Financial Services Cybersecurity Challenges, Tool Satisfaction, and 2023 Plans

FinServ survey reveals dissatisfaction with cloud security tools, visibility gaps on macOS and containers, and investment priorities for 2023

Canam Research

Executive Summary

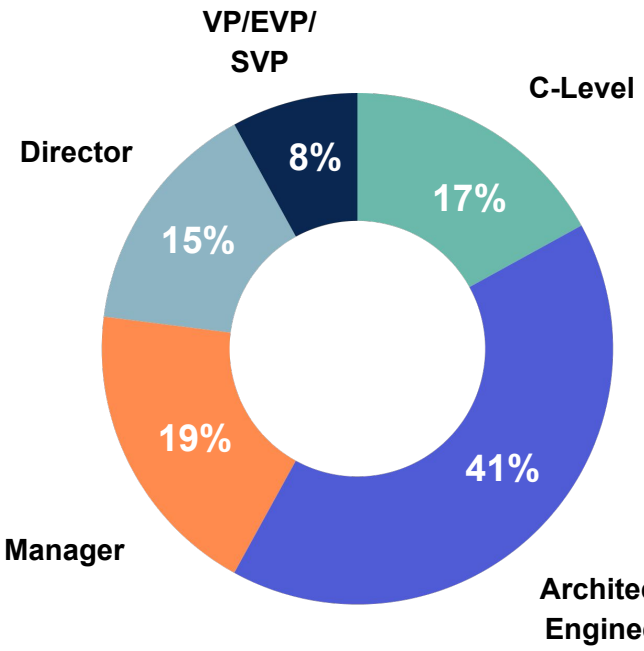
The security world has been upended since 2020. FinServ security professionals have a lot on their plates. They're dealing with risks emanating from the shift to work-from-home (WFH), the increasing prevalence of supply chain attacks, and accelerating cloud adoption.

Uptycs partnered with Canam Research to conduct a survey regarding cloud and endpoint security. Responses represent seventy-five security C-level, VPs, directors, engineers, and managers from financial services firms having 1,000 or more employees.

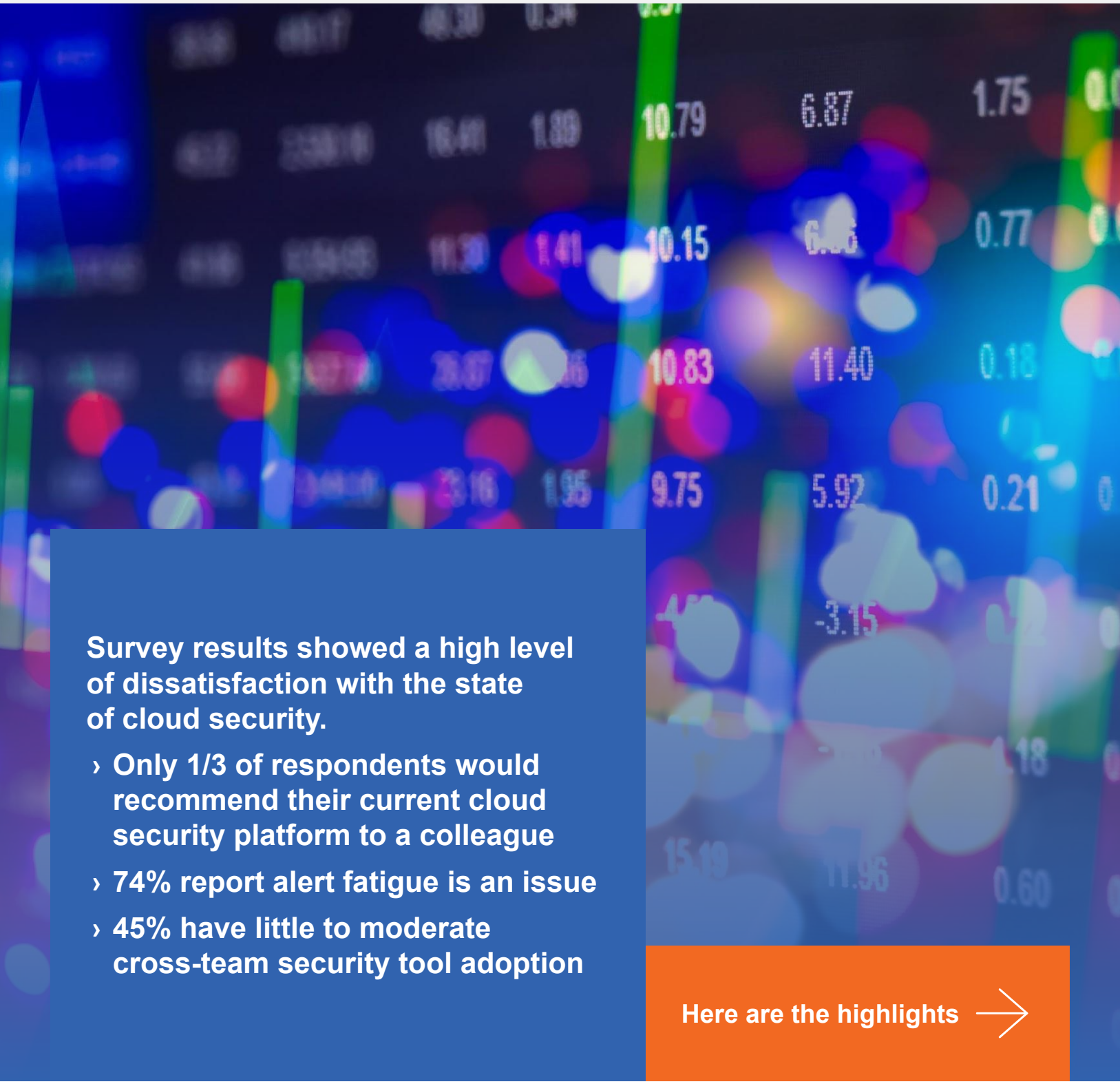
Survey sought to understand

- Satisfaction with current cloud security platform
- Biggest cybersecurity challenges and specific security concerns
- Ability to identify and remediate security threats
- Security standards and models being used to guide cloud security operations
- Security strength and visibility

Respondents by seniority



Executive Summary



Survey results showed a high level of dissatisfaction with the state of cloud security.

- **Only 1/3 of respondents would recommend their current cloud security platform to a colleague**
- **74% report alert fatigue is an issue**
- **45% have little to moderate cross-team security tool adoption**

Here are the highlights

Executive Summary

When it comes to cloud security…

Respondents are generally not pleased with their current cloud security platform

Only 31% of respondents are OK with their current platform

69% are either neutral or unhappy

Relying on security tech stacks instead of single platforms creates issues

26% of respondents say their tech stack is not well integrated

20% report they have no single source of truth

They have a low degree of confidence that their cloud tools are working

56% of respondents are either not totally—or only somewhat—confident in their ability to detect and remediate cloud threats in real time

Nearly 20% indicate they're not able to perform real-time threat mitigation

Only 13% state they're very confident in their ability to identify and remediate cloud security threats

Executive Summary

And when it comes to security in general, here's what they report:

Threat detection and risk management are, unsurprisingly, their top concerns

45% of respondents state threat detection is their biggest cybersecurity challenge

42% believe risk management is their biggest challenge

Data breaches continue to haunt the dreams of security leaders

54% indicate that a data breach or data loss is their biggest cloud security concern. Configuration management issues also weigh heavily on their minds

They can do better adopting security tools across teams

45% of respondents report they have either a low or moderate level of cross-team adoption

They're using many frameworks and models, but one edges out the others

54% use the NIST Cybersecurity Framework to guide their cloud security operations, making it the most popular model among respondents

Snapshot:
Impact of alert fatigue on the organization

Alert fatigue is a big issue

- **74%** of respondents report that alert fatigue remains either a moderate or a major problem

- In other words…
  only **26%** believe their organization is handling alerts well

Snapshot:
Cross-team adoption for tools to achieve effective cloud security

Cross-team tool adoption remains low

- Only **15%** of participants report they have a high level of cross-team security tool adoption

- **85%** struggle to get outside teams off the bench and engaged in their cloud security

Cloud Security Responses

Canam Research

On a scale of 0–10, how likely are you to recommend your current cloud security platform to a friend or colleague?

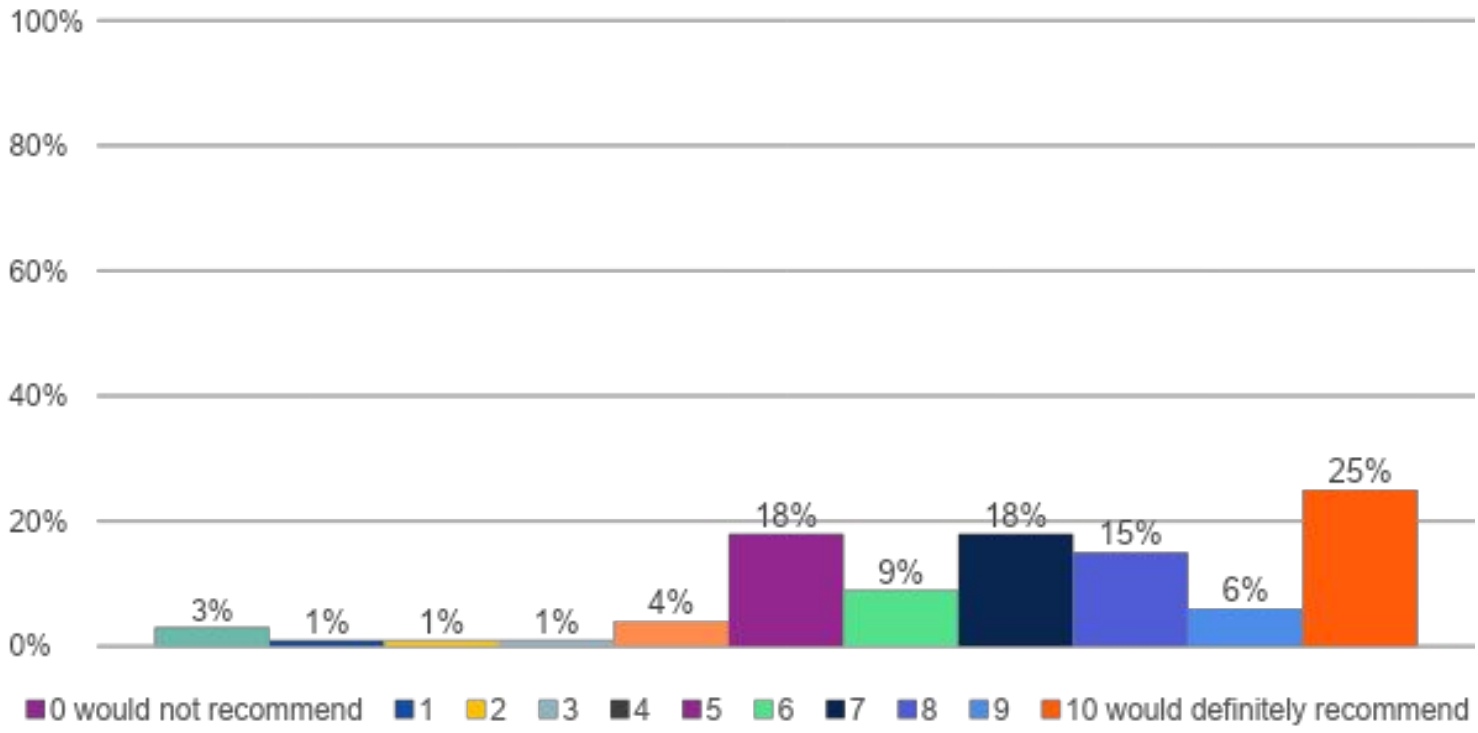
31% of respondents are net promoters of their current cloud security platform

33% are neutral or passive

36% are detractors

When 69% of respondents are at best *ho-hum* about their cloud security platform, there's room for improvement

9–10 = Net Promoters	7–8 = Neutral	0–6 = Detractors

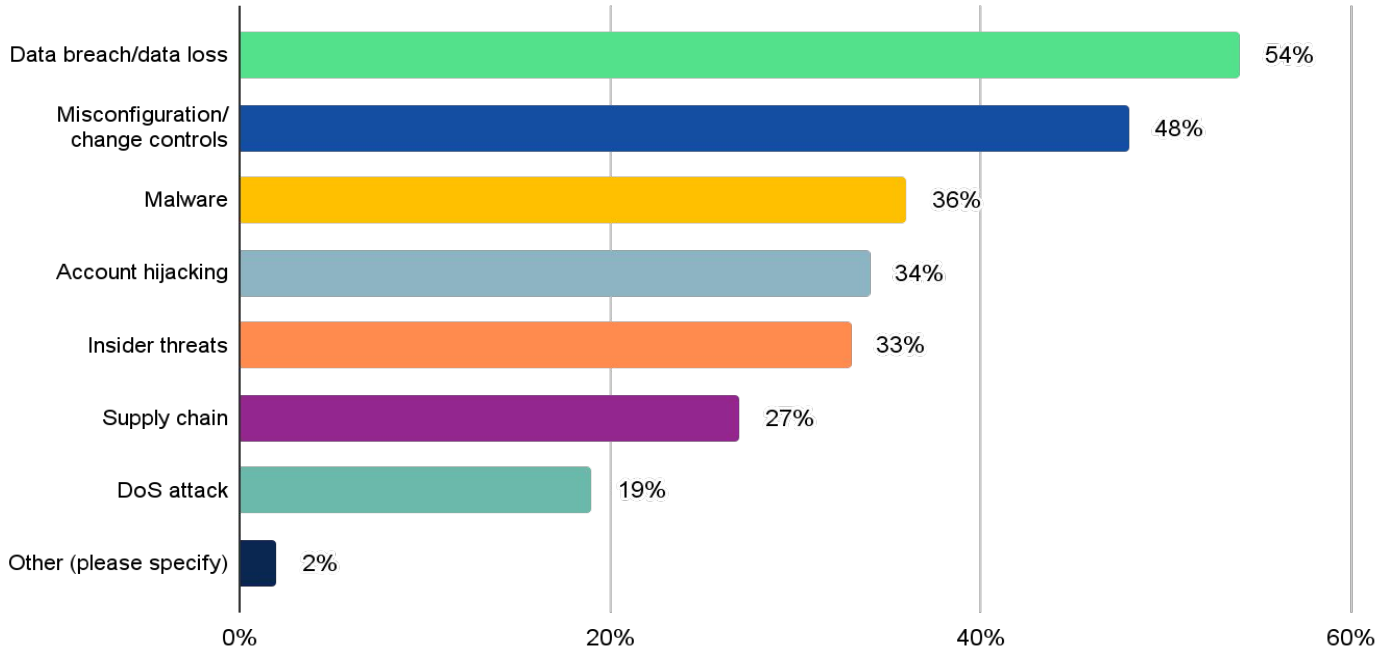


Which specific cloud security threats are the biggest concern or challenge to your organization?

A data breach or data loss is the biggest concern for security teams

The number of respondents reporting that misconfiguration or change controls are the biggest issue illustrates the complexity of configuration management within cloud infrastructure. **Supply chain attacks rank higher than DoS attacks, the latter having traditionally been the main concern for security leaders.**

A quick check of Google Trends shows that before December 2020, supply chain attacks weren't really on anyone's radar. It appears that fallout from the SolarWinds breach has had a long tail.

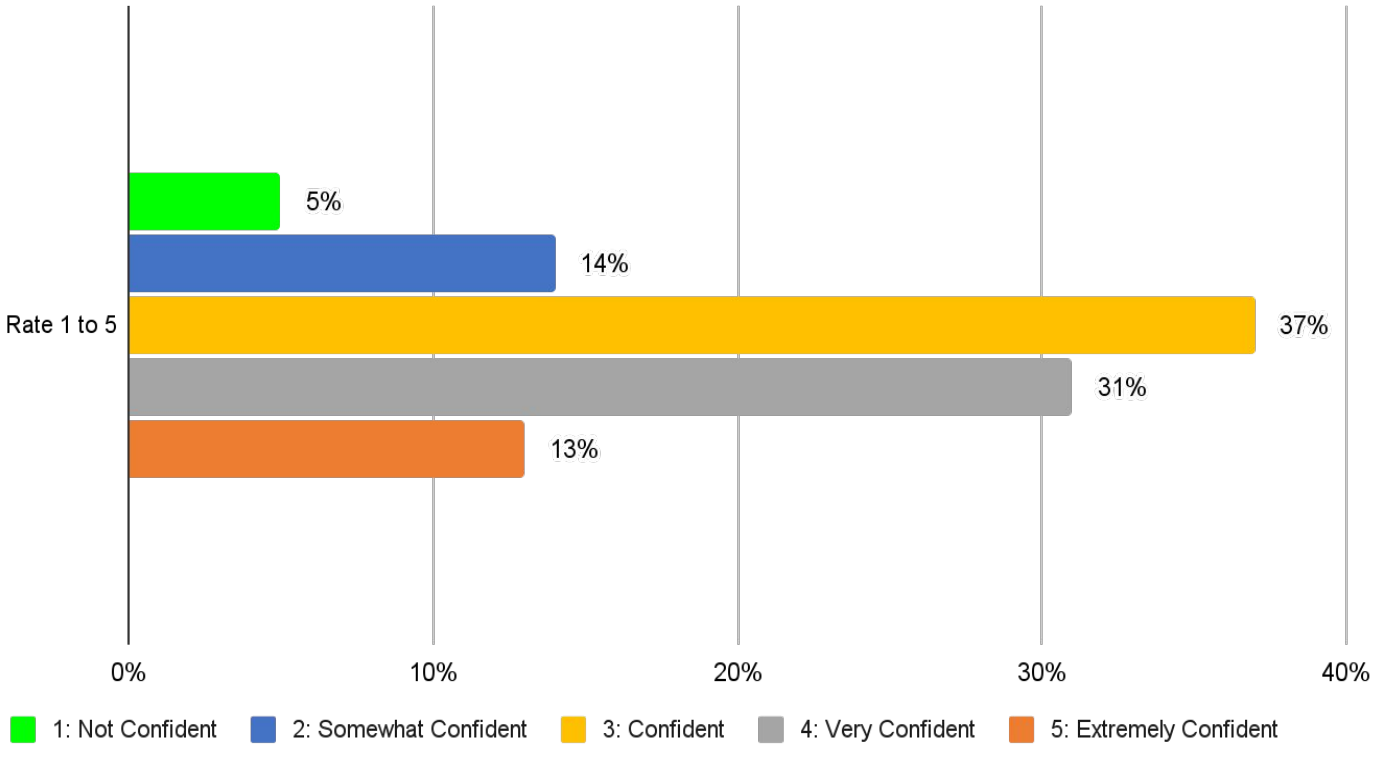


On a scale of 1–5, rate your confidence in being able to identify and remediate cloud security threats in real time.

Real-time threat identification and remediation can be difficult to achieve… and the responses reflect this.

Only **13%** of participants state they're very confident in their ability to identify and remediate cloud security threats.

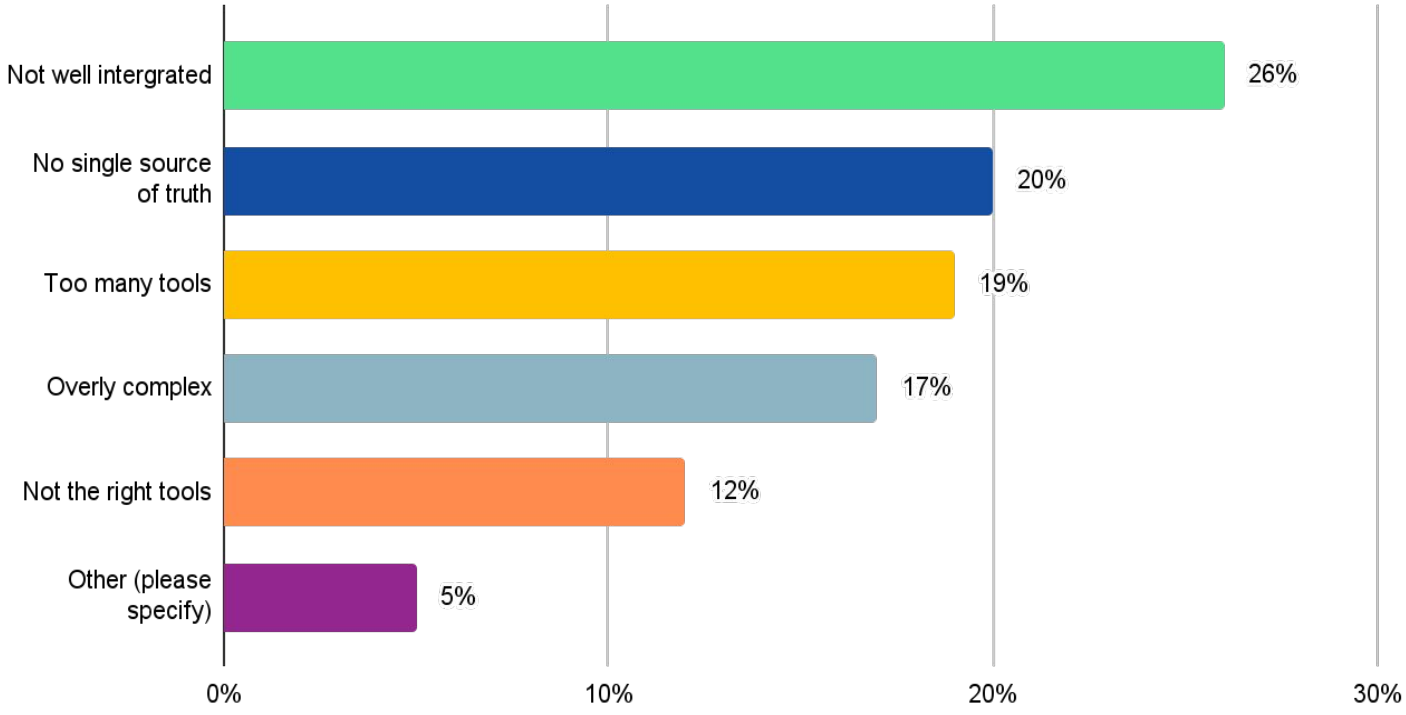
Nearly **20%** indicate they're not able to do real-time threat mitigation, which opens up their organizations to significant risk.



What is the biggest challenge in your cloud security tech stack?

Building a tech stack to address one-off issues can lead to subsequent headaches. Respondents have many issues with their tech stacks. But in picking just one, the most likely answer is **lack of integration**, followed by **no single source of truth.**

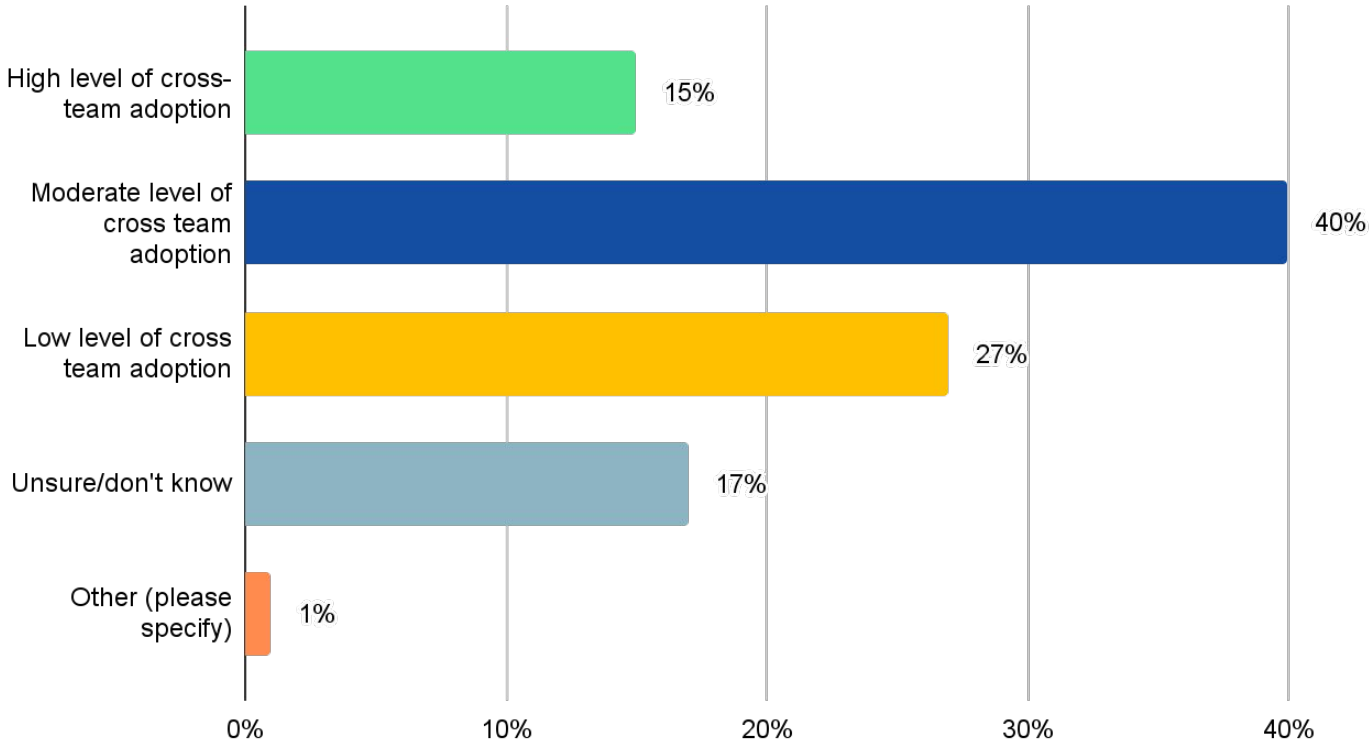
Answers are somewhat evenly distributed; they reflect a common set of problems imposed by a traditional stack (comprised of single-use tools) vs. an integrated platform.



Which of the following best describes the level of cross-team tool adoption to achieve effective cloud security?

Cross-team adoption of security tools means an organization is more likely to have in-depth security.

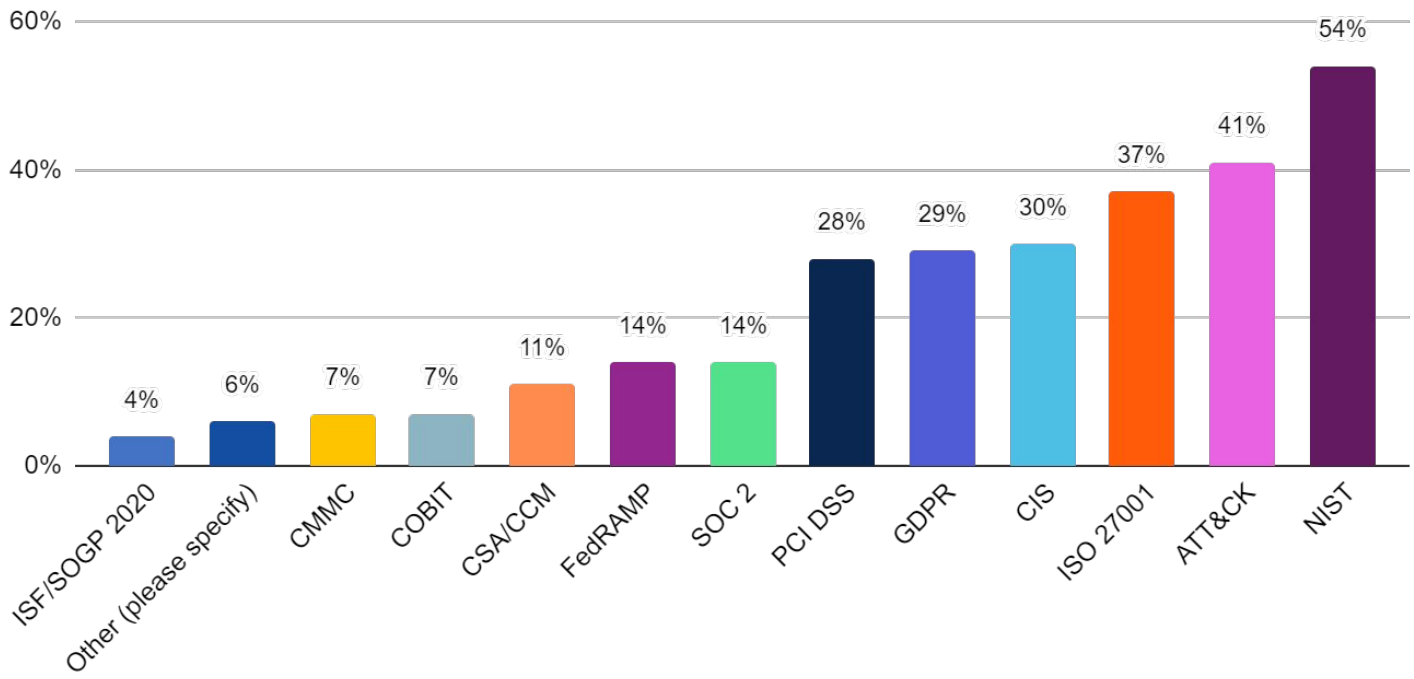
A majority of respondents have achieved at least some degree of cross-team tool adoption, but 45% are still struggling.



Which cybersecurity standards or models does your organization use to guide cloud operations? (Check all that apply.)

Many models and frameworks can help guide security, but the NIST Cybersecurity Framework remains the post popular. It's a powerful tool for enabling organizations to develop and maintain strong cloud security.

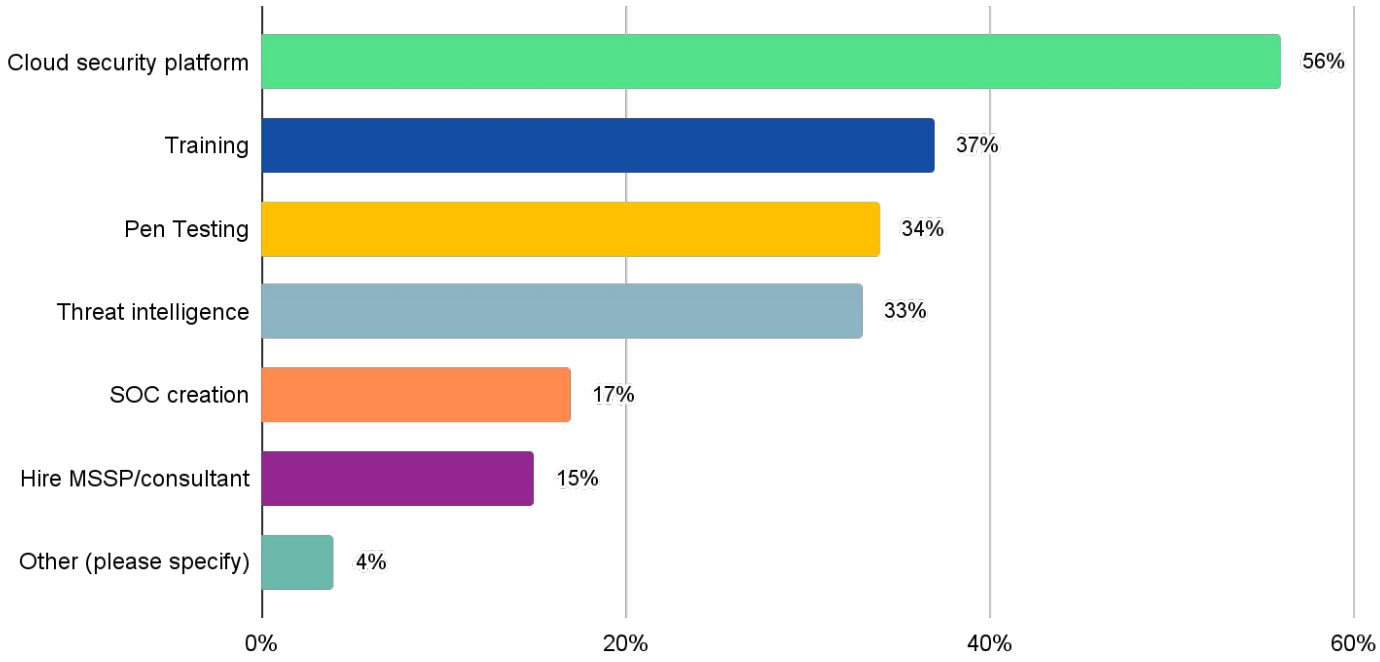
A variety of other models are used, reflecting the diversity of organizations participating in the survey. Most use more than one model or framework.



What will your organization focus on in the next twelve months to improve cloud security? (Choose top three.)

Most participants plan to focus on their cloud security platform to improve security, which makes sense given the levels of dissatisfaction reflected the survey scoring.

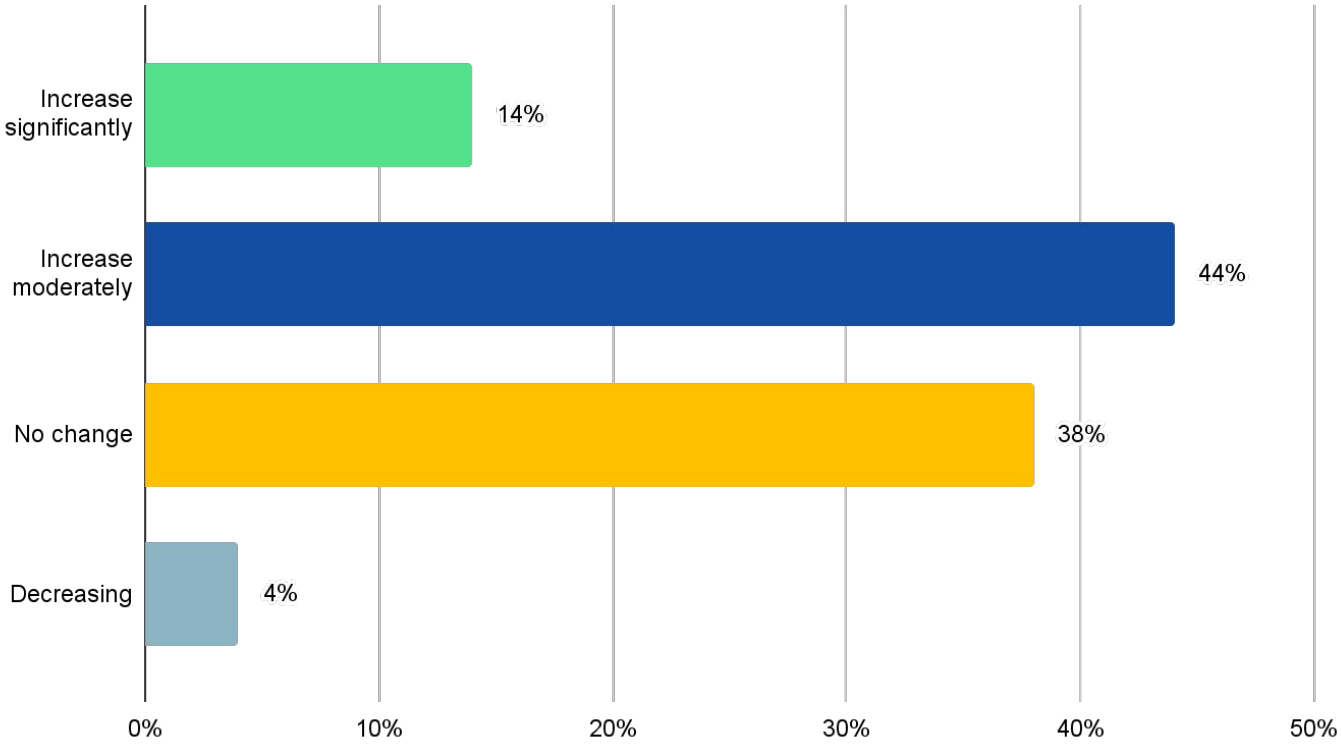
Only about a third are pleased with what they have now. Given the effective wishlist seen earlier, teams are likely pursuing 1) tools that provide greater integration, 2) a single source of truth, and 3) the ability to do real-time detection in the cloud.



Which of the following best describes your cloud security budget for the next 12 months?

58% of organizations are increasing cloud security budgets. It's likely they have no choice in light of increasing and ongoing cloud application investments across the enterprise.

Interestingly, **42%** of organizations show no increase—or even a decrease in spend. This roughly tracks with the **40%** that have either low or unknown ROI for their programs, thus indicating that demonstrated ROI might foreshadow an increased budget.



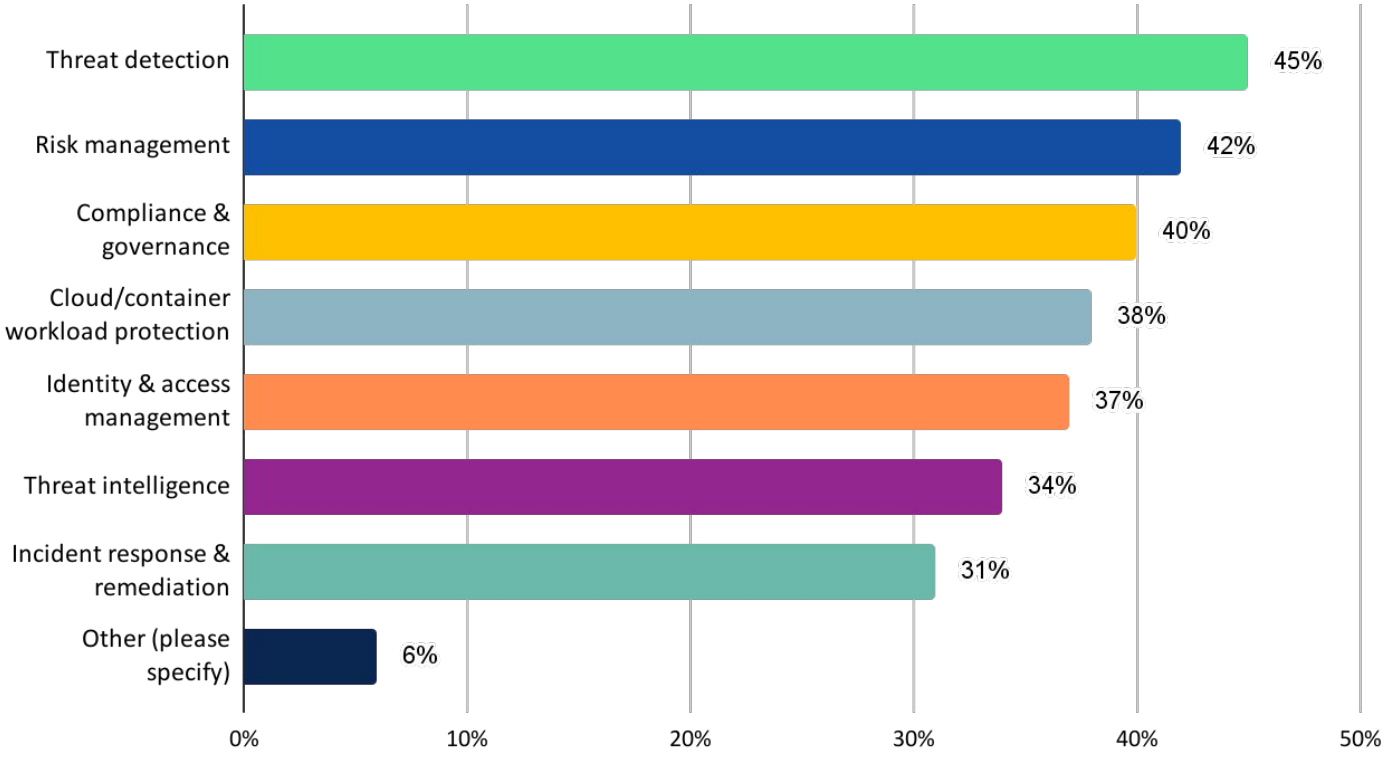
General Cybersecurity Responses

Canam Research

What are your organization's biggest cybersecurity challenges?

Security teams have a lot on their plate. Perhaps this is obvious, but survey responses reveal just how many vital tasks vie for their attention.

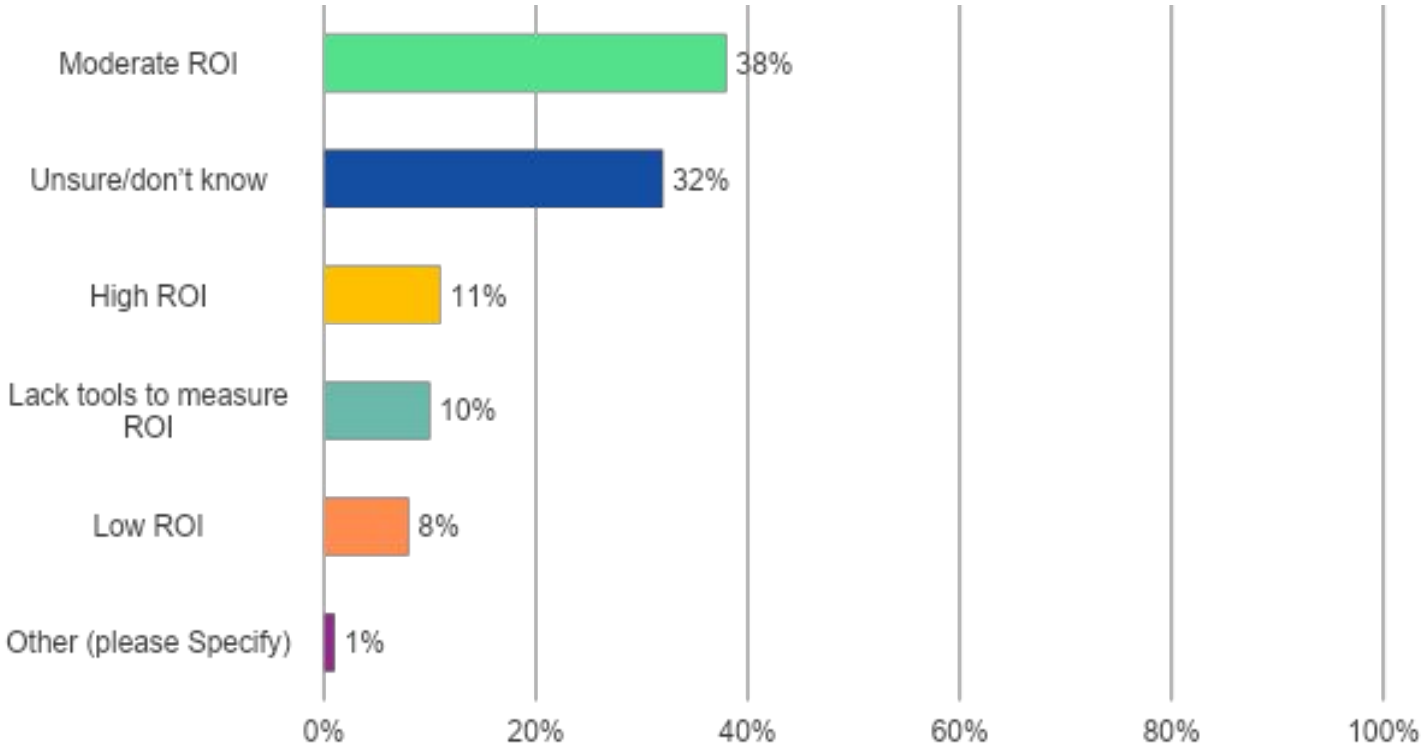
Threat detection is the biggest challenge, but doesn't significantly overshadow a number of other concerns requiring security team resources and attention.



Which of the following best describes the ROI for your current cybersecurity spend?

Assessing ROI on cybersecurity spending is notoriously difficult. After all, the benefit is to not experience a costly security breach, and it's difficult to prove the value of a negative.

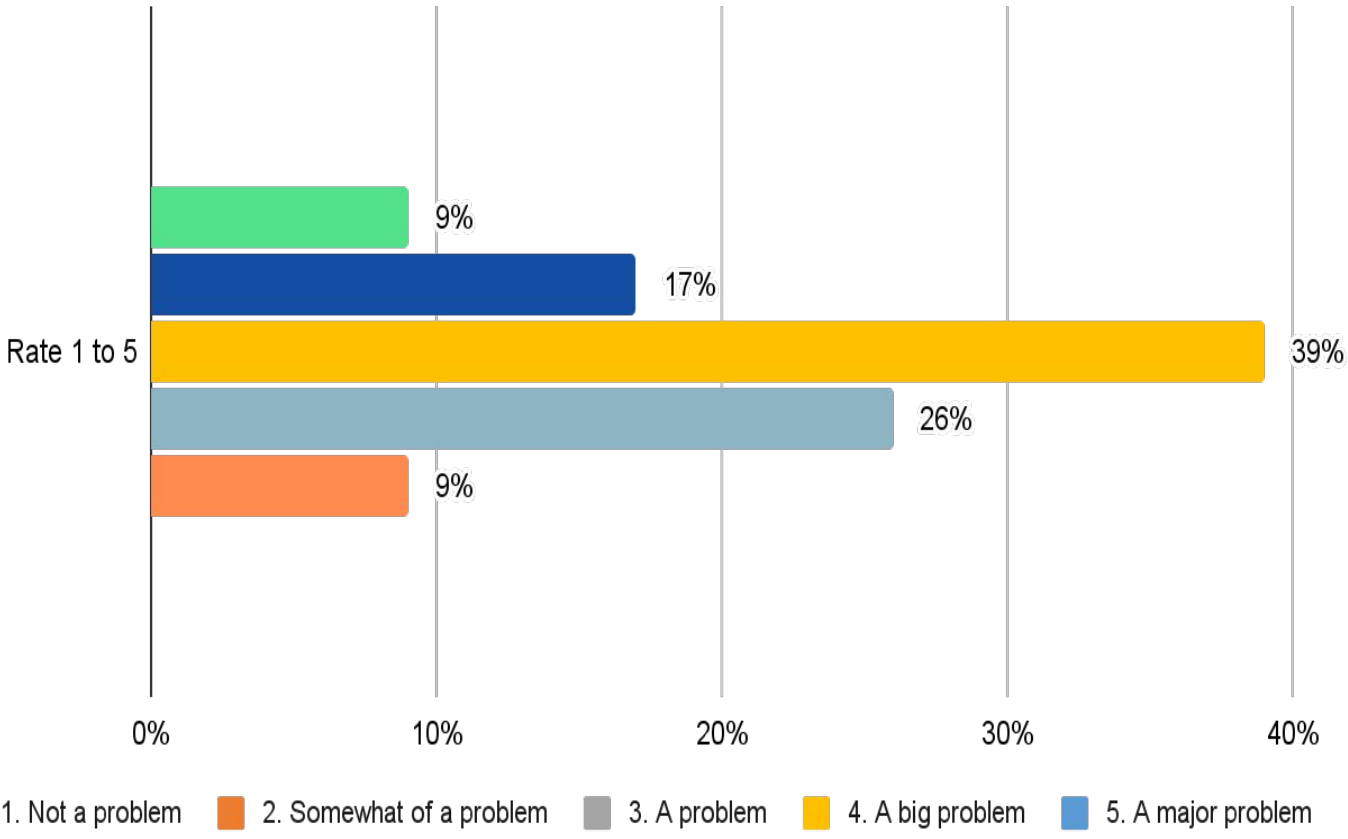
Only about half of respondents have success with delivering ROI for their security spend. The remainder either aren't sure or deliver low ROI.



On a scale of 1–5, rate the impact of alert fatigue on your organization.

Unsurprisingly, alert fatigue remains a big issue, despite many tools and services to make alert processing easier and more manageable.

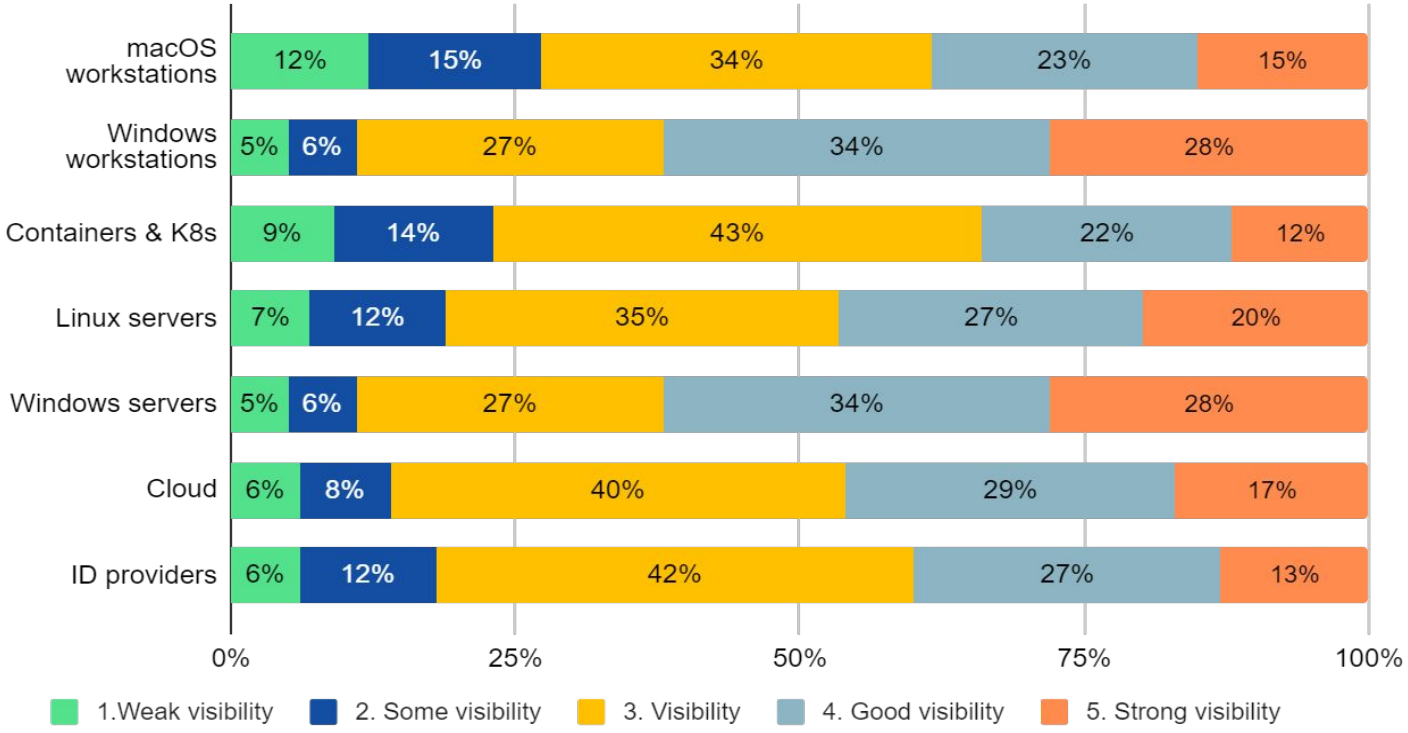
Only about a quarter of respondents have solved the issue, with **35%** truly struggling with alert fatigue.



On a scale of 1–5, rate the strength of security visibility for the following asset categories.

Asset visibility was rated strongest with Windows environments and **weakest among macOS and container/K8s.**

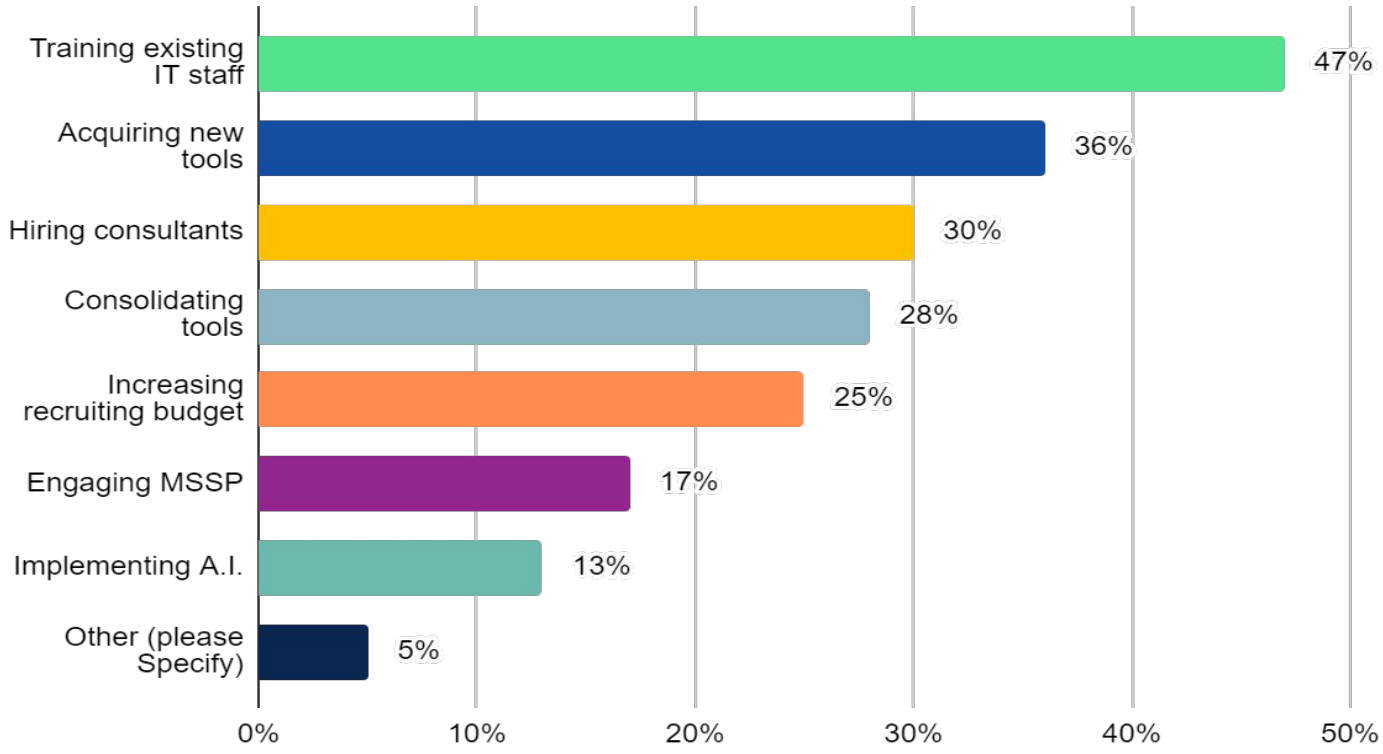
The spread of environments shows just how difficult securing the modern enterprise is for most security teams. With so many disparate operating systems, endpoints, and environments, lack of integration or a single source of truth can become a big issue.



What is your organization doing to address shortages in qualified security staff?

Security staffing has been a well-known issue dating back to at least 2018. As organizations seek to retain talent, the following responses reveal that addressing such shortages requires a varied approach.

Training is the most popular response, but companies are also outsourcing, implementing AI, and deploying new tools to make teams more efficient.



About Uptycs

Your developer's laptop is just a hop away from cloud infrastructure. Attackers don't think in silos, so why would you have siloed solutions protecting public cloud, private cloud, containers, laptops, and servers?

Uptycs reduces risk by prioritizing your responses to threats, vulnerabilities, misconfigurations, sensitive data exposure, and compliance mandates across your modern attack surface—all from a single platform, UI, and data model. This includes the ability to tie together threat activity as it traverses on-prem and cloud boundaries, thus delivering a more cohesive enterprise-wide security posture.

Looking for acronym coverage? We have that, too, including CNAPP, CWPP, CSPM, KSPM, CIEM, CDR, and XDR. Start with your Detection Cloud, Google-like search, and the attack surface coverage you need today. Be ready for what's next.

Shift your cybersecurity up with Uptycs. Learn how at: https://uptycs.com