall Street Reform and Consumer Protection Act. Compliance with these rules and regulations increases our legal and financial compliance costs, makes some activities more difficult, time-consuming or costly and increases demand on our systems and resources. Additionally, we regularly monitor our compliance with applicable financial reporting standards and SEC and applicable listing standard requirements and review new pronouncements, drafts and interpretations thereof that are relevant to us. We might be required to change our accounting policies, alter our operational policies and implement new or enhance existing systems, or we may be required to restate our published financial statements, as a result of new standards or requirements, changes to existing standards or requirements and changes in their interpretation. Such changes to existing standards or requirements or changes in their interpretation may have an adverse effect on our reputation, business, financial position and profit, or cause an adverse deviation from our revenue and operating profit target, which may negatively impact our financial results. Additionally, we may incur substantial professional fees and expend significant management efforts, and we may need to hire additional staff with the appropriate experience and compile systems and processes necessary to adopt these new standards and disclosure or governance requirements. For example **, a number of climate disclosure regulations have been enacted, including the Corporate Sustainability Reporting Directive and the State of California' s climate disclosure legislation, and other entities, including the SEC, may enact additional climate disclosure requirements. These rules may require disclosure on climate- related risks, risk management, governance and targets, and will require the company to calculate and disclose greenhouse gas emissions data and obtain assurance reports on these disclosures. Ongoing compliance with these regulations is expected to be challenging and will heighten the compliance risks identified above. Additionally, our failure or perceived failure to comply with these disclosure requirements could lead to regulatory investigations, litigation, reputational harm, and other adverse business consequences. In addition** , in July 2023, the SEC adopted rules requiring the disclosure of information about a material cybersecurity incident on Form 8- K within four business days of determining that the incident is material, unless the US Attorney General concludes that such a disclosure would pose a substantial risk to national security or public safety. ~~Additionally, these~~ **These** rules **also** require disclosures describing the processes used to identify, assess and manage cybersecurity risks, management' s role in assessing and managing material risks from cybersecurity threats and the board of directors' role in overseeing cybersecurity risks. Unstable market and economic conditions may have material adverse consequences on our business, financial condition and share price. The global economy, including credit and financial markets, ~~has~~ recently experienced extreme volatility and disruptions, including severely diminished liquidity and credit availability, declines in consumer confidence, declines in economic growth, increases in unemployment rates, ~~increases in~~ inflation ~~rates~~ , ~~higher~~ interest ~~rates~~ **rate fluctuations** and uncertainty about economic stability. For example, in recent years the ~~COVID- 19 pandemic,~~ high rates of inflation, high interest rates and concerns about an economic recession in the United States or other major markets resulted in widespread unemployment, economic slowdown and extreme volatility in the capital markets. ~~The~~ **In 2022 and 2023, the** Federal Reserve ~~recently~~ raised interest rates multiple times in response to concerns about inflation **. While the Federal Reserve decreased interest rates in 2024, interest rates remain high** and **the Federal Reserve** is **not** expected to ~~continue to raise~~ **significantly decrease interest** rates **in the immediate future** . Higher interest rates, coupled with reduced government spending and volatility in financial markets, including with respect to foreign exchange, may increase economic uncertainty and affect consumer spending. For example, during periods with a relatively strong U. S. dollar, our products are more expensive for existing and prospective international customers, which has impacted, and could in the future impact, the budgets and purchasing decisions of certain of our existing and prospective international customers. If the equity and credit markets deteriorate, including as a result of political unrest or war, it may make any necessary debt or equity financing more difficult to obtain in a timely manner or on favorable terms, more costly or more dilutive. Increased inflation rates can adversely affect us by increasing our costs, including labor and employee benefit costs. In addition, higher inflation also could increase our customers' operating costs, which could result in reduced budgets for our customers, longer sales cycles and potentially less demand for our products. Any significant increases in inflation and related increase in interest rates could have a material adverse effect on our business, results of operations and financial condition. Catastrophic events may disrupt our business. Our corporate headquarters are located in Columbia, Maryland. The area around Washington, D. C. could be subject to terrorist attacks. Additionally, we rely on our network and third- party infrastructure and enterprise applications, internal technology systems and our website for our development, marketing, operational support, hosted services and sales activities. We have both hybrid remote and in- person work policies, however, substantially all of our employees have continued to work in a hybrid environment, which may pose additional security risks. Our business operations are subject to interruption by natural disasters, including those related to the long- term effects of climate change, and other catastrophic events such as fire, floods, power loss, telecommunications failure, cyberattack, war or terrorist attack, or epidemic or pandemic. To the extent such events impact our corporate headquarters, other facilities, or off- premises infrastructure, we may be unable to continue our operations and may endure system interruptions, reputational harm, delays in our software development, lengthy interruptions in our services, breaches of data security and loss of critical data, all of which could have an adverse effect on our future operating results. Our business, financial condition and results of operations could be materially adversely affected by the recent conflict in the Middle East and subsequent hostilities in the region, as well as any negative impact on the regional or global economies and capital markets resulting therefrom or from the ongoing conflict between Ukraine and Russia and any other geopolitical tensions. U. S. and global markets have experienced volatility and disruption following the escalation of geopolitical tensions, including the conflict in the Middle East, the ongoing conflict between Ukraine and Russia and increasing tensions between China and Taiwan. The length, scale and impact of these military conflicts are highly unpredictable and could continue to result in market

disruptions, including significant volatility in commodity prices, credit and capital markets, disruption in the energy market as well as supply chain interruptions. Furthermore, our research and development teams for Tenable OT Security and for Tenable Cloud Security are primarily located in Tel Aviv, Israel. Recent and ongoing hostilities in the region may have a material impact on our ability to deliver on our product roadmaps for these solutions. It is impossible to predict the extent to which our operations, or those of our partners or customers, will be impacted in the short and long term, or the ways in which these conflicts may impact our business. The extent and duration of the military action, sanctions and resulting market disruptions are impossible to predict, but could be substantial. Risks Related to Government Regulation, Data Collection and Intellectual Property Our business could be adversely affected if our employees cannot obtain and maintain required security clearances or we cannot establish and maintain a required facility security clearance. Certain U. S. government contracts may require our employees to maintain various levels of security clearances, and may require us to maintain a facility security clearance, to comply with Department of Defense, or DoD, requirements. The DoD has strict security clearance requirements for personnel who perform work in support of classified programs. Obtaining and maintaining a facility clearance and security clearances for employees can be a difficult, sometimes lengthy process. If we do not have employees with the appropriate security clearances, then a customer requiring classified work could terminate an existing contract or decide not to renew the contract upon its expiration. To the extent we are not able to obtain or maintain a facility security clearance, we may not be able to bid on or win new classified contracts, and existing contracts requiring a facility security clearance could be terminated. Any failure to protect our proprietary technology and intellectual property rights could substantially harm our business and operating results. Our success and ability to compete depend in part on our ability to protect our proprietary technology and intellectual property. To safeguard these rights, we rely on a combination of patent, trademark, copyright and trade secret laws and contractual protections in the United States and other jurisdictions, all of which provide only limited protection and may not now or in the future provide us with a competitive advantage. At December 31, ~~2023~~ **2024** , we had ~~38~~ **47** issued patents and ~~21~~ **22** patent applications pending in the United States relating to our technology. We cannot assure you that any patents will issue from any patent applications, that patents that issue from such applications will give us the protection that we seek or that any such patents will not be challenged, invalidated or circumvented. Any patents that may issue in the future from our pending or future patent applications may not provide sufficiently broad protection and may not be enforceable in actions against alleged infringers. Obtaining and enforcing software patents in the United States is becoming increasingly challenging. Any patents we have obtained or may obtain in the future may be found to be invalid or unenforceable in light of recent and future changes in the law. We have registered the " Tenable ~~,~~ " **and** " Nessus, " ~~" Tenable. io " and" Lumin" trademarks~~ and our Tenable logo in the United States and certain other countries. We have registrations and / or pending applications for additional trademarks ~~in the United States~~ ; however, we cannot assure you that any future trademark registrations will be issued for pending or future applications or that any registered trademarks will be enforceable or provide adequate protection of our proprietary rights. While we have copyrights in our software, we do not typically register such copyrights with the Copyright Office. This failure to register the copyrights in our software may preclude us from obtaining statutory damages for infringement under certain circumstances. We also license software from third parties for integration into our software, including open source software and other software available on commercially reasonable terms. We cannot assure you that such third parties will maintain such software or continue to make it available. In order to protect our unpatented proprietary technologies and processes, we rely on trade secret laws and confidentiality and invention assignment agreements with our employees, consultants, strategic partners, vendors and others. Despite our efforts to protect our proprietary technology and trade secrets, unauthorized parties may attempt to misappropriate, copy, reverse engineer or otherwise obtain and use them. In addition, others may independently discover our trade secrets, in which case we would not be able to assert trade secret rights, or develop similar technologies and processes. Further, several agreements may give customers limited rights to access portions of our proprietary source code, and the contractual provisions that we enter into may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property and may not provide an adequate remedy in the event of unauthorized use or disclosure of our proprietary technology or intellectual property rights. Moreover, policing unauthorized use of our technologies, trade secrets and intellectual property is difficult, expensive and time- consuming, particularly in foreign countries where the laws may not be as protective of intellectual property rights as those in the United States and where mechanisms for enforcement of intellectual property rights may be weak. To the extent that we expand our activities outside of the United States, our exposure to unauthorized copying and use of our solutions and proprietary information may increase. We may be unable to determine the extent of any unauthorized use or infringement of our solutions, technologies or intellectual property rights. There can be no assurance that the steps that we take will be adequate to protect our proprietary technology and intellectual property, that others will not develop or patent similar or superior technologies, solutions or services, or that our trademarks, patents, and other intellectual property will not be challenged, invalidated or circumvented by others. Furthermore, effective trademark, patent, copyright, and trade secret protection may not be available in every country in which our software is available or where we have employees or independent contractors. In addition, the legal standards relating to the validity, enforceability, and scope of protection of intellectual property rights in internet and software- related industries are uncertain and still evolving. In order to protect our intellectual property rights, we may be required to spend significant resources to monitor and protect these rights. Litigation brought to protect and enforce our intellectual property rights could be costly, time- consuming and distracting to management and could result in the impairment or loss of portions of our intellectual property. Furthermore, our efforts to enforce our intellectual property rights may be met with defenses, counterclaims and countersuits attacking the validity and enforceability of our intellectual property rights. Our failure to secure, protect and enforce our intellectual property rights could seriously adversely affect our brand and adversely impact our business. We may be subject to intellectual property rights claims by third parties, which are extremely costly to defend, could require us to pay significant damages and could limit our ability to use certain technologies. Companies in the software and technology industries, including some of our current and potential competitors,

own significant numbers of patents, copyrights, trademarks and trade secrets and frequently enter into litigation based on allegations of infringement or other violations of intellectual property rights. In addition, many of these companies have the capability to dedicate substantially greater resources to enforce their intellectual property rights and to defend claims that may be brought against them. The litigation may involve patent holding companies or other adverse patent owners that have no relevant product revenue and against which our patents may therefore provide little or no deterrence. In the past, we have been subject to allegations of patent infringement that were unsuccessful, and we expect in the future to be subject to claims that we have misappropriated, misused, or infringed other parties' intellectual property rights, and, to the extent we gain greater market visibility or face increasing competition and as we acquire more companies, we face a higher risk of being the subject of intellectual property infringement claims, which is not uncommon with respect to enterprise software companies. We may in the future be subject to claims that employees or contractors, or we, have inadvertently or otherwise used or disclosed trade secrets or other proprietary information of our competitors or other parties. To the extent that intellectual property claims are made against our customers based on their usage of our technology, we have certain obligations to indemnify and defend such customers from those claims. The term of our contractual indemnity provisions often survives termination or expiration of the applicable agreement. Large indemnity payments, defense costs or damage claims from contractual breach could harm our business, results of operations and financial condition. There may be third- party intellectual property rights, including issued or pending patents that cover significant aspects of our technologies or business methods, including those relating to companies we acquire. Any intellectual property claims, with or without merit, could be very time- consuming, could be expensive to settle or litigate, could divert our management' s attention and other resources and could result in adverse publicity. These claims could also subject us to making substantial payments for legal fees, settlement payments, and other costs or damages, potentially including treble damages if we are found to have willfully infringed patents or copyrights. These claims could also result in our having to stop making, selling, offering for sale, or using technology found to be in violation of a third party' s rights. We might be required to seek a license for the third- party intellectual property rights, which may not be available on reasonable terms or at all. Even if a license is available to us, we may be required to pay significant upfront fees, milestones or royalties, which would increase our operating expenses. Moreover, to the extent we only have a license to any intellectual property used in our solutions, there may be no guarantee of continued access to such intellectual property, including on reasonable terms. As a result, we may be required to develop alternative non- infringing technology, which could require significant effort and expense. If a third party is able to obtain an injunction preventing us from accessing such third- party intellectual property rights, or if we cannot license or develop technology for any infringing aspect of our business, we would be forced to limit or stop sales of our software or cease business activities covered by such intellectual property, and may be unable to compete effectively. Any of these results would adversely affect our business, results of operations, financial condition and cash flows. Portions of our solutions utilize open source software, and any failure to comply with the terms of one or more of these open source licenses could negatively affect our business. Our software contains software made available by third parties under so- called " open source " licenses. From time to time, there have been claims against companies that distribute or use open source software in their products and services, asserting that such open source software infringes the claimants' intellectual property rights. We could be subject to suits by parties claiming that what we believe to be licensed open source software infringes their intellectual property rights. Use and distribution of open source software may entail greater risks than use of third- party commercial software, as open source licensors generally do not provide warranties or other contractual protections regarding infringement claims or the quality of the code. In addition, certain open source licenses require that source code for software programs that are subject to the license be made available to the public and that any modifications or derivative works to such open source software continue to be licensed under the same terms. Further, certain open source licenses also include a provision that if we enforce any patents against the software programs that are subject to the license, we would lose the license to such software. If we were to fail to comply with the terms of such open source software licenses, such failures could result in costly litigation, lead to negative public relations or require that we quickly find replacement software which may be difficult to accomplish in a timely manner. Although we monitor our use of open source software in an effort both to comply with the terms of the applicable open source licenses and to avoid subjecting our software to conditions we do not intend, the terms of many open source licenses have not been interpreted by U. S. courts, and there is a risk that these licenses could be construed in a way that could impose unanticipated conditions or restrictions on our ability to commercialize our product or operate our business. By the terms of certain open source licenses, we could be required to release the source code of our software and to make our proprietary software available under open source licenses, if we combine or distribute our software with open source software in a certain manner. In the event that portions of our software are determined to be subject to an open source license, we could be required to publicly release the affected portions of our source code, re- engineer all, or a portion of, that software or otherwise be limited in the licensing of our software, each of which could reduce or eliminate the value of our product. Many of the risks associated with usage of open source software cannot be eliminated, and could negatively affect our business, results of operations and financial condition. Risks Related to An Investment in Our Common Stock Our stock price may be volatile, and the value of our common stock may decline. The market price of our common stock may fluctuate substantially and depends on a number of factors, including those described in this " Risk Factors " section, many of which are beyond our control and may not be related to our operating performance. Factors that could cause fluctuations in the market price of our common stock include the following: • actual or anticipated changes or fluctuations in our operating results; • the financial projections we may provide to the public, any changes in these projections or our failure to meet these projections; • announcements by us or our competitors of new products or new or terminated significant contracts, commercial relationships or capital commitments; • industry or financial analyst or investor reaction to our press releases, other public announcements and filings with the SEC; • rumors and market speculation involving us or other companies in our industry; • price and volume fluctuations in the overall stock market from time to time; • changes in operating performance and stock market valuations of other technology companies

generally, or those in our industry in particular; • failure to comply with the terms of the Credit Agreement; • sales of shares of our common stock by us or our stockholders; • failure of industry or financial analysts to maintain coverage of us, changes in financial estimates by any analysts who follow our company, or our failure to meet these estimates or the expectations of investors; • actual or anticipated developments in our business or our competitors' businesses or the competitive landscape generally; • litigation involving us, our industry or both, or investigations by regulators into our operations or those of our competitors; • developments or disputes concerning our intellectual property rights or our solutions, or third- party proprietary rights; • announced or completed acquisitions of businesses or technologies by us or our competitors; • new or proposed laws or regulations or new interpretations of existing laws or regulations applicable to our business, including ~~proposed~~ changes to the U. S. corporate income tax rate and capital gains tax rates; • any major changes in our management or our Board of Directors; • general economic conditions and slow or negative growth of our markets; and • other events or factors, including those resulting from public health crises such as pandemics or similar outbreaks, war, incidents of terrorism or responses to these events. Recently, the stock markets have experienced extreme price and volume fluctuations that have affected and continue to affect the market prices of equity securities of many companies, high rates of inflation and interest rates, disruptions in access to bank deposits or lending commitments due to bank failures and uncertainty about economic stability and concerns about an economic recession in the United States or other major markets, the ongoing military conflict between Ukraine and Russia, the ongoing conflict in the Middle East, increasing tensions between China and Taiwan and macroeconomic conditions. These fluctuations have often been unrelated or disproportionate to the operating performance of those companies. Broad market and industry fluctuations, as well as general economic, political, regulatory and market conditions, may negatively impact the market price of our common stock. In the past, companies that have experienced volatility in the market price of their securities have been subject to securities class action litigation. We may be the target of this type of litigation in the future, which could result in substantial costs and divert our management' s attention. If securities or industry analysts do not publish research or reports about our business, or publish negative reports about our business, our stock price and trading volume could decline. The trading market for our common stock will depend, in part, on the research and reports that securities or industry analysts publish about us or our business. We do not control these analysts or the content and opinions included in their reports. If our financial performance fails to meet analyst estimates or one or more of the analysts who cover us downgrade our shares or change their opinion of our shares, our share price would likely decline. In addition, the stock prices of many companies in the technology industry have declined significantly after those companies have failed to meet, or significantly exceed, the financial guidance publicly announced by the companies or the expectations of analysts. If our financial results fail to meet, or exceed, our announced guidance or the expectations of analysts or public investors, analysts could downgrade our common stock or publish unfavorable research about us. If one or more of these analysts cease coverage of our company or fail to regularly publish reports on us, we could lose visibility in the financial markets, which could cause our share price or trading volume to decline. Future sales of substantial amounts of our common stock in the public markets by us or our stockholders, or the perception such sales might occur, could reduce the price that our common stock might otherwise attain. Sales of a substantial number of shares of our common stock in the public market by us or our stockholders, or the perception that these sales might occur, could depress the market price of our common stock, impair our ability to raise capital through the sale of additional equity securities and make it more difficult for you to sell your common stock at a time and price that you deem appropriate. Further, the number of new shares of our common stock issued by us in connection with raising additional capital in connection with a financing, acquisition, investment or otherwise could result in substantial dilution to our existing stockholders. In addition, we have filed registration statements on Form S- 8 under the Securities Act registering the issuance of shares of common stock subject to options and other equity awards issued or reserved for future issuance under our equity incentive plans. Shares registered under these registration statements, and under additional registration statements on Form S- 8 that we may file to register additional shares of common stock pursuant to provisions of our equity incentive plans that provide for an automatic increase in the number of shares reserved and available for issuance each year, are available for sale in the public market subject to vesting arrangements and exercise of options and the restrictions of Rule 144 under the Securities Act in the case of our affiliates. We do not intend to pay dividends for the foreseeable future and, as a result, your ability to achieve a return on your investment will depend on appreciation in the price of our common stock. We have never declared or paid any cash dividends on our common stock and do not intend to pay any cash dividends in the foreseeable future. We anticipate that we will retain all of our future earnings for use in the development of our business and for general corporate purposes. Any determination to pay dividends in the future will be at the discretion of our Board of Directors. Accordingly, investors must rely on sales of their common stock after price appreciation, which may never occur, as the only way to realize any future gains on their investments. In addition, our Credit Agreement contains restrictive covenants that prohibit us, subject to certain exceptions, from paying dividends on our common stock. We cannot guarantee that our share repurchase program will be fully consummated or that it will enhance stockholder value, and any share repurchases we make could affect the price of our common stock. On November 27, 2023, we announced that our Board of Directors authorized a share repurchase program of up to $ 100 million of shares of our outstanding common stock **. In October 2024, our Board of Directors increased the repurchase authorization by $ 200 million** . Share repurchases under the program may be made from time to time, in the open market, in privately negotiated transactions and otherwise, at the discretion of management and in accordance with applicable federal securities laws, including Rule 10b- 18 of the Exchange Act, and other applicable legal requirements. Such repurchases may also be made in compliance with Rule 10b5- 1 trading plans entered into by us. The timing and amount of repurchases, if any, will be subject to liquidity, stock price, market and economic conditions, compliance with applicable legal requirements such as Delaware surplus and solvency tests, compliance with our credit agreement, and other relevant factors. The share repurchase program does not obligate us to repurchase any dollar amount or number of shares, and the program may be suspended or discontinued at any time, which may result in a decrease in the price of our common stock. The share repurchase program could affect the price of our common stock,

increase volatility, and diminish our cash reserves, and we may fail to realize the anticipated long- term stockholder value. Additionally, the Inflation Reduction Act of 2022, enacted on August 16, 2022, imposes a one- percent non- deductible excise tax on repurchases of stock that are made by U. S. publicly traded corporations. Anti- takeover provisions in our charter documents and under Delaware law could make an acquisition of us more difficult, limit attempts by our stockholders to replace or remove members of our Board of Directors and our current management and could negatively impact the market price of our common stock. Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that could delay or prevent a change in control of our company. These provisions could also make it difficult for stockholders to elect directors that are not nominated by the current members of our Board of Directors or take other corporate actions, including effecting changes in our management. These provisions include: • a classified Board of Directors with three- year staggered terms, which could delay the ability of stockholders to change the membership of a majority of our Board of Directors; • the ability of our Board of Directors to issue shares of preferred stock and to determine the price and other terms of those shares, including preferences and voting rights, without stockholder approval, which could be used to significantly dilute the ownership of a hostile acquirer; • the exclusive right of our Board of Directors to elect a director to fill a vacancy created by the expansion of our Board of Directors or the resignation, death or removal of a director, which prevents stockholders from being able to fill vacancies on our Board of Directors; • a prohibition on stockholder action by written consent, which forces stockholder action to be taken at an annual or special meeting of our stockholders; • the requirement that a special meeting of stockholders may be called only by the chairperson of our Board of Directors, Chief Executive Officer or president (in the absence of a chief executive officer) or a majority vote of our Board of Directors, which could delay the ability of our stockholders to force consideration of a proposal or to take action, including the removal of directors; • the requirement for the affirmative vote of holders of at least 66 2 / 3 % of the voting power of all of the then outstanding shares of the voting stock, voting together as a single class, to amend the provisions of our amended and restated certificate of incorporation relating to the issuance of preferred stock and management of our business or our amended and restated bylaws, which may inhibit the ability of an acquirer to affect such amendments to facilitate an unsolicited takeover attempt; • the ability of our Board of Directors, by majority vote, to amend our amended and restated bylaws, which may allow our Board of Directors to take additional actions to prevent an unsolicited takeover and inhibit the ability of an acquirer to amend our amended and restated bylaws to facilitate an unsolicited takeover attempt; and • advance notice procedures with which stockholders must comply to nominate candidates to our Board of Directors or to propose matters to be acted upon at a stockholders' meeting, which may discourage or deter a potential acquirer from conducting a solicitation of proxies to elect the acquirer' s own slate of directors or otherwise attempting to obtain control of us. These provisions may prohibit large stockholders, in particular those owning 15 % or more of our outstanding voting stock, from merging or combining with us for a certain period of time. Our amended and restated certificate of incorporation provides that the Court of Chancery of the State of Delaware or the U. S. federal district courts will be the exclusive forums for substantially all disputes between us and our stockholders, which could limit our stockholders' ability to obtain a favorable judicial forum for disputes with us or our directors, officers or other employees. Our amended and restated certificate of incorporation provides that the Court of Chancery of the State of Delaware is the sole and exclusive forum for the following types of actions or proceedings under Delaware statutory or common law: • any derivative action or proceeding brought on our behalf; • any action asserting a breach of fiduciary duty owed by any of our directors, officers or other employees to us or our stockholders; • any action asserting a claim against us arising pursuant to any provisions of the Delaware General Corporation Law, our amended and restated certificate of incorporation or our amended and restated bylaws; or • any action asserting a claim against us that is governed by the internal affairs doctrine. This provision would not apply to suits brought to enforce a duty or liability created by the Exchange Act. Furthermore, Section 22 of the Securities Act creates concurrent jurisdiction for federal and state courts over all such Securities Act actions. Accordingly, both state and federal courts have jurisdiction to entertain such claims. To prevent having to litigate claims in multiple jurisdictions and the threat of inconsistent or contrary rulings by different courts, among other considerations, our amended and restated certificate of incorporation further provides that the federal district courts of the United States of America will be the exclusive forum for resolving any complaint asserting a cause of action arising under the Securities Act. While the Delaware courts have determined that such choice of forum provisions are facially valid, a stockholder may nevertheless seek to bring a claim in a venue other than those designated in the exclusive forum provisions. In such instance, we would expect to vigorously assert the validity and enforceability of the exclusive forum provisions of our amended and restated certificate of incorporation. This may require significant additional costs associated with resolving such action in other jurisdictions and there can be no assurance that the provisions will be enforced by a court in those other jurisdictions. These exclusive forum provisions may limit a stockholder' s ability to bring a claim in a judicial forum that it finds favorable for disputes with us or our directors, officers or other employees, which may discourage such lawsuits against us and our directors, officers or other employees. If a court were to find either exclusive forum provision in our amended and restated certificate of incorporation to be inapplicable or unenforceable in an action, we may incur significant additional costs associated with resolving the dispute in other jurisdictions, all of which could seriously harm our business. General Risks We are subject to anti- corruption laws, anti- bribery and similar laws with respect to our domestic and international operations, and non- compliance with such laws can subject us to criminal and / or civil liability and materially harm our business and reputation. We are subject to the anti- bribery laws of the jurisdictions in which we operate. These include the FCPA, the U. S. domestic bribery statute contained in 18 U. S. C. § 201, the U. S. Travel Act, the U. K. Bribery Act 2010, and other anti- corruption laws in countries in which we conduct activities. Anti- corruption laws are interpreted broadly and prohibit our company from authorizing, offering, or providing, directly or indirectly, improper payments or benefits in order to gain or maintain business, including payments to recipients in the public or private sector. We use third- party law firms, accountants, and other representatives for regulatory compliance, sales, and other purposes in several countries. We sell directly and indirectly, via third- party representatives, to both private and government sectors in the United States and in other

jurisdictions. Our employees and third- party representatives interact with these customers, which may include government officials. We can be held liable for the corrupt or other illegal activities of these third- party representatives, our employees, contractors, and other agents, even if we do not explicitly authorize such activities. Noncompliance with these laws could subject us to whistleblower complaints, investigations, sanctions, settlements, prosecution, other enforcement actions, disgorgement of profits, significant fines, damages, other civil and criminal penalties or injunctions, suspension and / or debarment from contracting with certain persons, the loss of export privileges, reputational harm, adverse media coverage, and other collateral consequences. If any subpoenas or investigations are launched, or governmental or other sanctions are imposed, or if we do not prevail in any possible civil or criminal litigation, our reputation, business, results of operations and financial condition could be materially harmed. In addition, responding to any action will likely result in a materially significant diversion of management' s attention and resources and significant defense costs and other professional fees. Enforcement actions and sanctions could further harm our business, results of operations, and financial condition. Moreover, as an issuer of securities, we also are subject to the accounting and internal controls provisions of the FCPA. These provisions require us to maintain accurate books and records and a system of internal controls sufficient to detect and prevent corrupt conduct. Failure to abide by these provisions may have an adverse effect on our business, operations or financial condition. We are subject to governmental export and import controls and economic and trade sanctions that could impair our ability to conduct business in international markets and subject us to liability if we are not in compliance with applicable laws and regulations. The United States and other countries maintain and administer export and import laws and regulations. Our products are subject to U. S. export control and import laws and regulations, including the U. S. Export Administration Regulations, U. S. Customs regulations, and various economic and trade sanctions administered by the U. S. Treasury Department' s Office of Foreign Assets Control. We are required to comply with these laws and regulations. If we fail to comply with such laws and regulations, we and certain of our employees could be subject to substantial civil or criminal penalties, including the possible loss of export or import privileges; fines, which may be imposed on us and responsible employees or managers; and, in extreme cases, the incarceration of responsible employees or managers. Obtaining the necessary authorizations, including any required license, for a particular sale may be time- consuming, is not guaranteed and may result in the delay or loss of sales opportunities. In addition, changes in our solutions, or changes in applicable export or import laws and regulations may create delays in the introduction and sale of our products in international markets or, in some cases, prevent the export or import of our solutions to certain countries, governments or persons altogether. Any change in export or import laws and regulations or economic or trade sanctions, shift in the enforcement or scope of existing laws and regulations, or change in the countries, governments, persons or technologies targeted by such laws and regulations could also result in decreased use of our products, or in our decreased ability to export or sell our products to existing or potential customers. Any decreased use of our products or limitation on our ability to export or sell our products would likely adversely affect our business, financial condition, and results of operations. Furthermore, we incorporate encryption technology into certain of our solutions. Various countries regulate the import of certain encryption technology, including import permitting and licensing requirements, and have enacted laws that could limit our ability to distribute our solutions or could limit our customers' ability to implement our solutions in those countries. Encrypted products and the underlying technology may also be subject to export control restrictions. Governmental regulation of encryption technology and regulation of imports or exports of encryption solutions, or our failure to obtain required import or export approval for our solutions, could harm our international sales and adversely affect our revenue. Compliance with applicable laws and regulations regarding the export and import of our solutions, including with respect to new solutions or changes in existing solutions, may create delays in the introduction of our solutions in international markets, prevent our customers with international operations from deploying our solutions globally or, in some cases, could prevent the export or import of our solutions to certain countries, governments, entities or persons altogether. Moreover, U. S. export control laws and economic sanctions programs prohibit the shipment of certain products and services to countries, governments and persons that are subject to U. S. economic embargoes and trade sanctions. Any violations of such economic embargoes and trade sanction regulations could have negative consequences, including government investigations, penalties and reputational harm. Changes to and uncertainties in the interpretation and application of tax laws and regulations could materially affect our tax obligations and effective tax rate. The tax regimes to which we are subject or under which we operate, including income and non- income taxes, are unsettled and may be subject to significant change. The issuance of additional regulatory or accounting guidance related to existing or future tax laws, or changes to tax laws or regulations proposed or implemented by the current or a future U. S. presidential administration, Congress, or taxing authorities in other jurisdictions, including jurisdictions outside of the United States, could materially affect our tax obligations and effective tax rate. ~~For example, beginning in 2022, U. S. taxpayers are required to capitalize and amortize certain research and development expenditures over five years if incurred in the United States and fifteen years if incurred in non- U. S. jurisdictions. Although legislative proposals have been made to repeal or defer the capitalization requirement, there can be no assurance that the provision will be repealed or otherwise modified. In addition, the recently enacted Inflation Reduction Act includes, among other provisions, a 15 % minimum tax on the book income of certain large corporations, as well as a 1 % excise tax imposed on certain stock repurchases by public corporations. It is possible that these changes could increase our future tax liability.~~ Furthermore, the Organization for Economic Co- operation and Development, or OECD, is leading work on proposals, commonly referred to as " BEPS 2. 0 ", which, ~~if and~~ to the extent ~~implemented~~ **enacted** , ~~would~~ **will** make ~~important~~ changes to the international tax system. These proposals are based on two " pillars ", involving the allocation of taxing rights in respect of certain multinational enterprises above a fixed profit margin to the jurisdictions in which they carry on business (subject to certain revenue threshold rules which we do not currently meet but **may** ~~expect to~~ meet in the future), referred to as ~~the~~ Pillar One ~~proposal~~ , and imposing a minimum effective tax rate on certain multinational enterprises, referred to as ~~the~~ Pillar Two ~~proposal~~ . A number of countries **in which we operate** have enacted ~~with effect from the start of 2024~~ , or are planning to enact **,** core elements of the Pillar Two ~~rules. Based on our current~~

~~understanding of the minimum revenue thresholds contained in the Pillar Two proposal, we may be within the scope of its~~ rules. The OECD has issued administrative guidance providing transition and safe harbor rules in relation to the implementation of ~~the~~ Pillar Two ~~proposal~~. We are monitoring **minimum revenue threshold requirements and** developments and evaluating the potential impacts of these ~~new~~ rules, including on our effective tax rates and considering our eligibility to qualify for ~~these~~ -- **the available** safe harbor rules. Any of the foregoing could increase our tax obligations and require us to incur additional material costs to ensure compliance with any such rules in the countries where we do business. In addition, forecasts of our income tax position and effective tax rate for financial accounting purposes are complex and subject to significant judgment and uncertainty because our income tax position for each year combines the effects of a mix of profits earned and losses incurred by us in various tax jurisdictions with a broad range of income tax rates, as well as changes in the valuation of deferred tax assets and liabilities, the impact of various accounting rules and tax laws (and changes to these rules and tax laws), the results of examinations by various tax authorities, and the impact of any acquisition, business combination or other reorganization or financing transaction. To forecast our global tax rate, we estimate our pre- tax profits and losses and tax expense by jurisdiction. If the mix of profits and losses, our ability to use tax assets and attributes, our assessment of the need for valuation allowances, effective tax rates by jurisdiction or other factors are different than those estimated, our actual tax rate could be materially different than forecasted, which could have a material impact on our business, financial condition and results of operations. Our operating results may be negatively affected if we are required to pay additional taxes, including sales and use tax, value added tax, or other transaction taxes, and we could be subject to liability with respect to all or a portion of past or future sales. We currently collect and remit sales and use, value added and other transaction taxes in certain of the jurisdictions where we do business based on our assessment of the amount of taxes owed by us in such jurisdictions. However, in some jurisdictions in which we do business, we do not believe that we owe such taxes, and therefore we currently do not collect and remit such taxes in those jurisdictions or record contingent tax liabilities in respect of those jurisdictions. A successful assertion that we are required to pay additional taxes in connection with sales of our solutions, or the imposition of new laws or regulations or the interpretation of existing laws and regulations requiring the payment of additional taxes, would result in increased costs and administrative burdens for us. If we are subject to additional taxes and determine to offset such increased costs by collecting and remitting such taxes from our customers, or otherwise passing those costs through to our customers, companies may be discouraged from using our solutions. Any increased tax burden may decrease our ability or willingness to compete in relatively burdensome tax jurisdictions, result in substantial tax liabilities related to past or future sales or otherwise harm our business and operating results. Our ability to use net operating losses to offset future taxable income may be subject to certain limitations. At December 31, ~~2023~~ **2024** we had U. S. federal, state and foreign net operating loss carryforwards, or NOLs, of $ ~~372~~ **353** million, $ ~~246~~ **239. 3 million, and $ 468** million, respectively, available to offset future taxable income, some of which will begin to expire in 2030. A lack of future taxable income would adversely affect our ability to utilize certain of our NOLs before they expire. Under current law, Federal NOLs incurred in taxable years beginning after December 31, 2017 can be carried forward indefinitely, but the deductibility of such federal NOLs **in a taxable year** is limited to 80 % of taxable income **in such year. Certain foreign jurisdictions have annual limitations on the use of NOLs**. In addition, under the provisions of the Internal Revenue Code of 1986, as amended, or the Internal Revenue Code, changes in our ownership may limit the amount of pre- change NOLs that can be utilized annually in the future to offset taxable income. Section 382 **and 383** of the Internal Revenue Code ~~imposes~~ **impose** limitations on a company' s ability to use its NOLs **and other tax assets** to offset its taxable income if one or more stockholders or groups of stockholders that each own at least 5 % of the company' s stock increase their aggregate ownership (by value) by more than 50 percentage points over their lowest ownership percentages within a rolling three- year period. Similar rules may apply under state and foreign tax laws. Based upon an analysis at December 31, ~~2023~~ **2024**, we do not expect these limitations to materially impair our ability to use our NOLs **and other tax assets** prior to expiration. However, if changes in our ownership occurred after such date, or occur in the future, our ability to use our NOLs **and other tax assets** may be limited. Subsequent statutory or regulatory changes in respect of the utilization of NOLs **and other tax assets** for federal, state or foreign purposes, such as suspensions on the use of NOLs or limitations on the deductibility of NOLs carried forward, or other unforeseen reasons, may result in our existing NOLs expiring or otherwise being unavailable to offset future income tax liabilities. For these reasons, we may not be able to utilize a material portion of our NOLs **and other tax assets**, even if we achieve profitability. We are obligated to maintain proper and effective internal controls over financial reporting, and any failure to maintain the adequacy of these internal controls may adversely affect investor confidence in our company and, as a result, the value of our common stock. We are required, pursuant to Section 404 of the Sarbanes- Oxley Act ~~, or Section 404,~~ to furnish a report by management on, among other things, the effectiveness of our internal control over financial reporting on an annual basis. This assessment includes disclosure of any material weaknesses identified by our management in our internal control over financial reporting. We are also required to disclose significant changes made in our internal control procedures on a quarterly basis. 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 cannot assure you that there will not be material weaknesses or significant deficiencies in our internal control over financial reporting in the future. Any failure to maintain internal control over financial reporting could severely inhibit our ability to accurately report 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 or significant deficiency in our internal control over financial reporting, we could lose investor confidence in the accuracy and completeness of our financial reports, the market price of our common stock could decline, and we could be subject to sanctions or investigations by the Nasdaq, the SEC or other regulatory authorities. Failure to remedy any material weakness in our internal control over financial reporting, or to maintain other effective control systems required of public companies, could also restrict our future access to the capital markets.