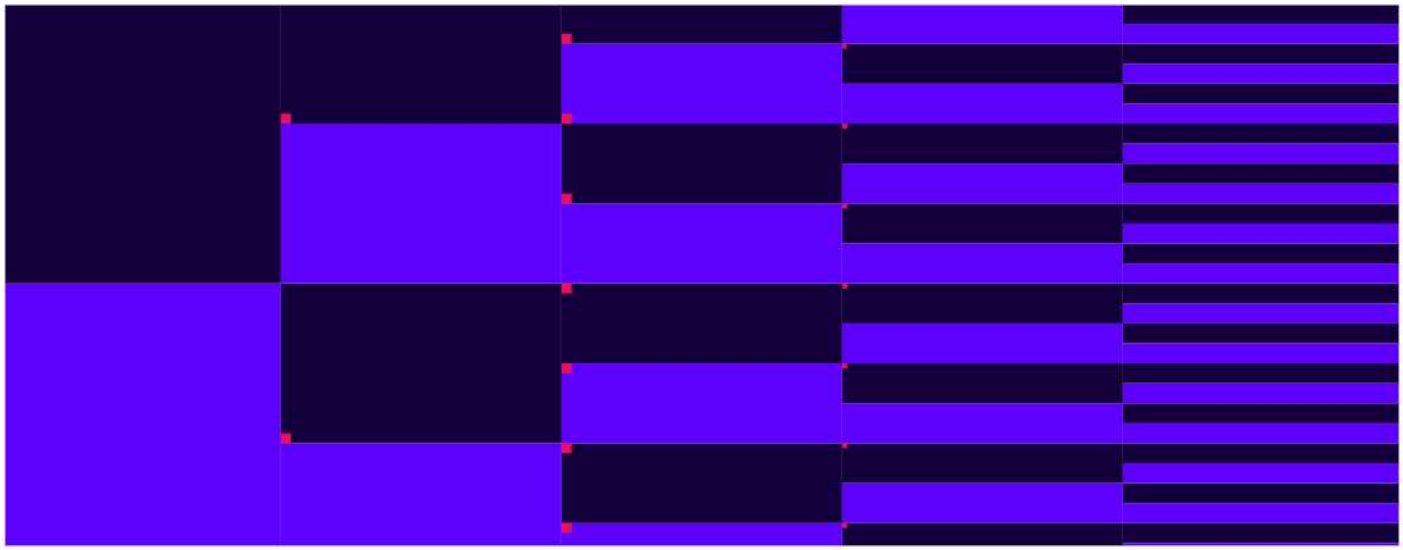
SentinelOne
Secure Tomorrow™

CYBEREDGE GROUP℠

2024 Cloud Security Report

Gain dozens of actionable insights from 400+ organizations on cloud security threats and solutions

Table of Contents



Introduction

The SentinelOne 2024 Cloud Security 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 April 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 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 on cloud security threats and solutions. Here are our top five takeaways:

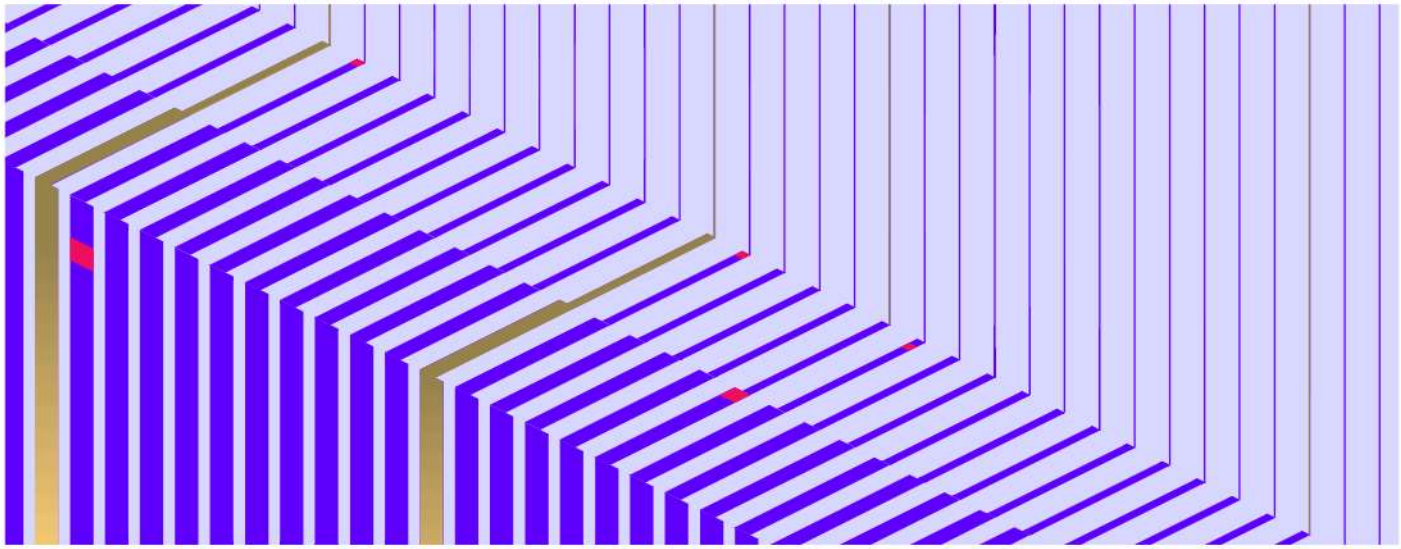
1. **Cloud security is no longer a niche**
   As organizations transition more data and applications to the internet, cloud security has become a field as rich and complex as any area of information security. Survey results confirm that cloud security professionals are seriously concerned about 10 different types of risks and threats. To counter these risks and threats, most have deployed seven or more cloud security technologies. Almost every cybersecurity domain now has a role to play in cloud security.

2. **Confidence, balanced by concern**
   Organizations are mostly confident about their capabilities in several core cloud security functions such as threat detection, incident investigation, and vulnerability assessment. However, they are concerned about other areas such as cloud asset discovery and configuration security. Also, it is clear that most cloud security teams need to improve their ability to investigate alerts promptly and filter out false positive alerts.

3. **Factors inhibiting effective response**
   Several issues are preventing cloud security teams from effectively validating and prioritizing cloud security events. The biggest barrier by far is a shortage of experienced IT security personnel. Other important factors relate to an overwhelming volume of security data, too many stand-alone cloud security tools, and a lack of integration between the tools, and insufficiently automated processes.

4. **A wide range of cloud security technologies are now mainstream**
   Seven key cloud security technologies are already in production in at least 45% of all organizations: cloud detection and response, vulnerability management, cloud infrastructure entitlement management, cloud security posture management, data security posture management, application security posture management, and cloud workload protection.

5. **Benefits from unified cloud security platforms**
   Several survey findings confirm that most organizations are struggling to manage multiple cloud security point products. Many are looking at unified cloud security platforms to simplify management, automate workflows, and integrate data silos.



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 shows how respondents rate the importance of 10 key cloud security technologies. It also explores several areas of concern: factors that inhibit cloud security teams from analyzing alerts, problems caused by too many cloud security tools, and the percentage of organizations that say they have to struggle with too much cloud security data.

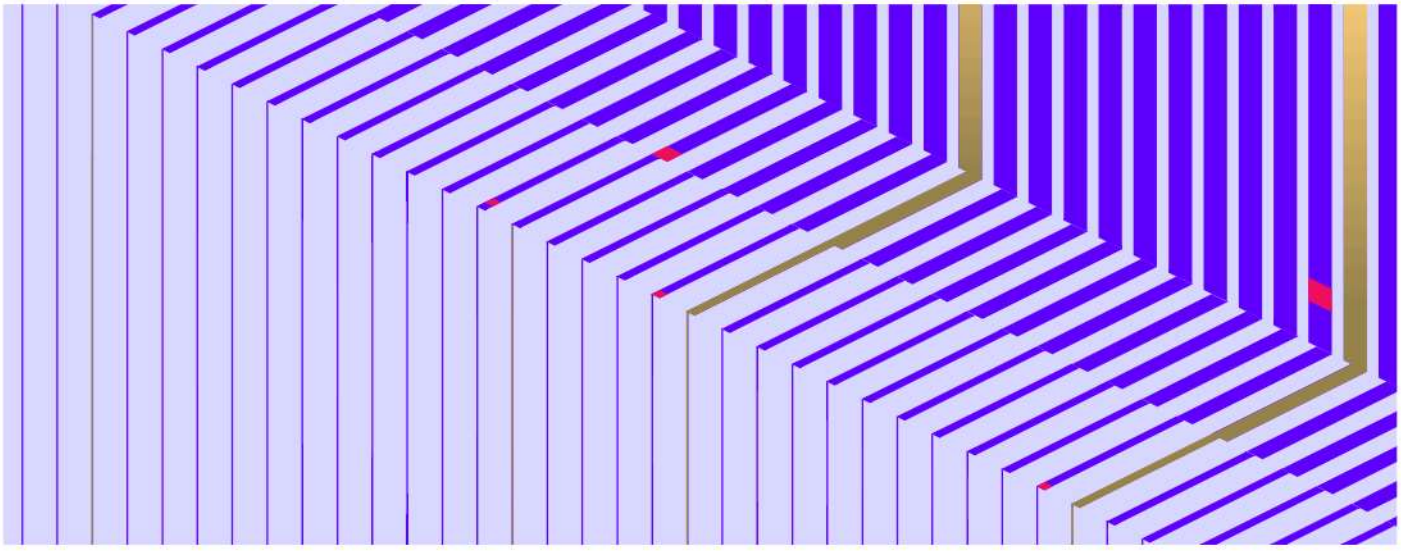
Section 3: Current and Future Investment

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 respondent's expectations related to benefits from unified cloud security platforms and the embedding of AI in cloud security solutions.

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 losing sleep over data breaches, malware and fileless attacks, unauthorized access, and violations of data privacy regulations. Other major concerns include account hijacking, denial of service attacks, and insecure APIs (page 7).
- **Cloud security capabilities** Respondents are mostly confident about their organization's capabilities for threat detection, incident investigation, and vulnerability assessment. However, they are worried about cloud asset discovery and configuration security (page 9).
- **Alert investigation timing** Just over one-third of organizations are investigating 90% or more of cloud security alerts within 24 hours. We consider that excellent performance. But the other two-thirds are not doing nearly as well (page 9).
- **False positive alerts** In more than half of organizations at least 40% of the cloud security alerts that reach security operations teams are false positives. That is likely to lead to overworked and frustrated security teams and potentially damaging mistakes (page 11).

Perceptions and Concerns

- **Cloud security technologies** The most important cloud security technologies, according to respondents, are cloud detection and response (CDR), vulnerability management (VM), cloud, data, and application security posture management (CSPM, DSPM, and ASPM), and cloud workload protection (CWP) (page 13).
- **Inhibitors of good security** The biggest factors preventing organizations from validating and prioritizing cloud security alerts are "Shortage of experienced IT security personnel," "Too many cloud security events," and "Too many data silos and lack of integration" (page 15).
- **Problems from multiple tools** The most serious problems related to using too many cloud security tools are "High total cost of licenses," "Multiple management consoles," and "Lack of integration between data silos" (page 17).
- **Struggles with too much data** 62% or respondents agree with the statement: "My organization generates so much cloud security data that our cloud security team often struggles to derive and prioritize actionable insights" (page 19).

Current and Future Investments

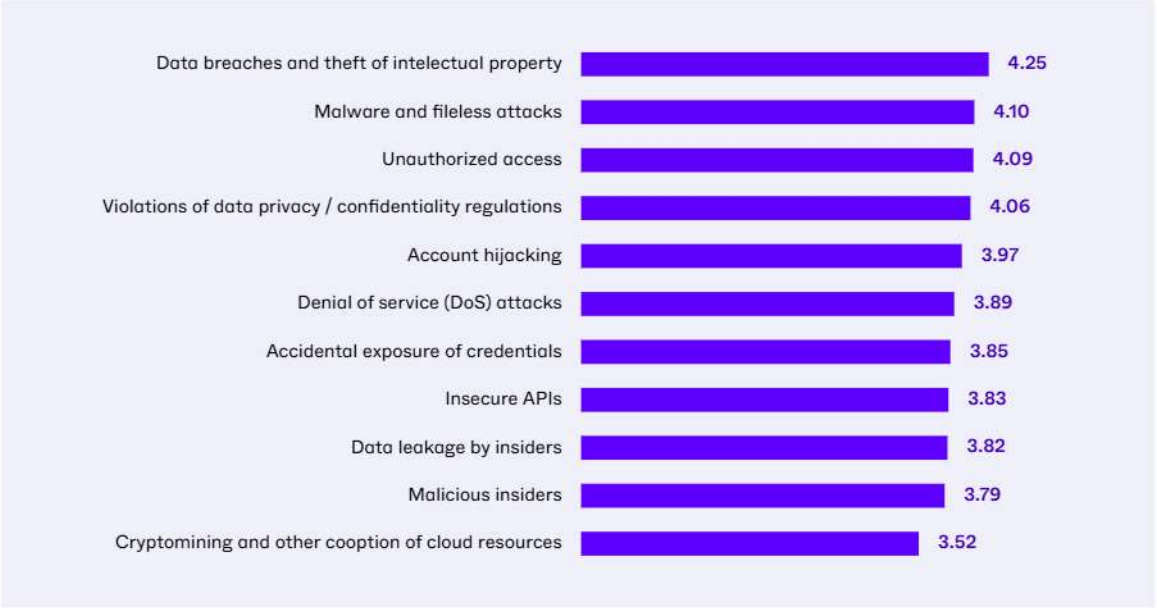
- **Adequacy of investment** A majority of respondents agree that their organization's investment in cloud security is adequate. Even so, the desired results are not being achieved.
- **Technology deployment plans** Seven key cloud security technologies are mainstream: CDR, VM, CIEM, CSPM, DSPM, ASPM, and CWP. (page 21).
- **Cloud security platforms** The characteristics most important for selecting a unified cloud security platform are ease of administration, highly automated workflows, ease of deployment, and the ability to ingest and analyze data from both legacy and cloud sources (page 22).
- **AI for cloud security** Expected benefits from artificial intelligence in cloud security solutions include speeding up incident response, detecting attacks faster, better risk scoring, increasing the effectiveness of the cloud security team, and prioritizing remediation better (page 23).

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.



When it comes to data and applications in the cloud, security teams face a wide range of security risks and threats. Which ones are keeping them up at night? To find out, we asked survey respondents to rate their level of concern for 11 significant risks and threats on a scale of 1 to 5, with 1 being "least concern" and 5 being "greatest concern."

Four of the threats were rated higher than 4 on the scale, indicating a very high level of concern (see Figure 1). However, the other seven were not far behind, all rated between 3.5 and 4. This validates the idea that cloud security is a complex discipline whose practitioners face a broad threat landscape.

Respondents are most concerned about "Data breaches and theft of intellectual property" (rated 4.25 on the scale of 1 to 5), "Malware and fileless attacks" (4.10), and "Unauthorized access" (4.09). These have long been top issues for data center security, and these results confirm that they are central to cloud security as well.

Rounding out the top four is "Violations of data privacy and confidentiality regulations" (4.06). This high level of concern demonstrates that cloud security is not only about preventing data breaches and ransomware attacks. Today, compliance with privacy and confidentiality regulations is also a fundamental goal. It is likely to play an even more prominent role in cloud security as the privacy requirements expand in standards such as the EU General Data Protection Regulation (GDPR), HIPAA, PCI DSS, and the California Consumer Privacy Act.

The relatively high level of concern for "Account hijacking" (3.97) and "Denial of service attacks" (3.89) highlight the fact that cloud applications and infrastructure are exposed to a wide variety of external threats.

A rating of 3.83 for "Insecure APIs" attests the fact that application security, although typically the responsibility of application development groups rather than security teams, is also a significant concern for the latter.

We found it very interesting that risks related to insiders, although rated slightly lower, are also taken very seriously by cloud security managers and practitioners. These include "Accidental exposure of credentials" (3.85), "Data leakage by insiders" (3.82), and "Malicious insiders" (3.79).

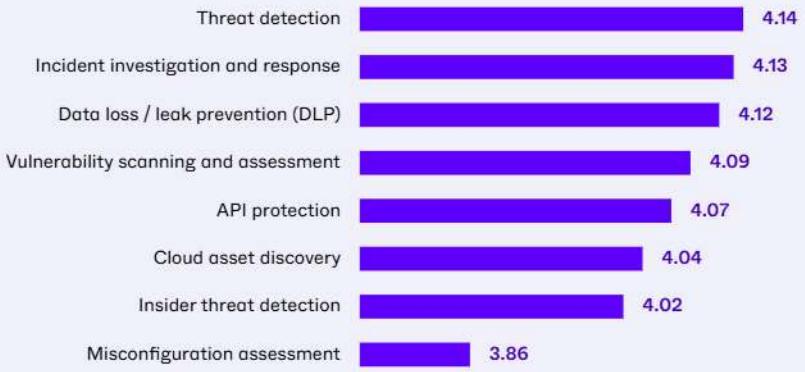
One striking conclusion from these results: almost every cybersecurity function now has a role to play in cloud security. These include network and infrastructure security, data protection, application security, privacy and compliance, fraud prevention, and security awareness training for employees.

Respondents are most concerned about "Data breaches and theft of intellectual property".

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.



Speaking of cybersecurity functions, how comfortable are organizations about their capabilities (including people and processes) in critical areas? We asked respondents to rate the adequacy of their organization's cloud security capabilities on a scale from 1 ("least adequate") to 5 ("most adequate").

The good news is that organizations are mostly confident about their capabilities in core cloud security functions such as "Threat detection" (4.14), "Incident investigation and response" (4.13), and "Data loss or leak prevention (DLP)" (4.12) (see Figure 2). Many have been able to extend existing processes for threat detection and incident response, honed over many years in data centers, to cover their cloud domains.

Confidence is also high for "Vulnerability scanning and assessment" (4.09) and "API protection" (4.07). These are areas where many organizations have made considerable investments over the past few years.

However, ratings drop down a notch, to 4.04, for "Cloud asset discovery." In the past, most application software and data stores resided on corporate-owned servers, making asset discovery relatively straightforward.

Today, application workloads and databases can be scattered over multiple cloud platforms, and employees can be connecting with SaaS applications, cloud storage services, code repositories, and other information assets not monitored by (and sometimes invisible to) security teams. In this environment, asset discovery and classification has become much more difficult for security teams – and more critical.

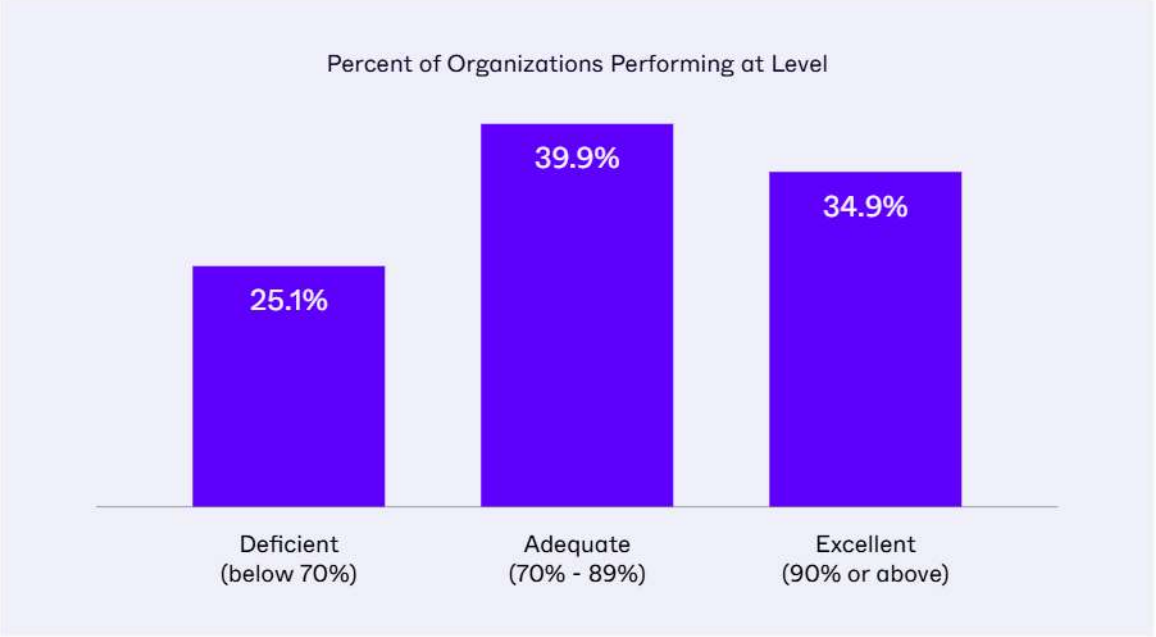
According to respondents, their organizations' biggest weak spot is "Misconfiguration assessment" (3.86): their ability to assess and protect the configurations controlling the behavior of cloud platforms and infrastructure. Without solid configuration security, threat actors can escalate their privileges, expose and exfiltrate sensitive data, disrupt operations, and basically bring cloud environments to their knees. Configuration mistakes by system and application administrators and other insiders can have the same effects, as well as creating vulnerabilities that adversaries can exploit. Cloud security posture management (CSPM) solutions are designed to reduce these risks, which has made them one of the "rising stars" of cloud security technologies.

According to respondents, their organizations' biggest weak spot is 'Misconfiguration assessment': their ability to assess and protect the configurations controlling the behavior of cloud platforms and infrastructure.

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.



Even before organizations began transitioning applications to the cloud, security operations teams complained about being overwhelmed by alerts. They struggled mightily to address at least the most serious alerts quickly enough to contain attacks before they caused major damage. How are they doing now, with cloud security alerts?

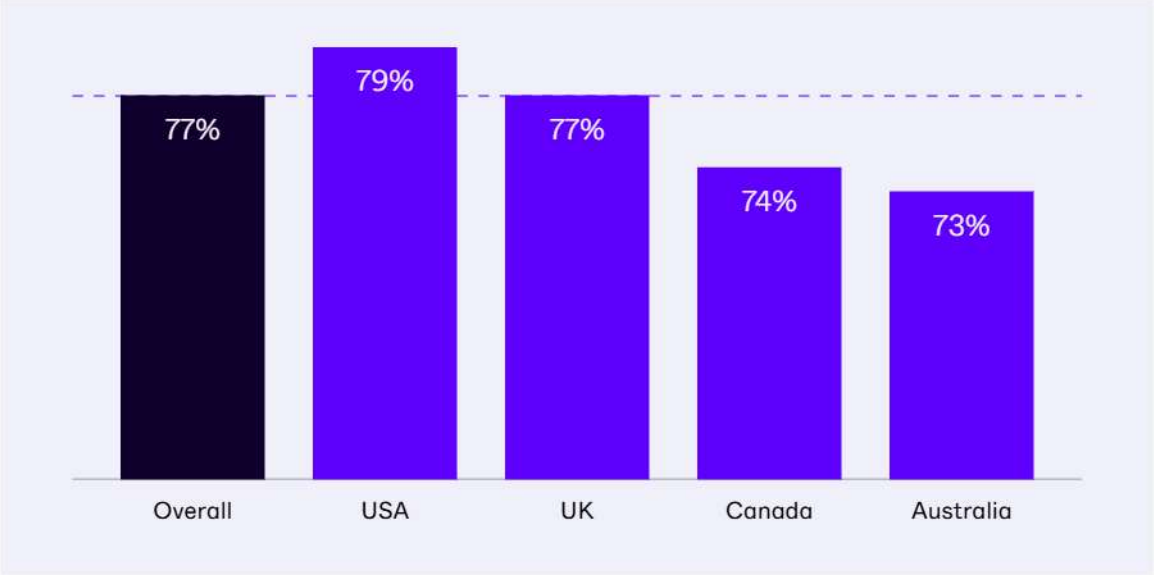
We asked respondents to the percentage of cloud security alerts their organizations are able to investigate within 24 hours, and grouped their responses into three categories (see Figure 3).

Our "excellent" category consists of the just over one-third of organizations (34.9%, to be precise) that investigate 90% or more of cloud security alerts within 24 hours. That's not perfect: even one uninvestigated alert can result in a data breach or other major problem. But given the current realities of limited staff and high alert volumes, analyzing at least nine out of ten alerts within a day is quite credible.

Our "adequate" category is the roughly two out of five organizations (39.9%) that investigate between 70% and 89% of cloud security alerts within 24 hours. This group is in a class half full/glass half empty range: addressing 70%-89% within a day reflects a lot of effort, but being slow to get to the other 11%-30% is a cause for concern. We say to those organizations: "not terrible, but you need to work on this area."

Finally, about one-quarter or organizations (25.1%) fall into our "deficient" category, investigating less than 70% of cloud security alerts within 24 hours. These organizations should be very concerned.

Figure 4:
Average (mean) percentage of cloud security alerts investigated within 24 hours, overall and by country.



We also calculated the average (mean) response for the sample as a whole, and for the respondents in each country (see Figure 4).

The overall average is 77% of cloud security alerts investigated within 24 hours. Again, this implies that around half of organizations are doing okay, but the other half should be very concerned.

The overall average is 77% of cloud security alerts investigated within 24 hours. This implies that around half of organizations are doing okay, but the other half should be very concerned.

The results for the USA are slightly better than the sample as a whole (79% versus 77%). Organizations in the UK are right at the overall average. However, Canada and Australia are lagging, at 74% and 73%, respectively.

Of course, these figures aren't the whole story. All alerts are not created equal. Organizations that can reduce false positives and prioritize critical alerts will reduce risk the most. We will discuss that next.

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.

All security operations teams waste time investigating security alerts that turn out to be false positives, i.e., threats that are not relevant to the organization. For example, a malware sample detected on the network wouldn't be relevant if the organization has controls that will detect and block it, or if it exploits a vulnerability in a system the organization doesn't use. While some security teams waste relatively little time with false positive cloud alerts, others find themselves swamped by them (see Figure 5).

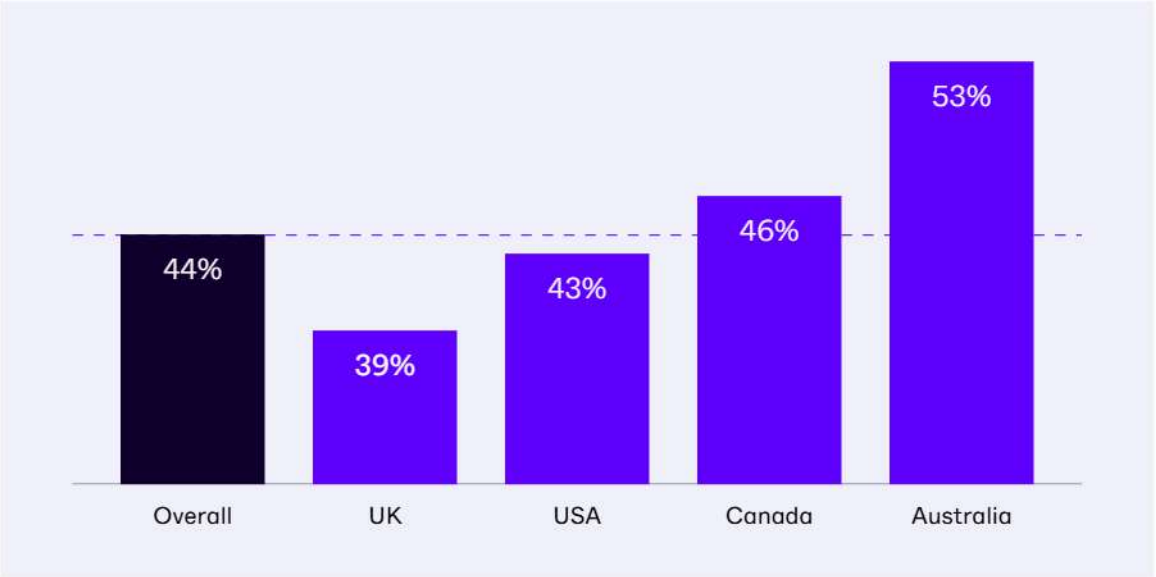
The two columns on the left side of Figure 5 represent organizations who are best at filtering out irrelevant alerts, so that false positives make up less than 20% of the cloud security alerts that get through to their security teams. These two columns account for almost a quarter of the organizations in the survey (23%). Achieving results at that level requires pulling together data from a wide range of cloud security tools and using advanced technologies like AI and security analytics to separate the false positives from the meaningful alerts.

The third and fourth columns from the left represent the 21.5% of organizations in which between 20% and 39% of the alerts received are false positives. We consider that group to be in the "acceptable but could improve" range.

The five columns remaining columns show that in more than half of organizations (55.3%) at least 40% of cloud security alerts are false positives. Those are conditions that likely lead to overworked and frustrated security teams, at a minimum. And imagine being among the 10.6% of security operations teams who have to work through the 80% or more of alerts that turn out to be false positives!

We think organizations at these levels should do serious work to improve their filtering capabilities. Their security operations groups will not only be tired and frustrated, but are likely to start making mistakes and failing to identify serious issues.

Figure 6:
Average (mean) percentage of cloud security alerts that are false positives, overall and by country.



The fact that some organizations have much better performance than others is also illustrated by Figure 6. The average (mean) for all organizations in the survey is 44% of all alerts reaching the security operations team being false positives. Kudos for UK security teams: their median is a comparatively excellent 39%. US organizations average 43%, and those in Canada 46%. As in the previous question, Australia has the greatest opportunity for improvement.

One more observation about Figure 5. The size of the bars on the left side show that there are no insurmountable barriers to strong performance in this area. Excellent results are achievable with the right cloud security tools and processes.

In more than half of organizations at least 40% of cloud security alerts are false positives.

Section 2: Perceptions and Concerns

Cloud Security Technologies

On a scale of 1 to 5, with 5 being highest, rate the importance of each of the following cloud security technologies in defending your organization's cloud infrastructure:

Figure 7:
Importance of cloud security technologies, on a scale of 1 to 5, with 5 highest.

As we discussed on pages 7 and 8, security teams face a wide range of threats. As cloud transitions have progressed, quite a few technologies have evolved to protect against those threats. We asked survey respondents to rate the importance to their organization of 10 of those cloud security technologies on a scale of 1 to 5, with 1 being "least important" and 5 being "most important." The responses are shown in Figure 7.

The cloud security technology at the top of the list is "Cloud detection and response (CDR)," which was rated 4.29 on the scale of 1 to 5. As its name suggests, CDR technology detects malicious and suspicious activities in cloud domains and provides data and context for fast, accurate containment and remediation. CDR capabilities are a core element of today's cloud security defenses.

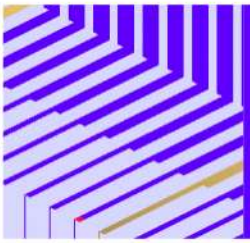
The second-ranked technology is "Vulnerability management (VM)," which was rated 4.24. Products in this category search for vulnerabilities and misconfigurations across cloud and container environments.

The next three technologies on the list are "Cloud security posture management (CSPM)" (4.15), "Data security posture management (DSPM)" (4.15), and "Application security posture management (ASPM)" (4.11). These involve creating centralized visibility into vulnerabilities, risks, and security defenses related to, respectively, cloud platforms, cloud-hosted databases and file storage services, and cloud-based applications. They also assess overall security posture in those areas, provide alerts about critical weaknesses, warn of non-compliance with security standards, and help prioritize areas for improvement. "Kubernetes security posture management (KSPM)," farther down our list at 3.94, provides similar capabilities for Kubernetes code and runtime environments.

Respondents rate two additional cloud security technologies 4.09 out of 5: "Runtime security and cloud workload protection (CWP)" and "Cloud infrastructure entitlement management (CIEM)." Runtime security and CWP solutions monitor cloud workloads running on virtual machines, servers, and containers in real-time to identify and investigate possible attacks. CIEM products manage entitlements and permissions to ensure that access policies are enforced and control access by both human and non-human users.

"Infrastructure as code (IaC) scanning" (4.0) is not as widely deployed as most of the other cloud security technologies on our list, but it can be extremely valuable for DevSecOps groups. IaC scanning involves analyzing the software code used to provision and configure cloud infrastructure for applications. It ensures that infrastructure definition files, templates, and scripts do not contain errors that create vulnerabilities and misconfigurations when applications are deployed to cloud platforms.

Which brings us to "Secrets scanning." Secrets scanning solutions are not as well-known as the other cloud security technologies on this list, which accounts for their relatively low score (3.80). However, we think you are going to be hearing a lot more about them in the near future, because they help protect against some potentially catastrophic events. Secrets scanning solutions search software code repositories inside an organization and on the web, as well as other locations where code can be found. They identify secrets such as passwords and other credentials, API and encryption keys, and security certificates that are exposed or have already been leaked. AWS keys are one example of such a secret. They could allow a threat actor to take control of the organization's entire AWS footprint, delete data, and disable application workloads.



Secrets scanning solutions are not as well-known as the other cloud security technologies on this list... but we think you are going to be hearing a lot more about them in the near future, because they help protect against some potentially catastrophic events.

The responses to this question illustrate once again that cloud security involves a wide range of perspectives and technologies. However, readers should note that cloud security vendors have taken steps to reduce tool sprawl by integrating many of the technologies on our list into an integrated cloud-native application protection platform (CNAPP).

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 8:
Factors most significantly inhibiting validation and prioritization of cloud security events.

One of the techniques used in continuous improvement programs is to determine the factors most impeding progress toward a goal. That information enables organizations to focus resources on reducing or eliminating major impediments. To that end, we asked respondents to select from a list the three factors that most significantly inhibit their organization from validating and prioritizing cloud security events.

For several years now, CyberEdge surveys have found a shortage of IT security staff issue to be the #1 or #2 inhibitor of cybersecurity effectiveness. This survey shows that the same applies to cloud security programs, in spades. The inhibiting factor our respondents cite most often, by a large margin, is "Shortage of experienced IT security personnel," selected by 44.8% (see Figure 8). Clearly, the demand for cloud security expertise is growing much faster than the supply.

This finding has several important implications:

- Organizations won't be able to address cloud security issues by throwing more people at them; the people aren't available.
- A program to train current employees with IT backgrounds in cloud security may be more economical than trying to recruit outside candidates.
- Organizations should consider deploying a unified cloud security platform to improve the productivity of the existing security team.

On pages 22 and 23 we discuss how a unified cloud security platform can improve team productivity through simplified administration, automated workflows, security tool integration, etc.

Back to our list of inhibitors. Almost a third of respondents select as one of the top three "Too many cloud security events" (30.2%). This reflects both the high volume of attacks against cloud data and applications and organizations' inability to filter out false positives (discussed on page 11).

The factor in third place on the list is "Too many data silos and lack of integration" (30.0%). This confirms that many organizations are forced to work with multiple cloud security point products that don't talk to each other. Hopefully, this inhibitor will become less significant as more security teams move to cloud security platforms.

Next comes "Lack of effective cloud security tools" (28.5%). This is indicative of the relative immaturity of many of the cloud security solutions now on the market. This issue, too, should decrease in importance over time as security products improve.

The inhibiting factors rounding out the list are "Inefficient manual processes" (25.7%), "Too many cloud security tools" (24.9%), and "Lack of contextual data" (23.7%).

Figure 9:
Organizations that do or do not face challenges validating and prioritizing cloud security events.

We also gave the survey respondents the option of saying "We have no challenges validating and prioritizing cloud security events." About one in seven (14.6%) choose that response (see Figure 9). That is consistent with responses to other questions in the survey indicating that a few organizations really have their act together, but not very many. Still, the fact that some have overcome these challenges is hopeful; success is possible, even if not yet common.

For several years now, CyberEdge surveys have found a shortage of IT security staff issue to be the #1 or #2 inhibitor of cybersecurity effectiveness. This survey shows that the same applies to cloud security programs.

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 10:
Most serious problems caused by too many cloud security tools.

In cybersecurity fields where threats and defenses evolve rapidly, it is common for organizations to acquire newly-available security tools in an ad hoc manner. At a certain point, however, working with a large number of point products can be problematic.

How does this pattern play out in cloud security? To find out, we asked respondents about the problems caused by having too many cloud security tools – and if tool sprawl is or is not an issue for their organizations.

The problem selected most often was "High total cost of licenses," cited by 43.8% of the respondents (see Figure 10). That issue is straightforward: acquiring many tools is likely to drive total licensing costs higher.

The next three problems are also typical in environments with multiple tools from different vendors: "Multiple management consoles" (39.8%), "Lack of integration between data silos" (39.5%), and "Time and effort to install, configure, and maintain multiple tools" (also 39.5%). These factors all:

- Drive up integration and administration costs
- Interfere with fast threat detection and response
- Exacerbate the effects of the shortage of skilled personnel (see page 15)

In fact, in three of the eight major industries covered in this survey (finance, technology and electronics, and telecommunications and internet), one or another of these three is rated as the #1 problem caused by too many tools, ahead of license costs.

The other two problems on our list, "Excessive time and effort to procure licenses" and "Too many customer support people," were cited less often (28.7% and 17.1% respectively), yet often enough to still be considered important for many organizations.

But is tool sprawl really a common problem in cloud security? Well, yes, it is. We gave survey respondents the option of saying "We don't have too many cloud security tools." Only 13.4% selected that response (see Figure 11).

Figure 11:
Organizations that do or do not have too many cloud security tools.

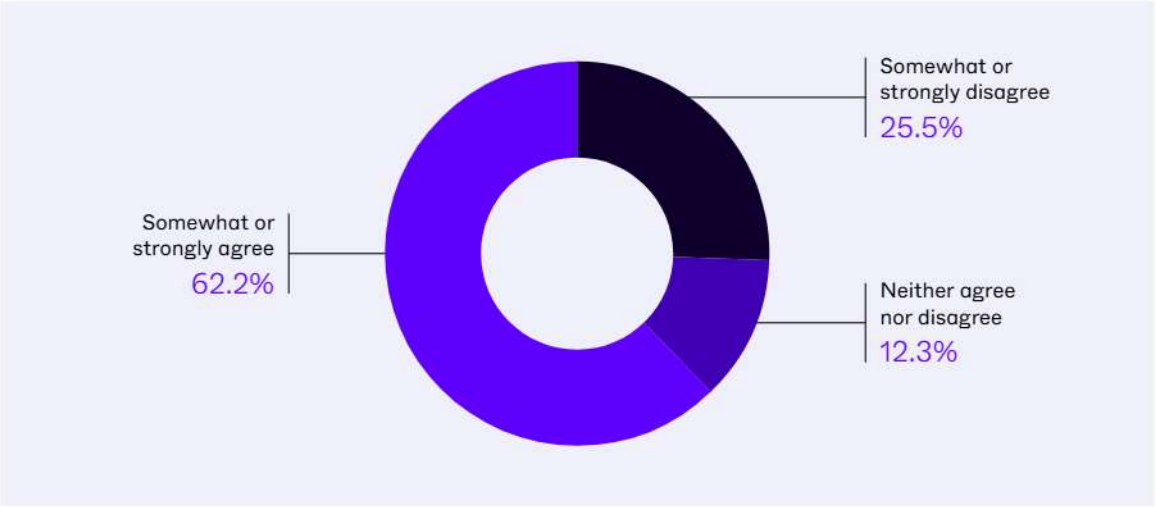
But is tool sprawl really a common problem in cloud security? Well, yes, it is. We gave survey respondents the option of saying "We don't have too many cloud security tools." Only 13.4% selected that response.

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 12:

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



In some areas of cybersecurity, security teams wish they had more data to help them detect and analyze attacks and prepare responses. In other areas, teams have trouble wading through vast oceans of information and alerts to grasp the critical points. To find out where cloud security teams fit on this spectrum, we asked respondents to describe their agreement with the statement "My organization generates so much cloud security data that our cloud security team often struggles to derive and prioritize actionable insights."

A clear majority, more than three of five (62.2%) somewhat or strongly agree with that statement. Only 25.6% somewhat or strongly disagree (see Figure 12).

If you are interested in the exact breakdown, 18.3% strongly agree, 43.9% (the largest group) somewhat agree, 12.3% neither agree nor disagree, 16.5% somewhat disagree, and 9.0% strongly disagree.

These findings confirm that many more organizations struggle because of having too much unfiltered security data than struggle from having too little. Clearly, many need to do a better job eliminating false positives and duplicate alerts so that security teams can find and respond to the most serious attacks.

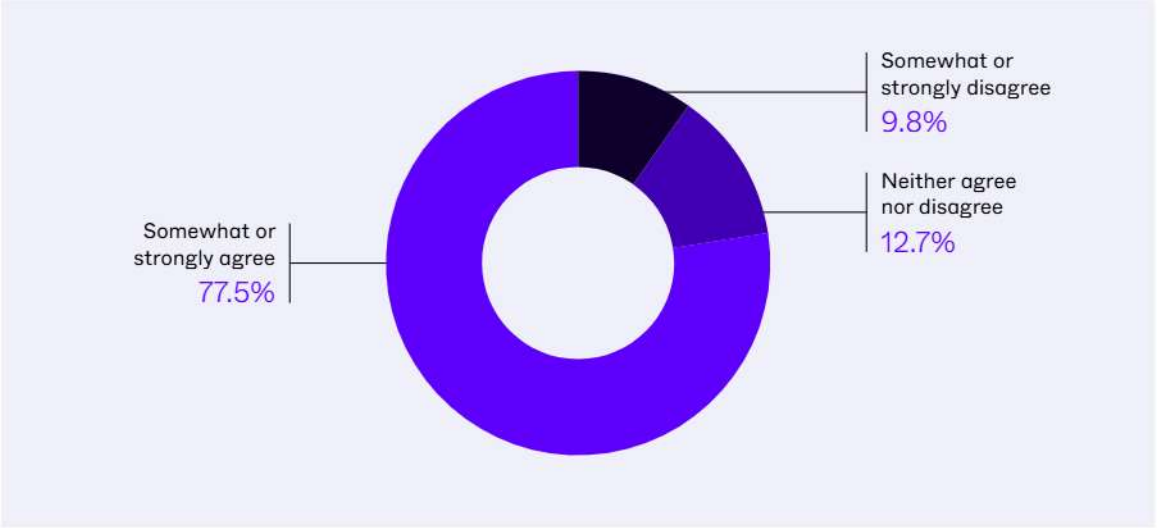
Looking at the countries polled in this survey, agreement with the statement was slightly higher than average in Australia, about average in the UK and USA, and somewhat below average in Canada.

Section 3: Current and Future Investment

Adequacy of Investment in Cloud Security

Describe your agreement with the following statement: "Our organization's investment in cloud security tools, services, and staffing is sufficient to protect us from today's threats."

Figure 13:
Agreement that their organization's investment in cloud security tools, services, and staffing is sufficient to protect them from today's threats.



Is adequate funding for cloud security a big issue for our respondents? Yes and no.

A solid majority (77.5%) somewhat or strongly agree that "Our organization's investment in cloud security tools, services, and staffing is sufficient to protect us from today's threats," but a significant group (22.5%) are not willing to agree with that statement (see Figure 13). Even if there is enough cloud security budget, it is clear from the findings throughout this report that the desired results are not being achieved.

The breakdown: 31.1% strongly agree, 46.4% somewhat agree, 12.7% neither agree nor disagree, 8.3% somewhat disagree, and 1.5% strongly disagree.

Responses differed significantly across major industries. For example, agreement with the statement was significantly higher in the technology and electronics sector, and significantly lower in government and education. Government and educational institutions often lack the flexibility to increase or reallocate budgets quickly as cybersecurity needs change.

It is worth noting that overall spending on cloud security is only part of the story. The other part is whether funds are being spent in the right places. We hope to investigate that question in a future survey.

Even though cloud security budget is adequate, the desired results are not being achieved.

Deployment Plans for Cloud Security Technologies

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

Figure 14:
Deployment plans for cloud security technologies

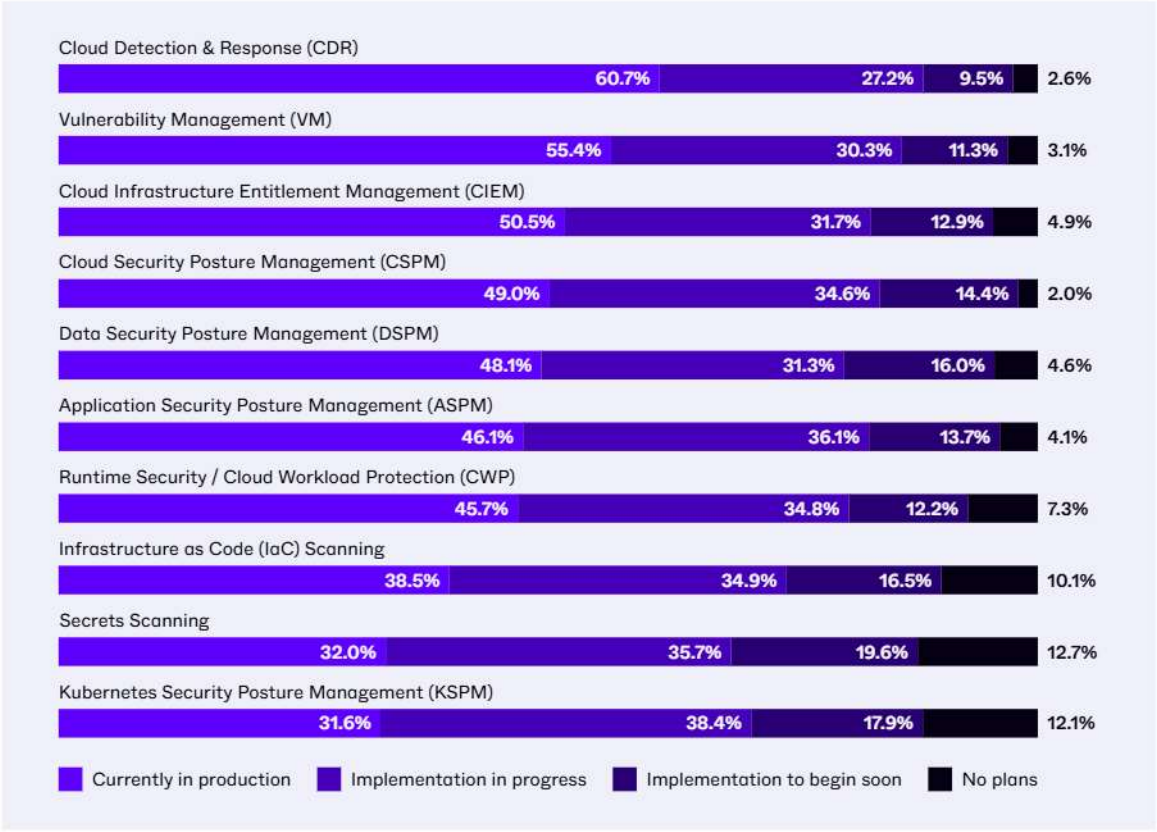


Figure 7 on page 13 shows how survey respondents rated the importance to their organization of 10 key cloud security technologies. Eight of the ten were rated 4.0 or higher on a scale of 1 to 5 – that is to say, are very important. Also, these technologies are receiving a lot of attention from analysts and reporters. But are organizations actually implementing them?

Figure 14 on this page illustrates their implementation plans. For each technology, the light blue bar segment on the left indicates the percentage of organizations that are currently using the technology in production. The medium blue and dark blue segments represent the percentage with implementation in progress and planning to begin implementation soon, respectively. The red segment is for organizations that have no current plans to implement the technology.

Observation #1

A wide range of cloud security technologies are now mainstream. Three of the technologies in Figure 14 are already in production in more than half of all organizations: "Cloud detection and response (CDR)" (60.7%), "Vulnerability management (VM)" (55.4%), and "Cloud infrastructure entitlement management (CIEM)" (50.5%). Four more technologies are live in at least 45% of organizations: "Cloud security posture management (CSPM)" (49.0%), "Data security posture management (DSPM)" (48.1%), "Application security posture management (ASPM)" (46.1%), and "Runtime security and cloud workload protection (CWP)" (45.7%). When you add in the "Implementation in progress" percentages, six out of these seven reach 80% or more and the seventh is almost there. And the remaining three technologies are not far behind: "Infrastructure as code (IaC) scanning" (in production in 38.5% of the organizations), "Secrets scanning" (32.0%), and "Kubernetes security posture management (KSPM)" (31.6%). That's pretty mainstream.

Observation #2

Action has been aligned with importance. If we compare Figure 7 and Figure 14, we see that the cloud security technologies respondents ranked as most important are, for the most part, the ones most often implemented.

Observation #3

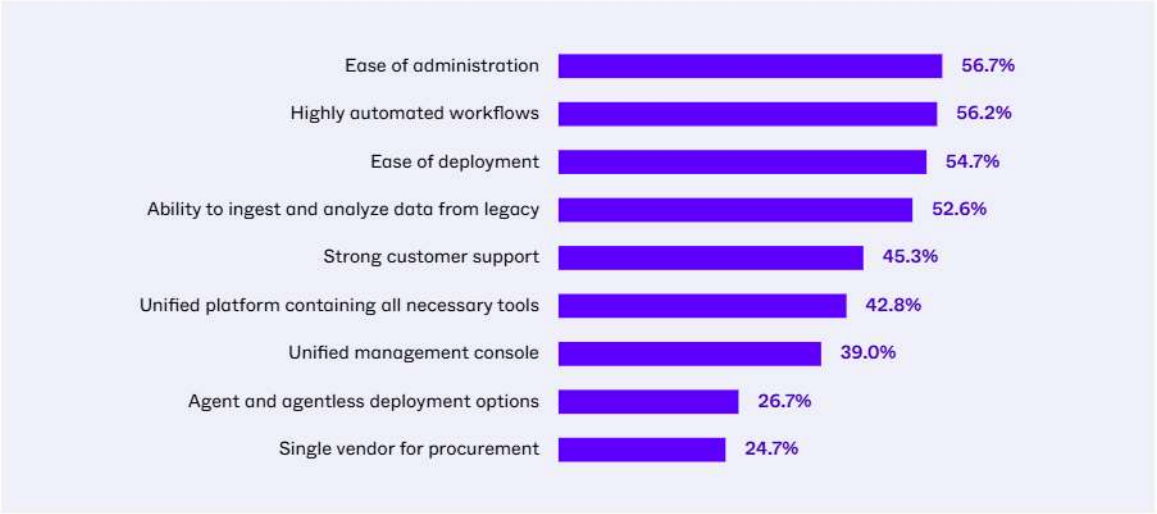
First-class cloud security now involves a wide range of technologies that need to be acquired, learned, and integrated to fully protect cloud-based data and applications.

First-class cloud security now involves a wide range of technologies that need to be acquired, learned, and integrated.

Selecting a Cloud Security Platform

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

Figure 15:
Most important characteristics when selecting a unified cloud security platform.



Several findings in this survey confirm that most organizations are struggling with multiple cloud security point products and could benefit from replacing some of those with a unified cloud security platform. But what characteristics are organizations looking for when they evaluate such platforms?

The responses selected most often and third-most often, “Ease of administration” (56.7%) and “Ease of deployment” (54.7%). This shows that organizations are extremely interested in cloud security platforms that don’t require a lot of staff time to implement and manage. This is consistent with the earlier finding that personnel shortages are currently the biggest factor preventing security teams from validating and prioritizing cloud security events.

The second most prized characteristic on the list is “Highly automated workflows” (56.2%). Automated workflows can have a tremendous impact on organizations’ ability to detect and respond to attacks, and also to reduce the cost of managing cloud security.

The fourth pick on this list of desirable characteristics is "Ability to ingest and analyze data from both legacy and cloud sources" (52.6%). Without this capability, organizations can't achieve complete visibility into their hybrid 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" (45.3%), "Unified platform containing all necessary tools" (42.8%), and "Unified management console" (39.0%).

The rankings of these characteristics differ somewhat from country to country and industry to industry. For example, the most-desired characteristic in a unified cloud security platform is "Ease of administration" in Canada and Australia, "Highly Automated Workflows" in the US, and "Ease of deployment" in the UK. The top criteria is "Ease of administration" in several industries, but in manufacturing and technology and electronics it is "Highly Automated Workflows," and in healthcare and retail it is "Ability to ingest and analyze data from legacy as well as cloud sources."

AI in Cloud Security Solutions

Which of the following benefits does your organization expect to experience from artificial intelligence embedded in cloud security solutions?

Figure 16:
Benefits expected from AI embedded in cloud security solutions.

AI is a very hot topic for security teams. But what specific benefits do they expect to experience from AI embedded in cloud security solutions?

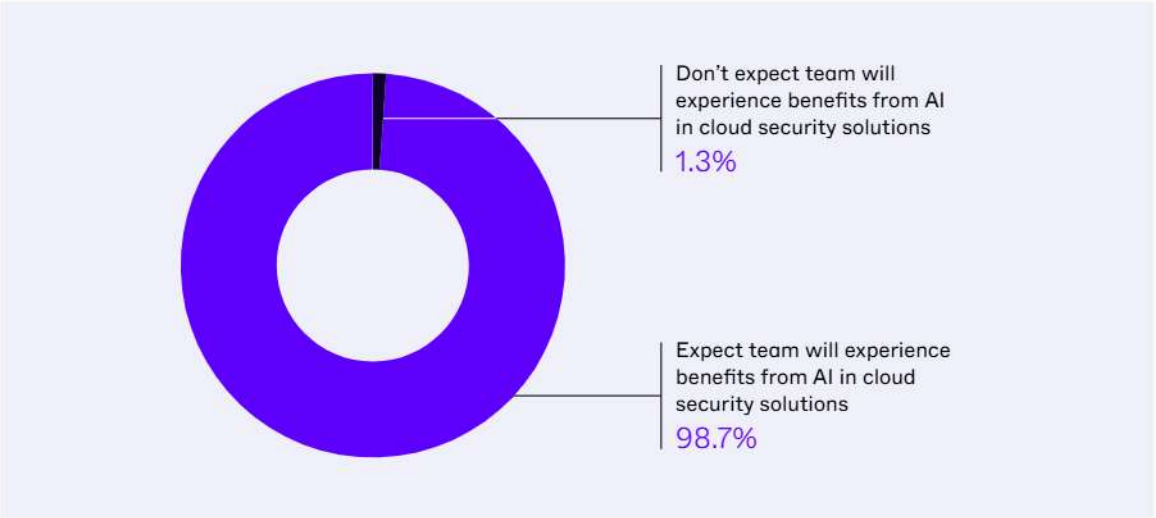
As shown in Figure 16, they want speed and more speed. The two benefits cited most often are both about accelerating processes: "Speed up incident response" (57.8%) and "Detect attacks faster" (57.3%).

In third place is "Better analyze and score risks" (52.8%). The survey respondents want AI to help them determine what resources and activities will have the biggest impact on reducing risk.

The fourth expected benefit is "Increase the effectiveness of current cloud security team" (48.2%). AI promises to be a force multiplier that can make everyone on the security team more productive.

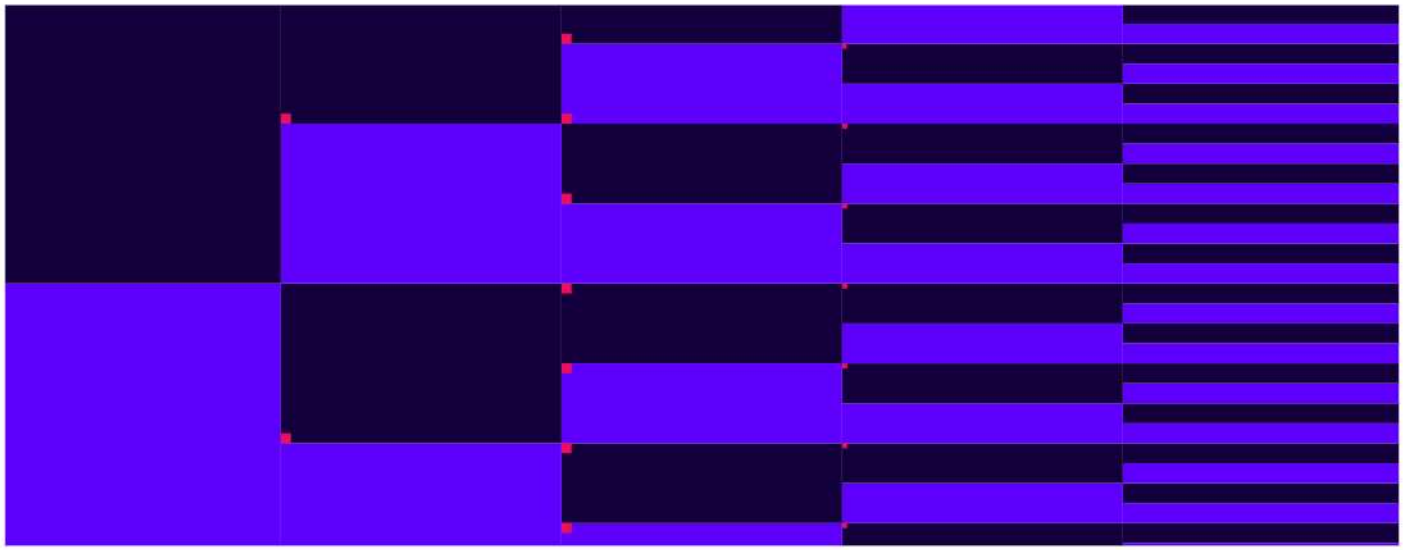
Figure 17:

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



Other expected benefits include "Better prioritize remediation (46.0%), "Generate more actionable insights into threats" (45.5%), and "Reduce data noise and false positives" (43.4%).

In addition, we gave respondents the option to say that they don't expect AI will benefit their security team. Not surprisingly, security professionals with that opinion are rare: only 1.3% of the survey respondents (see Figure 17).



Conclusions

Cloud Security is Today's Foremost Security Battlefield

Threat actors have recognized that most of their most lucrative targets are now on cloud platforms. As a result, the information security arms race that previously revolved around corporate data centers has now pivoted to focus on cloud assets. Cloud security teams now face just as broad a range of threats and compliance issues and must manage just as broad a range of defenses as any information security domain. While they are reasonably confident about their capabilities in many areas, there are some that definitely need immediate improvement. And as cloud-related risks multiply and intensify, organizations will have to keep investing in this area.

Skills Shortages Drive Needs for Integration and Automation

This survey, like many others, has found that a shortage of skilled security professionals is the biggest obstacle to effective cybersecurity. Unless an organization has an unlimited budget, it simply won't be able to throw more people at cloud security problems. In many areas, the only way forward will be to increase the productivity and effectiveness of current security staffs by (a) integrating stand-alone cloud security tools and (b) better automating more cloud security workflows for detecting and responding to attacks.

AI Has a Major Role to Play in Cloud Security

Artificial intelligence is going to make threat actors more effective very soon. That's exactly why cloud security teams need to deploy AI-enhanced security technologies just as fast to make their own security teams more productive and effective. The best way to do that is to work with cloud security solution vendors who incorporate AI into their products for attack detection and response, vulnerability management, remediation, and other functions.

Appendix 1: Survey Demographics

This report is based on survey results obtained from 400 qualified participants hailing from four countries (see Figure 18). 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 19). More than two-thirds (69%) of our respondents hold executive or managerial positions in cybersecurity.

Figure 18:
Survey respondents by country.

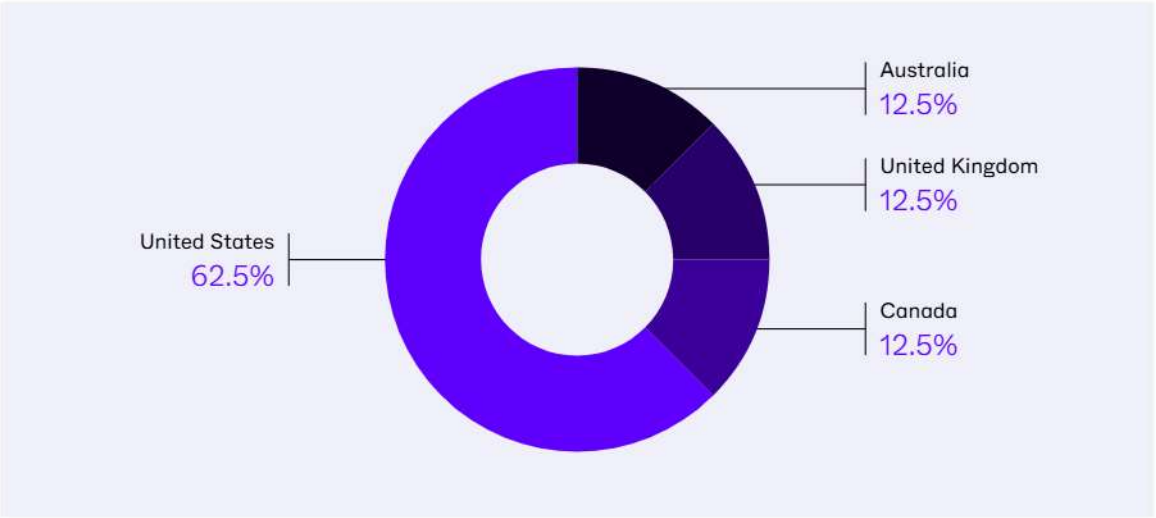
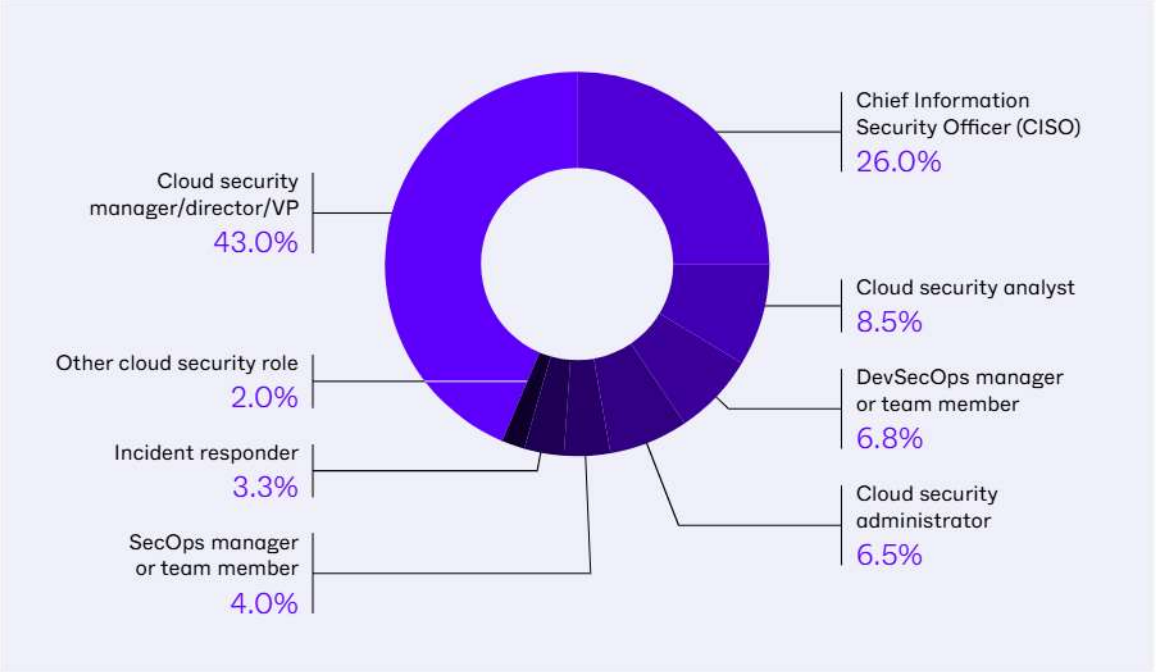


Figure 19:
Survey respondents by role.



All participants in this survey were working for organizations with 500 or more employees (see Figure 20). They spanned 8 major industries (plus "Other") with no single industry composing more than 16.3% of the total participants (see Figure 21).

Figure 20:
Survey respondents by organization employee count.

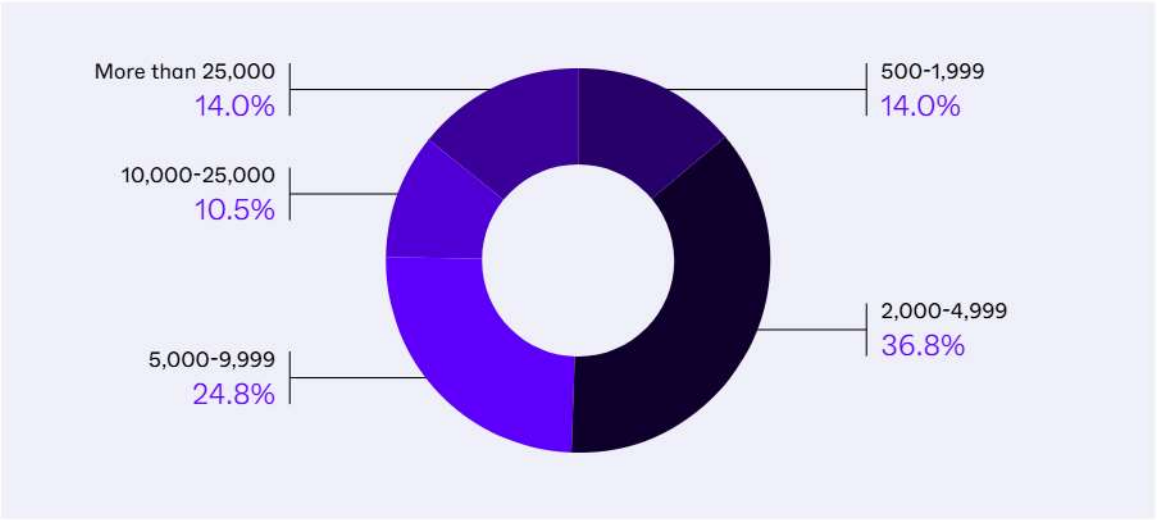
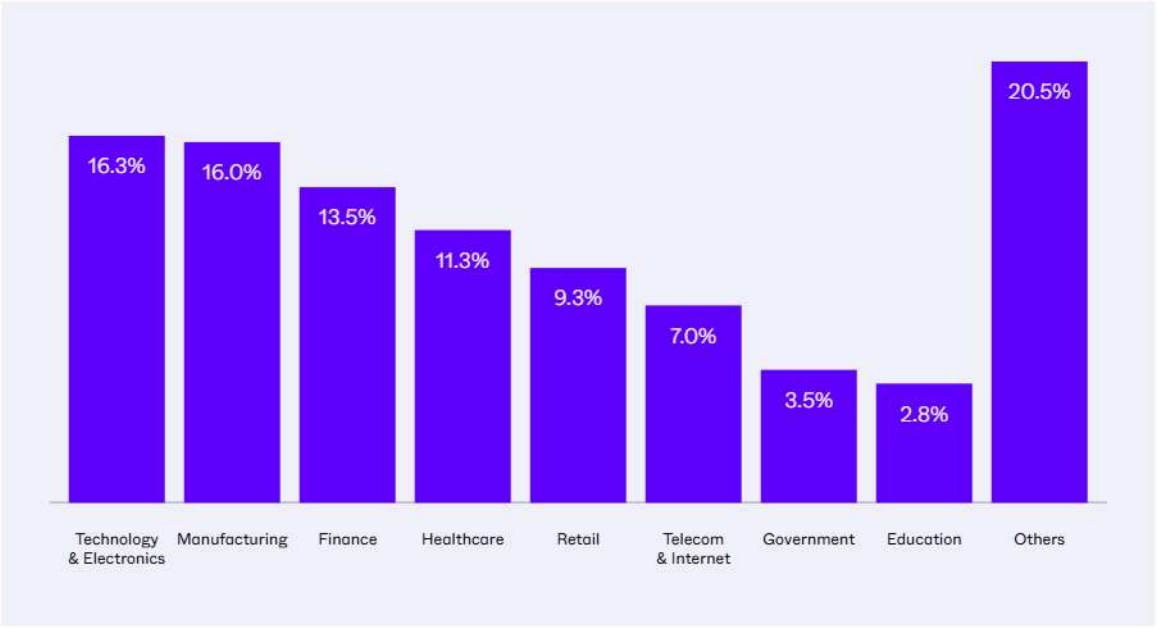


Figure 21:
Survey respondents by industry.



Appendix 2: Research Methodology

CyberEdge developed a 15-question survey instrument in partnership in partnership with SentinelOne. The survey was completed by 400 IT security professionals in the United States, Canada, the United Kingdom, and Australia in April 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 Rick Bosworth and Andy Wool for sharing their cloud security knowledge and perspectives with us.

Appendix 3: About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

Appendix 4: About CyberEdge Group

Founded in 2012, CyberEdge is the largest research, marketing, and publishing firm to serve the cybersecurity vendor community, working with approximately one in every six 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

About SentinelOne

SentinelOne is the world's most advanced cybersecurity platform. The SentinelOne Singularity™ Platform detects, prevents, and responds to cyber-attacks at machine speed, empowering organizations to secure endpoints, cloud workloads, containers, identities, and mobile and network-connected devices with intelligence, speed, accuracy, and simplicity. Over 11,500 customers—including Fortune 10, Fortune 500, and Global 2000 companies, as well as prominent governments—all trust SentinelOne to Secure Tomorrow.

24_MKTG_Product_Report_001_Cloud_Threat_Report_r8_07152024