Risk Factors Comparison 2024-02-22 to 2023-02-23 Form: 10-K

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

An investment in our common stock involves a high degree of risk. You should carefully consider the risks and uncertainties described below, and all other information contained in this Annual Report on Form 10- K, including our consolidated financial statements and the related notes, before making a decision to invest in our common stock. Our business, operating results, financial condition, or prospects could be materially and adversely affected by any of these risks and uncertainties. In that case, the trading price of our common stock could decline, and you might lose all or part of your investment. In addition, the risks and uncertainties discussed below are not the only ones we face. Our business, operating results, financial performance or prospects could also be harmed by risks and uncertainties not currently known to us or that we currently do not believe are material. Risks Related to Our Business and Industry Our quarterly and annual operating results may vary from period to period, which could result in our failure to meet expectations with respect to operating results and cause the trading price of our stock to decline. Our operating results 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, from both existing and new customers; • the extent to which customers subscribe for additional solutions; • changes in customer renewals of our solutions; • timing of deals signed within the applicable fiscal period; • seasonal buying patterns of our customers; • timely invoicing or changes in billing terms of customers; • the length of our sales cycle for our products and services; • price competition; • the timing and success of new product or service introductions by us or our competitors or any other changes in the competitive landscape of our industry, including consolidation among our competitors; • the introduction or adoption of new technologies that compete with our solutions; • decisions by potential customers to purchase IT, security and compliance products or services from other vendors; • general economic conditions, both domestically and in the foreign markets in which we sell our solutions; • changes in foreign currency exchange rates; • changes in the growth rate of the IT, security and compliance market; • actual or perceived security breaches **and incidents** , technical difficulties or interruptions with our service; • failure of our products and services to operate as designed; • publicity regarding security breaches **and incidents** generally and the level of perceived threats to IT security; • the announcement or adoption of new regulations and policy mandates or changes to existing regulations and policy mandates; • the amount and timing of operating costs and capital expenditures related to the operations and expansion of our business; • pace and cost of hiring employees; • expenses associated with our existing and new products and services; • the timing of sales commissions relative to the recognition of revenues; • insolvency or credit difficulties confronting our customers, affecting their ability to purchase or pay for our solutions; • our ability to integrate any products or services that we have acquired or may acquire in the future into our product suite or migrate existing customers of any companies that we have acquired or may acquire in the future to our products and services; • future accounting pronouncements or changes in our accounting policies; • our effective tax rate, changes in tax rules, tax effects of infrequent or unusual transactions, and tax audit settlements; • the amount and timing of income tax that we recognize resulting from stock- based compensation; • the timing of expenses related to the development or acquisition of technologies, services or businesses; and • potential goodwill and intangible asset impairment charges associated with acquired businesses. Further, the interpretation and application of international laws and regulations in many cases is uncertain, and our legal and regulatory obligations in foreign jurisdictions are subject to frequent and unexpected changes, including the potential for various regulatory or other governmental bodies to enact new or additional laws or regulations or to issue rulings that invalidate prior laws or regulations. Each factor above or 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 operating results. This variability and unpredictability could result in our failure to meet expectations with respect to operating results, or those of securities analysts or investors, for a particular period. In addition, a significant percentage of our operating expenses are fixed in nature and based on forecasted trends in revenues. Accordingly, in the event of shortfalls in revenues, we are generally unable to mitigate the negative impact on margins in the short term by reducing our operating expenses. If we fail to meet or exceed expectations for our operating results for these or any other reasons, the trading price of our common stock could fall and we could face costly lawsuits, including securities class action suits. If we do not successfully anticipate market needs and opportunities or are unable to enhance our solutions and develop new solutions that meet those needs and opportunities on a timely or cost- effective basis, we may not be able to compete effectively and our business and financial condition may be harmed. The IT, security and compliance market is characterized by rapid technological advances, customer price sensitivity, short product and service life cycles, intense competition, changes in customer requirements, frequent new product introductions and enhancements and evolving industry standards and regulatory mandates. Any of these factors could create downward pressure on pricing and gross margins, and could adversely affect our renewal rates, as well as our ability to attract new customers. Our future success will depend on our ability to enhance existing solutions, introduce new solutions on a timely and cost- effective basis, meet changing customer needs, extend our core technology into new applications, and anticipate and respond to emerging standards and business models. We must also continually change and improve our solutions in response to changes in operating systems, application software, computer and communications hardware, networking software, shared cloud platform infrastructures, programming tools and computer language technology. We may not be able to anticipate future market needs and opportunities or develop enhancements or new solutions to meet such needs or opportunities in a timely manner or at all. The market for cloud solutions for IT, security and compliance continues to evolve, and it is uncertain whether our new solutions will gain market acceptance. Our solution enhancements or new solutions could fail to attain sufficient market acceptance for many reasons, including: •

failure to timely meet market demand for product functionality; • inability to identify and provide intelligence regarding the attacks or techniques used by cyber- attackers; • inability to inter- operate effectively with the database technologies, file systems or web applications of our prospective customers; • defects, errors or failures; • delays in releasing our enhancements or new solutions; • negative publicity about their performance or effectiveness; • introduction or anticipated introduction of products by our competitors; • poor business conditions, causing customers to delay IT, security and compliance purchases; • easing or changing of external regulations related to IT, security and compliance; and • reluctance of customers to purchase cloud solutions for IT, security and compliance. Furthermore, diversifying our solutions and expanding into new IT, security and compliance markets will require significant investment and planning, require that our research and development and sales and marketing organizations develop expertise in these new markets, bring us more directly into competition with IT, security compliance providers that may be better established or have greater resources than we do, require additional investment of time and resources in the development and training of our channel partners and entail significant risk of failure. If we fail to anticipate market requirements or fail to develop and introduce solution enhancements or new solutions to satisfy those requirements in a timely manner, such failure could substantially decrease or delay market acceptance and sales of our present and future solutions and cause us to lose existing customers or fail to gain new customers, which would significantly harm our business, financial condition and results of operations. If we fail to continue to effectively scale and adapt our platform to meet the performance and other requirements of our customers, our operating results and our business would be harmed. Our future growth depends to a significant extent on our ability to continue to meet the expanding needs of our customers as their use of our cloud platform grows. As these customers gain more experience with our solutions, the number of users and the number of locations where our solutions are being accessed may expand rapidly in the future. In order to ensure that we meet the performance and other requirements of our customers, we intend to continue to make significant investments to develop and implement new proprietary and third- party technologies at all levels of our cloud platform. These technologies, which include databases, applications and server optimizations, and network and hosting strategies, are often complex, new and unproven. We may not be successful in developing or implementing these technologies. To the extent that we do not effectively scale our platform to maintain performance as our customers expand their use of our platform, our operating results and our business may be harmed. If we are unable to renew existing subscriptions for our IT, security and compliance solutions, sell additional subscriptions for our solutions and attract new customers, our operating results would be harmed. We offer our ~~Qualys Cloud~~ **cloud** ~~Platform~~ **platform** and integrated suite of solutions pursuant to a software- as- a- service model, and our customers purchase subscriptions from us that are generally one year in length. Our customers have no obligation to renew their subscriptions after their subscription period expires, and they may not renew their subscriptions at the same or higher levels or at all. As a result, our ability to grow depends in part on customers renewing their existing subscriptions and purchasing additional subscriptions and solutions. Our customers may choose not to renew their subscriptions to our solutions or purchase additional solutions due to a number of factors, including their satisfaction or dissatisfaction with our solutions, the prices of our solutions, the prices of products or services offered by our competitors, reductions in our customers' spending levels due to the macroeconomic environment or other factors. If our customers do not renew their subscriptions to our solutions, renew on less favorable terms, or do not purchase additional solutions or subscriptions, our revenues may grow more slowly than expected or decline and our operating results would be harmed. In addition, our future growth depends in part upon increasing our customer base. Our ability to achieve significant growth in revenues in the future will depend, in large part, upon continually attracting new customers and obtaining subscription renewals to our solutions from those customers. If we fail to attract new customers, our revenues may grow more slowly than expected and our operating results would be harmed. Our current research and development efforts may not produce successful products or enhancements to our platform that result in significant revenue, cost savings or other benefits in the near future. We must continue to dedicate significant financial and other resources to our research and development efforts if we are to maintain our competitive position. However, developing products and enhancements to our platform is expensive and time consuming, and there is no assurance that such activities will result in significant new marketable products or enhancements to our platform, design improvements, cost savings, revenue or other expected benefits. If we spend significant resources 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. Our platform, website and internal systems may be subject to intentional disruption or other security incidents that could result in liability and adversely impact our reputation and future sales. We and our service providers face threats from a variety of sources, including attacks on our networks and systems from numerous sources, including traditional " hackers, " sophisticated nation- state and nation- state supported actors, other sources of malicious code (such as viruses and worms), ransomware, social engineering, denial of service attacks, and phishing attempts. We and our service providers could be a target of cyber- attacks or other malfeasance designed to impede the performance of our solutions, penetrate our network security or the security of our cloud platform or our internal systems, misappropriate proprietary information and / or cause interruptions to our services. We and our service providers have experienced and may continue to experience security incidents and attacks of varying degrees from time to time. ~~For example, in December 2020, we were notified by a service provider, Accellion, of a zero- day vulnerability affecting an Accellion FTA server that we deployed to transfer information as part of our customer support system. In response to this incident, we engaged third- party forensic experts to investigate and determined that attackers illegally obtained certain information from the Accellion FTA server. We notified affected customers, as we deemed was required or appropriate.~~ We have incurred costs to respond to ~~this~~ **such** ~~incident~~ **incidents** and may continue to incur costs to support our efforts to enhance our security measures. Additionally, due to political uncertainty and military actions **in parts** ~~associated with Russia' s invasion~~ of ~~Ukraine~~ **Eastern Europe and the Middle East**, we and our service providers are vulnerable to heightened risks of cybersecurity incidents and security and privacy breaches from or affiliated with nation- state actors, including attacks that could materially disrupt our systems, operations and services. Our solutions, platforms, and system, and those of our service providers, may also suffer

security incidents as a result of non- technical issues, including intentional or inadvertent acts or omissions by our employees or service providers. With the increase in personnel working remotely ~~during the current COVID- 19 pandemic~~ , we and our service providers are at increased risk for security breaches **and incidents** . We have taken and intend to continue to take steps to monitor and enhance the security of our solutions, cloud platform, and other relevant systems, IT infrastructure, networks, and data; however, the unprecedented scale of remote work may require additional personnel and resources, which nevertheless cannot be guaranteed to fully safeguard our solutions, our cloud platform, or any systems, IT infrastructure networks, or data upon which we rely. Further, because our operations involve providing IT security solutions to our customers, we may be targeted for cyber- attacks and other security incidents. A breach in **or incident impacting** our data security ~~or~~ **,** an attack against our service availability, or ~~that of~~ **any breach, incident, or attack impacting** our third- party service providers, could impact our networks or networks secured by our solutions, creating system disruptions or slowdowns and exploiting security vulnerabilities of our solutions, and the information stored on our networks or those of our third- party service providers could be accessed, used, publicly disclosed, altered, lost, or stolen, which could subject us to liability and cause us financial harm. If an actual or perceived disruption in the availability of our solutions or the breach **or other compromise** of our security measures or those of our service providers occurs, it could adversely affect the market perception of our solutions, result in a loss of competitive advantage, have a negative impact on our reputation, or result in the loss of customers, channel partners and sales, and it may expose us to the loss **, unavailability** or alteration of information, **claims, demands and** litigation, regulatory **investigations,** actions and ~~investigations~~ **other proceedings** and possible liability. Any such actual or perceived security breach **or incident** or disruption could also divert the efforts of our technical and management personnel. We **and our service providers may face difficulties or delays in identifying and responding to any security breach or incident. We** also may incur significant costs and operational consequences of investigating, remediating, eliminating and putting in place additional tools and devices designed to prevent actual or perceived security incidents, as well as ~~the~~ costs **to respond to and otherwise address any breach or incident, including any** to comply with any notification obligations resulting from any security incidents. In addition, any such actual or perceived security breach **or incident** could impair our ability to operate our business and provide solutions to our customers. If this happens, our reputation could be harmed, our revenues could decline and our business could suffer. Although we maintain insurance coverage that may be applicable to certain liabilities in the event of a security breach or other security incident, we cannot be certain that our insurance coverage will be adequate for liabilities that actually are incurred, that insurance will continue to be available to us on economically reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that exceed available insurance coverage or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co- insurance requirements, could have a material and adverse effect on our business, including our financial condition, operating results and reputation. Our sales cycle can be long and unpredictable, and our sales efforts require considerable time and expense. As a result, revenues may vary from period to period, which may cause our operating results to fluctuate and could harm our business. The timing of sales of subscriptions for our solutions can be difficult to forecast because of the length and unpredictability of our sales cycle, particularly with large transactions **and in the current macroeconomic environment** . We sell subscriptions to our IT, security and compliance 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. Further, the length of time that potential customers devote to their testing and evaluation, contract negotiation and budgeting processes varies significantly, which has also made our sales cycle long and unpredictable. The length of the sales cycle for our solutions typically ranges from six to twelve months but can be more than eighteen months. 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 revenues, which could harm our business. Adverse economic conditions or reduced IT spending may adversely impact our business. Our business depends to a significant extent on the overall demand for IT and on the economic health of our current and prospective customers. Economic weakness, customer financial difficulties, supply chain constraints, change in interest rates, inflationary pressures and potential for a recession, and constrained spending on IT security, **as well as longer sales cycles,** which factors we have experienced in ~~2022~~ **2023** , have resulted and may in the future result in decreased revenue and earnings. Such factors have made and could in the future make it difficult to accurately forecast our sales and operating results and could negatively affect our ability to provide accurate forecasts to our contract manufacturers. In addition, continued governmental budgetary challenges in the United States and Europe, inflationary pressures and potential for a recession, and geopolitical turmoil in many parts of the world, including the ongoing military ~~conflict~~ **conflicts** ~~between Russia~~ **in parts of Eastern Europe** and ~~Ukraine~~ **the Middle East** , and other disruptions to global and regional economies and markets in many parts of the world, as well as uncertainties related to changes in public policies such as domestic and international regulations, taxes or international trade agreements, have and may continue to put pressure on global economic conditions and overall spending on IT security and may further increase inflation, both in the U. S. and globally, which could increase our operating costs in the future and reduce overall spending on IT security. General economic weakness may also lead to longer collection cycles for payments due from our customers, an increase in customer bad debt, restructuring initiatives and associated expenses, and impairment of investments. Furthermore, the continued weakness and uncertainty in worldwide credit markets, including the sovereign debt situation in certain countries in the European Union, may adversely impact our European operations, as well as our current and potential customers' available budgetary spending, which could lead to delays or reductions in planned purchases of our solutions. Uncertainty about future economic conditions also makes it difficult to forecast operating results and to make decisions about future investments. Future or continued economic weakness for us or our customers, failure of our customers and markets to recover from such weakness, customer financial difficulties, and reductions in spending on IT security could have a material adverse effect on demand for our platform and consequently on our business, financial condition and

results of operations. Our IT, security and compliance solutions are delivered from ~~11~~ **14** shared cloud platforms, and any disruption of service at these facilities would interrupt or delay our ability to deliver our solutions to our customers which could reduce our revenues and harm our operating results. We currently host substantially all of our solutions from third- party shared cloud platforms located in the United States, Canada, Switzerland, the Netherlands, United Arab Emirates, Australia, United Kingdom **, Italy, the Kingdom of Saudi Arabia** and India. These facilities are vulnerable to damage or interruption from earthquakes, hurricanes, floods, fires, cybersecurity attacks, terrorist attacks, employee negligence, power losses, telecommunications failures and similar events. The facilities also could be subject to break- ins, sabotage, intentional acts of vandalism and other misconduct. The occurrence of a natural disaster, an act of terrorism or misconduct, a decision to close the facilities without adequate notice or other unanticipated problems could result in interruptions in our services. Some of our shared cloud platforms are not currently redundant and we may not be able to rapidly move our customers from one shared cloud platform to another, which may increase delays in the restoration of our service for our customers if an adverse event occurs. We have added shared cloud platforms to provide additional capacity and to enable disaster recovery. We continue to build out these facilities; however, these additional facilities may not be operational in the anticipated time- frame and we may incur unplanned expenses. Additionally, our existing shared cloud platform providers have no obligations to renew their agreements with us on commercially reasonable terms, or at all. If we are unable to renew our agreements with the facilities providers on commercially reasonable terms or if in the future we add additional shared cloud platform providers, we may experience costs or downtime in connection with the loss of an existing facility or the transfer to, or addition of, new facilities. Any disruptions or other performance problems with our solutions could harm our reputation and business and may damage our customers' businesses. Interruptions in our service delivery might reduce our revenues, cause us to issue credits to customers, subject us to potential liability and cause customers to terminate their subscriptions or not renew their subscriptions. We face competition in our markets, and we may lack sufficient financial or other resources to maintain or improve our competitive position. We compete with a large range of established and emerging vulnerability management vendors, compliance vendors and data security vendors in a highly fragmented and competitive environment. We face significant competition for each of our solutions from companies with broad product suites and greater name recognition and resources than we have, as well as from small companies focused on specialized security solutions. We compete with large and small public companies, such as Broadcom (Symantec Enterprise Security), CrowdStrike, Palo Alto Networks, Rapid7, Tenable Holdings, as well as privately held security providers including Axonius, Checkmarx, Flexera, Invicti, Ivanti, Tanium, HelpSystems (Tripwire), Trustwave Holdings ~~and~~ **,** Veracode **and Wiz** . We also seek to replace IT, security and compliance solutions that organizations have developed internally. As we continue to extend our cloud platform' s functionality by further developing IT, security and compliance solutions, such as ~~web application scanning~~ **Cybersecurity Asset Management** and ~~firewalls~~ **Patch Management** , we expect to face additional competition in these new markets. Our competitors may also attempt to further expand their presence in the IT, security and compliance market and compete more directly against one or more of our solutions. We believe that the principal competitive factors affecting our markets include product functionality, breadth of offerings, flexibility of delivery models, ease of deployment and use, total cost of ownership, scalability and performance, customer support and **the** extensibility of **our** platform. Many of our existing and potential competitors have competitive advantages, including: • greater brand name recognition; • larger sales and marketing budgets and resources; • broader distribution networks and more established relationships with distributors and customers; • access to larger customer bases; • greater customer support resources; • greater resources to make acquisitions; • greater resources to develop and introduce products that compete with our solutions; • greater resources to meet relevant regulatory requirements; and • substantially greater financial, technical and other resources. As a result, our competitors may be able to respond more quickly and effectively than we can to new or changing opportunities, technologies, standards or customer requirements. With the introduction of new technologies, the evolution of our service and new market entrants, we expect competition to intensify in the future. In addition, some of our larger competitors have substantially broader product offerings and can bundle competing products and services with other software offerings. As a result, customers may choose a bundled product offering from our competitors, even if individual products have more limited functionality than our solutions. These competitors may also offer their products at a lower price as part of this larger sale, which could increase pricing pressure on our solutions and cause the average sales price for our solutions to decline. These larger competitors are also often in a better position to withstand any significant reduction in capital spending and will therefore not be as susceptible to economic downturns. Furthermore, our current and potential competitors may establish cooperative relationships among themselves or with third parties that may further enhance their resources and product and services offerings in the markets we address. In addition, current or potential competitors may be acquired by third parties with greater available resources. As a result of such relationships and acquisitions, our current or potential competitors might be able 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. The sales prices of our solutions are subject to competitive pressures and may decrease, which may reduce our gross profits and adversely impact our financial results. The sales prices for our solutions may decline for a variety of reasons, including competitive pricing pressures, discounts, a change in our mix of solutions and subscriptions, anticipation of the introduction of new solutions or subscriptions, or promotional programs. Competition continues to increase in the market segments in which we participate, and we expect competition to further increase in the future, thereby leading to increased pricing pressures. Larger competitors with more diverse product and service offerings may reduce the price of products or subscriptions that compete with ours or may bundle them with other products and subscriptions. Additionally, although we price our products and subscriptions worldwide in U. S. Dollars, ~~Euros~~ **Euro** , British Pounds, Canadian Dollars, Japanese Yen and Indian Rupee, currency fluctuations in certain countries and regions may negatively impact

actual prices that partners and customers are willing to pay in those countries and regions, or the effective prices we realize in our reporting currency. We cannot assure you that we will be successful in developing and introducing new offerings with enhanced functionality on a timely basis, or that our new product and subscription offerings, if introduced, will enable us to maintain our prices and gross profits at levels that will allow us to maintain positive gross margins and profitability. If our solutions fail to help our customers achieve and maintain compliance with regulations and industry standards, our revenues and operating results could be harmed. We generate a portion of our revenues from solutions that help organizations achieve and maintain compliance with regulations and industry standards. For example, many of our customers subscribe to our IT, security and compliance solutions to help them comply with the security standards developed and maintained by the Payment Card Industry Security Standards Council, or the PCI Council, which apply to companies that store cardholder data. Industry organizations like the PCI Council may significantly change their security standards with little or no notice, including changes that could make their standards more or less onerous for businesses. Governments may also adopt new laws or regulations, or make changes to existing laws or regulations, ~~that~~ **which** could impact the demand for or value of our solutions. If we are unable to adapt our solutions to changing regulatory standards in a timely manner, or if our solutions fail to assist with or expedite our customers' compliance initiatives, our customers may lose confidence in our solutions and could switch to products offered by our competitors. In addition, if regulations and standards related to data security, vulnerability management and other IT, security and compliance requirements are relaxed or the penalties for non- compliance are changed in a manner that makes them less onerous, our customers may view government and industry regulatory compliance as less critical to their businesses, and our customers may be less willing to purchase our solutions. In any of these cases, our revenues and operating results could be harmed. If our solutions fail to detect vulnerabilities or incorrectly detect vulnerabilities, our brand and reputation could be harmed, which could have an adverse effect on our business and results of operations. If our solutions fail to detect vulnerabilities in our customers' IT infrastructures, or if our solutions fail to identify and respond to new and increasingly complex methods of attacks, our business and reputation may suffer. There is no guarantee that our solutions will detect all vulnerabilities. Additionally, our IT, security and compliance solutions may falsely detect vulnerabilities or threats that do not actually exist. For example, some of our solutions rely on information on attack sources aggregated from third- party data providers who monitor global malicious activity originating from a variety of sources, including anonymous proxies, specific IP addresses, botnets and phishing sites. If the information from these data providers is inaccurate, the potential for false indications of security vulnerabilities increases. These false positives, while typical in the industry, may impair the perceived reliability or usability of our solutions and may therefore adversely impact market acceptance of our solutions and could result in negative publicity, loss of customers and sales, increased costs to remedy any incorrect information or problem, or claims by aggrieved parties. Similar issues may be generated by the misuse of our tools to identify and exploit vulnerabilities. Further, our solutions sometimes are tested against other security products, and may fail to perform as effectively, or to be perceived as performing as effectively, as competitive products for any number of reasons, including misconfiguration. To the extent current or potential customers, channel partners, or others believe there has been an occurrence of an actual or perceived failure of our solutions to detect a vulnerability or otherwise to function as effectively as competitive products in any particular test, or indicates our solutions do not provide significant value, our business, competitive position, and reputation could be harmed. In addition, our solutions do not currently extend to cover all mobile and personal devices that employees may bring into an organization. As such, our solutions would not identify or address vulnerabilities in all mobile and personal devices, and our customers' IT infrastructures may be compromised by attacks that infiltrate their networks through such devices. An actual or perceived security breach or **incident or loss,** theft **, unavailability or other compromise** of the sensitive data of one of our customers, regardless of whether the breach is attributable to the failure of our solutions, could adversely affect the market' s perception of our security solutions. If we are unable to continue the expansion of our sales force, sales of our solutions and the growth of our business would be harmed. We believe that our growth will depend, to a significant extent, on our success in recruiting and retaining a sufficient number of qualified sales personnel and their ability to obtain new customers, manage our existing customer base and expand the sales of our newer solutions. We plan to continue to expand our sales force and ~~make a significant investment~~ ---- **invest** in our sales and marketing activities. Our recent hires and planned hires may not become as productive as quickly as we would like, and we may be unable to hire or retain sufficient numbers of qualified individuals in the future in the competitive markets where we do business. Competition for highly skilled personnel is frequently intense and we may not be able to compete for these employees. If we are unable to recruit and retain a sufficient number of productive sales personnel, sales of our solutions and the growth of our business may be harmed. Additionally, if our efforts do not result in increased revenues, our operating results could be negatively impacted due to the upfront operating expenses associated with expanding our sales force. We rely on third- party channel partners to generate a substantial amount of our revenues, and if we fail to expand and manage our distribution channels, our revenues could decline and our growth prospects could suffer. Our success significantly depends to a significant extent on establishing and maintaining relationships with a variety of channel partners and we anticipate that we will continue to depend on these partners in order to grow our business. For the years ended December 31, **2023,** 2022 ~~,~~ **and** 2021 ~~and 2020~~ , we derived approximately **43 %,** 42 % ~~,~~ **and** 41 % ~~and 42 %, respectively,~~ of our revenues from sales of subscriptions for our solutions through channel partners, and the percentage of revenues derived from channel partners may increase in future periods. Our agreements with our channel partners are generally non- exclusive and do not prohibit them from working with our competitors or offering competing solutions, and many of our channel partners have more established relationships with our competitors. If our channel partners choose to place greater emphasis on products of their own or those offered by our competitors, do not effectively market and sell our solutions, or fail to meet the needs of our customers, then our ability to grow our business and sell our solutions may be adversely affected. In addition, the loss of one or more of our larger channel partners, who may cease marketing our solutions with limited or no notice, and our possible inability to replace them, could adversely affect our sales. Moreover, our ability to expand our distribution channels depends in part on

our ability to educate our channel partners about our solutions, which can be complex. Our failure to recruit additional channel partners, or any reduction or delay in their sales of our solutions or conflicts between channel sales and our direct sales and marketing activities may harm our results of operations. Even if we are successful, these relationships may not result in greater customer usage of our solutions or increased revenues. In addition, the financial health of our channel partners and our continuing relationships with them are important to our success. Some of these channel partners may be unable to withstand adverse changes in economic conditions, which could result in insolvency and / or the inability of such distributors to obtain credit to finance purchases of our products and services. In addition, weakness in the end- user market could negatively affect the cash flows of our channel partners who could, in turn, delay paying their obligations to us, which would increase our credit risk exposure. Our business could be harmed if the financial condition of some of these channel partners substantially weakened and we were unable to timely secure replacement channel partners. A significant portion of our customers, channel partners and employees are located outside of the United States, which subjects us to a number of risks associated with conducting international operations, and if we are unable to successfully manage these risks, our business and operating results could be harmed. We market and sell subscriptions to our solutions throughout the world and have personnel in many parts of the world. In addition, we have sales offices and research and development facilities outside the United States and we conduct, and expect to continue to conduct, a significant amount of our business with organizations that are located outside the United States, particularly in Europe and Asia. Therefore, we are subject to risks associated with having international sales and worldwide operations, including: • foreign currency exchange fluctuations; • trade and foreign exchange restrictions; • economic or political instability in foreign markets, including as a result of increasing tensions between India and China; • greater difficulty in enforcing contracts, accounts receivable collection and longer collection periods; • changes in regulatory requirements; • tax laws (including U. S. taxes on foreign subsidiaries); • difficulties and costs of staffing and managing foreign operations; • 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; • costs of complying with U. S. laws and regulations for foreign operations, including the Foreign Corrupt Practices Act, import and export control laws, tariffs, trade barriers, economic sanctions and other regulatory or contractual limitations on our ability to sell our solutions in certain foreign markets, and the risks and costs of non- compliance; • 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, acts of terrorism, hostilities or war; • management communication and integration problems resulting from cultural differences and geographic dispersion; and • multiple and possibly overlapping tax structures. Some of our business partners also have international operations and are subject to the risks described above. Even if we are able to successfully manage the risks of international operations, our business may be adversely affected if our business partners are not able to successfully manage these risks. Our business, including the sales of subscriptions of our solutions, may be subject to foreign governmental regulations, which vary substantially from country to country and change from time to time. Failure 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 ensure compliance with these laws and policies, there can be no assurance that all of 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 operations, our business and operating results could be adversely affected. In addition, as of December 31, ~~2022~~ **2023** , approximately 75 % of our employees were located outside of the United States, with 66 % of our employees located in Pune, India. Accordingly, we are exposed to changes in laws governing our employee relationships in various U. S. and foreign jurisdictions, including laws and regulations regarding wage and hour requirements, fair labor standards, employee data privacy, unemployment tax rates, workers' compensation rates, citizenship requirements and payroll and other taxes which may have a direct impact on our operating costs. We may continue to expand our international operations and international sales and marketing activities. Expansion in international markets has required, and will continue to require, significant management attention and resources. We may be unable to scale our infrastructure effectively or as quickly as our competitors in these markets and our revenues may not increase to offset any increased costs and operating expenses, which would cause our results to suffer. We are exposed to fluctuations in currency exchange rates, which could negatively affect our financial condition and results of operations. Our reporting currency is the U. S. dollar and we generate a majority of our revenues in U. S. dollars. However, for the year ended December 31, ~~2022~~ **2023** , we incurred approximately 29 % of our expenses in foreign currencies, primarily ~~Euros~~ **Euro** , British Pounds, and Indian Rupee, principally with respect to salaries and related personnel expenses associated with our European and Indian operations. Additionally, for the year ended December 31, ~~2022~~ **2023** , approximately ~~24~~ **23** % of our revenues were generated in foreign currencies. Accordingly, changes in exchange rates may have a material adverse effect on our business, operating results and financial condition. The exchange rate between the U. S. dollar and foreign currencies has fluctuated substantially in recent years and may continue to fluctuate substantially in the future. We expect that a majority of our revenues will continue to be generated in U. S. dollars for the foreseeable future and that a significant portion of our expenses, including personnel costs, as well as capital and operating expenditures, will continue to be denominated in the Euro, British Pound and Indian Rupee. The result of our operations may be adversely affected by foreign exchange fluctuations. We use derivative financial instruments to reduce our foreign currency exchange risks. We use foreign currency forward contracts to mitigate the impact of foreign currency fluctuations of certain non- U. S. dollar denominated net asset positions, to date primarily cash, accounts receivable and operating lease liabilities (non- designated), as well as to manage foreign currency

fluctuation risk related to forecasted transactions (designated). However, we may not be able to purchase derivative instruments that are adequate to insulate ourselves from foreign currency exchange risks. Additionally, our hedging activities may contribute to increased losses as a result of volatility in foreign currency markets. If the market for cloud solutions for IT, security and compliance does not evolve as we anticipate, our revenues may not grow and our operating results would be harmed. Our success depends to a significant extent on the willingness of organizations to increase their use of cloud solutions for their IT, security and compliance. Some organizations may be reluctant to use cloud solutions because they have concerns regarding the risks associated with the reliability or security of the technology delivery model associated with these solutions. If other cloud service providers experience security incidents, loss of customer data, disruptions in service delivery or other problems, the market for cloud solutions as a whole, including our solutions, may be negatively impacted. Moreover, organizations that have invested substantial personnel and financial resources to integrate on- premise software into their businesses may be reluctant or unwilling to migrate to a cloud solution. Organizations that use on- premise security products, such as network firewalls, security information and event management products or data loss prevention solutions, may also believe that these products sufficiently protect their IT infrastructure and deliver adequate security. Therefore, they may continue spending their IT security budgets on these products and may not adopt our IT, security and compliance solutions in addition to or as a replacement for such products. If customers do not recognize the benefits of our cloud solutions over traditional on- premise enterprise software products, and as a result we are unable to increase sales of subscriptions to our solutions, then our revenues may not grow or may decline, and our operating results would be harmed. Our business and operations have continued to grow since inception, and if we do not appropriately manage any future growth, or are unable to improve our systems and processes, our operating results may be negatively affected. We have continued to grow over the last several years, with revenues increasing from $ ~~363~~ **411** . ~~0~~ **2** million in ~~2020~~ **2021** to $ ~~489~~ **554** . ~~7~~ **5** million in ~~2022~~ **2023** , and headcount increasing from 1, 498 employees at the beginning of ~~2020~~ **2021** to 2, ~~143~~ **188** employees as of December 31, ~~2022~~ **2023** . We rely on information technology systems to help manage critical functions such as order processing, revenue recognition and financial forecasts. To manage any future growth effectively we must continue to improve and expand our IT systems, financial infrastructure, and operating and administrative systems and controls, and continue to manage headcount, capital and processes in an efficient manner. We may not be able to successfully implement improvements to these systems and processes in a timely or efficient manner. Our failure to improve our systems and processes, or their failure to operate in the intended manner, may result in our inability to manage the growth of our business and to accurately forecast our revenues, expenses and earnings, or to prevent certain losses. In addition, as we continue to grow, our productivity and the quality of our solutions may also be adversely affected if we do not integrate and train our new employees quickly and effectively. Any future growth would add complexity to our organization and require effective coordination across our organization. Failure to manage any future growth effectively could result in increased costs, harm our results of operations and lead to investors losing confidence in our internal systems and processes. We depend on the continued services and performance of our senior management and other key employees, the loss of any of whom could adversely affect our business, operating results and financial condition. Our future performance depends to a significant extent on the continued services and continuing contributions of our senior management and other key employees, to execute on our business plan and to identify and pursue new opportunities and product innovations. We do not maintain key- man insurance for any member of our senior management team. Our senior management and key employees are generally employed on an at- will basis, which means that they could terminate their employment with us at any time. From time to time, there may be changes in our senior management team resulting from the termination or departure of executives ~~. For example, we recently announced that we and our Chief Revenue Officer mutually agreed to end his employment on March 31, 2023~~ . The loss of the services of our senior management or other key employees for any reason could significantly delay or prevent the achievement of our development and strategic objectives and harm our business, financial condition and results of operations. If we are unable to hire, retain and motivate qualified personnel, our business may suffer. Our future success depends, in part, on our ability to continue to attract and retain highly skilled personnel. The loss of the services of any of our key personnel, the inability to attract or retain qualified personnel or delays in hiring required personnel, particularly in engineering and sales, may seriously harm our business, financial condition and results of operations. Any of our employees may terminate their employment at any time. Competition for highly skilled personnel is frequently intense, especially within our industry, and we may not be able to compete for such personnel. We are required under accounting principles generally accepted in the United States (U. S. GAAP) to recognize compensation expense in our operating results for employee stock- based compensation under our equity grant programs, which may negatively impact our operating results and may increase the pressure to limit stock- based compensation that we might otherwise offer to current or potential employees, thereby potentially harming our ability to attract or retain highly skilled personnel. In addition, to the extent we hire personnel from competitors, we may be subject to allegations that they have been improperly solicited or divulged proprietary or other confidential information, which could result in a diversion of management' s time and our resources. A portion of our revenues are generated by sales to government entities, which are subject to a number of challenges and risks. Government entities have historically been particularly concerned about adopting cloud- based solutions for their operations, including security solutions, and increasing sales of subscriptions for our solutions to government entities may be more challenging than selling to commercial organizations. Selling to government entities can be highly competitive, expensive and time- consuming, often requiring significant upfront time and expense without any assurance that we will win a sale. We have invested in the creation of a cloud offering certified under the Federal Information Security Management Act for government usage but we cannot be sure that we will continue to sustain or renew this certification, that the government will continue to mandate such certification or that other government agencies or entities will use this cloud offering. Government demand and payment for our solutions may be impacted by public sector budgetary cycles and funding authorizations, with funding reductions or delays adversely affecting public sector demand for our solutions. Government entities may have contractual or other legal rights to terminate contracts with our channel partners for convenience or due to a

default, and any such termination may adversely impact our future results of operations. Governments routinely investigate and audit government contractors' administrative processes, and any unfavorable audit could result in the government refusing to continue buying our solutions, a reduction of revenues or fines or civil or criminal liability if the audit uncovers improper or illegal activities. Any such penalties could adversely impact our results of operations in a material way. Our success in acquiring and integrating other businesses, products or technologies could impact our financial position. In order to remain competitive, we have in the past and may in the future seek to acquire additional businesses, products, services or technologies. For example, we acquired certain intellectual property of ~~Spell Security on July 24, 2020, certain intellectual property of~~ TotalCloud on August 19, 2021 and certain assets of Blue Hexagon on October 4, 2022. The environment for acquisitions in our industry is very competitive and acquisition candidate purchase prices may exceed what we would prefer to pay. Moreover, achieving the anticipated benefits of past and future acquisitions will depend in part upon whether we can integrate acquired operations, products and technology in a timely and cost- effective manner, and even if we achieve benefits from acquisitions, such acquisitions may still be viewed negatively by customers, financial markets or investors. The acquisition and integration process is complex, expensive and time- consuming, and may cause an interruption of, or loss of momentum in, product development and sales activities and operations of both companies, as well as divert the attention of management, and we may incur substantial cost and expense. We may issue equity securities which could dilute current stockholders' ownership, incur debt, assume contingent or other liabilities and expend cash in acquisitions, which could negatively impact our financial position, stockholder equity and stock price. We may not find suitable acquisition candidates, and acquisitions we complete may be unsuccessful. If we consummate a transaction, we may be unable to integrate and manage acquired products and businesses effectively or retain key personnel. If we are unable to effectively execute acquisitions, our business, financial condition and operating results could be adversely affected. We rely on software- as- a- service vendors to operate certain functions of our business and any failure of such vendors to provide services to us could adversely impact our business and operations. We rely on third- party software- as- a- service vendors to operate certain critical functions of our business, including financial management and human resource management. If these services become unavailable due to extended outages or interruptions or because they are no longer available on commercially reasonable terms or prices, our expenses could increase, our ability to manage our finances could be interrupted and our processes for managing sales of our solutions and supporting our customers could be impaired until equivalent services, if available, are identified, obtained and integrated, all of which could harm our business. Incorrect or improper implementation or use of our solutions could result in customer dissatisfaction and harm our business and reputation. If our customers are unable to implement our solutions successfully, customer perceptions of our platform and solutions may be impaired or our reputation and brand may suffer. Our customers have in the past inadvertently misused our solutions, which triggered downtime in their internal infrastructure until the problem was resolved. Additionally, any failure to implement and configure our solutions correctly may result in our solutions failing to detect vulnerabilities or compliance issues, or otherwise to perform effectively, and may result in disruptions to our customers' IT environments and businesses. Any misuse of our solutions, including any failure to implement and configure them appropriately, could result in disruption to our customers' businesses, customer dissatisfaction, negative impacts on the perceived reliability or effectiveness of our solutions, and claims and litigation, and may result in negative press coverage, negative effects on our reputation and competitive position, a loss of sales, customers, and channel partners, and harm our financial results. We recognize revenues from subscriptions over the term of the relevant service period, and therefore any decreases or increases in bookings are not immediately reflected in our operating results. We recognize revenues from subscriptions over the term of the relevant service period, which is typically one year. As a result, most of our reported revenues in each quarter are derived from the recognition of deferred revenues relating to subscriptions entered into during previous quarters. Consequently, a shortfall in demand for our solutions in any period may not significantly reduce our revenues for that period, but could negatively affect revenues in future periods. Accordingly, the effect of significant downturns in bookings may not be fully reflected in our results of operations until future periods. We may be unable to adjust our costs and expenses to compensate for such a potential shortfall in revenues. Our subscription model also makes it difficult for us to rapidly increase our revenues through additional bookings in any period, as revenues are recognized ratably over the subscription period. Our business is subject to the risks of earthquakes, fire, power outages, floods and other catastrophic events, and to interruption by man- made problems such as terrorism. A significant natural disaster, such as an earthquake, fire or a flood, or a significant power outage could have a material adverse impact on our business, operating results and financial condition. Our corporate headquarters and a significant portion of our operations are located in the San Francisco Bay Area, a region known for seismic activity. In addition, natural disasters could affect our business partners' ability to perform services for us on a timely basis. In the event we or our business partners are hindered by any of the events discussed above, our ability to provide our solutions to customers could be delayed, resulting in our missing financial targets, such as revenues and net income, for a particular quarter. Further, if a natural disaster occurs in a region from which we derive a significant portion of our revenues, customers in that region may delay or forego subscriptions of our solutions, which may materially and adversely impact our results of operations for a particular period. In addition, war, acts of terrorism, pandemics or other health emergencies, or responses to these events could cause disruptions in our business or the business of our business partners, customers or the economy as a whole. All of the aforementioned risks may be exacerbated if the disaster recovery plans for us and our suppliers prove to be inadequate. To the extent that any of the above results in delays of customer subscriptions or commercialization of our solutions, our business, financial condition and results of operations could be adversely affected. Risks Related to Intellectual Property, Legal, Tax and Regulatory Matters Undetected software errors or flaws in our solutions could harm our reputation, decrease market acceptance of our solutions or result in liability. Our solutions may contain undetected errors or defects when first introduced or as new versions are released. We have experienced these errors or defects in the past in connection with new solutions and solution 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 of these solutions. Since our

customers use our solutions for IT, security and compliance reasons, any errors, defects, disruptions in service or other performance problems with our solutions, or any other failure of our solutions to detect vulnerabilities or compliance problems or otherwise to perform effectively, may result in disruptions or damage to the business of our customers, including security breaches or compliance failures. Additionally, any such issues, or the perception that they have occurred, whether or not relating to any actual or perceived error or defect in our solutions, could hurt our reputation and competitive position and we may incur significant costs, the attention of key personnel could be diverted, our customers may delay or withhold payment to us or elect not to renew, we could face a loss of sales, customers, and channel partners, and other significant problems with our relationships with customers and channel partners may arise. We may also be subject to liability claims for damages related to actual or perceived errors or defects in our solutions. A material liability claim or other occurrence that harms our reputation or decreases market acceptance of our solutions may harm our business, competitive and financial position, and operating results. Although we maintain insurance coverage that may be applicable to certain liabilities in connection with these matters, we cannot be certain that our insurance coverage will be adequate for liabilities that actually are incurred, that insurance will continue to be available to us on economically reasonable terms, or at all, or that any insurer will not deny coverage as to any future claim. The successful assertion of one or more large claims against us that exceed available insurance coverage or the occurrence of changes in our insurance policies, including premium increases or the imposition of large deductible or co- insurance requirements, could have a material and adverse effect on our business, including our financial condition, operating results and reputation. Our solutions could be used to collect and store personal information of our customers' employees or customers, and therefore privacy and other data handling concerns could result in additional cost and liability to us or inhibit sales of our solutions. We collect the names and email addresses of our customers in connection with subscriptions to our solutions. Additionally, the data that our solutions collect to help secure and protect the IT infrastructure of our customers may include additional personal or confidential information of our customers' employees and their customers **, and we may collect, store and otherwise process personal or confidential information more generally in connection with our business and operations** . Personal privacy has become a significant issue in the United States and in many other countries where we offer our solutions. The regulatory framework for privacy issues worldwide is currently evolving and is likely to remain uncertain for the foreseeable future. Many federal, state and foreign government bodies and agencies have adopted or are considering adopting laws and regulations regarding the collection, use, disclosure and retention of personal information. In the United States, these include, for example, rules and regulations promulgated under the authority of the Federal Trade Commission, the Health Insurance Portability and Accountability Act of 1996, the Gramm- Leach- Bliley Act, and state breach notification laws. Internationally, virtually every jurisdiction in which we operate has established its own data security and privacy legal framework with which we or our customers must comply. These privacy, data protection and information security laws and regulations may result in ever- increasing regulatory and public scrutiny and escalating levels of enforcement and sanctions. Additionally, new laws and regulations relating to privacy and data protection continue to be proposed and enacted. For example, the European Union has adopted the Global Data Protection Regulation (" GDPR "). This regulation, which took effect in May of 2018, provides for substantial obligations relating to the handling, storage and other processing of data relating to individuals and administrative fines for violations, which can be up to four percent of the previous year' s annual revenue or € 20 million, whichever is higher. The GDPR may be subject to new or changing interpretations by courts, and our interpretation of the law and efforts to comply with the rules and regulations of the law may be ruled invalid. Similarly, the California Consumer Privacy Act (" CCPA ") requires covered companies to, among other things, provide new disclosures to California consumers and affords such consumers new rights to opt- out of certain sales of personal information. The CCPA also creates a private right of action for statutory damages for certain breaches of information. ~~Certain aspects of the CCPA and its interpretation remain uncertain and are likely to remain uncertain for an extended period.~~ Additionally ~~, a new privacy law~~ , the California Privacy Rights Act (" CPRA "), was approved by voters in the November 3, 2020 election. The CPRA ~~modifies~~ **modified** the CCPA significantly, creating obligations relating to consumer data beginning on January 1, 2022, ~~and~~ **with** enforcement **authorized as of** ~~is expected to commence on~~ July 1, 2023 ~~. Passage of the CPRA has resulted in further uncertainty and may require us to incur additional costs and expenses in an effort to comply~~ . In addition, other states have enacted or proposed legislation that regulates the collection, use, and sale of personal information, **including** ~~and such regimes might not be compatible with the GDPR~~ , **for example, Washington' s My Health, My Data Act and legislation similar to** the CCPA ~~or~~ **adopted in Virginia, Colorado, Utah, Connecticut, Iowa, Indiana, Montana, Tennessee, Oregon, Florida, Delaware, and Texas. Aspects of** the **CCPA,** CPRA ~~or may require us to undertake additional practices. Accordingly~~ , ~~we~~ **and these other new and evolving state laws, as well their interpretation and enforcement, remain uncertain. We** cannot ~~yet~~ predict the impact of the CCPA, ~~CRPA~~ **CPRA ,** or other evolving privacy and data protection obligations on our business or operations, but ~~it~~ **they** may require us to modify our data processing practices and policies and incur substantial costs and expenses in an effort to comply. The privacy, data protection, and information security laws and regulations we must comply with also are subject to change. For example, the United Kingdom **has** enacted a Data Protection Act ~~in May 2018~~ **, and has implemented legislation referred to as the " UK GDPR, "** that substantially ~~implements~~ **implement** the GDPR **in** ~~, but~~ the United Kingdom ~~'~~ **following the United Kingdom'** s exit from the European Union ~~, commonly referred~~ **. This legislation provides for substantial penalties for noncompliance of up** to **the greater of £ 17. 5 million or four percent of the previous year' s annual revenues. While the European Union** ~~as~~ **has deemed the United Kingdom an** " ~~Brexit,~~ **adequate country** " **to which personal data** could ~~lead~~ **be exported from the European Economic Area (" EEA "), this decision is required** to ~~further legislative~~ **be renewed after four years of being in effect** and ~~regulatory changes~~ **may be modified, revoked, or challenged in the interim, creating uncertainty regarding transfers of personal data to the United Kingdom from the EEA** . It remains unclear how United Kingdom data protection laws or regulations will develop in the medium to longer term and how data transfers to and from the United Kingdom will be regulated. Additionally, we have ~~joined~~ **self- certified under**

the EU- U. S. **Data** Privacy ~~Shield~~ Framework and a related program, the Swiss- U. S. **Data** Privacy ~~Shield~~ Framework, and **have** adopted certain standard contractual clauses approved by the European Commission (" SCCs ") as part of our data processing agreements with regard to certain transfers of personal data from the ~~European Economic Area (" EEA ")~~ to the U. S. ~~to ensure that we work with vendors that have adopted the same, where appropriate. While both~~ **Both** the EU- U. S. **Data** Privacy ~~Shield~~ Framework and SCCs have **, however,** been subject to legal challenge **. In its** ~~, we continue to analyze the~~ July **16,** 2020 **opinion,** ~~" Schrems II " decision by~~ the ~~Court of Justice of the~~ **CJEU imposed additional obligations on companies when relying on SCCs to transfer personal data. The** European ~~Union~~ **Commission has published revised SCCs addressing the CJEU concerns on June 4, 2021, that are required to be implemented. The United Kingdom has adopted new standard contractual clauses** (" ~~CJEU~~ **UK SCCs** ") **, that became effective as of March 21, 2022,** and ~~its impact on our~~ **which also are required to be implemented. The EU- U. S. Data Privacy Framework, Swiss- U. S. Data Privacy Framework revised SCCs and UK SCCs, guidance and opinions of regulators, and other developments relating to cross- border** data transfer ~~mechanisms as well as subsequent guidance from data privacy regulators and new SCCs published by the European Commission in June 2021, and we~~ may **require us** ~~find it necessary or appropriate~~ to **implement** ~~take different or~~ additional ~~steps with respect to transfers of~~ **contractual and technical safeguards for any** personal data **transferred out of Europe** , which may ~~result in~~ **increase compliance costs, lead to** increased **regulatory scrutiny** ~~costs of compliance and limitations on our~~ **or** ~~customers~~ **liability,** and ~~us~~ **which may adversely impact our business, financial condition and operating results** . We may be unsuccessful in maintaining legitimate means for our transfer and receipt of personal data from the EEA or Switzerland. We may experience reluctance or refusal by current or prospective European customers to use our products, and we and our customers may face a risk of enforcement actions by data protection authorities in the EEA relating to personal data transfers to us and by us from the EEA. Any such enforcement actions could result in substantial costs and diversion of resources, distract management and technical personnel and negatively affect our business, operating results and financial condition. Some countries also are considering or have passed legislation requiring local storage and processing of data, or similar requirements, which could increase the cost and complexity of delivering our services. In addition to laws and regulations, privacy advocacy and industry groups or other private parties may propose new and different privacy standards that either legally or contractually apply to us. Because the interpretation and application of privacy and data protection laws, regulations, standards and contractual obligations are uncertain, it is possible that they may be interpreted and applied in a manner that is, or perceived to be, inconsistent with our data management practices or the features of our solutions. If so, in addition to the possibility of regulatory investigations and enforcement actions, fines, lawsuits and other claims, other forms of injunctive or operations- limiting relief, and damage to our reputations and loss of goodwill, we could be required to fundamentally change our business activities and practices or modify our solutions and may face limitations in our ability to develop new solutions and features, any of which could have an adverse effect on our business. Any inability to adequately address privacy concerns, even if unfounded, or any actual or perceived inability to comply with applicable privacy or data protection laws, regulations and privacy standards, could result in cost and liability to us, damage our reputation, inhibit sales of subscriptions and harm our business. Furthermore, the costs of compliance with, and other burdens imposed by, the laws, regulations, and privacy standards that are applicable to the businesses of our customers may limit the use and adoption of, and reduce the overall demand for, our solutions. Privacy concerns, whether valid or not valid, may inhibit market adoption of our solutions particularly in certain industries and foreign countries **. We use AI / machine learning technologies in our solutions that could result in harm to our business and operating results. We have incorporated and may continue to incorporate additional AI / machine learning solutions and features into our solutions, and these solutions and features may become more important to our operations or to our future growth over time. We expect to rely on AI / machine learning solutions and features to help drive future growth in our business, but there can be no assurance that we will realize the desired or anticipated benefits from AI / machine learning or at all. We may also fail to properly implement or market our AI / machine learning solutions and features. Our competitors or other third parties may incorporate AI / machine learning into their products, offerings, and solutions more quickly or more successfully than us, which could impair our ability to compete effectively and adversely affect our results of operations. Additionally, our offerings based on AI / machine learning may expose us to additional claims, demands and proceedings by private parties and regulatory authorities and subject us to legal liability as well as brand and reputational harm. The legal, regulatory, and policy environments around AI / machine learning are evolving rapidly, and we may become subject to new and evolving legal and other obligations. These and other developments may require us to make significant changes to our use of AI / machine learning, including by limiting or restricting our use of AI / machine learning, and which may require us to make significant changes to our policies and practices, which may necessitate expenditure of significant time, expense, and other resources, AI / machine learning also presents emerging ethical issues that could harm our reputation and business if our use of AI / machine learning becomes controversial** . Our solutions contain third- party open source software components, and our failure to comply with the terms of the underlying open source software licenses could restrict our ability to sell our solutions. Our solutions contain software licensed to us by third- parties under so- called " open source " licenses, including the GNU General Public License, the GNU Lesser General Public License, the BSD License, the Apache License and others. 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. If we combine our proprietary software with open source software in certain ways, we could, in some circumstances, be required to release the source code of our proprietary software to the public. Disclosing the source code of our proprietary software could make it easier for cyber attackers and other third parties to discover vulnerabilities in or to defeat the protections of our solutions, which could result in our solutions failing to provide our customers with the security they expect from our services. This could harm our business and reputation. Disclosing our proprietary source code also could allow our competitors to create similar products with lower development effort and time and ultimately could result in a loss of sales for us. Any of these events could have a material adverse effect on our business, operating results and financial condition. 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 solutions 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 solutions. In this event, we could be required to seek licenses from third parties to continue offering our solutions, to make our proprietary code generally available in source code form, to re- engineer our solutions or to discontinue the sale of our solutions if re- engineering could not be accomplished on a timely basis, any of which could adversely affect our business, operating results and financial condition. We use third- party software and data that may be difficult to replace or cause errors or failures of our solutions that could lead to lost customers or harm to our reputation and our operating results. We license third- party software as well as security and compliance data from various third parties to deliver our solutions. In the future, this software or data may not be available to us on commercially reasonable terms, or at all. Any loss of the right to use any of this software or data could result in delays in the provisioning of our solutions until equivalent technology or data is either developed by us, or, if available, is identified, obtained and integrated, which could harm our business. In addition, any errors or defects in or failures of this third- party software or data could result in errors or defects in our solutions or cause our solutions to fail, which could harm our business and be costly to correct. Many of these providers attempt to impose limitations on their liability for such errors, defects or failures, and if enforceable, we may have additional liability to our customers or third- party providers that could harm our reputation and increase our operating costs. We will need to maintain our relationships with third- party software and data providers, and to obtain software and data from such providers that do not contain any errors or defects. Any failure to do so could adversely impact our ability to deliver effective solutions to our customers and could harm our operating results. Failure to protect our proprietary technology and intellectual property rights could substantially harm our business and operating results. The success of our business depends in part on our ability to protect and enforce our trade secrets, trademarks, copyrights, patents and other intellectual property rights. We attempt to protect our intellectual property under copyright, trade secret, patent and trademark laws, and through a combination of confidentiality procedures, contractual provisions and other methods, all of which offer only limited protection. We primarily rely on our unpatented proprietary technology and trade secrets. Despite our efforts to protect our proprietary technology and trade secrets, unauthorized parties may attempt to misappropriate, reverse engineer or otherwise obtain and use them. The contractual provisions that we enter into with employees, consultants, partners, vendors and customers may not prevent unauthorized use or disclosure of our proprietary technology or intellectual property rights and may not provide an adequate remedy in the event of unauthorized use or disclosure of our proprietary technology or intellectual property rights. Moreover, policing unauthorized use of our technologies, solutions 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. We may be unable to determine the extent of any unauthorized use or infringement of our solutions, technologies or intellectual property rights. The process of obtaining patent protection is expensive and time- consuming, and we may not be able to prosecute all necessary or desirable patent applications at a reasonable cost or in a timely manner, if at all. We may choose not to seek patent protection for certain innovations and may choose not to pursue patent protection in certain jurisdictions. Furthermore, it is possible that our patent applications may not result in granted patents, that the scope of our issued patents will be limited or not provide the coverage originally sought, that our issued patents will not provide us with any competitive advantages, or that our patents and other intellectual property rights may be challenged by others or invalidated through administrative processes or litigation. In addition, issuance of a patent does not guarantee that we have an absolute right to practice the patented invention. As a result, we may not be able to obtain adequate patent protection or to enforce our issued patents effectively. From time to time, legal action by us may be necessary to enforce our patents and other intellectual property rights, to protect our trade secrets, to determine the validity and scope of the intellectual property rights of others or to defend against claims of infringement or invalidity. Such litigation could result in substantial costs and diversion of resources and could negatively affect our business, operating results and financial condition. If we are unable to protect our intellectual property rights, we may find ourselves at a competitive disadvantage to others who need not incur the additional expense, time and effort required to create the innovative solutions that have enabled us to be successful to date. Assertions by third parties of infringement or other violations by us of their intellectual property rights could result in significant costs and harm our business and operating results. Patent and other intellectual property disputes are common in our industry. Some companies, including some of our competitors, own large numbers of patents, copyrights and trademarks, which they may use to assert claims against us. Third parties may in the future assert claims of infringement, misappropriation or other violations of intellectual property rights against us. They may also assert such claims against our customers or channel partners whom we typically indemnify against claims that our solutions infringe, misappropriate or otherwise violate the intellectual property rights of third parties. As the numbers of products and competitors in our market increase and overlaps occur, claims of infringement, misappropriation and other violations of intellectual property rights may increase. Any claim of infringement, misappropriation or other violation of intellectual property rights by a third party, even those without merit, could cause us to incur substantial costs defending against the claim and could distract our management from our business. The patent portfolios of our most significant competitors are larger than ours. This disparity

may increase the risk that they may sue us for patent infringement and may limit our ability to counterclaim for patent infringement or settle through patent cross- licenses. In addition, future assertions of patent rights by third parties, and any resulting litigation, may involve patent holding companies or other adverse patent owners who have no relevant product revenues and against whom our own patents may therefore provide little or no deterrence or protection. There can be no assurance that we will not be found to infringe or otherwise violate any third- party intellectual property rights or to have done so in the past. An adverse outcome of a dispute may require us to: • pay substantial damages, including treble damages, if we are found to have willfully infringed a third party' s patents or copyrights; • cease making, licensing or using solutions that are alleged to infringe or misappropriate the intellectual property of others; • expend additional development resources to attempt to redesign our solutions or otherwise develop non- infringing technology, which may not be successful; • enter into potentially unfavorable royalty or license agreements in order to obtain the right to use necessary technologies or intellectual property rights; and • indemnify our partners and other third parties. In addition, royalty or licensing agreements, if required or desirable, may be unavailable on terms acceptable to us, or at all, and may require significant royalty payments and other expenditures. Some licenses may also be non- exclusive, and therefore our competitors may have access to the same technology licensed to us. Any of the foregoing events could seriously harm our business, financial condition and results of operations. Governmental export or import controls could subject us to liability if we violate them or limit our ability to compete in foreign markets. Our solutions are subject to U. S. export controls, specifically, the Export Administration Regulations and economic sanctions enforced by the Office of Foreign Assets Control. We incorporate encryption technology into certain of our solutions. These encryption solutions and the underlying technology may be exported only with the required export authorizations, including by license, a license exception or other appropriate government authorizations. U. S. export controls may require submission of an encryption registration, product classification and / or annual or semi- annual reports. Governmental regulation of encryption technology and regulation of imports or exports of encryption products, or our failure to obtain required import or export authorization for our solutions, when applicable, could harm our international sales and adversely affect our revenues. Compliance with applicable regulatory requirements regarding the export of our solutions, including with respect to new releases of our solutions, may create delays in the introduction of our solutions in international markets, prevent our customers with international operations from deploying our solutions throughout their globally- distributed systems or, in some cases, prevent the export of our solutions to some countries altogether. In addition, various countries regulate the import of our appliance- based solutions and have enacted laws that could limit our ability to distribute solutions or could limit our customers' ability to implement our solutions in those countries. Any new export or import restrictions, new legislation or shifting approaches in the enforcement or scope of existing regulations, or in the countries, persons or technologies targeted by such regulations, could result in decreased use of our solutions by existing customers with international operations, declining adoption of our solutions by new customers with international operations and decreased revenues. If we fail to comply with export and import regulations, we may be fined or other penalties could be imposed, including denial of certain export privileges. If we are required to collect higher sales and use or other taxes on the solutions we sell, we may be subject to liability for past sales and our future sales may decrease. Taxing jurisdictions, including state and local entities, have differing rules and regulations governing sales and use or other taxes, and these rules and regulations are subject to varying interpretations that may change over time. In particular, the applicability of sales taxes to our subscription services in various jurisdictions is unclear. It is possible that we could face sales tax audits and that our liability for these taxes could exceed our estimates as tax authorities could still assert that we are obligated to collect additional amounts as taxes from our customers and remit those taxes to those authorities. We could also be subject to audits with respect to state and international jurisdictions for which we may not have accrued tax liabilities. A successful assertion that we should be collecting additional sales or other taxes on our services in jurisdictions where we have not historically done so and do not accrue for sales taxes could result in substantial tax liabilities for past sales, discourage customers from purchasing our solutions or otherwise harm our business and operating results. Changes in our income tax provision or adverse outcomes resulting from examination of our income tax returns could adversely affect our operating results. We could be subject to additional taxes. We are subject to income taxes in the United States and various foreign jurisdictions, and our domestic and international tax liabilities are subject to the allocation of expenses in differing jurisdictions. Our tax rate is affected by changes in the mix of earnings and losses in countries with differing statutory tax rates, certain non- deductible expenses ~~and~~ **,** excess tax benefits arising from stock- based compensation, other tax benefits and credits, and the valuation of deferred tax assets and liabilities. Increases in our effective tax rate could harm our operating results. Additionally, significant judgment is required in evaluating our tax positions and our worldwide tax provisions. During the ordinary course of business, there are many activities and transactions for which the ultimate tax determination is uncertain. In addition, our tax obligations and effective tax rates could be adversely affected by changes in the relevant tax, accounting and other laws, regulations, principles and interpretations, including those relating to income tax nexus, by recognizing tax losses or lower than anticipated earnings in jurisdictions where we have lower statutory rates and higher than anticipated earnings in jurisdictions where we have higher statutory rates, by changes in foreign currency exchange rates, or by changes in the valuation of our deferred tax assets and liabilities. The ~~United States~~ **Tax Cuts and Jobs Act of 2017** introduced a ~~new 1 % excise~~ **Base Erosion and Anti- Abuse Tax which imposes a minimum** tax on ~~share repurchases occurring~~ **adjusted income of corporations with average applicable gross receipt of at least $ 500 million for prior three tax years and that make certain payments to related foreign persons. While these rules do not impact our results of operations in the current year, these could impact our financial results in future periods. The Organization for Economic Cooperation and Development has issued model rules in connection with the Base Erosion and Profit Shifting integrated framework that determine multi- jurisdictional taxing rights (Pillar One) and the minimum rate of tax applicable to certain types of income (Pillar Two). Many countries have enacted legislation to apply the Pillar Two directive for tax years beginning in January 2024, which generally provides for a minimum effective tax rate of 15 %** on ~~or after January 1, 2023 as part of~~ the

income arising in each jurisdiction where ~~Inflation Reduction Act. The amount of share repurchases subject to~~ the **Company operates** ~~excise tax will be reduced by the fair market value of any shares issued during the taxable year~~ . We do not ~~expect this provision~~ **anticipate these rules** to have **an** ~~a material~~ impact ~~to~~ **on** our **current year' s financial** results **. If applicable in the future, these could have an impact on our financial results, the extent** of ~~operations~~ **which is currently uncertain** . We may be audited in various jurisdictions, and such jurisdictions may assess additional taxes, sales taxes and value- added taxes against us. Although we believe our tax estimates are reasonable, the final determination of any tax audits or litigation could be materially different from our historical tax provisions and accruals, which could have a material adverse effect on our operating results or cash flows in the period or periods for which a determination is made. Risks Related to Ownership of Our Common Stock Market volatility may affect our stock price and the value of an investment in our common stock and could subject us to litigation. The trading price of our common stock has been, and may continue to be, subject to significant fluctuations in response to a number of factors, most of which we cannot predict or control, including: • announcements of new solutions, services or technologies, commercial relationships, acquisitions or other events by us or our competitors; • fluctuations in stock market prices and trading volumes of securities of similar companies; • general market conditions and overall fluctuations in U. S. equity markets; • variations in our operating results, or the operating results of our competitors; • changes in our financial guidance or securities analysts' estimates of our financial performance; • changes in accounting principles; • sales of large blocks of our common stock, including sales by our executive officers, directors and significant stockholders; • additions or departures of any of our key personnel; • announcements related to litigation; • changing legal or regulatory developments in the United States and other countries; and • discussion of us or our stock price by the financial press and in online investor communities. In addition, the stock market in general, and the stocks of technology companies such as ours in particular, have experienced substantial price and volume volatility that is often seemingly unrelated to the operating performance of particular companies. These broad market fluctuations may cause the trading price of our common stock to decline. In the past, securities class action litigation has often been brought against a company after a period of volatility in the trading price of its common stock. We may become involved in this type of litigation in the future. Any securities litigation claims brought against us could result in substantial expenses and the diversion of our management' s attention from our business. Our actual operating results may differ significantly from our guidance. From time to time, we have released, and may continue to release, guidance in our quarterly earnings conference calls, quarterly earnings releases, or otherwise, regarding our future performance that represents our management' s estimates as of the date of release. This guidance, which includes forward- looking statements, has been and will be based on projections prepared by our management. These projections are not prepared with a view toward compliance with published guidelines of the American Institute of Certified Public Accountants, and neither our registered public accountants nor any other independent expert or outside party compiles or examines the projections. Accordingly, no such person expresses any opinion or any other form of assurance with respect to the projections. Projections are based upon a number of assumptions and estimates that, while presented with numerical specificity, are inherently subject to significant business, economic and competitive uncertainties and contingencies, many of which are beyond our control and are based upon specific assumptions with respect to future business decisions, some of which will change. We intend to state possible outcomes as high and low ranges which are intended to provide a sensitivity analysis as variables are changed but are not intended to imply that actual results could not fall outside of the suggested ranges. The principal reason that we release guidance is to provide a basis for our management to discuss our business outlook with analysts and investors. We do not accept any responsibility for any projections or reports published by any such third parties. Guidance is necessarily speculative in nature, and it can be expected that some or all of the assumptions underlying the guidance furnished by us will not materialize or will vary significantly from actual results. Accordingly, our guidance is only an estimate of what management believes is realizable as of the date of release. Actual results may vary from our guidance and the variations may be material. In light of the foregoing, investors are urged not to rely upon our guidance in making an investment decision regarding our common stock. Any failure to successfully implement our operating strategy or the occurrence of any of the events or circumstances set forth in this " Risk Factors " section in this Annual Report on Form 10- K could result in our actual operating results being different from our guidance, and the differences may be adverse and material. Future sales of shares by existing stockholders could cause our stock price to decline. The market price of shares of our common stock could decline as a result of substantial sales of our common stock, particularly sales by our directors, executive officers, employees and significant stockholders, a large number of shares of our common stock becoming available for sale, or the perception in the market that holders of a large number of shares intend to sell their shares. As of December 31, ~~2022~~ **2023** , we had approximately ~~37~~ **36** . ~~4~~ **9** million shares of our common stock outstanding. In addition, as of December 31, ~~2022~~ **2023** , there were approximately 1. ~~8~~ **4** million options and 1. 1 million restricted stock units outstanding. If such options are exercised and restricted stock units are released, these additional shares will become available for sale. As of December 31, ~~2022~~ **2023** , we had an aggregate of ~~2~~ **1** . ~~4~~ **8** million shares of our common stock reserved for future issuance under our Restated 2012 Equity Incentive Plan and 0. ~~6~~ **5** million shares reserved for future purchase under our 2021 Employee Stock Purchase Plan, which can be freely sold in the public market upon issuance. If a large number of these shares are sold in the public market, the sales could reduce the trading price of 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 February 12, 2018, we announced that our board of directors had authorized a $ 100. 0 million repurchase program. On each of October 30, 2018, October 30, 2019, May 7, 2020, February 10, 2021 and February 9, 2023, we announced that our board of directors had authorized an increase of $ 100. 0 million, and on each of November 3, 2021 and May 4, 2022, we announced that our board of directors had authorized an increase of $ 200. 0 million to the share repurchase program **. On February 7, 2024 we announced that our board of directors had authorized an increase of $ 200. 0 million to the share repurchase program** , resulting in an aggregate authorization of $ 1. ~~0~~ **2** billion to date ($ ~~900~~ **1** . 0 ~~million~~ **billion** as of December 31, ~~2022~~ **2023**). Although our board of

directors authorized the share repurchase program, we are not obligated to repurchase any specific dollar amount or to acquire any specific number of shares. The share repurchase program could affect the price of our common stock, increase volatility and diminish our cash reserves. In addition, it may be suspended or terminated at any time, which may result in a decrease in the price of our common stock. Finally, our share repurchases in 2023 **were** ~~will be~~ subject to a new 1 % excise tax introduced in the Inflation Reduction Act. The amount of share repurchases subject to the excise tax **are** ~~will be~~ reduced by the fair market value of any shares ~~issues~~ **issued** during the taxable year. ~~We~~ **This provision does not currently, nor** do ~~not~~ **we** expect **it** ~~this provision~~ to **in the future,** have a material impact to our results of operations. During the year ended December 31, ~~2022~~ **2023** , we repurchased ~~2~~ **1** . ~~5~~ **3** million shares of our common stock for approximately $ ~~317~~ **170** . ~~3~~ **8** million. As of December 31, ~~2022~~ **2023** , approximately $ ~~154~~ **83** . ~~5~~ **7** million remained available for share repurchases pursuant to our share repurchase program. We do not intend to pay dividends on our common stock and therefore any returns will be limited to the value of our stock. We have never declared or paid any cash dividend on our common stock. We currently anticipate that we will retain future earnings for the development, operation and expansion of our business and do not anticipate declaring or paying any cash dividends for the foreseeable future. Any return to stockholders will therefore be limited to the value of their stock. Anti- takeover provisions in our charter documents and under Delaware law could make an acquisition of us, which may be beneficial to our stockholders, more difficult and may prevent attempts by our stockholders to replace or remove our current management. Our amended and restated certificate of incorporation and amended and restated bylaws contain provisions that may delay or prevent an acquisition of us or a change in our management. These provisions include: • authorizing " blank check " preferred stock, which could be issued by our board of directors without stockholder approval and may contain voting, liquidation, dividend and other rights superior to our common stock, which would increase the number of outstanding shares and could thwart a takeover attempt; • a classified board of directors whose members can only be dismissed for cause; • the prohibition on actions by written consent of our stockholders; • the limitation on who may call a special meeting of stockholders; • the establishment of advance notice requirements for nominations for election to our board of directors or for proposing matters that can be acted upon at stockholder meetings; and • the requirement of at least two- thirds of the outstanding capital stock to amend any of the foregoing second through fifth provisions. In addition, because we are incorporated in Delaware, we are governed by the provisions of Section 203 of the Delaware General Corporation Law, which limits the ability of stockholders owning in excess of 15 % of our outstanding voting stock to merge or combine with us. Although we believe these provisions collectively provide for an opportunity to obtain greater value for stockholders by requiring potential acquirers to negotiate with our board of directors, they would apply even if an offer rejected by our board of directors were considered beneficial by some stockholders. In addition, these provisions may frustrate or prevent any attempts by our stockholders to replace or remove our current management by making it more difficult for stockholders to replace members of our board of directors, which is responsible for appointing the members of our management. General Risk Factors Disruptive technologies could gain wide adoption and supplant our cloud- based IT, security and compliance solutions, thereby weakening our sales and harming our results of operations. The introduction of products and services embodying new technologies could render our existing solutions obsolete or less attractive to customers. Our business could be harmed if new IT, security and compliance technologies are widely adopted. We may not be able to successfully anticipate or adapt to changing technology or customer requirements on a timely basis, or at all. If we fail to keep up with technological changes or to convince our customers and potential customers of the value of our solutions even in light of new technologies, our business could be harmed and our revenues may decline. We may not maintain profitability in the future. We may not be able to sustain or increase our growth or maintain profitability in the future. We plan to continue to invest in our infrastructure, new solutions, research and development and sales and marketing, and as a result, we cannot assure you that we will maintain profitability. We may incur losses in the future for a number of reasons, including without limitation, the other risks and uncertainties described in this Annual Report on Form 10- K. 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 again achieve or maintain profitability in the future. Forecasts of market growth may prove to be inaccurate, and even if the markets in which we compete achieve the forecasted growth, there can be no assurance that our business will grow at similar rates, or at all. Growth forecasts relating to the expected growth in the market for IT, security and compliance and other markets are subject to significant uncertainty and are based on assumptions and estimates which may prove to be inaccurate. Even if these markets experience the forecasted growth, we may not grow our business at similar rates, or at all. Our growth is subject to many factors, including our success in implementing our business strategy, which is subject to many risks and uncertainties. Accordingly, forecasts of market growth should not be taken as indicative of our future growth. Our financial results are based in part on our estimates or judgments relating to our critical accounting policies. These estimates or judgments may prove to be incorrect, which could harm our operating results and result in a decline in our stock price. **The preparation of financial statements in conformity with 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 titled " Part II, Item 7- Management' s Discussion and Analysis of Financial Condition and Results of Operations, " the results of which form the basis for making judgments about the carrying values of assets, liabilities, equity, revenues and expenses that are not readily apparent from other sources. Our operating results may be adversely affected if our assumptions change or if actual circumstances differ from those in our assumptions, which could cause our operating results to fall below the expectations of securities analysts and investors, resulting in a decline in our stock price. Significant assumptions and estimates used in preparing our consolidated financial statements include those related to revenue recognition, accounting for income taxes and stock- based compensation. Changes in financial accounting standards may cause**

adverse and unexpected revenue fluctuations and impact our reported results of operations. We prepare our financial statements in accordance with U. S. GAAP. These principles are subject to interpretation by the SEC and various bodies formed to interpret and create appropriate accounting principles. A change in these accounting standards or practices could harm our operating results and could have a significant effect on our reporting of transactions and reported results and may even retroactively affect previously reported transactions. New accounting pronouncements and varying interpretations of accounting pronouncements have occurred and may occur in the future. Changes to existing rules or the questioning of current practices may harm our operating results or require that we make significant changes to our systems, processes and controls or the way we conduct our business. If we fail to maintain an effective system of internal control over financial reporting, our ability to produce timely and accurate financial statements or comply with applicable regulations could be impaired. As a public company, we are subject to the reporting requirements of the Securities Exchange Act of 1934, or the Exchange Act, the Sarbanes- Oxley Act of 2002, or the Sarbanes- Oxley Act, and the rules and regulations of the NASDAQ Stock Market. To continue to comply with the requirements of being a public company, we may need to undertake various actions, such as implementing additional internal controls and procedures and hiring additional accounting or internal audit staff. Our internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements in accordance with U. S. GAAP. Our current controls and any new controls that we develop may become inadequate because of changes in conditions in our business. Any failure to maintain effective controls, or any difficulties encountered in their improvement, could harm our operating results or cause us to fail to meet our reporting obligations. Any failure to maintain effective internal control over financial reporting also could adversely affect the results of periodic management evaluations regarding the effectiveness of our internal control over financial reporting that we are required to include in our periodic reports we file with the SEC under Section 404 of the Sarbanes- Oxley Act. While we were able to assert in our Annual Report on Form 10- K that our internal control over financial reporting was effective as of December 31, 2023, we cannot predict the outcome of our testing in future periods. If we are unable to assert in any future reporting period that our internal control over financial reporting is effective (or if our independent registered public accounting firm is unable to express an opinion on the effectiveness of our internal controls), investors may lose confidence in our operating results and our stock price could decline. In addition, if we are unable to continue to meet these requirements, we may not be able to remain listed on the NASDAQ Stock Market.