SALT

State of the CISO

A global report on priorities, pain points, and security gaps

2023

Survey conducted by: Global SURVEYZ

Table of Contents

Introduction and Key Findings

Introduction and Methodology

Digital initiatives represent the cornerstone of business innovation today, and the rollout of these new services has had a tremendous impact on companies around the globe. In this survey, we set out to discover how the digital-first economy has specifically impacted the role of the CISO/CSO. In addition to bringing awareness to the evolving role of the CISO, the survey strove to delve into the broader business ramifications of these changes, so organizations can better understand how digital initiatives are impacting risk and how companies can better protect themselves.

The survey asked CISOs about the effects of digitalization across a number of different dimensions – from the top security and personal challenges, to the biggest security control gaps, to the struggle to find good talent, to the impact that global trends are having, to the cyber knowledge level of their boards of directors.

The rapid pace of the digital-first economy has transformed the role of the CISO. For CISOs around the world, the adoption of digitalization has made securing critical data more challenging than ever before. But the challenges extend beyond business impacts. CISOs cite many personal challenges that have also resulted from the acceleration of digitalization. They fear potential litigation as a result of security breaches, they have more job-related stress, they worry about personal liability, and they often don't have enough time to fulfill the requirements of their job.

Global trends have also played a part in transforming the CISO role – in particular, the speed of AI adoption. AI has become more widely used by cyber criminals across the globe, giving them the ability to dramatically scale their attacks and cause harm to organizations. To counter these threats, CISOs themselves must harness the power of AI for good, using it to "catch" and stop AI-driven attacks, putting more pressure on them to quickly adopt new solutions to safeguard their and their customers' critical assets.

Perhaps the most significant findings are the security control gaps that have arisen as a consequence of new digital initiatives. Digitalization has generated multiple security threats and risks, the biggest among them the application programming interface (API). Foundational to how applications are built today, APIs also play a crucial role in other top areas of CISO concern, including third-party vendors/ supply chains and cloud-based applications. This huge and expanding attack surface gives bad actors many access points into organizations' digital applications and data. Consequently, APIs have become an increasingly attractive target for cyber criminals. Why? They're relatively easy to hack, attacks are difficult to detect and can't be found by existing security tooling, and the rewards for successfully hacking APIs are very high because APIs transport companies' most valuable digital data. In fact, the attack surface has grown so significantly, APIs are predicted to become the biggest security vulnerability ever, according to industry research firm Gartner. While awareness of the need for API security has clearly grown, its implementation is not yet pervasive.

Being on the security front lines, CISOs feel the risks of digitalization most sharply. But the potential impact of a digital breach affects the entire enterprise, costing organizations not only in damage to their brand reputation but also in mitigation costs, fines, and potential litigation. Therefore, increasing security for these vital digital initiatives must be a priority for the whole business – not just the security team. C-level executives must do their part to enable and aid the business by prioritizing and funding new security requirements created by digitalization. Digital transformation is all about moving fast. To drive business acceleration, security must "not get in the way" while simultaneously ensuring the safety of the organization's critical data and services. By closing the top security control gaps caused by digitalization, companies can help alleviate the concern that "moving fast could put the business at risk."

Methodology

To get more insight into current priorities, security gaps and pain points for C-level security leaders, we commissioned a survey of 300 CISOs/CSOs.

Global Surveyz Research, an independent survey company, administered the survey online. Respondents represented companies in the US, UK, Western Europe (France, Netherlands) and Brazil, with 500 or more employees, across a variety of industries, including financial services (including fintech), healthcare, insurance, pharmaceutical, and eCommerce.

The respondents were recruited through a global B2B research panel and invited via email to complete the survey, with all responses collected during April 2023. The average amount of time spent on the survey was 7 minutes and 30 seconds. The answers to most of the non-numerical questions were randomized to prevent order bias in the answers.

Key Findings

1 The Healthcare and Financial Services industries face the biggest security impact due to the rapid pace of digital transformation initiatives

The proliferation of modern digital services and applications continues to complicate the security landscape and introduce new security control gaps. 89% of CISOs worldwide agree that moving fast with digital transformation can introduce unforeseen risks in securing organization data (Figure 2). However, of those who agree most strongly (37%), the top two industries (Figure 3) are healthcare (47%) and financial services or technologies (43%), which makes sense, as these sectors are experiencing a comparatively high level of digital innovation and disruption.

Because offering digital services has become critical in these industries to remain competitive and meet consumer expectations, healthcare and financial services organizations introduce new digital services at a faster pace. Consequently, these sectors see more “pain” and challenges earlier – and more frequently – than in other industries. Paradoxically, the survey also shows that these sectors have the most difficulty justifying the cost of security investments to protect new digital transformation initiatives (Figure 5), making the CISO role in healthcare and financial services even more challenging.

2 Almost half of CISOs worldwide have concerns that a security breach in their organization may result in personal litigation and liability

Virtually all respondents (99%) admit they face personal challenges as a result of digital transformation (Figure 6), with the top concerns being personal litigation stemming from security breaches (48%) and increased personal risk/liability (45%).

With several high-profile CISO lawsuits making waves recently, the trend of security leaders opting for roles below CISO level, or requesting indemnification, is growing. CISOs have fears of being found personally liable in the event of a security breach, potentially putting their own livelihood at risk. To alleviate fears, organizations need security processes and tooling that provide CISOs with a comprehensive view into potential security risks. With proven risk mitigation capabilities, CISOs can more effectively demonstrate and close security control gaps, gaining reassurance and lowering their concerns regarding personal liability. At a time when the CISO role is more important than ever, senior-level company executives cannot risk losing the best candidates to worries over personal risk or litigation.

3

78% of CISOs are prioritizing API security more highly than two years ago, and 95% of CISOs say API security is a planned priority over the next two years

With the growth of the digital-first economy over the past couple of years, the usage of APIs has exploded. As the glue that drives all digital initiatives, APIs either directly or indirectly impact most of the top security control gaps. They also have the most potential to impede the success of an organization's digital transformation programs. Given the fact that APIs are embedded into all digital services, it's not surprising that 78% of respondents say their organizations are prioritizing API security more highly now, compared to 2021 (Figure 8). Moreover, CISOs say API security prioritization will increase further, with 95% of CISOs worldwide reporting their organizations have made API security a planned priority over the next two years. The biggest security control gap for CISOs in their digital initiatives (Figure 7) is supply chain/third-party vendors (38%). Because effective data sharing across third parties and supply chains relies on APIs to function, this gap also further highlights the API security pain point. Business innovation, digitalization, cloud migration, and effective API security are all tightly interrelated. Working on these initiatives in a unified way helps businesses reduce their risk.

4

The speed of AI adoption is the global development most impacting the CISO's role

Multiple global developments are contributing to the complexity of the CISO role, including macro-economic uncertainty, the geo- political climate, and layoffs (Figure 11). But the leading global trend impacting CISOs worldwide – when combining respondents' ratings of medium, high, and very high impact – is the speed of AI adoption (94%).

The rise of AI in virtually every industry has transformed the security landscape, and CISOs worry about how this dynamic will affect their organizations. AI serves as a unique cyber defense tool with its ability to quickly analyze large volumes of data and assess and learn from potential attacks. However, AI can also be a security threat. Cyber criminals have already turned to AI for its ability to provide new ways to attack organizations' infrastructures. Using more widely available generative AI technologies, such as Chat GPT, for example, bad actors can generate malicious emails and even script attacks at a much faster rate. CISOs must always understand the adversary, and the adversary is using AI. As CISOs learn to navigate the associated threats and security ramifications of AI, they must also learn to harness AI "defensively" for their organization's security.

5 91% of CISOs say hiring of qualified cybersecurity talent remains a significant issue to deliver digital transformation initiatives

Because digital services introduce new types of cybersecurity attacks, its defense demands new knowledge and capabilities, making the hiring of qualified talent essential. 91% of CISOs say that qualified cybersecurity talent is critical to their ability to deliver digital transformation initiatives (Figure 12). In addition, CISOs cite the lack of qualified cybersecurity talent as the top security challenge resulting from digitalization. (Figure 4). The shortage of sufficiently qualified talent makes it harder for organizations to find and hire people who understand the new technologies and have the skills necessary to address the new security risks and challenges. Moreover, the inability to find and retain qualified security talent can hinder CISOs' – and businesses' – success in a digital-first world.

> As organizations accelerate their digital transformation efforts, they naturally increase the use of APIs in many areas of business and AI. So it's promising to see that their API security efforts are finally moving upward. Sometimes companies can be penny wise but pound foolish when it comes to security investments. But given the high cost of major personal data breaches, API security has to rise in prominence, and do so sharply, in the near future."
>
> – Anton Chuvakin, security advisor at Office of the CISO, Google Cloud

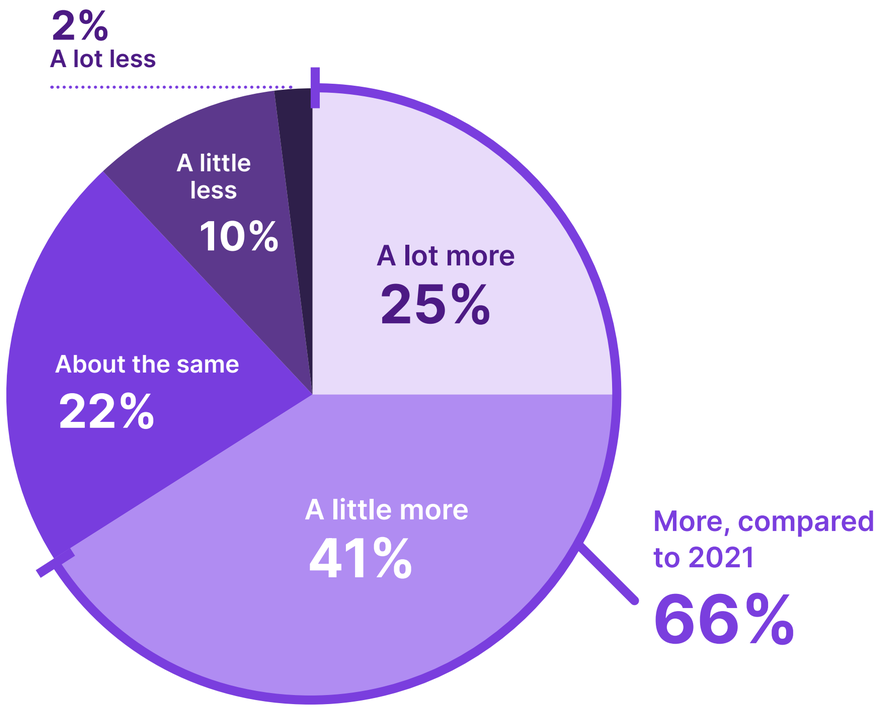
> We are entering the new reality of the "AI era" of cyber. CISOs know that AI attacks are evolving and becoming increasingly sophisticated – and that they're growing at an unprecedented rate. With security teams already at capacity defending a broad attack surface, the impact of escalating AI threats – as well as the necessity to implement an AI offense – clearly weighs heavily on today's CISOs."
>
> – Ed Amoroso, founder and CEO of TAG InfoSphere

Survey Report Findings

Two-Thirds of Companies Are Rolling Out More Digital Services Now Than Two Years Ago

Two thirds (66%) of CISOs worldwide say that they are deploying more digital transformation initiatives now compared to two years ago. Digital services have become essential to deliver modern business innovation, maintain a competitive advantage, and generate revenue growth. Companies lagging behind in digital transformation initiatives will find it increasingly difficult to compete with those who are embracing new digital services and thriving as a result.

Figure 1: Frequency of rolling out new digital services compared to two years ago



Nearly 90% of CISOs say Digital Transformation Introduces Unforeseen Risks

89% of CISOs say that moving fast with digital transformation initiatives introduces unforeseen risks in securing company data, while only 10% slightly disagree with that claim, and a mere 1% very much disagree.

Financial services and healthcare organizations appear to feel the pain of digitalization more acutely than other industries. While 37% of CISOs worldwide say they “very much agree” that digital services create additional risk, the number jumps to 43% for CISOs in financial services and 47% for CISOs in healthcare organizations.

For these industries, in particular, participating in the digital economy is a top business priority. The ability to innovate and bring new services to market quickly is essential to meet changing customer expectations in their sectors. Moreover, ensuring the safety of critical financial and personal health data in these industries is also paramount.

Figure 2: Moving fast with digital transformation initiatives can introduce unforeseen risks in security vital company data

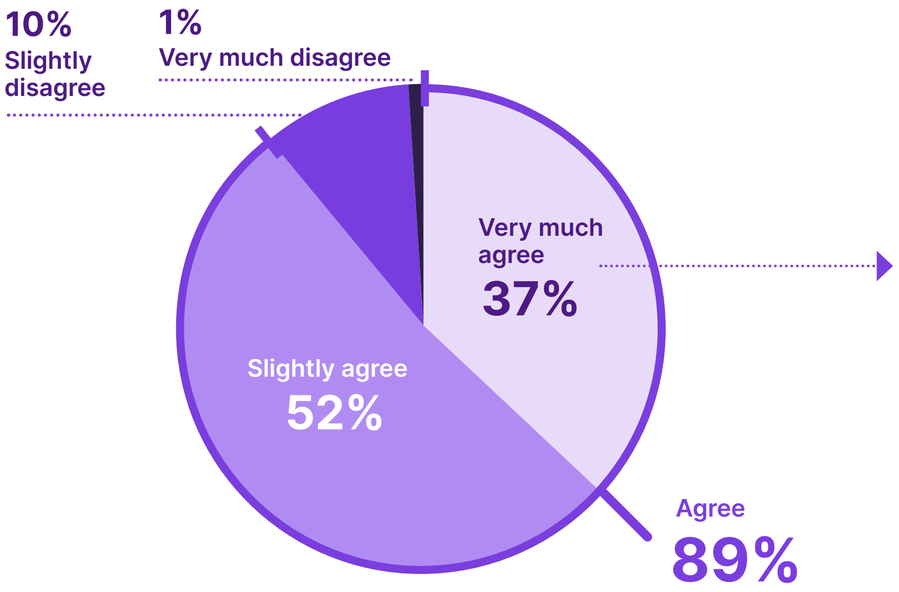
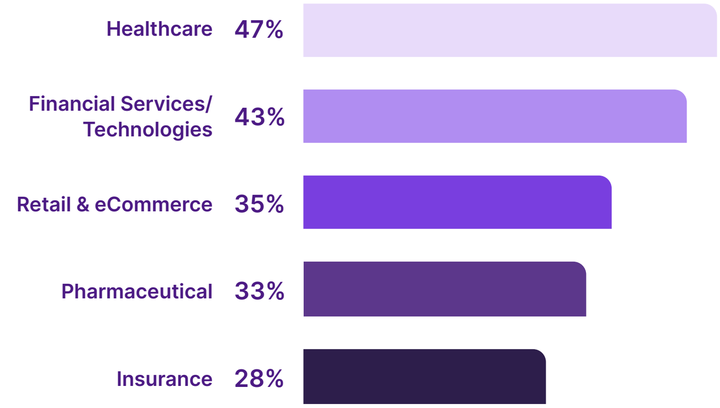


Figure 3: “Very Much Agree”, by Industry



Talent Tops the List of Security Challenges Resulting from Digital Transformation

CISOs worldwide say the lack of qualified cybersecurity talent is their biggest security challenge resulting from digitalization. New methods of security attacks and increasing risks require new qualifications. In addition, a lack of qualified talent also increases competition across companies to find and hire the right people.

But a talent shortage isn't the only challenge facing CISOs. In fact, CISOs face many challenges due to digital transformation, and they consider most to be of nearly equal levels of concern. This reality forces CISOs to devote time and resources to address multiple challenges simultaneously to mitigate security threats effectively.

In addition, while 34% percent of CISOS worldwide cite "difficulties justifying the cost of security investments" as a key challenge, that figure jumps for financial services and healthcare CISOs, to 43% and 38% respectively (Figure 5). As seen from previous responses, financial services and healthcare CISOs experience the security risks of digital transformation more keenly than the worldwide average (Figure 3). Disturbingly, these findings show they also experience the biggest challenges in justifying new security costs to cover those risks.

Figure 4: Top security challenges arising from digital transformation

Figure 5: Difficulty justifying cost of security investments, by industry

*Question allowed more than one answer and as a result, percentages will add up to more than 100%

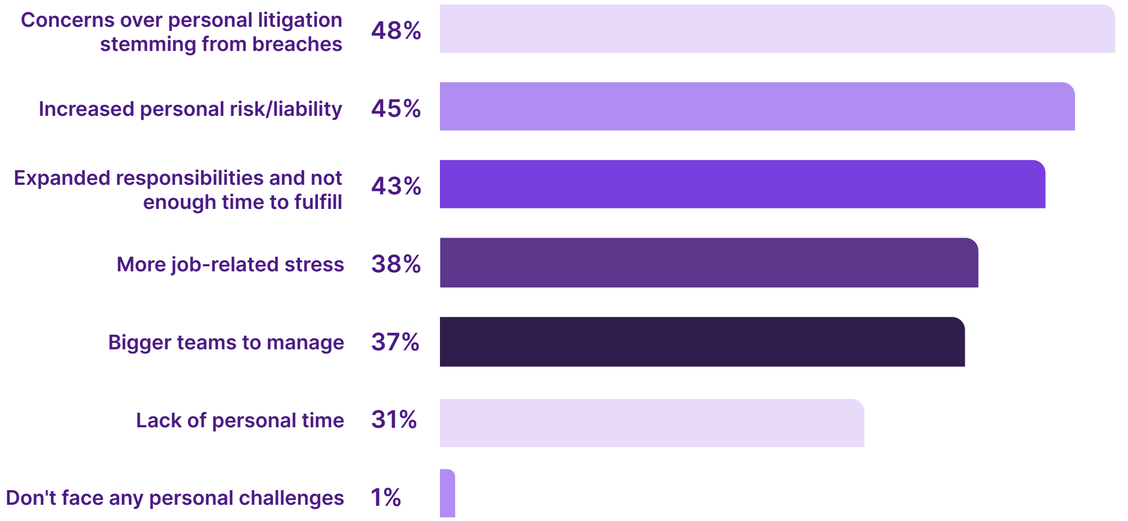
Litigation Concern is Top Personal Challenge Created by Digital Transformation

CISOs identify numerous personal challenges from digital transformation (Figure 6). At the very top of the list are concerns over personal litigation stemming from breaches (48%) and increased personal risk/liability (45%). Recent high-profile CISO lawsuits have likely contributed to these concerns.

The potential impact of these concerns can be grave for businesses. Anecdotally, we have heard of qualified CISOs considering taking a role a level below CISO, and many are requesting indemnification or insurance to compensate for the risk. This trend could potentially lead to a leadership gap and to companies paying CISOs higher salaries to attract them despite the risk of personal litigation associated with their job.

To solve this issue, business leaders must collaborate more closely with CISOs and ensure that appropriate precautions are in place to protect the business. Second, CISOs must be equipped with security solutions that provide a comprehensive view of all various, intertwined risks. With greater visibility and context, CISOs can demonstrate progress on risk mitigation and reduce security control gaps, lowering the risk of personal liability as a result of a breach. If CISOs lack the needed visibility, they can't detect or prevent potential threats.

Figure 6: Top personal challenges from digital transformation



*Question allowed more than one answer and as a result, percentages will add up to more than 100%

> In addition to upending many traditional security approaches, the digital-first economy has impacted a lot of us CISOs on a very personal level. The fact that my peers highlighted 'concerns over personal litigation stemming from breaches' as their top personal concern should be alarming to everyone in the industry. Qualified leaders may decide not to pursue the role if organizations don't have the right cyber tools or processes, or if they consider the personal risk too high."
>
> – Mike Towers, Chief Digital Trust Officer at Takeda Pharmaceuticals International

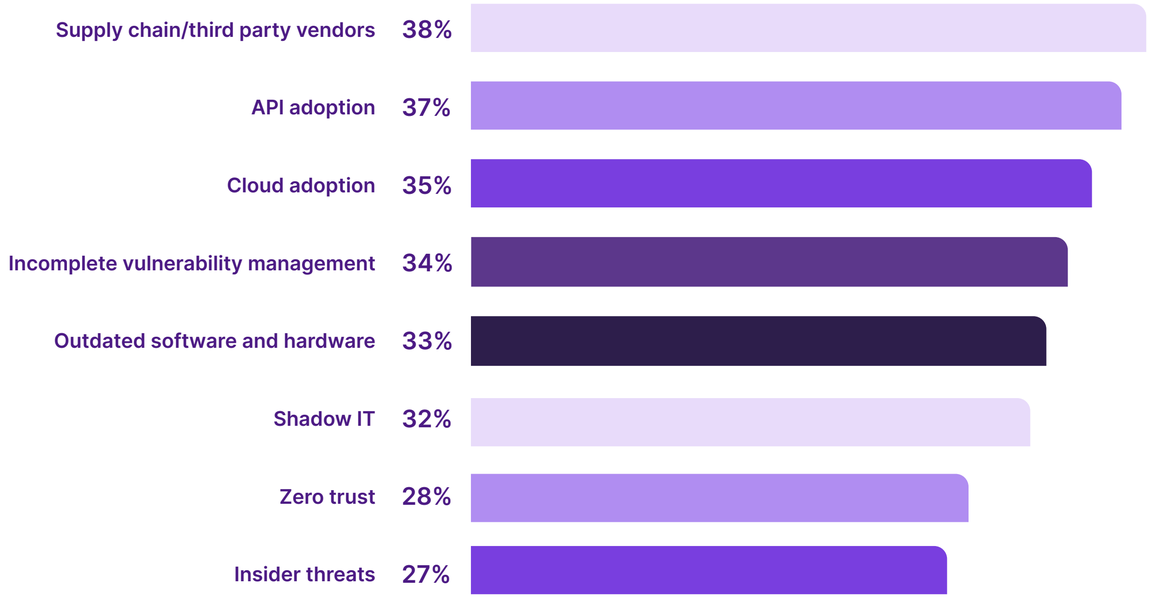
Supply Chain and APIs are Biggest Security Control Gaps in Digital Initiatives

CISOs identify supply chain or third-party vendors (38%), API adoption (37%), and cloud adoption (35%) as the top three security control gaps resulting from their digital initiatives.

With the growth of the digital-first economy over the past couple of years, the usage of APIs has exploded. As the delivery mechanism for sharing data across digital services and applications, APIs represent the key component of digital transformation. APIs also play a particularly critical role in CISOs' first and third concerns – supply chain/third-party vendors and cloud adoption. Because those services rely on APIs to run, organizations may be seeing a "double impact" of the need for API security, both to protect the APIs they know they are writing to support key applications and the APIs essential to supply chain and cloud initiatives.

> Security requirements have grown exponentially with digitalization, and we're moving faster than ever with those digital projects. Objective data on the security challenges brings more awareness to the problem set and helps us craft ways to work together to create a stronger and safer cybersecurity culture."
>
> – Julie Chickillo, VP, head of cybersecurity at Guild Education

Figure 7: Biggest security control gaps in digital initiatives



*Question allowed more than one answer and as a result, percentages will add up to more than 100%

78% of Organizations Place a Higher Priority on API Security Now vs. Two Years Ago

Along with the immense opportunity fueled by APIs comes potential risks. Moreover, if unaddressed, these risks could potentially impede the success of an organization's digital transformation programs. The survey findings show that organizations are starting to recognize that protecting digital initiatives demands prioritization of effective API security. While it is not surprising that 78% of CISOs view it as a higher priority than two years ago, it is a bit of a mystery that 5% of CISOs worldwide say API security is now a lower priority.

In addition, out of the 78% of CISOs who say API security is a higher priority, 34% report that API security is a "much higher" priority. Looking at the data by industry, however, we see that 43% of financial services CISOs say API security is a "much higher" priority – 9% higher than the global average. Retail and eCommerce CISOs follow at 37%.

Financial services and retail/ eCommerce have been particularly impacted by economic shifts and have turned to digitalization to drive business growth initiatives. Therefore, it stands to reason that they would have prioritized API security to a greater degree over the previous two years.

Figure 8: How organizations prioritize API security now compared to two years ago

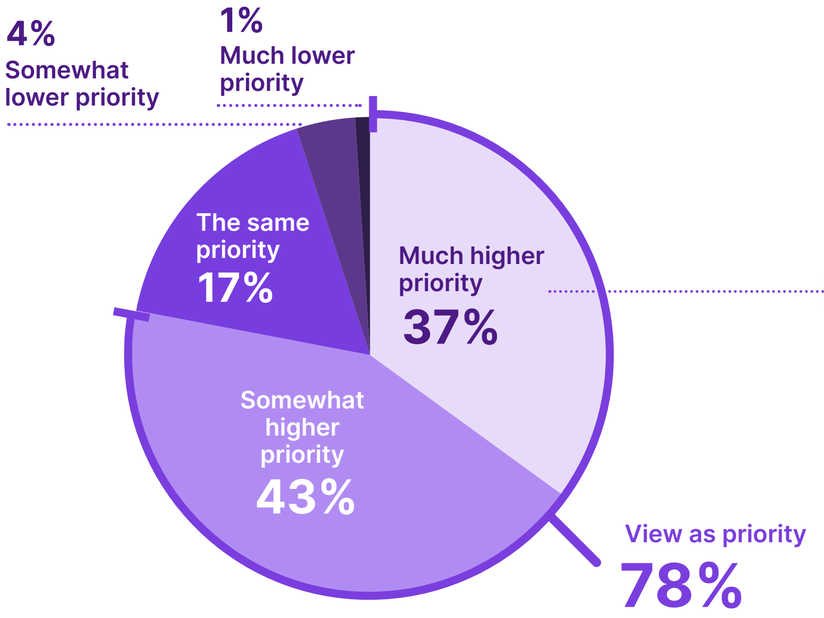
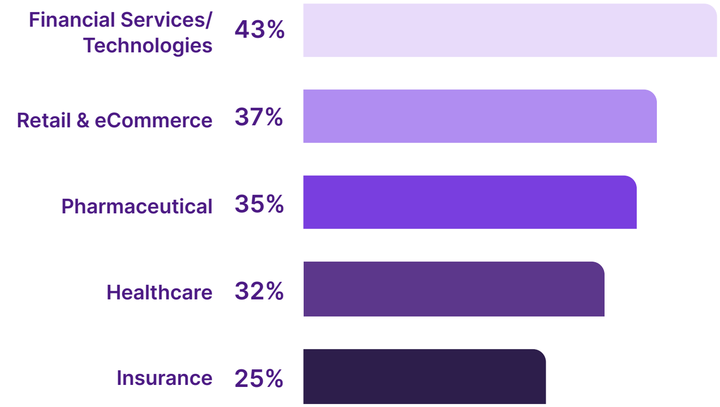


Figure 9: Which industries rate API security a "much higher priority" now



Nearly All CISOs Plan to Prioritize API Security over the Next Two Years

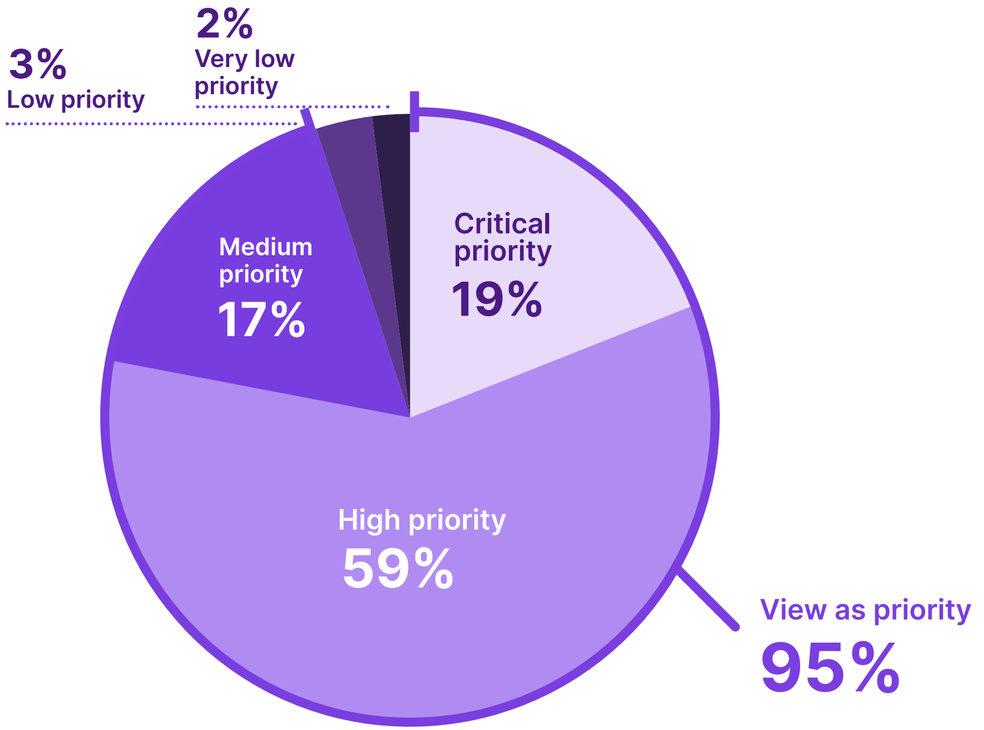
CISOs are well aware of their ever-expanding API ecosystem and their organization's increasing reliance upon them. APIs drive growth and profitability and enable these businesses to deliver their digital goods and services. Without API security programs that protect these crucial connectivity tools, companies put everything at risk – speed to market, competitive advantage, and the brand itself.

Therefore, it's no surprise that API security is at the forefront of security leaders' minds and they expect it to become an even higher priority in the coming years. In fact, 95% of CISOs worldwide say their organizations have made API security a planned priority over the next two years.

This finding also aligns with other industry research. The Gartner 2022 Innovation Insight for API Protection report, for example, found that "security leaders are looking for additional security capabilities to protect their APIs. They are expanding beyond their existing API gateways (GWs) and web application and API protection (WAAP) solutions – especially in industry verticals with high security requirements."

> Given the growing importance of APIs over the last several years for enabling modern businesses, it is surprising that API security has become mainstream only recently. The fact that security frameworks and regulations are slow to evolve is partly to blame, but hope is on the horizon. The Federal Financial Institutions Examination Council (FFIEC), which usually takes years to issue a new mandate, in just one year explicitly called out APIs as a separate attack surface, requiring financial institutions to inventory, remediate, and secure API connections."
>
> —Jeff Farinich, SVP technology and CISO at New American Funding

Figure 10: Plans for prioritizing API security over the next two years



A Variety of Global Developments are Significantly Impacting CISOs Today

Multiple simultaneous global developments are impacting the CISO role.

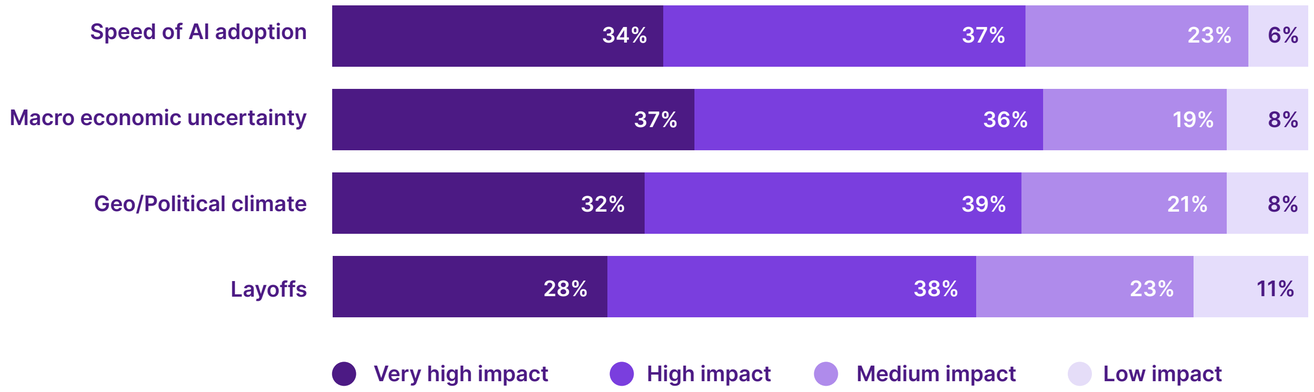
The leading development, when combining the respondents' rating of medium, high, and very high impact, is the speed of AI adoption (94%).

The rise of AI in virtually every industry is changing the security landscape. In 2021, the market for AI in global cybersecurity was $14.9 billion and is predicted to reach a whopping $133.8 billion by 2030, according to Acumen Research and Consulting.

CISOs must learn to navigate the associated threats and security ramifications. Because bad actors are already using AI on the offense, to create and accelerate threats and cyber attacks, CISOs must quickly adopt AI as a defensive tool for their organizations.

While AI clearly is a top issue of concern for CISOs, it is very closely followed by macro-economic uncertainty and the geo-political climate, which CISOs globally rank second and third, respectively. The reality is many global trends are impacting the CISO role and increasing the complexity of an already complex job.

Figure 11: Global trends impacting the role of the CISO



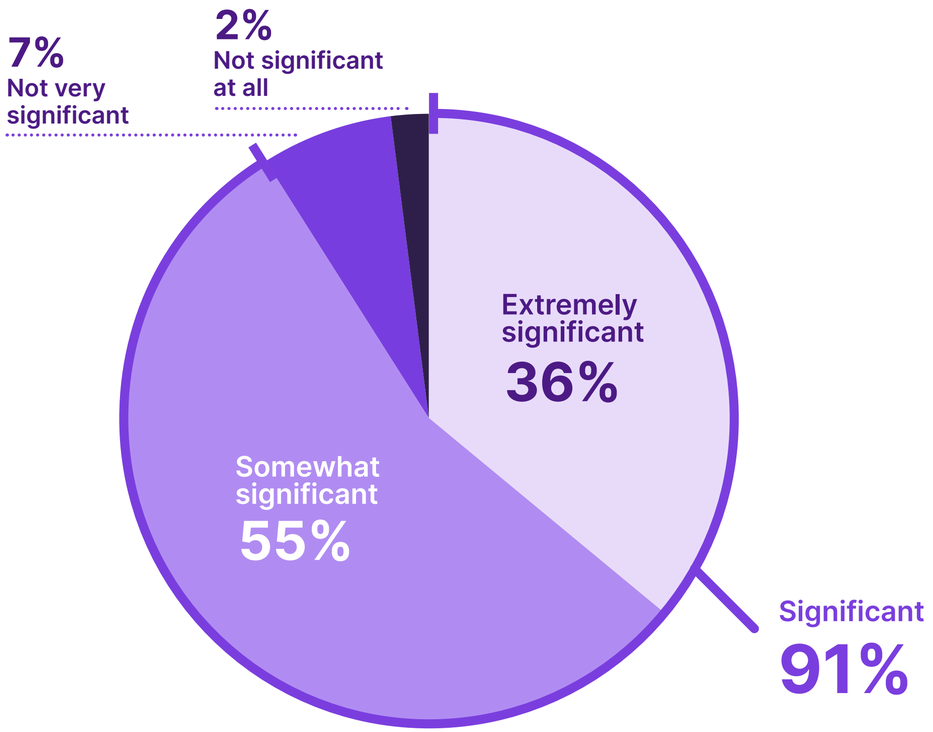
> The impact of AI has captured the imagination of all the CISOs I'm talking to, so I'm not surprised to see it cited as the global trend most impacting CISOs. We all realize that cyber attackers are already using AI – we as CISOs need to map out our game plan for using AI as part of our fabric of defenses to counter these threats."
>
> – George Gerchow, CSO and SVP of IT at Sumo Logic

The Struggle to find Qualified Cybersecurity Talent is Impacting Digital Transformation

Digital transformation has introduced new types of cybersecurity attacks. CISOs need security team members who understand emerging technologies and have the right skills and qualifications to address new security risks and threats.

91% of CISOs agree that finding and keeping qualified cybersecurity talent significantly impacts their ability to deliver on digital transformation initiatives. Given that the lack of qualified security talent remains the biggest challenge for CISOs (Figure 4), it could very well be that AI tooling is one of the compensating factors organizations can embrace to make up for the gap in skilled talent – at a minimum, AI-driven security solutions will need to help organizations bridge that gap.

Figure 12: Significance of cybersecurity talent on delivery of digital transformation initiatives



Boards of Directors are Knowledgeable about Cybersecurity

Most respondents indicate that their board members recognize cyber risk as a key business problem. More than half of CISOs (57%) already present on cyber risk mitigation to the board at least as often as every six months, and just over a quarter (26%) present at least once a quarter. In total, 83% of CISOs present to the board every six months or more often.

Board members' knowledge level about cybersecurity issues can likely be partially attributed to this steady cadence. The vast majority of CISOs (96%) say their organization's board of directors are knowledgeable about cybersecurity, with 63% indicating the board is "very knowledgeable" on the topic.

Maintaining a high level of board awareness about security risks and their potential impact on the business will be especially critical for organizations moving forward. In the US, new rules from the SEC will soon require public companies to disclose board members with security expertise.

Figure 13: Frequency of presentation on cyber risk mitigation at board level

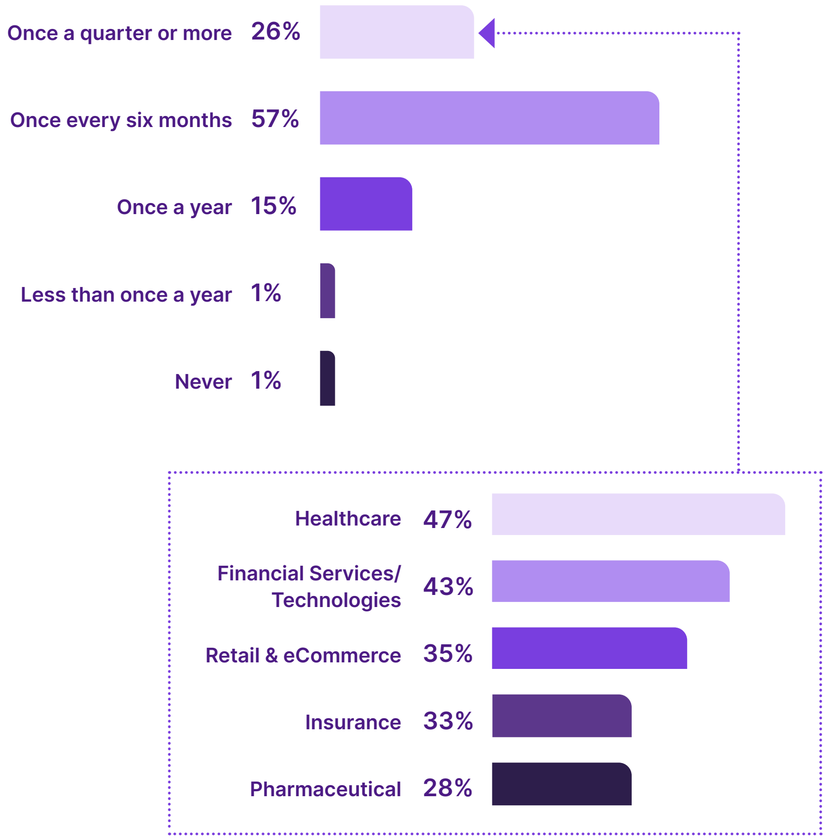
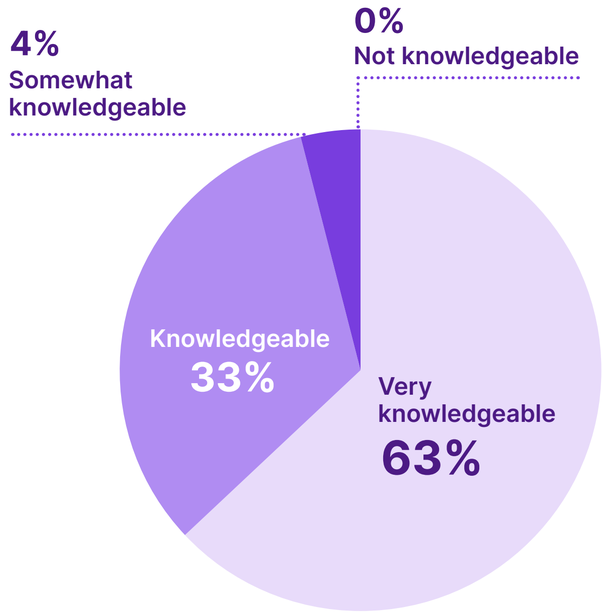


Figure 14: Cybersecurity knowledge of boards of directors



While Security Budgets Have Increased, Security Spending Power has Decreased

82% of CISOs report having a larger security budget compared to two years ago. However, given these same companies have seen an 87% increase in revenue, CISO spending power, as a percentage of revenue, has decreased in the last two years.

Also, a third of respondents (34%) cite cost justification and nearly 30% of CISOs cite lack of budget as key security challenges (Figure 4). Both of these findings suggest that CISOs still lack the funding they need to address new security requirements created by digital transformation.

Figure 15: Organization's revenue, compared to 2021

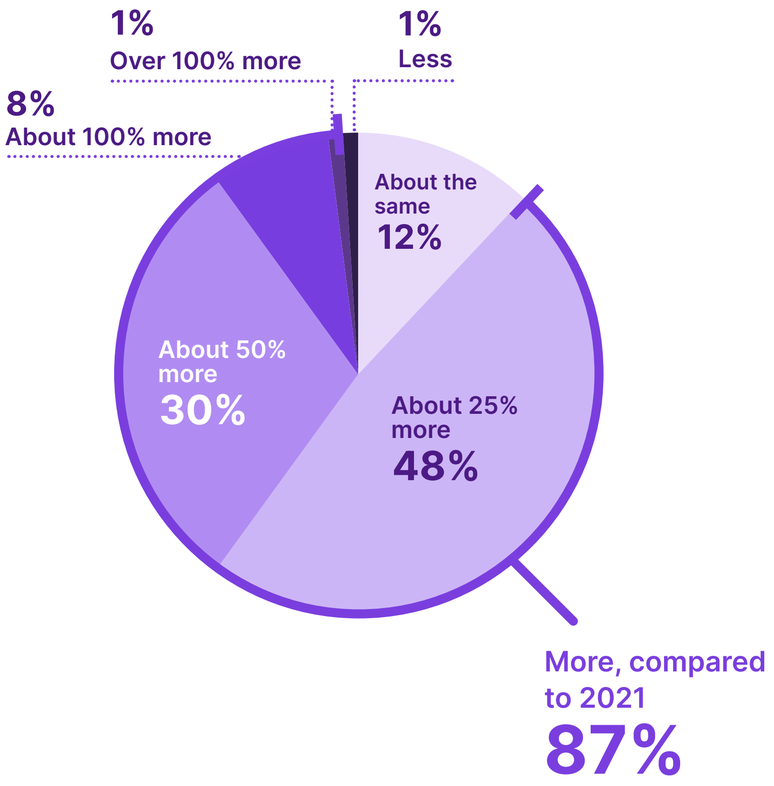
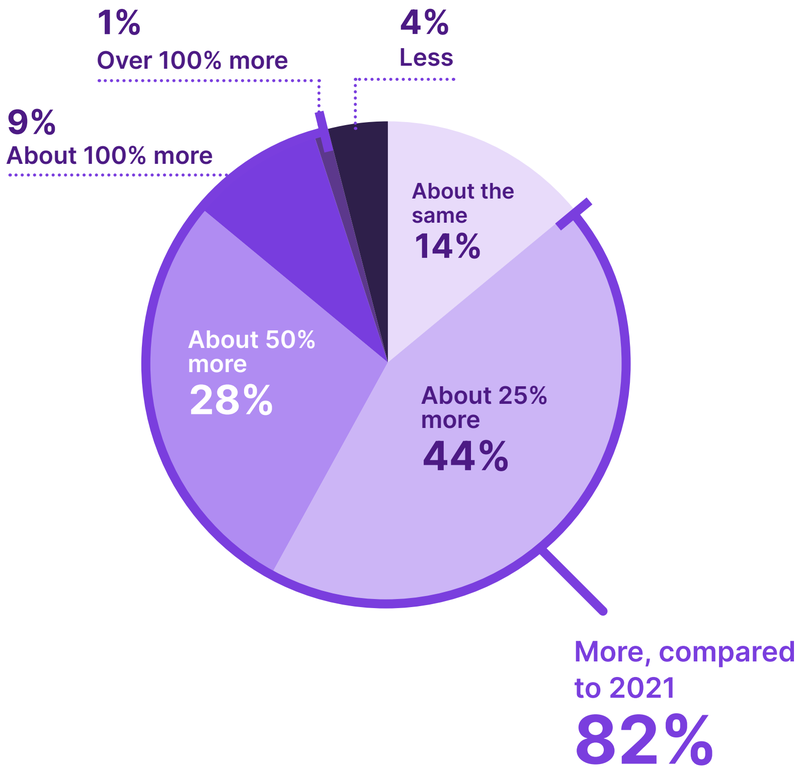


Figure 16: Organization's security budget, compared to 2021



Demographics

Country, Industry, Role, and Company Size

Figure 17: Respondents by country

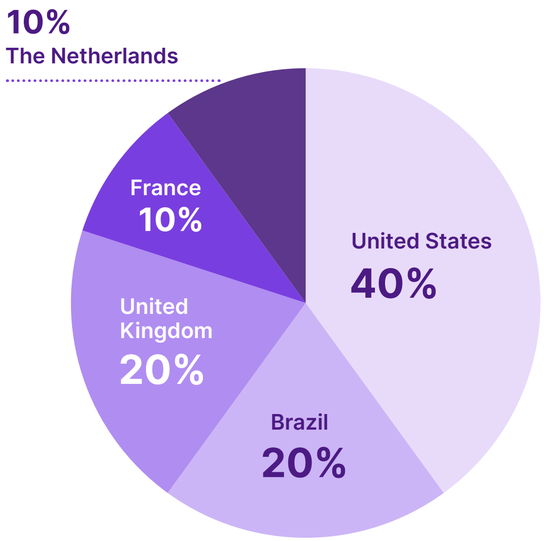


Figure 18: Respondents by industry

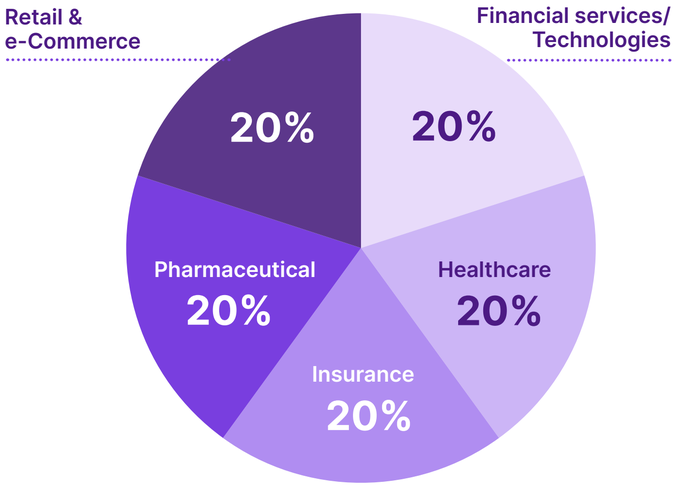


Figure 19: Respondents by role

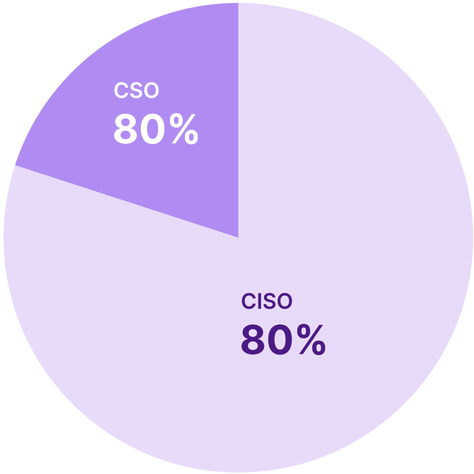
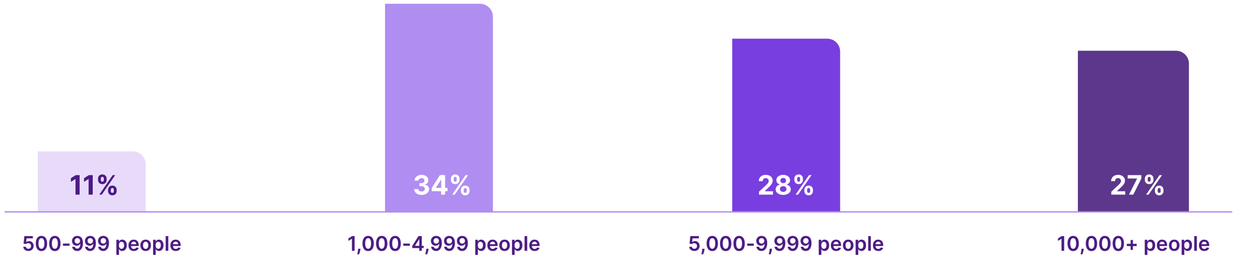


Figure 20: Respondents by company size



About Salt Security

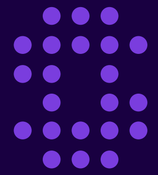
Salt Security pioneered API security and is the industry leader with a proven record of success. Salt customers include leading financial services, insurance, eCommerce/retail, pharmaceutical, and digital services companies.

Salt protects the APIs that form the core of every modern application. The patented Salt Security API Protection Platform is the only API security solution that combines the power of cloud-scale big data and time-tested ML/AI to detect and prevent API attacks. By correlating activities across millions of APIs and users over time, Salt delivers adaptive intelligence with real-time analysis and continuous insights for API discovery, threat protection, and hardening of APIs.

The Salt Security API Protection Platform deploys quickly and seamlessly integrates with a company's existing tools and workflows, including Jira, Slack, MuleSoft, AWS and more. The Salt platform gives customers immediate value and protection, so they can innovate with confidence and accelerate their digital transformation initiatives.

For more information, please visit: https://salt.security/ or email: info@salt.security.

Global Surveyz is a global research company providing customers with a survey report as-a-service offering that covers the whole process of creating an insightful and impactful B2B or B2C report for any target market. With a track record of over 200 successful survey projects globally, Global Surveyz has gained extensive knowledge and expertise in gathering, analyzing, and interpreting data from diverse industries and markets.



SALT

Securing Your Innovation