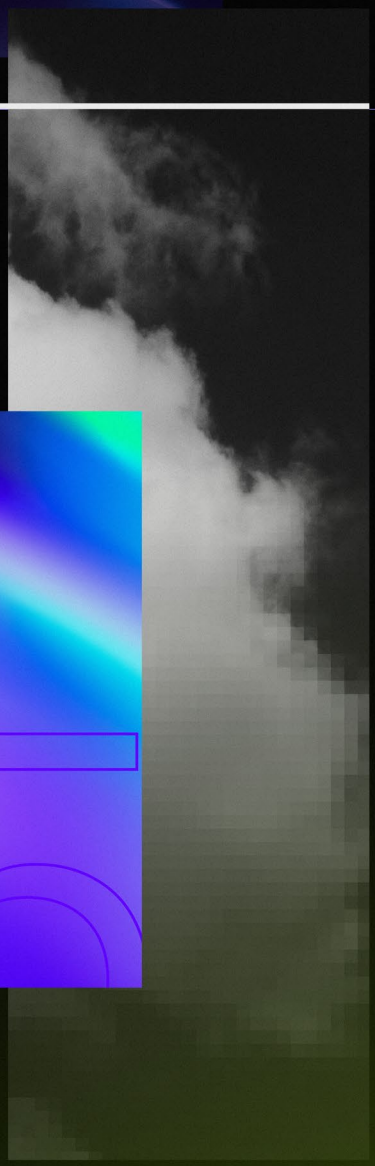
Cloud Security Survey Report 2025



SentinelOne

CYBEREDGE GROUP℠

Table of Contents

Introduction

The SentinelOne 2025 Cloud Security Survey Report examines the risks and threats cloud security teams are facing now, the defenses they have in place, the challenges they encounter protecting cloud-based data and applications, and their plans for implementing additional cloud security technologies.

In November 2024 we surveyed 400 cybersecurity managers and practitioners with knowledge about their organization's cloud security activities in four countries and a wide range of industries. We asked about their current cloud security operations and performance. We inquired about their perceptions of cloud security technologies now in place and the factors inhibiting them from validating and prioritizing security events. We also requested information about implementing new cloud security technologies, characteristics they seek in a unified cloud security platform, and benefits they expect to experience from artificial intelligence (AI) embedded in cloud security solutions.

Survey Demographics

400
Responses received from 400 qualified cybersecurity managers and practitioners

500
All from organizations with more than 500 employees

4
Representing four countries: United States, Canada, UK, and Australia

8
Representing eight major industries and several others

Our objective is to provide CIOs, CISOs, cybersecurity managers, and others with information on how their peers are managing cloud security and areas they seek to improve.

CyberEdge would like to thank our research sponsor, SentinelOne, who conceived this report and whose support has been essential to its success.

Top Five Insights

This report contains dozens of actionable insights into cloud security threats and solutions. Here are our top five takeaways:

1. **Cloud security contributes to all cybersecurity.**
   When we look at the threats that cloud security helps address, we see that it is an essential contributor to almost every cybersecurity domain. That includes identity and access management, compliance, fraud prevention, network security, data security, secure application development, encryption, and insider threat detection. Cloud attacks typically cross many boundaries, so to be successful, cloud security solutions must connect silos so they can detect complex sequences of malicious events wherever they occur.

2. **Too many and too much means too slow.**
   A vicious cycle is at work in cloud environments. An expanding cloud attack surface and new threats… lead to the need for more cloud security technologies… which lead IT security groups to deploy more point solutions… which lead to more management and integration issues… which lead to more alerts, lower quality alerts, and slower reaction to attacks.

3. **Automation and AI are finally kicking in.**
   Despite new challenges, this year cloud security teams are more confident than they were last year about their capabilities in areas such as threat detection and vulnerability scanning and assessment. That's because automated workflows, AI, and other technologies are having a measurable impact on the speed and accuracy of those and other cloud security activities.

4. **AI makes people more effective.**
   When security teams look at AI embedded in cloud security tools, they see capabilities to accelerate incident response, detect attacks sooner, reduce data noise and false positives, and otherwise make things go faster. But they also see AI as mitigating the longstanding cybersecurity skills shortage by enabling senior security professionals to perform more tasks in the same time period and less experienced ones to handle complex tasks sooner.

5. **Unified cloud security platforms address big challenges.**
   Many organizations are turning to unified cloud security platforms to overcome challenges created by too many security tools generating too much data and too many alerts. The platforms help address these challenges by providing visibility into security data across cloud platforms and services, filtering out false positive alerts, eliminating integration headaches, simplifying deployment and administration, managing automated workflows, and enabling agentless and agent-based scanning across hundreds of cloud workloads.

About This Report

The findings of this report are divided into three sections:

Section 1: Cloud Security Operations

This section of the report highlights the risks and threats that most concern cloud security teams and examines their level of confidence in their organization's current cloud security capabilities. It also quantifies how many cloud security alerts organizations are able to investigate within 24 hours, and how successful organizations are in preventing false positive alerts from overwhelming security operations teams.

Section 2: Perceptions and Concerns

This section of the report provides data on the expected benefits of AI for cloud security and shows how respondents rate the importance of 11 key cloud security technologies, as well as how satisfied they are with those technologies and with their own organization's cloud security tooling. It also explores several key issues: factors that inhibit cloud security teams from analyzing alerts, problems caused by too many cloud security tools, the percentage of organizations that struggle with too much cloud security data, and the importance of evidence of exploitability for prioritizing remediation.

Section 3: Current and Future Investment

The final section of the report covers views on whether organizations are investing enough in cloud security and where they stand on implementing key cloud security technologies. It also captures respondents' criteria for selecting a unified cloud security platform.

Navigating This Report

We encourage you to read this report from cover to cover so you can catch all the useful details. However, if you are seeking out specific topics of interest, there are three other ways to navigate through the report:

- **Table of Contents.** Each item in the Table of Contents pertains to specific survey questions. Click on any item to jump to its corresponding page.
- **Research Highlights.** The Research Highlights page showcases the most significant headlines of the report. Page numbers are referenced with each highlight so you can quickly learn more.

Research Highlights

Cloud Security Operations

- **Cloud security threats.** Cloud security teams are most worried about data breaches, malware, unauthorized access, and compliance failures. Cloud security is an essential contributor to almost every cybersecurity domain (page 7).
- **Cloud security functions.** Organizations are most confident about their capabilities for threat detection and vulnerability scanning and assessment. Increased confidence in these areas is due to AI improving the speed and accuracy of those tasks (page 9).
- **Alert investigation timing.** About half of organizations investigate between 70% and 89% of cloud security alerts within 24 hours. Without improvement, those organizations are likely to suffer significant breaches every few years (page 11).
- **False positive alerts.** Higher quantities and lower quality of alerts bog down cloud security teams. Organizations that use automated cloud security processes and AI are able to filter out more false positive (page 13).
- **Separating exploitable from theoretical risks.** Security professionals overwhelmingly agree that evidence of exploitability is very important for prioritizing vulnerabilities and other security issues (page 15).

Perceptions and Concerns

- **Benefits of AI.** Respondents indicate that AI embedded in cloud security tools can accelerate processes and increase the effectiveness of cloud security teams (page 17).
- **Importance of cloud security technologies.** Cloud detection and response (CDR), Cloud security posture management (CSPM), and Cloud infrastructure entitlement management (CIEM) solutions are key cloud security technologies (page 19).
- **Satisfaction with cloud security technologies.** Overall, survey respondents are satisfied with their core cloud security technologies, but are less sure about some of the emerging offerings (page 21).
- **Effectiveness of cloud security tooling.** Four out of five survey respondents are satisfied that their organization has enough cloud security tooling to handle its challenges.
- **Inhibitors of good security.** As in last year's survey, the factors most inhibiting organizations from validating cloud security alerts are a shortage of experienced IT security personnel, too many data silos, and too many cloud security tools (page 22).
- **Lack of an integrated platform.** Security teams are finding many problems caused by having many free-standing cloud security tools in lieu of a unified cloud security platform, including the time and effort required to install, configure, and manage the tools, a lack of integration, and time spent procuring many licenses (page 25).
- **Too much data.** Exactly two-thirds of respondents agree that their organization generates so much cloud security data that their team struggles to derive and prioritize actionable insights (page 27).

Current and Future Investments

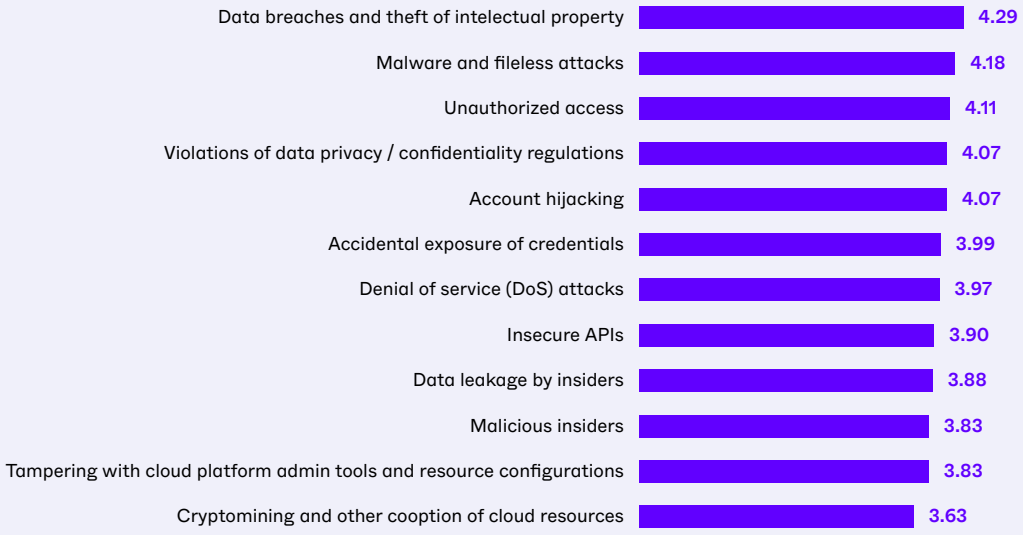
- **Technology deployment plans.** Six of the 11 cloud security technologies covered in this survey are already in production in more than half of organizations (page 29).
- **Criteria for cloud security platforms.** A unified cloud security platform can address many vexing cloud security challenges, provided it has automated workflows, is easy to deploy and administer, and can ingest data from both legacy and cloud sources (page 31).

Section 1: Cloud Security Operations

Cloud Security Risks and Threats

On a scale of 1 to 5, with 5 being highest, rate your overall concern for the following cloud security risks and threats:

Figure 1:
Overall concern for cloud security risks and threats, on a scale of 1 to 5, with 5 highest.



"Cloud security" covers a lot of cyberspace. The phrase refers to all the technologies, policies, processes, and people dedicated to protecting applications, data, platforms, and networks hosted on the internet. And those resources need to be protected from a very wide range of risks and threats.

Which of those risks and threats create the most anxiety for security teams? We asked survey respondents to rate their level of concern for 12 types of risks and threats on a scale of 1 to 5, with 1 being "least concern" and 5 being "greatest concern."

This year five threats were rated higher than 4 on the scale, indicating a very high level of concern (see Figure 1).

Respondents are most worried about "Data breaches and theft of intellectual property" (rated 4.29) and "Malware and fileless attacks" (4.18). These concerns show up in surveys as top issues across all cybersecurity domains; data breaches, theft, and malware are consistently rated among the top threats that keep CISOs up at night.

However, the next three threats "Unauthorized access" (4.11) "Violations of data privacy and confidentiality regulations" (4.07) and "Account hijacking" (also 4.07) illustrate how cloud security overlaps with specific cybersecurity domains. Cloud security teams and identity and access management (IAM) groups must work together to prevent unauthorized access. Keeping on the right side of regulatory authorities requires collaboration between cloud security experts and legal and regulatory staff. Blocking account hijacking usually is a joint project between cloud security and fraud prevention teams.

When we look at the next tier of threats – "Accidental exposure of credentials" (3.99), "Denial of service attacks" (3.97), "Insecure APIs (3.9)," and "Data leakage by insiders" (3.88) – we see more overlap between cloud security and other areas of cybersecurity. To be specific: fraud prevention (again), network security, data security, and secure application development. Accidental exposure of credentials also involves encryption – the cloud security team needs to be good at scanning for exposed secrets such as credentials, encryption keys, and tokens across all cloud platforms.

The biggest takeaway here is that, in today's diverse computing environment, cloud security is an essential contributor to almost every cybersecurity domain.

Another striking fact: the level of concern increased from the 2024 Cloud Security Report for every single threat category. That includes especially large jumps for "Accidental exposure of credentials," which went from 3.85 to 3.99, "Cryptomining and other cooption of cloud resources," which went from 3.52 to 3.63, and "Account hijacking," which rose from 3.97 to 4.07. These increases reflect the growing sophistication and volume of cloud-based attacks, as well as recognition that more and more mission-critical business processes are running on cloud platforms.

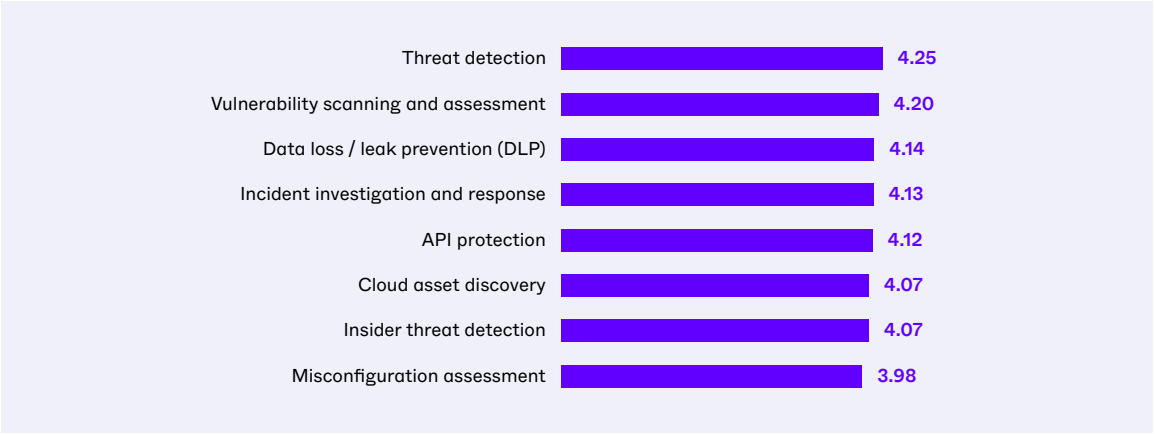
A final observation: the most concerning cloud security risks and threats are not new. The same threat categories that have plagued security teams for years are just as relevant today as they have ever been. In fact, they've become even more relevant, because factors like AI and automation have increased the sheer volume and sophistication of these attacks to unprecedented levels.

"The biggest takeaway here is that, in today's diverse computing environment, cloud security is an essential contributor to almost every cybersecurity domain."

Cloud Security Functions

On a scale of 1 to 5, with 5 being highest, rate the adequacy of your organization's capabilities (people and processes) in each of the following cloud security functions:

Figure 2:
Adequacy of capabilities of cloud security functions, on a scale of 1 to 5, with 5 highest.



Moving on from risks and threats to cybersecurity functional areas, we asked survey respondents to rate the adequacy of their organization's cloud security capabilities on a scale from 1 ("least adequate") to 5 ("most adequate").

Organizations are most confident about their capabilities in "Threat detection" (4.25) and "Vulnerability scanning and assessment" (4.20), as shown in Figure 2. These ratings show a notable increase from last year, when the figures were 4.14 and 4.13, respectively (see Figure 2).

Why the improvement? We think AI is finally having a measurable impact on the speed, reach, and accuracy of threat detection, vulnerability scanning, and other cloud security technologies. We will be examining the specific benefits of AI embedded in cloud security solutions on pages 17 and 33.

> Organizations are most confident about their capabilities in "Threat detection" (4.25) and "Vulnerability scanning and assessment"... These ratings show a notable increase from last year... Why the improvement? We think AI is finally having a measurable impact on the speed and accuracy of threat detection, vulnerability scanning, and other cloud security activites.

The next three responses to this question, which we would characterize as showing moderate confidence, are "Data loss or leak prevention (DLP)" (4.14), "Incident investigation and response" (4.13), and "API protection" (4.12). DLP and API protection are both essential capabilities for protecting sensitive data and ensuring that cloud-based applications don't have security flaws.

Incident investigation and response is obviously important for closing the window on ongoing attacks and preventing their recurrence. However, that function fell two places on our list, from second place in the last survey to fourth in this one. This may be because some types of attacks have become more "stealthy," and cloud security teams are concerned about their ability to analyze them quickly and accurately.

As we move down the list, organizations are somewhat less confident about their capabilities for “Cloud asset discovery” and “Insider threat detection” (both 4.07). The challenge in the case of the former is keeping up with the ever-expanding cloud attack surface, which adds new cloud services and SaaS applications every year.

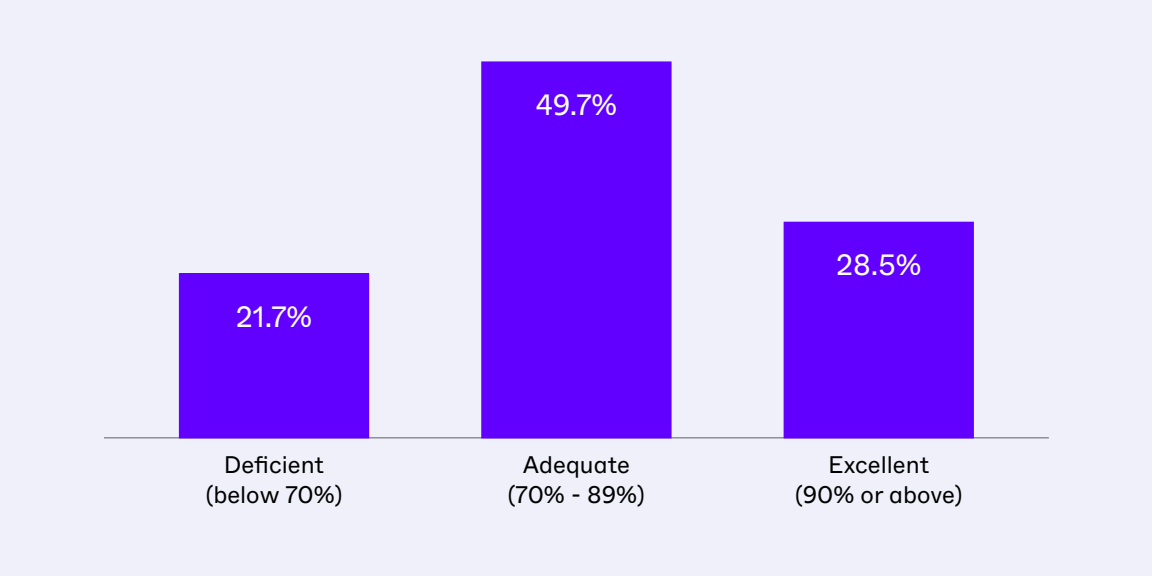
At the less confident end of the scale is “Misconfiguration assessment” (3.98). This involves finding and prioritizing misconfigurations in management and security tools for cloud platforms, applications, cloud services, networks, and security solutions that could allow threat actors to compromise, or even take command of, those assets.

However, although organizations are very concerned about their capabilities for misconfiguration assessment, their rating of this function increased by .12 from last year, the largest increase of any of the responses for this question. The growing confidence is most likely attributable to the increasing effectiveness of misconfiguration detection technology, allowing organizations to improve configuration and vulnerability scanning of their cloud applications and platforms.

Alerts Investigated Within 24 Hours

Approximately what percentage of your cloud security alerts are investigated within 24 hours?

Figure 3:
Percentage of cloud security alerts investigated within 24 hours.



Security operations teams frequently complain that they are overwhelmed with alerts. They struggle to address the most serious ones quickly enough to contain attacks before they cause major damage. To make matters worse, the quantity of cloud security alerts continues to increase as attack surfaces expand and the number of security tools monitoring them grows.

Are security teams investigating alerts in a timely manner? We asked respondents what percentage of cloud security alerts their organizations are able to investigate within 24 hours, and grouped their responses into three categories: (a) Excellent, (b) Adequate, and (c) Deficient.

Our criteria for "excellent" — able to investigate 90% or more of cloud security alerts within 24 hours — was met by 28.5% of organizations (see Figure 3). Kudos to this group.

Our "adequate" standard was reached by about half of organizations: 49.7%. In these enterprises, security teams investigate between 70% and 89% of cloud security alerts within 24 hours. That's not bad, but it implies that between 11% and 30% of alerts are not being looked at within a day of detection. We'd assess that performance as respectable, but without improvement those organizations are likely to suffer significant breaches every few years.

Slightly more than one-in-five organizations (21.7%) fall into our "deficient" category. They acknowledge that at least 30% of their cloud security alerts, and sometimes many more, are not being addressed in a 24-hour window. These organizations should be very concerned.

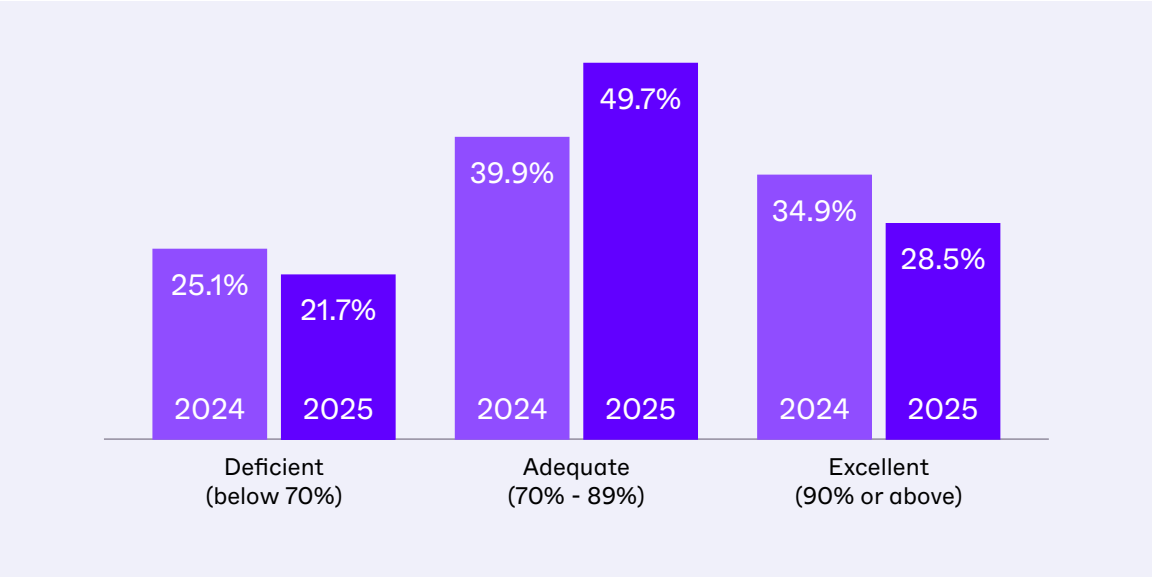
Our "adequate" standard was reached by about half of organizations: 49.7%. In these enterprises, security teams investigate between 70% and 89% of cloud security alerts within 24 hours... We'd assess that performance as respectable, but without improvement those organizations are likely to suffer significant breaches every few years.

The year-to-year trend is mixed. The number of organizations in the deficient category fell 3.8%, but the organizations that achieved excellence declined even more (by 6.4% — see Figure 4). That meant that the adequate group increased 9.8%. As we said a moment ago, that's not a desirable level for long run safety.

We also looked at the average (mean) by country. The results for the USA are slightly better than the sample as a whole (80% versus 78%). But the other three are slightly below: 76% for Australia, 75% for Canada, and 73% for the UK.

Figure 4:

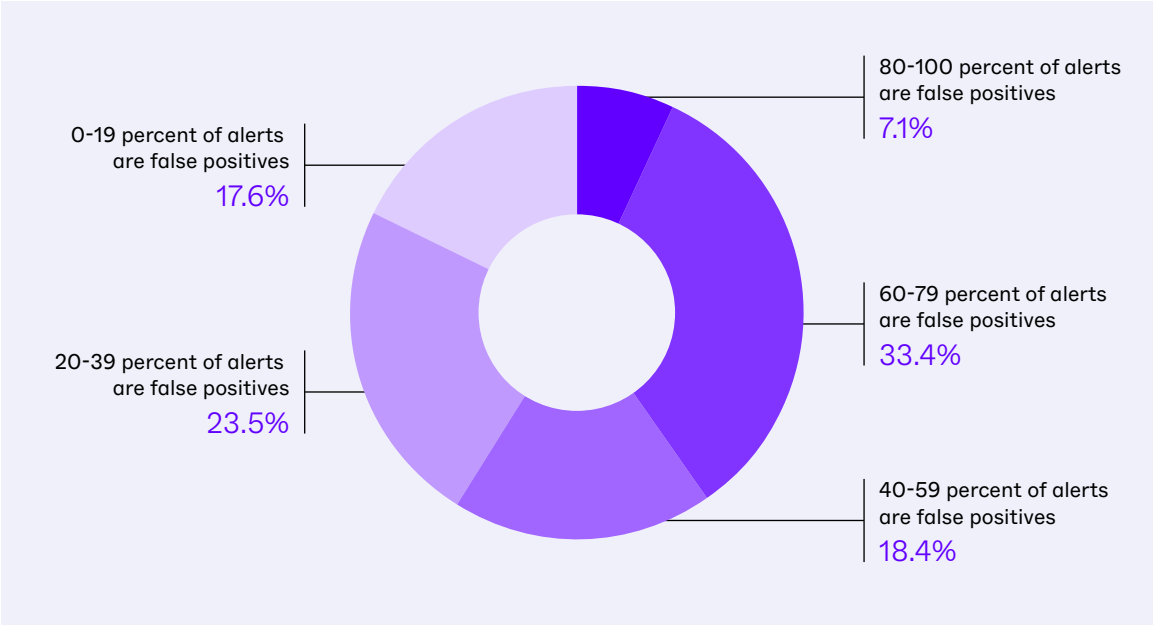
Percentage of cloud security alerts investigated within 24 hours, 2025 compared to 2024.



False Positive Alerts

Approximately what percentage of your cloud security alerts are false positives (i.e., alerts not relevant to your organization)?

Figure 5:
Percentage of cloud security alerts that are false positives.

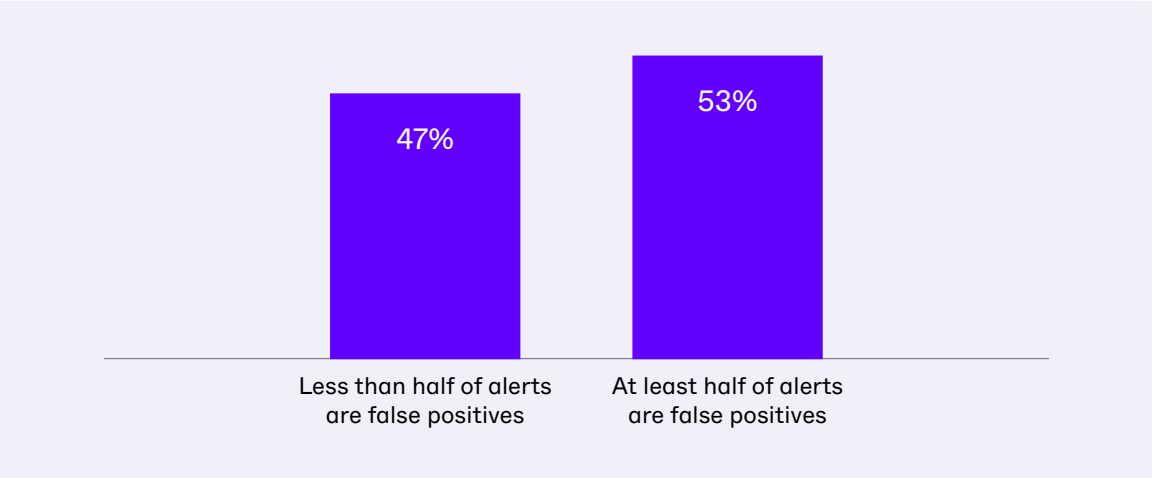


Not all alerts are equal. Inevitably, many are triggered by threats that are simply not relevant to a specific organization, for example because the enterprise already has controls in place to thwart them or because the attack requires compromising software or hardware that organization doesn't have. Yet, unless these false positive alerts are screened out, security teams will waste valuable time investigating them.

And there are a lot of false positive cloud alerts. As shown in Figure 5, a third of organizations report that 60%-79% of their alerts are false positives. And some have it even worse; an unfortunate 7% of cloud security teams are suffering from the fact that four out of five of their cloud security alerts are a waste of time.

A simple statistic jumps out of the responses to this question. More than half of organizations (53%) find that the majority of their cloud alerts are false positives (see Figure 6).

Figure 6:
Percentage of organizations with half of alerts as false positives.



Obviously, investigating these non-threatening alerts represents a lot of wasted time and effort. But equally important, those security operations groups are likely to be tired and frustrated, and therefore more prone to making mistakes and failing to analyze and contain the meaningful attacks.

Why are so many organizations having so much trouble filtering out false positive alerts? First, as noted earlier, the sheer *quantity* of cloud security alerts continues to increase. Second, because of the *quality* of the alerts. Many lack clarity and don't include necessary contextual information. Third, because most security teams are reluctant to drop alerts unless they have very precise evidence that they are irrelevant. They would rather accept a lot of false positives than run the risk of ignoring a few that just might be important.

Why are so many organizations having so much trouble filtering out false positive alerts? First... because sheer *quantity* of cloud security alerts continues to increase. Second, because of the *quality* of the alerts... Third, because most security teams are reluctant to drop alerts unless they have very precise evidence that they are irrelevant.

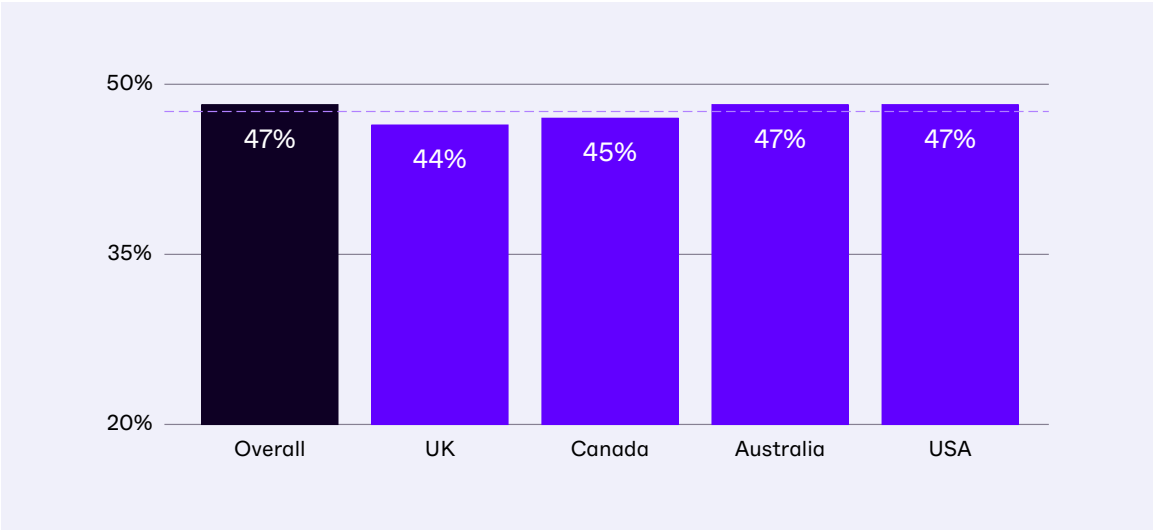
Yet another factor contributing to the plague of false positive alerts is that many security teams lack the tools to separate exploitable and non-exploitable vulnerabilities. SOC teams often spend a great deal of time following up on vulnerabilities that are rated as "critical" by a vulnerability scoring system but in practice can't lead to a successful attack because the organization has controls in place that disrupt the threat actor's kill chain. The importance of identifying exploitability is discussed in the next section of the report.

How do security teams achieve excellent or at least satisfactory results in this area? Typically, they have:

- Automated processes to pull together data from a wide range of cloud security solutions
- Tools that employ AI, security analytics, and threat intelligence to determine with precision which alerts are false positives.
- Automated processes and tools that utilize AI models to enable human analysts to quickly and accurately separate signals from noise for incidence response, threat hunting, and digital forensics.

For all the organizations in this survey, the average (mean) percentage of alerts that are false positives is 47%. That's up 3% from last year. The UK is doing the best among the countries included in the survey, averaging 44% false positives (see Figure 7). They are followed by Canada (45%), Australia (47%), and the U.S. (just over 47%).

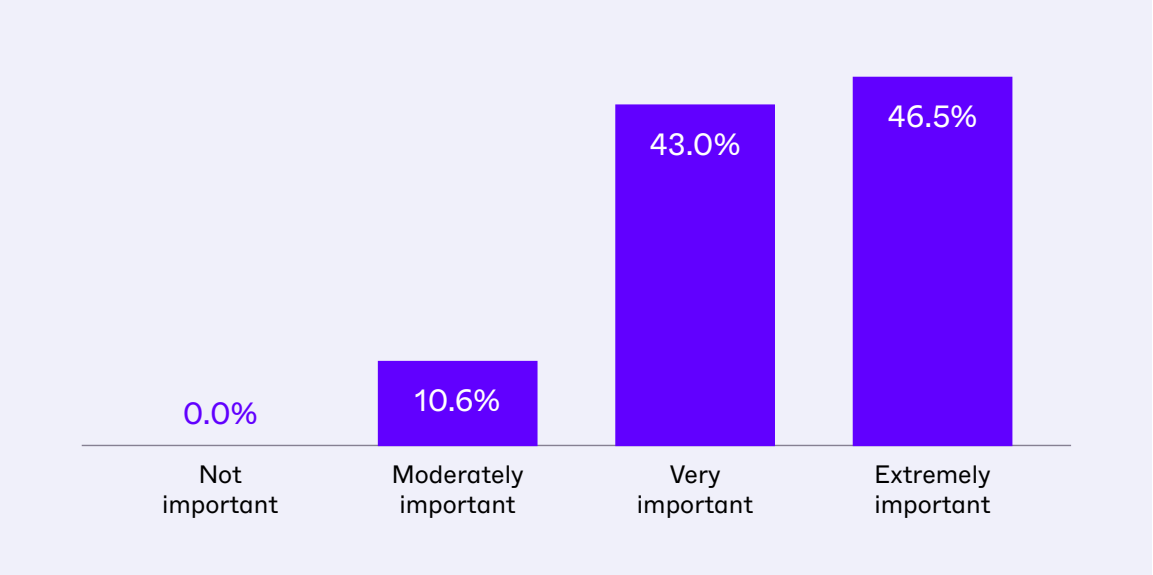
Figure 7:
Average (mean) percentage of cloud security alerts that are false positives, by country.



Importance of Evidence of Exploitability

How important to your organization is evidence of exploitability (i.e., potential impacts to vulnerable production workloads) for prioritizing cloud security backlog items and rapidly closing high-priority items?

Figure 8:
Importance of evidence of expoitability for prioritizing cloud security backlog items and rapidly closing high-priority items.



It is a truth universally acknowledged that most organizations have far more vulnerabilities, misconfigurations, over-permissioned cloud identities, and other security issues than security teams can hope to identify and remediate in a timely manner.

That truth has led many experts to suggest that cybersecurity teams should separate theoretical risks from those that are actually exploitable in their specific environments. In this context, “exploitable” means being part of a path leading to a vulnerable workload or other information asset. For example, a misconfiguration in a system used for software testing that has no access to production systems or real data is not much of a risk. In contrast, a vulnerability with a “Low” severity rating in a device with a path to a key corporate database is a real and imminent risk and should be a high priority for remediation.

Do cybersecurity teams agree with that idea? Do they value evidence of exploitability as an important factor for prioritizing their activities?

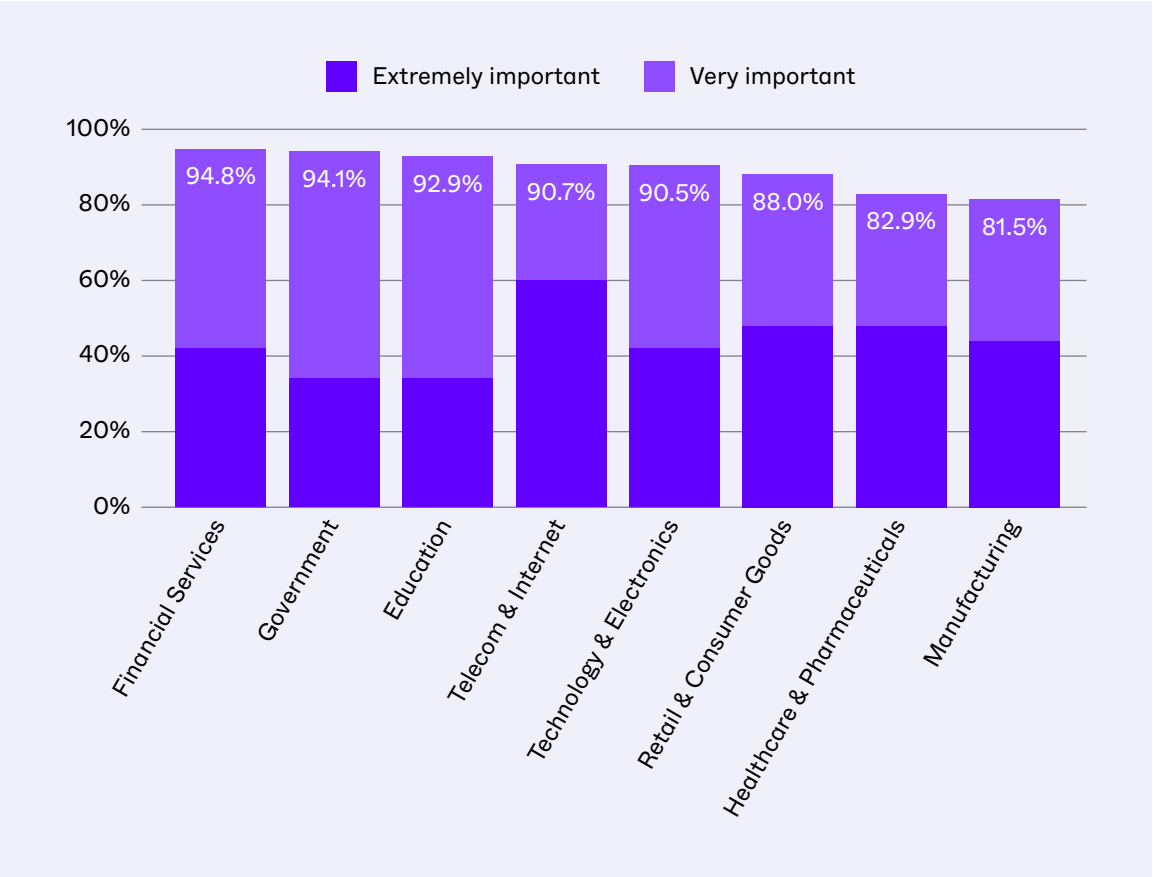
Yes, they certainly do. Nine out of 10 (89.4%) of respondents agree that evidence of exploitability is “Very important” or “Extremely important” for prioritizing cloud security backlog items and rapidly closing high-priority items (see Figure 8).

The remaining 10.6% of responders say evidence of exploitability is “Moderately important.” Exactly nobody rated it as “Not important.”

There is some variation by industry, as shown in Figure 9. However, even in the most skeptical industries, like healthcare and manufacturing, more than three out of four respondents think evidence of exploitability is very or extremely important. That's why cloud security solution providers have started to introduce tools that test exploitability paths to highlight which vulnerabilities and security issues lead to information assets and pose actual, rather than theoretical risks to the organization.

Figure 9:

Importance of evidence of expoitability for prioritizing cloud security backlog items and rapidly closing high-priority items, by country.



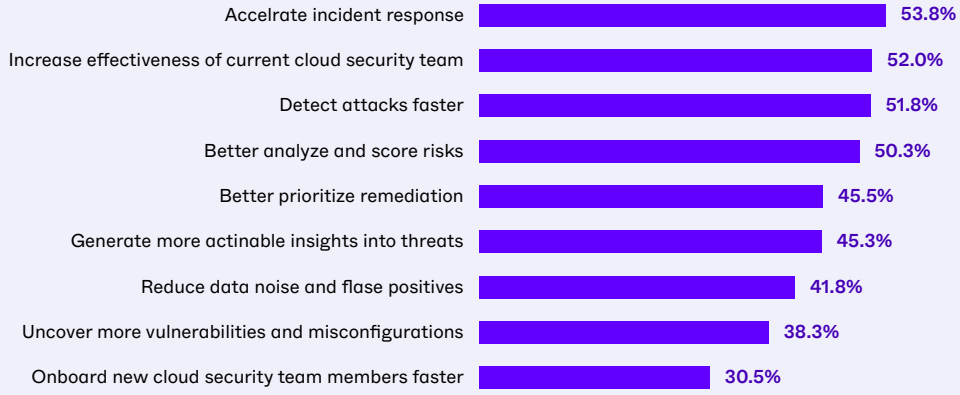
Even in the most skeptical industries... more than three out of four respondents think evidence of exploitability is very or extremely important. That's why cloud security solution providers have started to introduce tools that test exploitability paths to highlight which vulnerabilities and security issues lead to information assets and pose actual, rather than theoretical risks to the organization.

Section 2: Perceptions and Concerns

Benefits of AI in Cloud Security Tools

Which of the following benefits from embedding artificial intelligence in cloud security tools do you believe will impact your organization the most? (Select up to five.)

Figure 10:
Benefits from AI embedded in cloud security solutions that will impact the organization the most.



As we mentioned earlier, AI is having a measurable impact on the speed, reach, and accuracy of threat detection, vulnerability scanning, and other cloud security technologies. But what benefits from AI do organizations expect to have the most impact on cloud security?

Speed is at the top of the list. The #1 and #3 advantages of embedding AI in cloud security tools are "Accelerate incident response" (selected by 53.8% of the respondents) and "Detect attacks faster" (51.8%) (see Figure 10). These advantages stem from AI's ability to detect patterns associated with attacks in masses of data and to provide insights into effective responses.

Moving up from fourth place in last year's survey to second in this year's survey is "Increase the effectiveness of my current cloud security team" (52.0%). This reflects an increasing recognition that AI can not only speed up processes, it also helps people make better decisions. As we noted earlier, AI enables senior security professionals to perform more tasks in the same time period, and less experienced ones to handle tasks they would not have been ready to handle on their own. From the perspective of IT teams, AI fills gaps in experience and expertise.

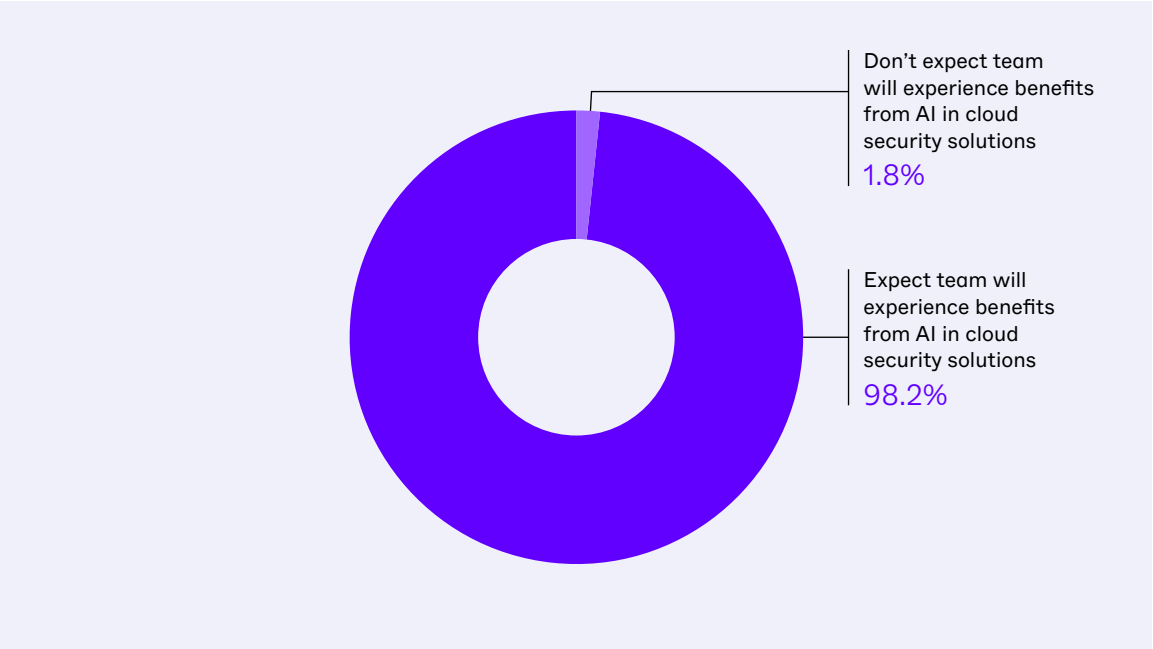
In fourth and fifth places are "Better analyze and score risks" (50.3%) and "Better prioritize remediation" (45.5%). Risk scoring and prioritization enable security teams to target resources toward activities that will have the biggest impact on reducing risk.

At the other end of the spectrum, enthusiasm is somewhat lower for "Uncover more vulnerabilities and misconfigurations" and "Onboard new cloud security team members faster." However, interest in these two applications of AI is growing. The former surged from 33.1% in the previous survey to 38.3% in this one, and the latter went from 27.5% to 30.5%.

We gave respondents the option to say that they don't expect AI will benefit their security team. However, security professionals with that opinion are rare: only 1.8% of the respondents surveyed (see Figure 11).

Figure 11:

Organizations that do or do not expect benefits from AI in cloud security situations.

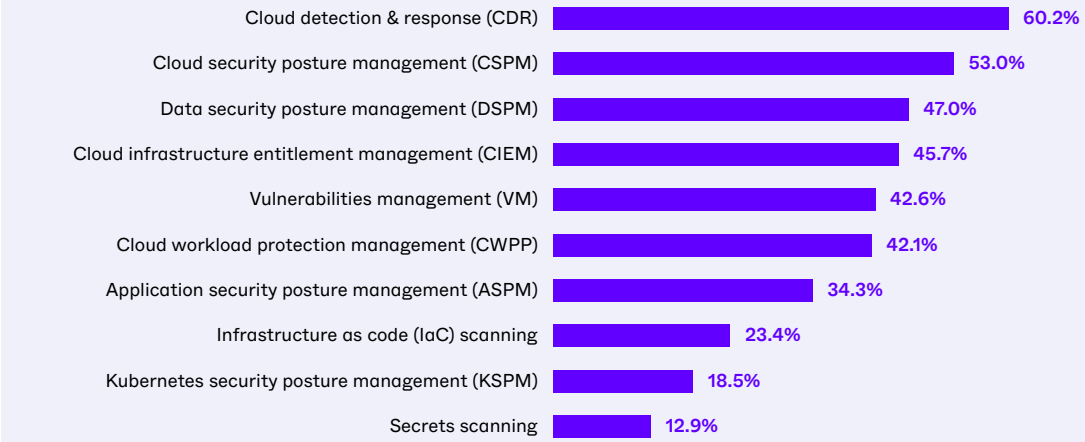


As we noted earlier, AI enables senior security professionals to perform more tasks in the same time period, and less experienced ones to handle tasks they would not have been ready to handle on their own. From the perspective of IT teams, AI fills gaps in experience and expertise.

Importance of Cloud Security Technologies

Which of the following cloud security technologies are most important for defending your organization's cloud infrastructure? (Select up to five.)

Figure 12:
Importance of cloud security technologies, on a scale from 1 to 5, with 5 highest.



Because cloud applications and data are subject to so many risks and threats, multiple cloud security technologies have evolved to protect them. We asked survey respondents to identify those most important to their organizations.

As shown in Figure 12, the two cloud security technologies cited most often were "Cloud detection and response (CDR)" (cited by 60.2% or respondents) and "Cloud security posture management (CSPM)" (53.0%).

CDR is a technology that provides real-time visibility, detection, and automated response across cloud environments. It automates the collection and correlation of forensic data and helps security teams identify suspicious activity and initiate actions to contain and mitigate attacks. CDR tools integrate with cloud-native application protection platforms (CNAPP) and security information and event management (SIEM) systems to proactively improve an organization's ability to defend against cloud threats.

CSPM solutions enable organizations to identify vulnerabilities and issues that undermine cloud security and affect compliance with industry frameworks and standards, automate policy enforcement, assess and document compliance, and improve their security posture over time.

> CSPM solutions enable organizations to identify vulnerabilities and issues that undermine cloud security and affect compliance... CIEM tools play a central, indispensable role in cloud security by consolidating the management of user identities and privileges... CWPP solutions protect workloads and identify misconfigurations, vulnerabilities, policy violations, and other security issues that might affect them.

The goals of “Data security posture management (DSPM)” (47.0%) products are similar to those of CSPM solutions, but focus primarily on controlling data and access to data.

“Cloud infrastructure entitlement management (CIEM)” tools (45.7%) play a central, indispensable role in cloud security by consolidating the management of user identities and privileges, monitoring how users (both human and non-human) access cloud resources, and enforcing policies based on the principle of least privilege and zero trust concepts.

“Cloud workload protection platform (CWPP)” solutions (42.1%) continuously monitor workloads, including virtual machines, on-premises servers, containers, and serverless functions to provide real-time protection for workloads and identify vulnerabilities, policy violations, and other security issues that might affect them.

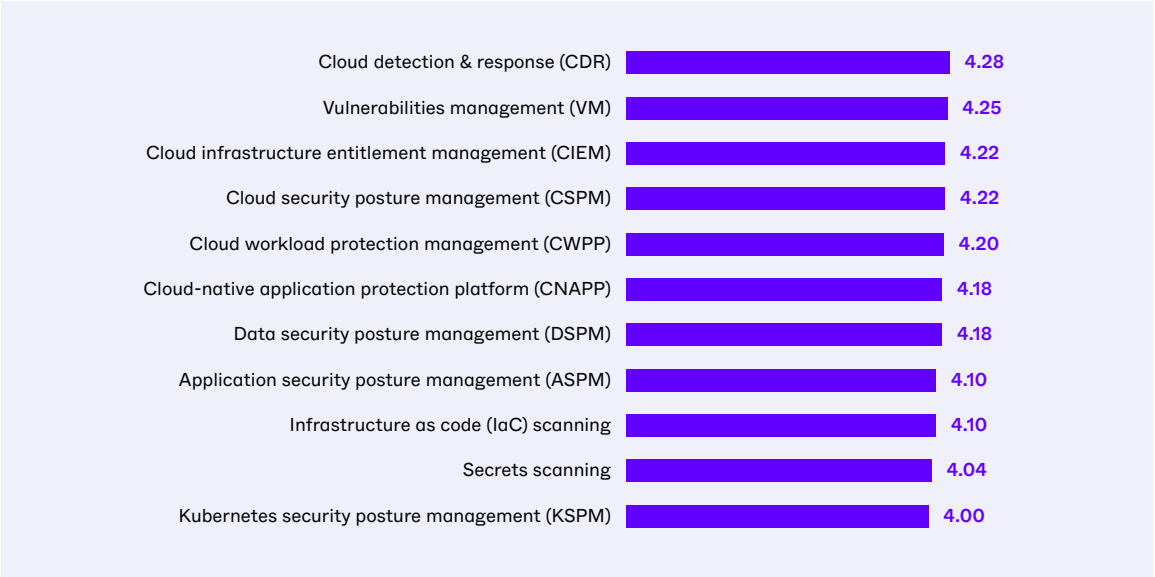
We want to call attention to the last response on this list: “Secrets scanning” (12.9%). This technology is highly valued by DevSecOps (development security operations) engineers and security-minded application developers but is not widely known by other security teams. However, we believe that is about to change. In this context, “secrets” include hardcoded credentials (such as passwords, API tokens, security certificates, and keys protecting access to cloud platform environments), encryption keys, and configuration files containing database passwords and API keys. In most organizations these keys can be found scattered across code repositories, version control systems, collaboration tools, and other inadequately protected locations. Threat actors who capture these secrets can not only breach cloud platforms and applications to steal data, potentially they can take control of operations or shut them down. As more security professionals come to appreciate the importance of DevSecOps and shift-left security (integrating security practices and vulnerability detection earlier in the software development life cycle), we anticipate that secrets scanning will be recognized as a “must have” capability.

As more security professionals come to appreciate the importance of DevSecOps and shift-left security (integrating security practices and vulnerability detection earlier in the software development life cycle), we anticipate that secrets scanning will be recognized as a “must have” capability.

Satisfaction with Cloud Security Technologies

On a scale of 1 to 5, with 5 being the highest, rate your organization's satisfaction with the performance of the following cloud security technologies.

Figure 13:
Satisfaction with the performance of cloud security technologies



After seeing how organizations rate the importance of 11 major cloud security technologies, we turn to the question of whether those technologies have been producing the expected results.

Survey respondents reported the highest levels of satisfaction with "Cloud detection and response (CDR)" (rated 4.28 on a scale of 1 to 5, with 5 highest), "Vulnerability management (VM)" (4.25), "Cloud security posture management (CSPM)" (4.22), "Cloud infrastructure entitlement management (CIEM)" (also 4.22), and "Cloud workload protection platform (CWPP)" (4.2) (see Figure 13).

As discussed in the previous section, these technologies enable cloud security teams to detect, monitor, analyze, and prioritize vulnerabilities, misconfigurations, policy violations, identity and access control problems, and other security issues, as well as helping them protect cloud-hosted workloads, prioritize risks, respond to cloud-based attacks, and deliver insights about their cloud security posture.

Since these five are among the most important cloud security technologies, it is good news that most organizations are satisfied with their performance.

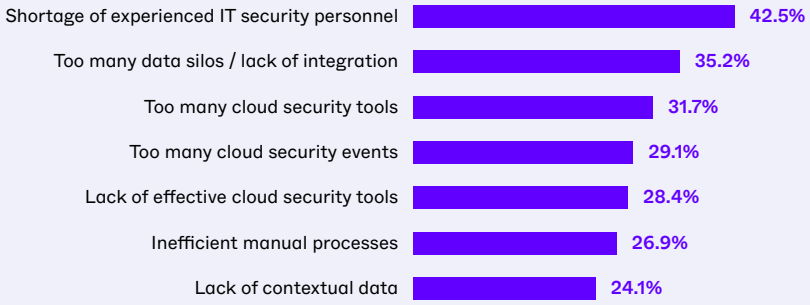
However, "Data security posture management (DSPM)," the technology that was listed as third most important in Figure 12, here is ranked in a tie for sixth in satisfaction, with a rating of 4.18. This suggests that some organizations may be concerned that one of the most important technologies is not performing up to expectations.

We should note that the four technologies at the bottom of the list — Application security posture management (ASPM), Infrastructure as code (IaC) scanning, Secrets scanning, Kubernetes security posture management (KSPM) — are operating under a disadvantage. As we will see in Figure 20, they are in earlier stages of deployment than the other solutions covered here. They may have lower satisfaction scores because they are still being tuned, or because they are simply less familiar to some of the respondents.

Factors Inhibiting Validation and Prioritization of Events

Which of the following factors most significantly inhibit your organization from validating and prioritizing cloud security events? (Select up to three.)

Figure 14:
Factors most significantly inhibiting validation and prioritization of cloud security events.



Some of the previous questions in this survey confirmed that most organizations struggle to validate and prioritize cloud security events in a timely manner. But what specific factors are preventing them from doing a better job?

The number one factor is "Shortage of experienced IT security personnel," selected by 42.5% of the respondents as one of their top three inhibitors (see Figure 14). This is consistent with last year's survey, and with many other surveys conducted by CyberEdge and other analysts. Staff shortages are a fact of life for cybersecurity teams across the world.

Here is a warning light flashing yellow: the issue of "Too many data silos/lack of integration" went from being picked by 30.0% of organizations last year to 35.2% this year. And here is a warning light flashing red: "Too many cloud security tools" went from being selected as a key problem by 24.9% last year to 31.7% in this survey, a striking increase of 6.8%. There are two ways of looking at these signals of increasing concern.

One view is that security teams are struggling to come to grips with the nature of cloud-based attacks. These often start with the compromise of a non-cloud asset (an endpoint with a vulnerability, a misconfigured on-premises web server, a stolen credential, an exposed encryption key) and move laterally through both cloud and on-premises applications and data stores. These attacks can only be detected, analyzed, and contained by gathering and correlating security data from many IT domains, including endpoints, cloud workloads, code repositories, identity and access management (IAM) systems, network devices, and security tools. Collecting and correlating data from all these silos can be extremely costly and time consuming, especially when SOC, development, and IT operations teams that don't usually work well together "own" different cloud and on-premises resources.

Alternately, we can look at these warning lights through a typical series of events:

1. As the cloud attack surface expands and threat actors develop new sophisticated attack techniques (see pages 7-10)...
2. Industry analysts identify the need for new security tools and concepts (e.g., cloud data/application/identity/extended/AI security posture management)...
3. Security solution vendors respond by delivering valuable new cloud security tools (see pages 19-20)...
4. IT security groups deploy several of these tools as point solutions, creating more management and integration issues.

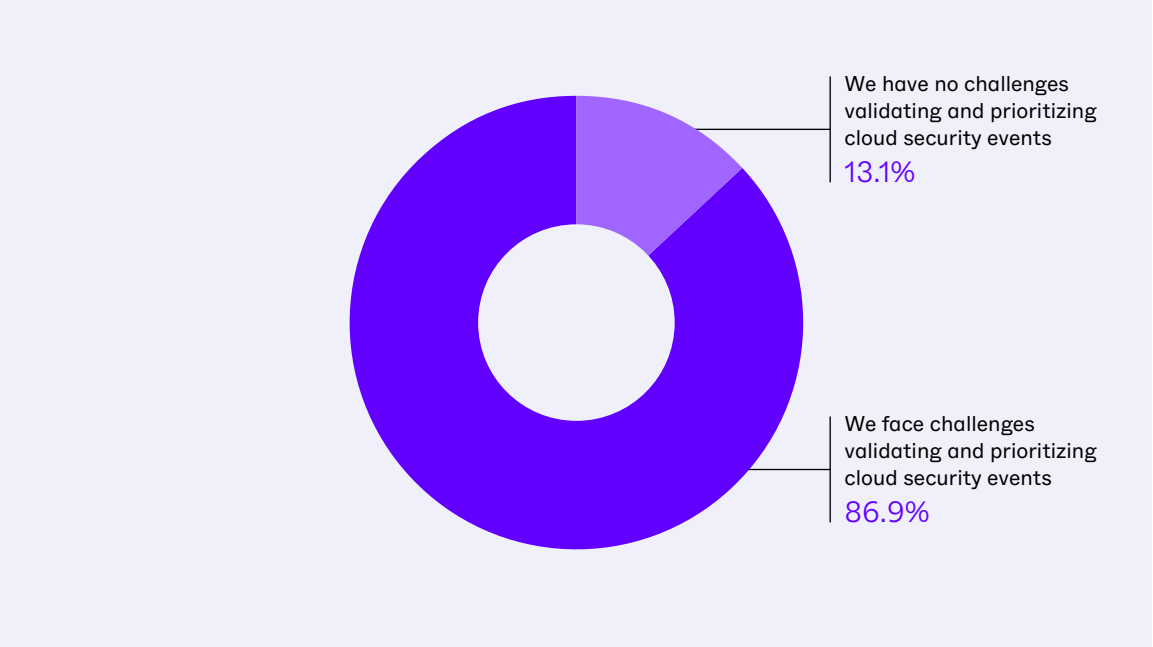
Either way of looking at the problem highlights the need for cloud security platforms that integrate multiple cloud security technologies. Only such platforms can provide visibility and correlate data for analysis across all the IT silos involved in cloud-based attacks.

Other factors inhibiting prompt analysis and response include "Too many cloud security events" (29.1%), "Lack of effective cloud security tools" (28.4%), "Inefficient manual processes" (26.9%), and "Lack of contextual data" (24.1%).

The overall picture we get from this data is that security teams are getting too many alerts, from too many sources, and face too many challenges analyzing and prioritizing them.

Don't feel alone if you have observed these issues in your organization. We gave survey respondents the option of saying "We have no challenges validating and prioritizing cloud security events." Only 13.1% choose that response (see Figure 15).

Figure 15:
Organizations that do or do not face chalenges validating and prioritizing cloud security events.



But we should not only focus on the negatives. Many of these issues can be met with:

- The increased use of AI and sophisticated simulation methods
- The deployment of cloud security platforms that provide visibility across cloud and non-cloud silos and integrate multiple cloud security technologies

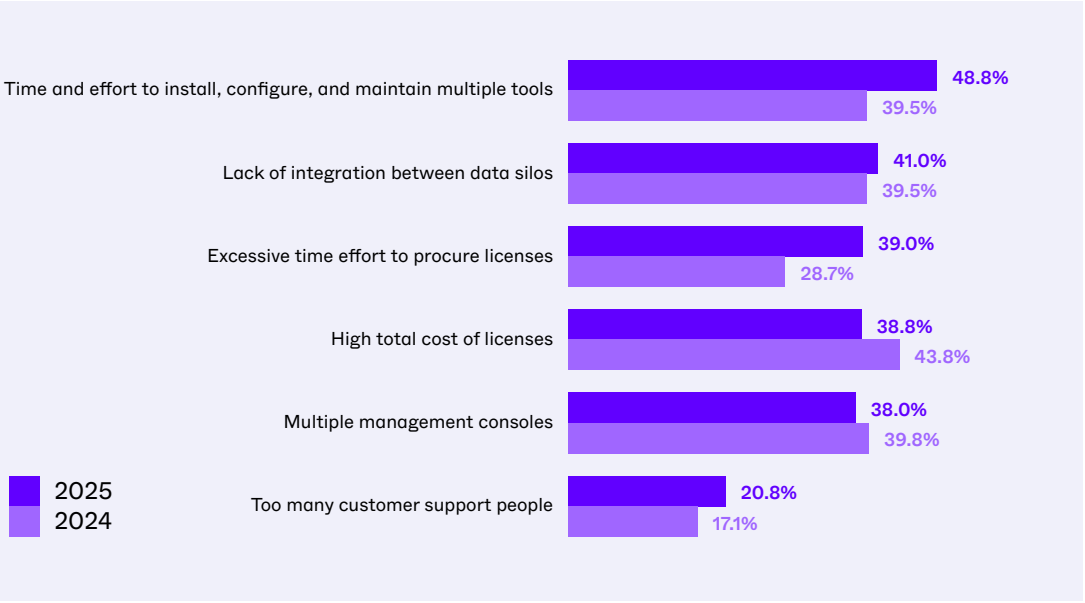
For example, AI-enabled cloud security platforms can eliminate many data integration problems, simplify management, provide unified visibility of many types of cloud security data, and perhaps most importantly, enable security teams to determine which threat signals must be addressed right away and which can wait until tomorrow.

Either way of looking at the problem highlights the need for cloud security platforms that integrate multiple cloud security technologies. Only such platforms can provide visibility and correlate data for analysis across all the IT silos involved in cloud-based attacks.

Problems Using Multiple Cloud Security Tools

If your organization uses multiple cloud security tools, which of the following problems have been most serious for you? (Select up to three.)

Figure 16:
Most serious problems caused by too many cloud security tools, 2025 compared to 2024.



In the responses to the last question we saw that many organizations cite "Too many cloud security tools" as a key factor preventing them from validating and prioritizing cloud security alerts. Here we drill down into some of the problems behind that issue by looking at changes from last year's survey results, because those are striking.

For example, the percentage of respondents selecting "Time and effort to install, configure, and maintain multiple tools," shot up by almost 10%, from 39.5% in the 2024 Cloud Security Report to 48.8% in this one (see Figure 16). That topic, which we might summarize as tool management, is now ranked far and away the top problem caused by having too many cloud security tools, after having been tied for third last year. The change stems from the growing number of cloud security tools being deployed and the increasing number of environments where they need to be installed and configured.

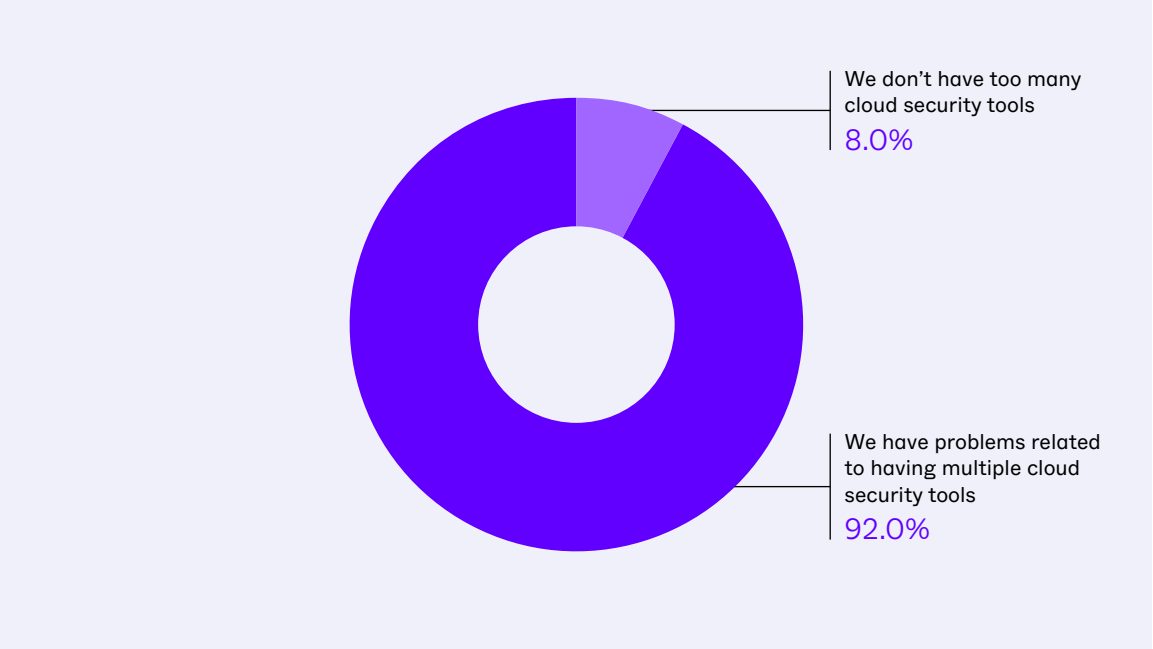
It is interesting to note that the largest decrease in responses compared to last year was in "High total cost of licenses." That problem was selected by 38.8% of respondents versus 43.8% in 2024, a 5.0% decline, falling from second place to fourth on this list. It appears that cloud security teams are less concerned about saving license fees and more concerned about protecting their time (which is consistent with the finding on the previous topic that a shortage of experienced IT security personnel is the greatest obstacle to handling cloud security alerts).

Also consistent with the findings in Figure 14: "Lack of integration between data silos" is a major issue, cited by 41.0% of respondents.

One final noteworthy change over the past year. In the 2024 survey, 13.4% of organizations said they don't have too many cloud security tools. This year, that figure fell to 8.0%. Now a full 92.0% of organizations con-

fess they are having problems related to having too many tools (see Figure 17).

Figure 17:
Most serious problems caused by too many cloud security tools, 2025 compared to 2024.



These concerns are all reasons why many organizations are moving toward unified cloud security platforms, whose benefits include ease of deployment, ease of administration, and a single vendor for procurement (see Figure 21 on page 31).

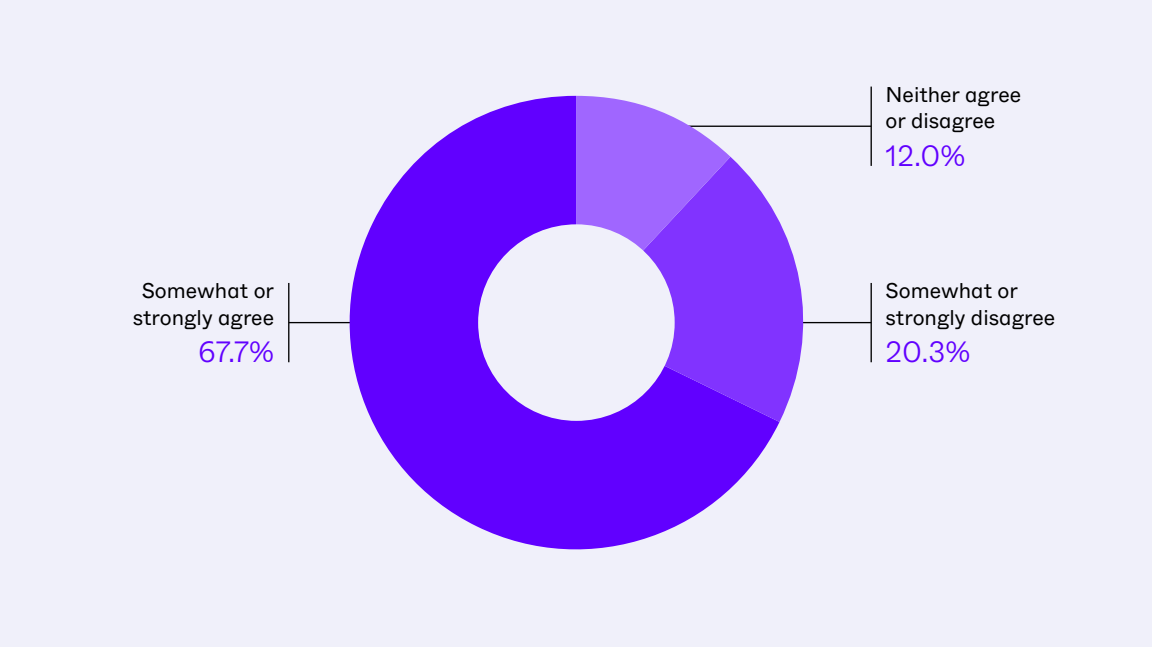
It appears that cloud security teams are less concerned about saving license fees and more concerned about protecting their time

Struggles with Volume of Cloud Security Data

Describe your agreement with the following statement: "My organization generates so much cloud security data that our cloud security team often struggles to derive and prioritize actionable insights.

Figure 18:

Agreement that their organization generates so much cloud security data that they often struggle to derive and prioritize actionable insights.



Exactly two-thirds of respondents (67.7%) somewhat or strongly agreed with the statement "My organization generates so much cloud security data that our cloud security team often struggles to derive and prioritize actionable insights" (see Figure 18). Only 20.3% somewhat or strongly disagreed with this statement, and another 12.0% neither agreed nor disagreed.

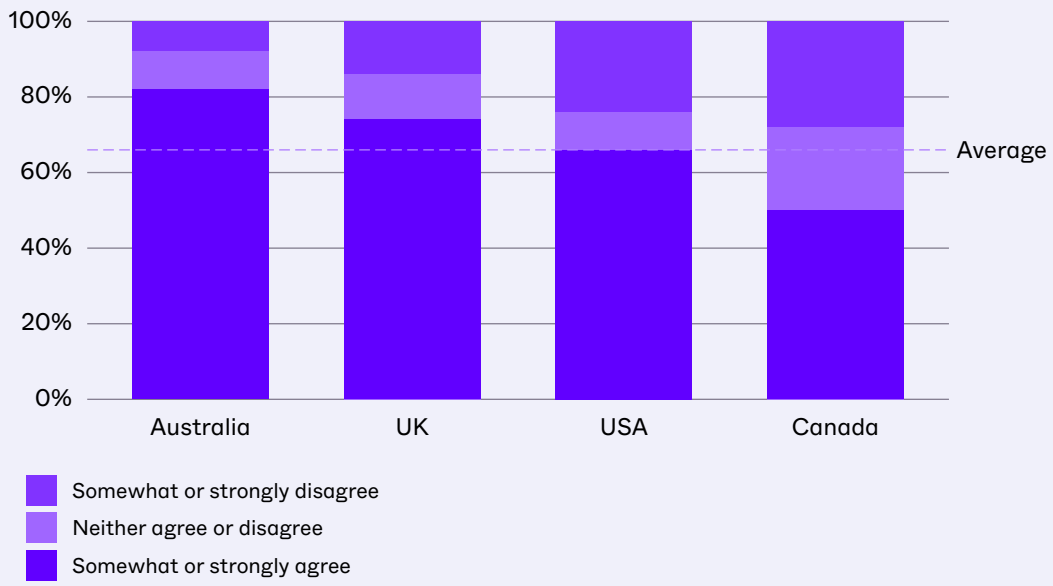
These findings confirm that the problem for most organizations is not too little cloud security data, but too much. Clearly many need to do a better job eliminating false positives and duplicative alerts so they can find and address the most serious attacks.

The year-to-year trend shows that this issue is becoming more serious over time. Compared to the last survey, the respondents saying they somewhat or strongly agreed increased more than 5%, while those who somewhat or strongly disagreed sank by about the same amount. The difference between those opinions increased by more than 10% over the year.

Among industries, agreement was significantly higher than average in manufacturing and finance and financial services, and healthcare and pharmaceuticals, and significantly below in education and government. Looking at the countries polled in this survey, agreement with the statement was highest in Australia lowest in Canada (see Figure 19).

Figure 19:

Agreement that their organization generates so much cloud security data that they often struggle to derive and prioritize actionable insights, by country.

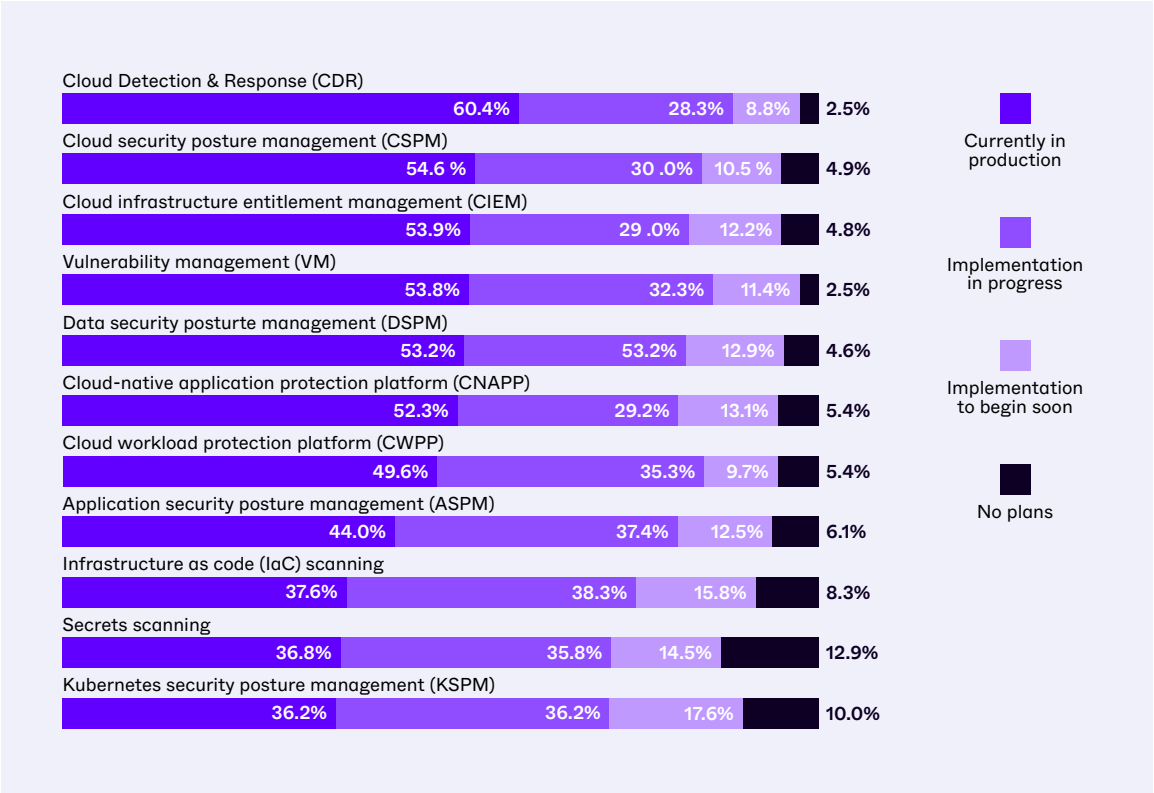


Section 3: Current and Future Investment

Deployment Plans for Cloud Security Technologies

Describe your organization's deployment plans for each of the following cloud security technologies.

Figure 20:
Deployment plans for cloud security technologies



Back on pages 13-14, we had survey respondents rate the importance of 11 major cloud security technologies and indicate how satisfied they are with their performance. Here we investigate whether those same 11 technologies have been or are planned to be deployed.

Six of the 11 cloud security technologies are already in production in more than half of organizations: "Cloud detection and response (CDR)," "Cloud security posture management (CSPM)," "Cloud infrastructure entitlement management (CIEM)," "Vulnerability Management," "Data security posture management (DSPM)," and "Cloud-native application protection platform (CNAPP)" (see Figure 20).

"Cloud workload protection platform (CWPP)" is in production in almost half of all organizations (49.6%), and the other solutions included in this question are running in at least one-third.

For most of these cloud security technologies, deployment levels continue to increase. Between the previous survey and this one, the "currently in production" rate increased from 49.0% to 54.6% for CSPM, from 50.5% to 53.9% for CIEM, from 48.1% to 53.2% for DSPM, from 32.0% to 36.8% for "Secrets scanning," and from 31.6% to 32.6% for Kubernetes security posture management (KSPM).

In fact, almost all these technologies can be considered proven, mainstream security solutions. All but two are either currently in production or being implemented in more than three-quarters of organizations.

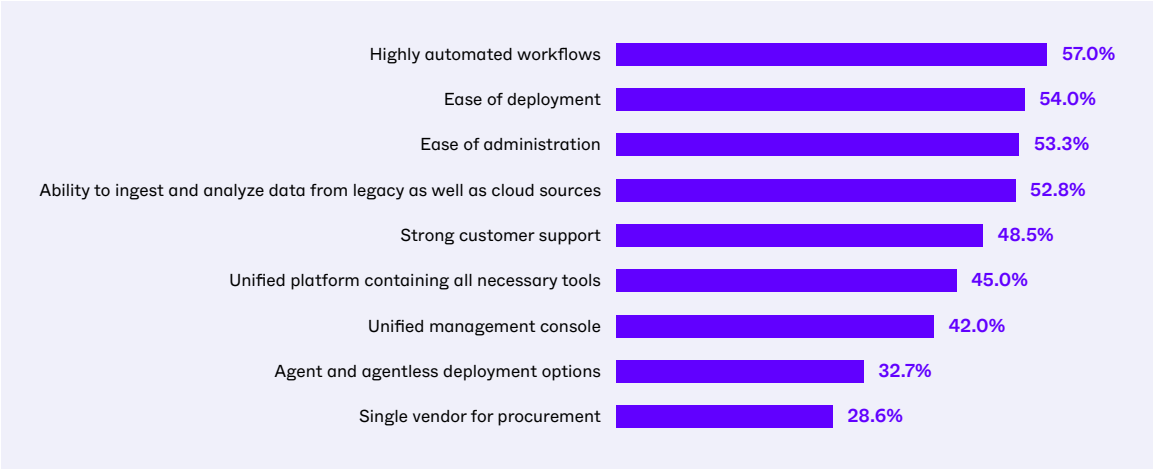
If you compare Figures 12 and 20, you will see that the order of the entries is almost the same. This shows that organizations are putting their money where their mouths are. That is, the cloud security technologies ranked as most important in Figure 12 are for the most part the ones most actively being used and implemented today.

If you compare Figures 12 and 20, you will see that the order of the entries is almost the same. This shows that organizations are putting their money where their mouths are. That is, the cloud security technologies ranked as most important in Figure 12 are for the most part the ones most actively being used and implemented today.

Criteria for Unified Cloud Security Platforms

Which characteristics are most important when selecting a unified cloud security platform? (Select up to five.)

Figure 21:
Most important characteristics when selecting a unified cloud security platform.



Unified cloud security platforms address many cloud security challenges, for example:

- Providing seamless visibility of security data across many cloud platforms and services
- Delivering automated workflows to correlate and analyze security data to generate alerts, flag compliance violations, and prioritize attack containment and remediation
- Enabling agentless and agent-based scanning across hundreds of endpoint types from a single console
- Offering single-vendor procurement and support

Data discussed earlier in this report suggest additional factors prompting organizations to centralize and strengthen their cloud security capabilities:

- New threats and expanding attack surfaces have created the need for innovative new cloud security technologies
- Organizations are struggling to integrate those technologies and correlate data from disparate technology silos

Finally, figures 14, 165, and 18 provide the strongest examples of the need for unified cloud security platforms.

But what specific benefits are organizations looking for in these platforms, and which are the most important?

The most prized characteristic on the list is “Highly automated workflows,” selected by 57.0% of the survey respondents (see Figure 21). Automated workflows can have a tremendous impact on an organization’s ability to detect and respond to attacks. They also simplify cloud security management activities and free up security professionals to work on high-priority tasks.

The next two selections on the list, “Ease of deployment” (54.0%) and “Ease of administration” (53.3%) show that organizations are extremely interested in cloud security platforms that don’t require a massive effort to implement and manage. This is consistent with the earlier finding that managing multiple cloud security tools and staffing shortages are currently the biggest factors preventing cloud security teams from achieving their goals.

The fourth pick on this list of desirable characteristics is “Ability to ingest and analyze data from both legacy and cloud sources” (52.8%). Without this capability, organizations can’t achieve complete visibility into their environment. Many also end up using two or more tools to handle the different sources, which raises costs and increases the time needed to respond to suspicious activities.

Other desirable characteristics include “Strong customer support” (48.5%), “Unified platform having all necessary tools” (45.0%), and “Unified management console” (42.0%).

> The most prized characteristic on the list is “Highly automated workflows”... Automated workflows can have a tremendous impact on an organization’s ability to detect and respond to attacks. They also simplify cloud security management activities and free up security professionals to work on high-priority tasks.

Conclusions

New Challenges on Top of Old Ones

There are some areas of cybersecurity where emerging threats tend to eclipse old ones, which gradually fade away. However, our data shows that cloud security is not like that. While new challenges continue to appear, the ones that plagued the industry 15 years ago are still here in force, including misconfigurations (now on cloud platform assets as well as on-premises systems), staff shortages, and security tools that don't talk to each other. In fact, many of the attacks that have been with us for a decade or more have increased their frequency and sophistication, largely through the powers of AI.

The impact of this phenomenon is that cloud security teams are being asked to address an ever-wider range of threats, in higher volumes, across broader attack surfaces, all at once. This is also putting pressure on cloud security vendors to offer more integrated, highly scalable solutions.

A Great Cocktail: Combine Integration, Automation, and AI

Wider attack surfaces demand more cloud security technologies, which generate more alerts, which overwhelm SOCs. More sophisticated threats can only be detected, analyzed, and contained by correlating security data from more sources. How can cloud security teams possibly keep up?

Only with a cocktail of integration, automation, and AI. Integration, to collect data efficiently from many sources and share it with multiple security tools. Automation, to speed up security processes with minimal human intervention. AI, to identify patterns in huge volumes of data and recommend optimum responses. Put only two of these together and the result will be bitter. But combine all three ingredients and you have a great concoction. Or better yet, let someone else combine the three of them for you.

Prioritization and Focus Are the Name of the Game

A lot of the improvements we see in cloud security involve doing more to prioritize risks and remediation activities. For example, obtaining and using evidence of exploitability enables security teams to focus on threats that really matter to a specific organization instead of those that are merely labelled "critical" by an outside party. Various types of security posture management (DSPM, ASPM, IDSPM, XSPM, AI-SPM, etc.) involve assessing risks in order to prioritize the most important issues. And integration, automation, and AI can be a powerful combination (see above) for narrowing choices and making decisions based on organizational policies and priorities.

Cloud Security is Where the Action Is

Cloud security work is fast paced. Constantly challenging. Often (or always?) stressful. But it's also a great place to observe almost all aspects of cybersecurity, see where the field is going, and master many of the most cutting-edge concepts and technologies of information technology. Embrace it.

Appendix 1: Survey Demographics

This report is based on survey results obtained from 400 qualified participants hailing from four countries (see Figure 22). Each participant was required to have a role as a cybersecurity manager or practitioner with knowledge about their organization's cloud security program (see Figure 23). Almost three-quarters (73.5%) of our respondents hold executive or managerial positions in cybersecurity.

Figure 22:
Survey respondents by country.

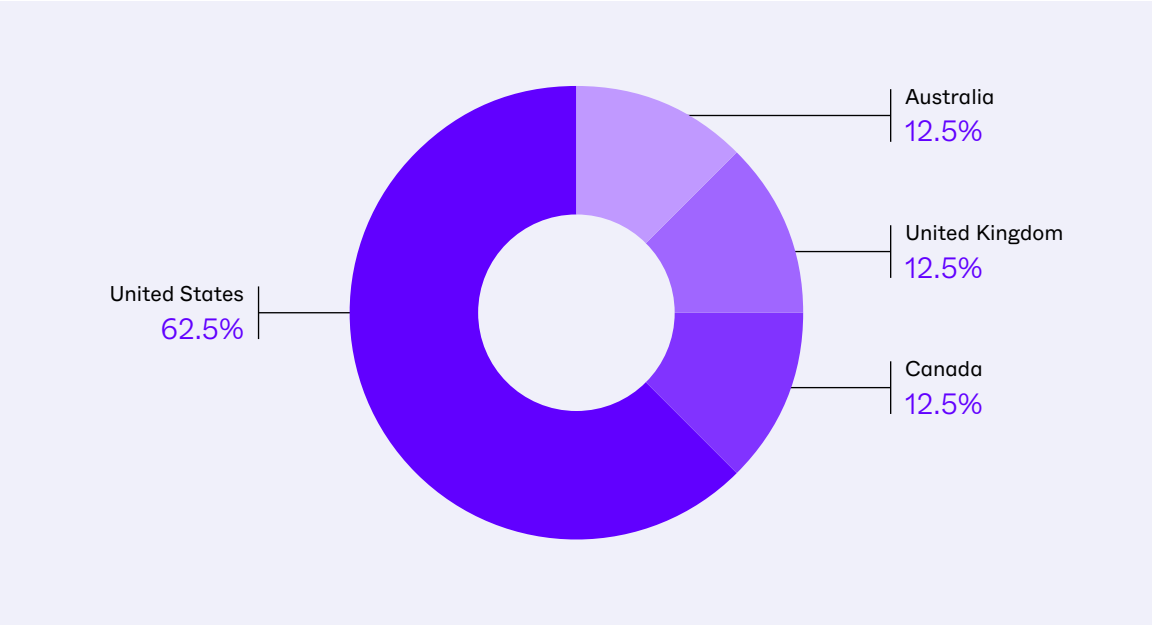
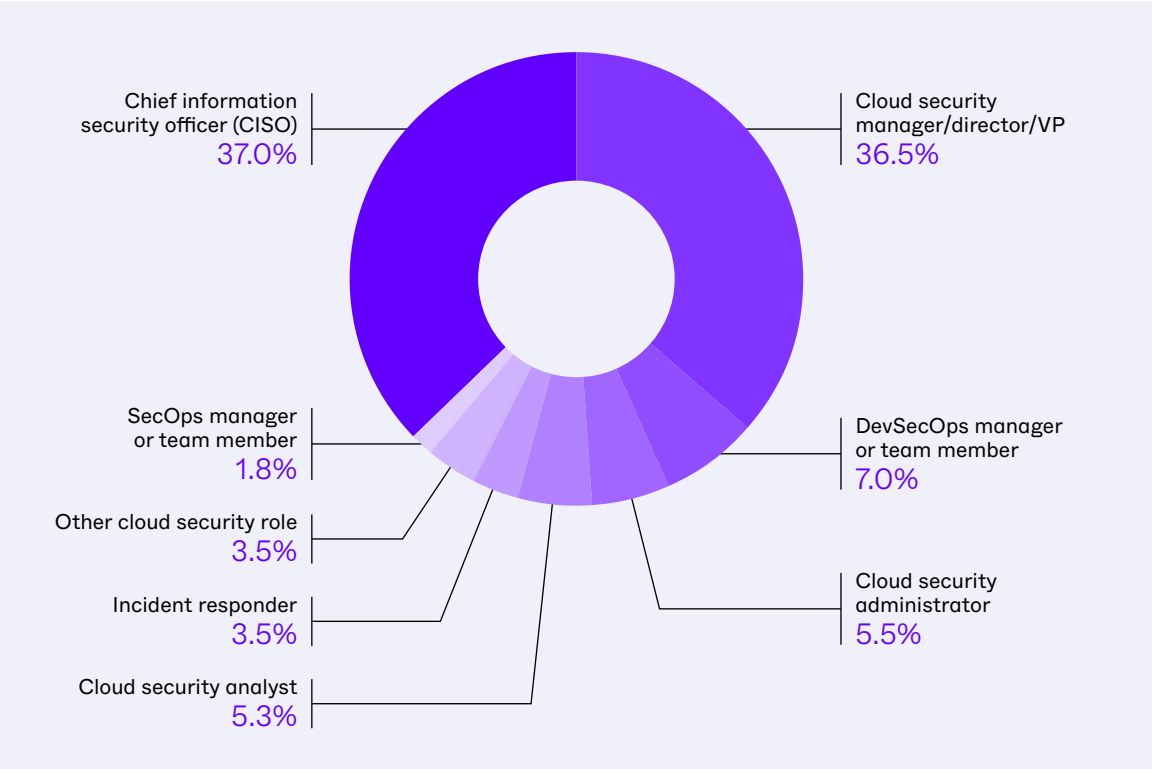


Figure 23:
Survey respondents by role.



All participants in this survey were working for organizations with 500 or more employees (see Figure 24). They spanned 8 major industries (plus “Other”) with no single industry composing more than 15.8% of the total participants (see Figure 25).

Figure 24:
Survey respondents by organization employee count.

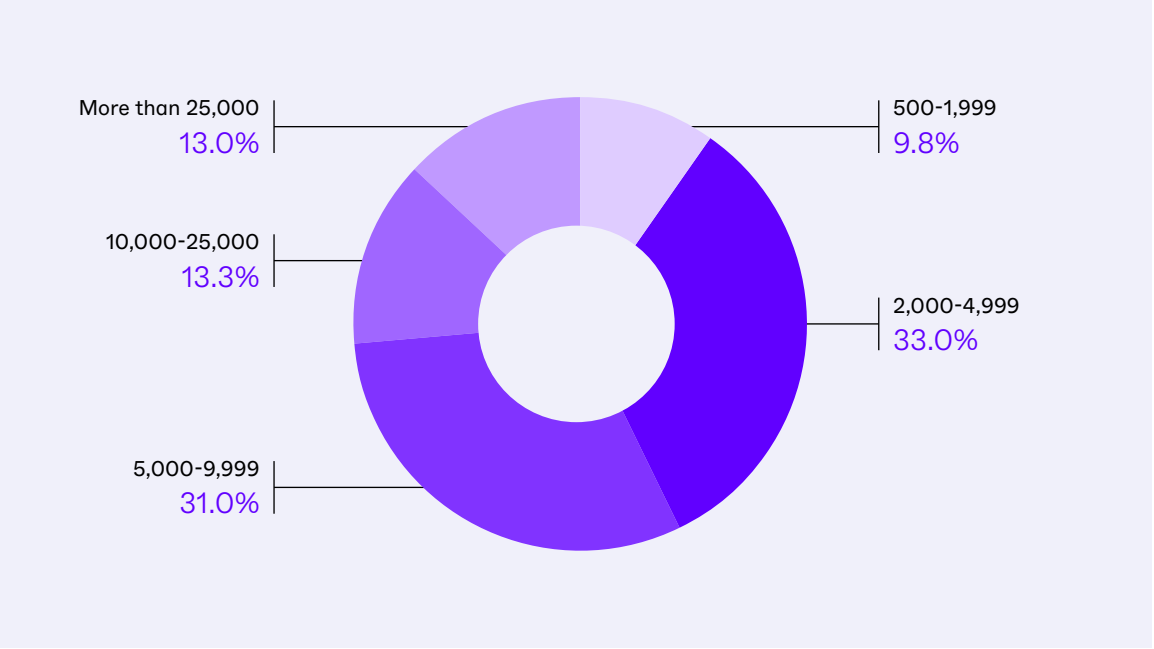
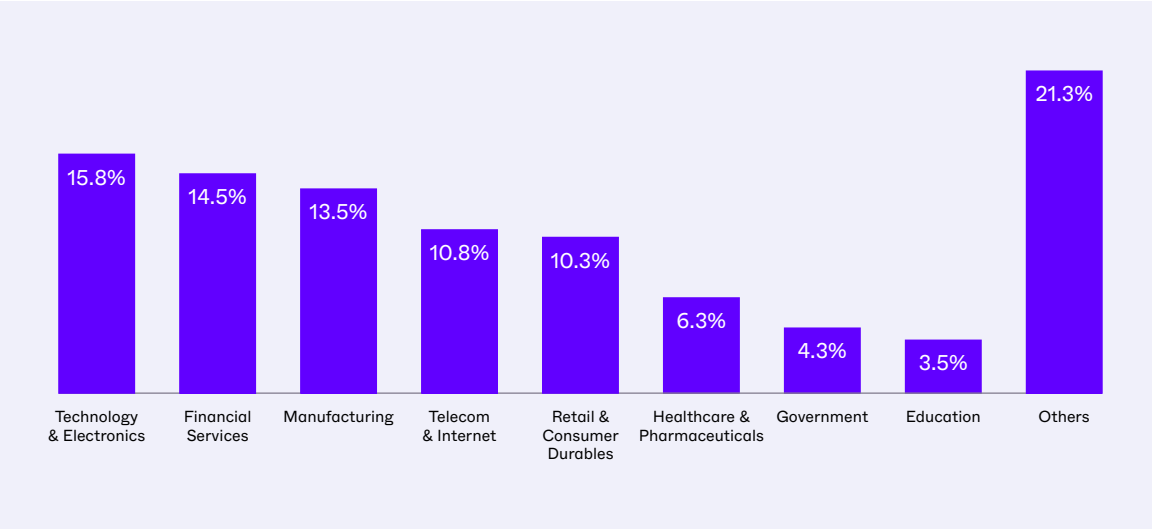


Figure 25:
Survey respondents by industry.



Appendix 2: Research Methodology

CyberEdge developed a 17-question survey instrument in partnership with SentinelOne. The survey was completed by 400 security professionals in the United States, Canada, the United Kingdom, and Australia in November 2024. The global margin of error for this research study (at a standard 95% confidence level) is 5%. All results pertaining to individual countries and industries should be viewed as anecdotal, as their sample sizes are much smaller. CyberEdge recommends making actionable decisions based on global data only.

All respondents had to meet two filter criteria: (1) they had to have a cybersecurity role; and (2) they had to be employed by a commercial or government organization with a minimum of 500 global employees.

At CyberEdge, survey data quality is paramount. CyberEdge goes to extraordinary lengths to ensure its survey data is of the highest caliber by following these industry best practices:

- Ensuring that the right people are being surveyed by (politely) exiting respondents from the survey who don't meet the respondent filter criteria of the survey (e.g., job role, company size)
- Ensuring that disqualified respondents (who do not meet respondent filter criteria) cannot restart the survey from the same IP address in an attempt to obtain the survey incentive
- Constructing survey questions in a way that eliminates survey bias and minimizes the potential for survey fatigue
- Only accepting completed surveys after the respondent has provided answers to all of the questions
- Randomizing survey responses when possible to prevent order bias
- Adding "Don't know" (or comparable) responses when possible so respondents aren't forced to guess at questions when they don't know the answer
- Eliminating responses from "speeders" who complete the survey in a fraction of the median completion time
- Eliminating responses from "cheaters" who apply consistent patterns to their responses (e.g., A,A,A,A and A,B,C,D,A,B,C,D)
- Ensuring the online survey is fully tested and easy to use on computers, tablets, and smartphones

CyberEdge would like to thank SentinelOne for making this research study possible. We'd particularly like to thank Adam Hall, Andy Wool, Cameron Sipes and Joseph Coletta for sharing their cloud security knowledge and perspectives with us.

Appendix 3: About Our Sponsor

SentinelOne is a leading AI-powered cybersecurity platform. Built on the first unified Security Data Lake, SentinelOne empowers the world to run securely by creating intelligent, data-driven systems that think for themselves, stay ahead of complexity and risk, and evolve on their own. Leading organizations—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments— trust SentinelOne to Secure Tomorrow™. Learn more at sentinelone.com.

Appendix 4: About CyberEdge Group

Founded in 2012, CyberEdge is the largest, fastest-growing research, marketing, and publishing firm to serve the cybersecurity vendor community, working with approximately one in every four established security vendors.

CyberEdge's highly acclaimed Cyberthreat Defense Report (CDR) and other single- and multi-sponsor survey reports have garnered numerous awards and have been featured by both business and technology publications alike, including The Wall Street Journal, Forbes, Fortune, USA Today, NBC News, ABC News, SC Magazine, DarkReading, CISO Magazine, and others.

CyberEdge has cultivated a reputation for delivering the highest-quality market research data, survey reports, analyst reports, white papers, and custom books and eBooks in the cybersecurity industry. The depth of its cybersecurity subject matter expertise and the breadth of its services are second to none.

To learn more about CyberEdge, connect to www.cyberedgegroup.com.

Contact Us

sales@sentinelone.com
+1-855-868-3733

sentinelone.com

For more information on SentinelOne's award-winning AI-Powered Singularity™ Cloud Security, visit s1.ai/CNAPP

About SentinelOne

SentinelOne is a leading AI-powered cybersecurity platform. Built on the first unified Data Lake, SentinelOne empowers the world to run securely by creating intelligent, data-driven systems that think for themselves, stay ahead of complexity and risk, and evolve on their own. Leading organizations—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—trust SentinelOne to Secure Tomorrow™.