# Securing Cloud Assets: How IT Security Pros Grade Their Own Progress

By Paula Musich
An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) Research Report
February 2021

Sponsored by:

TRUEFORT

EMA™ IT & DATA MANAGEMENT RESEARCH, INDUSTRY ANALYSIS & CONSULTING

# Securing Cloud Assets:
# How IT Security Pros Grade Their Own Progress

## Table of Contents


Introduction ..... 1

The **Who** of Cloud Security ..... 2

Applying Automation to Cloud Security ..... 4

The **What** of Cloud Security ..... 6

The Right Tool for the Job ..... 8

**Why** the Disconnect? ..... 11

Conclusion ..... 13

# Securing Cloud Assets: How IT Security Pros Grade Their Own Progress

## Introduction

Cybersecurity executives and industry pundits are fond of saying that information security should be everyone's responsibility. That is especially true when it comes to cloud security, given the ubiquitous access to cloud computing across the enterprise (otherwise known as shadow IT) and the fact that application developers, IT administrators, cloud administrators, IT security practitioners, and the cloud providers themselves all have a role in ensuring the security and privacy of enterprise data, applications, and workloads in the cloud. However, the painful reality is that all too often, cloud services users either assume that the cloud service provider has security for their accounts or they fail to understand who is responsible for what when it comes to the shared responsibility model.

As more enterprise computing moves to the cloud in all its forms (SaaS, PaaS, IaaS, or hybrid cloud deployments), IT security practitioners are struggling to keep up with the burgeoning use of those services. What many quickly discovered in the early days of cloud computing is that trying to apply existing security controls to cloud-based assets or workloads is a recipe for failure. At the same time, as enterprise developers abandoned traditional modes of application development to embrace a continuous integration/continuous delivery style of code development, the need for speedy detection and remediation of vulnerabilities became an exponentially more difficult task for IT security practitioners.

In response, a whole host of innovators responded with new security tools adapted to the unique security requirements of cloud computing, but gaps in security processes and policies remain. These gaps have caused more than a few big cloud computing breach headlines, including the Antheus Technologia biometric data breach in Brazil,[1] the BigFooty.com sports application breach in Australia,[2] and Microsoft's recent breach of an internal customer support database.[3] Misconfiguration errors for cloud-based assets have been on a steady rise since 2017, with the Verizon Data Breach Report of 2020 finding that errors are the second-most common source of data breaches behind hacking. This is especially true for organizations using AWS's Simple Storage System (S3) buckets, which are all too often misconfigured by customers so that they are open to public access.

As information security organizations struggle to adapt and understand the security requirements unique to each type of cloud service, and as they learn what security best practices look like for IaaS, PaaS, and SaaS services, EMA sought to assess where IT security practitioners believe they are along the path to better cloud security practices.

[1] The company did not password protect a database residing in the cloud
[2] Due to a misconfigured database on AWS
[3] Due to a misconfigured Azure security rule

## The *Who* of Cloud Security

As more cloud applications are created and as more applications are migrated to the cloud from private data centers, questions arise over which groups within IT are responsible for securing those newly minted cloud assets. Is it application developers? IT security? Infrastructure teams? Or are enterprises carving out cloud-focused teams that take responsibility for all aspects of managing cloud-based assets? The slam dunk answer is not necessarily IT security. Although that was true for 46% of all respondents in the EMA survey, another 28% reported that a separate cloud operations group held that responsibility within their organization, and 9% said that network operations teams were primarily responsible for cloud security. Six percent said responsibility was held by two or more groups, which most often meant that responsibility was shared between the IT security team and either a cloud operations group or infrastructure team. It is interesting to note that large enterprises rely slightly less on IT security to secure cloud assets. Only 39% of respondents in those organizations indicated that the IT security team was responsible for cloud security, with 29% assigning it to a cloud operations group and 13% to network operations.

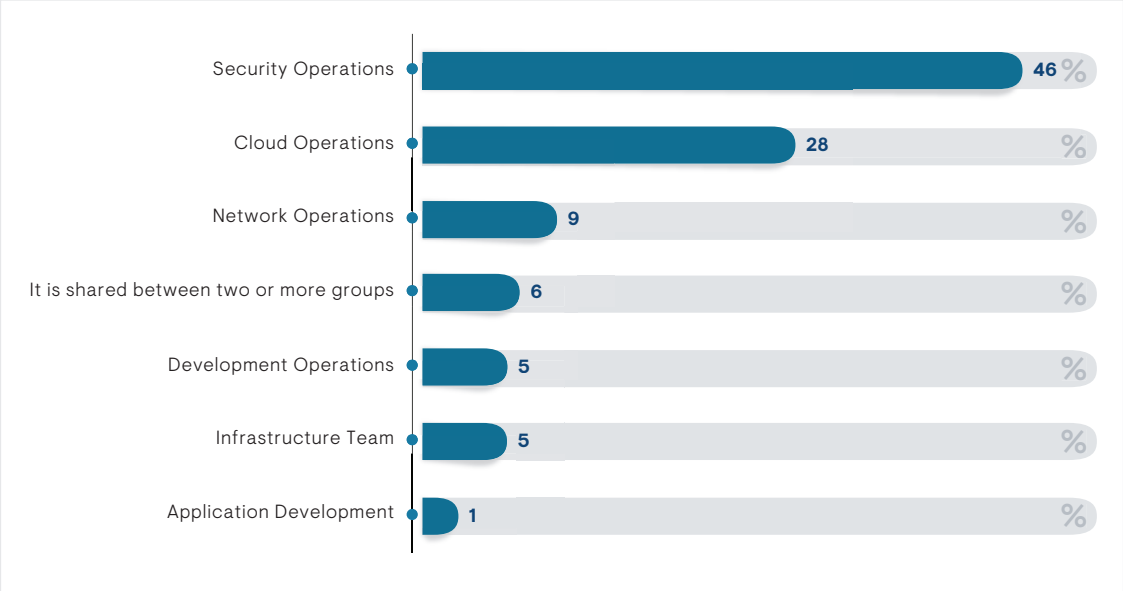


*Figure 1: Who is Responsible for Cloud Security?*

In looking at who owns the budget for acquiring cloud security tools, SMEs and large enterprises both largely point to the IT security team at 90% and 91%, respectively. Only 79% of midmarket organization respondents indicated IT security as the purse holder. Sixty-two percent of midmarket organizations say the cloud team holds that budget—a larger percentage than the other two organization sizes. Smaller organizations historically have led the adoption of cloud services, and their longer and fuller history of engagement with cloud services likely spurred them to create cloud teams that took responsibility for all aspects of managing their cloud usage, including securing it. Despite the trend toward creating more integrated teams across the development, security, and operations functions within IT (often referred to as DevSecOps), few of these teams own the budget for securing cloud assets. Still, responsibility for securing cloud assets is sometimes shared between different groups. In this case, budgets for acquiring security tools to protect cloud-based assets come from multiple groups beyond IT security.

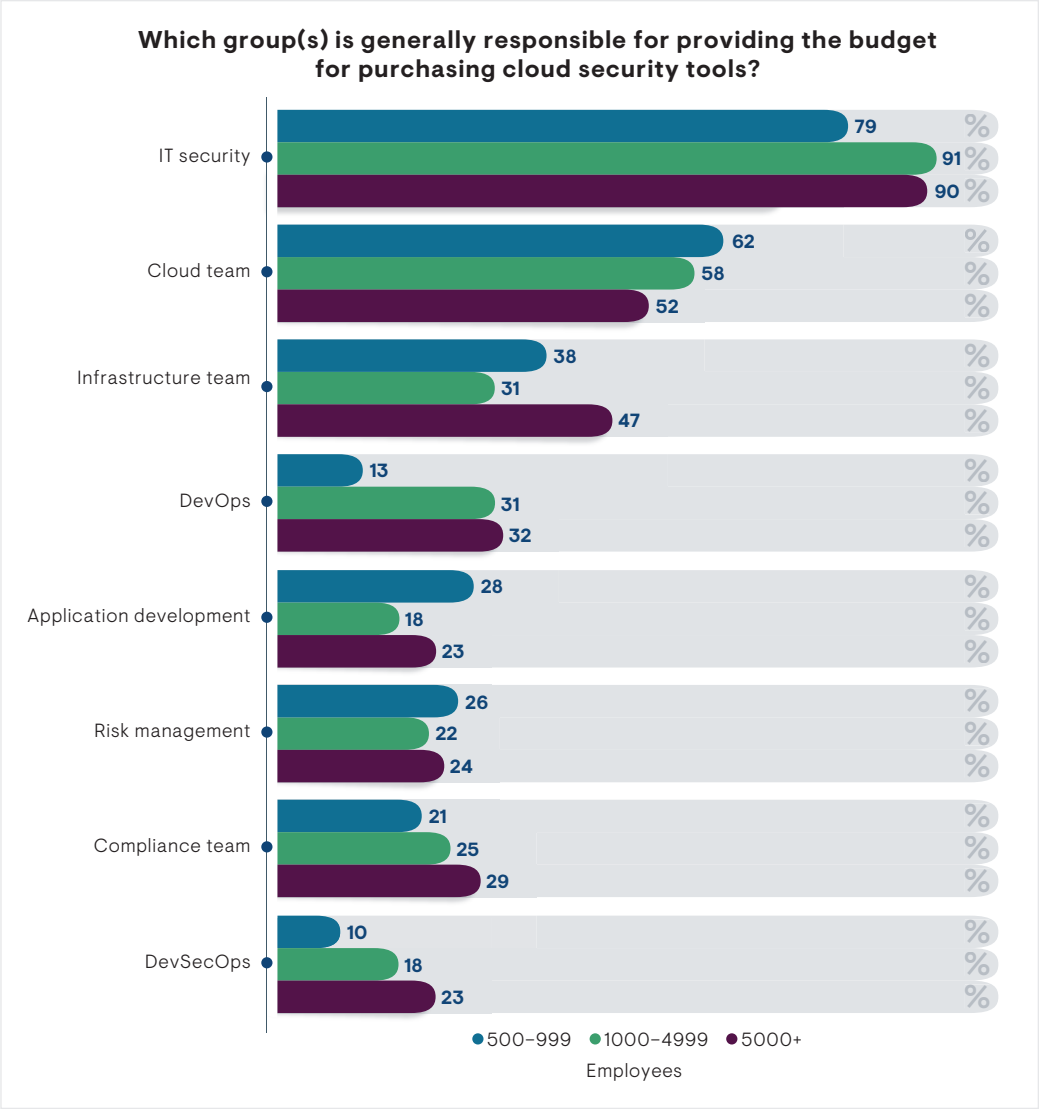


*Figure 2: Who Buys Cloud Security Tools Varies by Organization Size*

## Applying Automation to Cloud Security

As organizations continue to expand the number of cloud services they use, and as IT security teams struggle to keep up with the speed of cloud development, using automation to secure those deployments becomes increasingly critical. To gauge where organizations were in their use of automation, EMA asked respondents which of five different levels of automation their organizations had achieved in securing those cloud deployments. Most organizations are somewhere in between the least level of automation—manually managing policies and procedures—and the greatest level of automation, where automation is extensive and covers all the cloud domains in use by the organization. Fifteen percent of respondents reported one or the other of those two ends of the automation spectrum. The largest percentage of respondents (28%) reported running a growing series of automated functions from a central platform. This lines up to some extent with the most dominant approach to cloud security engagements, in which a centralized infrastructure team provides an orchestration/tooling layer (presumably with automation built in) for developers to use to get to cloud infrastructure. Another 22% reported automating basic provisioning. To get a sense of whether organizations that dedicate a larger share of the overall IT budget to security are further along in automating more cloud security functions, EMA compared answers to the automation question across different IT security budget allocations. In fact, there is an interesting split among organizations that allocate the greatest percentage of their IT budget to cybersecurity and how much automation they apply to cloud security. The largest percentage of those allocating at least 30% of their IT budgets to security claim extensive automation applied to all the cloud domains their organization uses, with 30% of those organizations reporting that approach. The next-largest percentage among that same group—27%—indicated their organizations manually manage security policies and procedures.

This stark contrast suggests that a healthy IT security budget relative to the overall IT budget does not necessarily translate into greater use of automation when it comes to cloud security. It's likely that some organizations with a large security team can afford to apply more skilled practitioners to the problem. How do those with a much smaller percentage of their IT budgets allocated to cyber-security approach automation of cloud security functions? The largest percentage of those whose organizations allocate 10% to 14% of their IT budgets to cybersecurity either use scripts to automate some cloud security functions, but still handle many tasks manually, or they run a growing series of automated functions from a centralized platform.

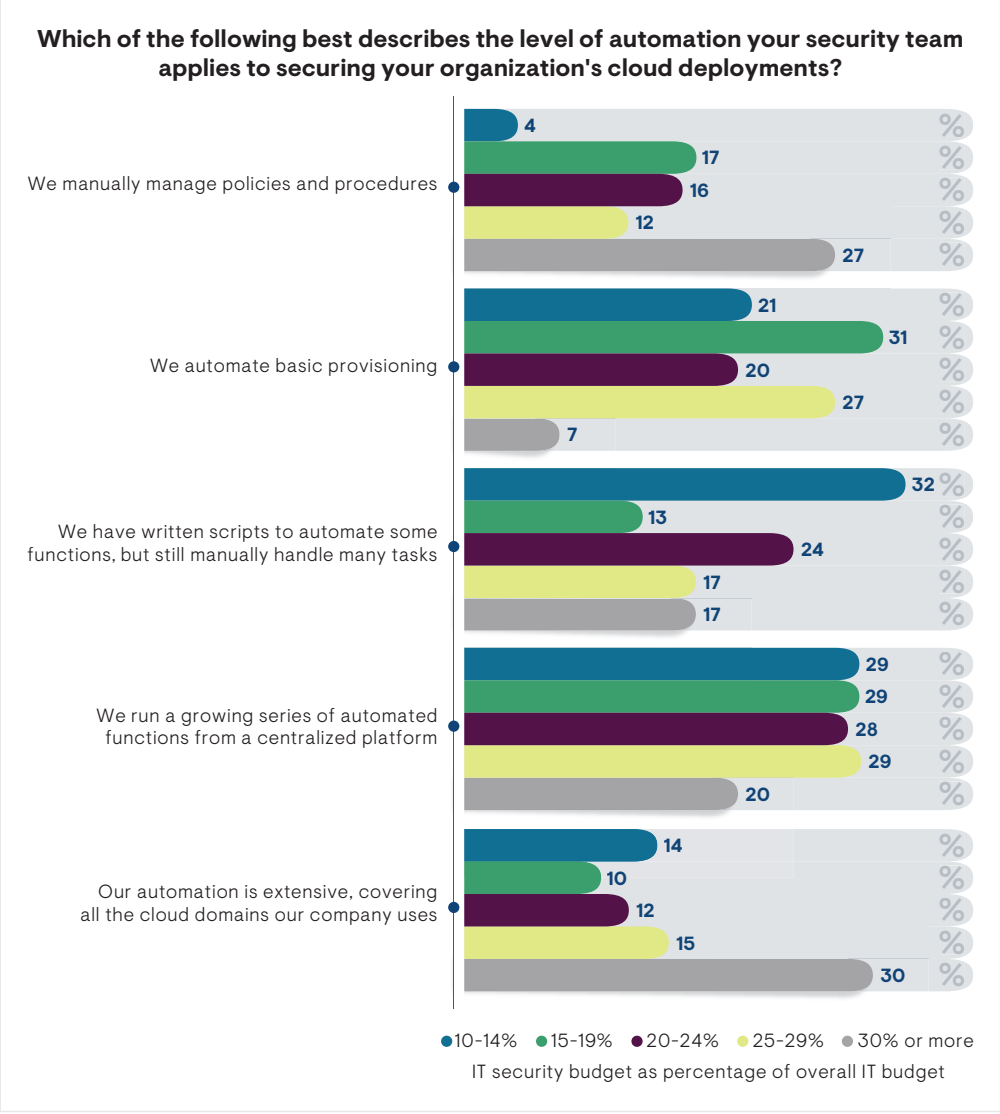


*Figure 3: Bigger IT Security Budgets Don't Mean More Cloud Security Automation*

## The *What* of Cloud Security

The complexity of those architectures and confusion around how to configure new services has led to an all-too-common scenario in which IT practitioners inadvertently expose sensitive data through misconfiguration of services. A prime example of that is the Capital One breach in 2019, when a misconfigured open-source web application firewall used in an AWS service was allowed to list all the files in any of Capital One's AWS storage buckets and read each file's content.

Contributing to the misconfiguration problem is a lack of understanding of the shared responsibility model and who is responsible for securing what in cloud services. While these are examples of the most common threats to cloud usage, there are plenty more that keep CISOs and other IT security practitioners up at night. Other types of threats include data exfiltration by malicious outsiders, insider threats, inadequate identity and access management for cloud-based assets, ransomware, and more. To gauge which threats are believed to post the biggest risk to organizations' cloud usage, EMA asked respondents to rank a list of 14 different threats to cloud-based assets according to how big a risk each posed to their individual organizations. Given the extensive amount of coverage applied to the misconfiguration issue, it's no surprise that the largest percentage of respondents ranked data loss/exposure due to misconfigured cloud infrastructure as the biggest risk to their organization's cloud usage at 16%. This was followed by 14% of respondents who thought their biggest cloud risk was data exfiltration by malicious outsiders, 11% ranked account hijacking as the biggest cloud risk, and 10% ranked a lack of a cloud security architecture and strategy as the top cloud risk. Rounding out the top five biggest cloud risks is malicious insider threats, with 9% indicating that as the biggest threat.

On the other end of the spectrum, there appears to be a lot of trust in the shared responsibility model. Only 1% of respondents gave the risk of failure of the shared responsibility model as a top concern. This in itself suggests a lack of understanding of the model, since the misconfiguration issue is caused by cloud customer error, not cloud provider error. Only 3% ranked data exfiltration by over-privileged users as the top cloud risk, and only 3% ranked insecure interfaces and APIs as the top risk. What's interesting is that the top three number-one rankings of cloud risk only represented 41% of all respondents, which suggests that there isn't a lot of agreement on what the biggest cloud security risks are. There was an apparent disconnect in comparing the ranking that respondents gave to the risk of inadequate identity and access management for cloud-based assets and other questions focused on machine-generated identities for cloud applications. The ranking of the former risk appeared somewhere in the middle for most respondents. When asked how concerned respondents were about the potential for machine-generated identities for cloud applications that contain high-level access privileges to be exploited by malicious actors, 40% of all respondents said they were very concerned, while 26% said they were extremely concerned. It is possible that respondents believe their security team has put in place adequate controls to prevent such exploits from taking place, given that 92% said it was either very or extremely important to control privileged access to cloud application environments by non-human actors.

There was some variability of which cloud risks were the top concern in looking at differently size organizations. For example, while the largest percentage of midmarket and SME respondents indicated that the top cloud risk to their organizations was data loss exposure due to misconfigured infrastructure at 23% and 17%, respectively, the largest percentage of respondents representing large enterprises viewed the top risk as data exfiltration by malicious outsiders at 18%. It's likely that large enterprises have dedicated more resources to securing their cloud-based assets, including dedicating more IT security practitioners to cloud security, and they believe they have a better handle on the cloud architectures their organization is working with. Still, for large enterprises, the second vote-getter as top cloud risk is lack of a cloud security architecture and strategy. This suggests that some large enterprises are further along in their journey to secure cloud assets than others.


*Figure 4: Top-Ranked Cloud Security Risks by Organization Size*

An interesting dichotomy on just how respondents' organizations assess these cloud security risks arose in two different questions posed to them about their organizations' ability to assess and report on cloud security posture and how they achieve that. When asked if their organizations had the ability to assess and report on their organizations' overall cloud workload security risk posture, 98% affirmed that capability. Then only 41% said their organizations were using a cloud security posture management tool. It's likely that these organizations are using a mix of tools to achieve visibility and reporting, including cloud security monitoring and analytics tools. Fifty-five percent of respondents said their organizations were using such monitoring tools.

## The Right Tool for the Job

When it comes to security tools used to secure cloud-based assets, it appears that IT security's approach to cloud security has advanced to a more mature level for a majority of respondents. The market has largely moved beyond trying to apply existing security controls used in internal data centers to cloud-based assets. The largest percentage of respondents indicated their organizations were adopting newer best-of-breed, cloud-native controls to protect cloud apps and workloads at 35%. That was followed closely by hybrid controls that span both internal data centers and those of cloud providers at 30%. These two approaches were especially favored by large enterprises, with 31% and 35% of those organizations selecting those two options, respectively. SMEs, on the other hand, tend to more heavily favor best-of-breed, cloud-native security tools, with 41% of those indicating that choice, while midmarket organizations more often favor hybrid security controls. Only 20% of all respondents said they were applying existing on-premises controls to cloud-based apps and workloads. It's good to see this percentage shrinking and it's likely to continue on its downward trajectory. It's worth noting that only 7% of security teams among the sample base are relying on proprietary security controls offered by each cloud provider to secure workloads and applications, although 13% of large enterprises are taking this approach.

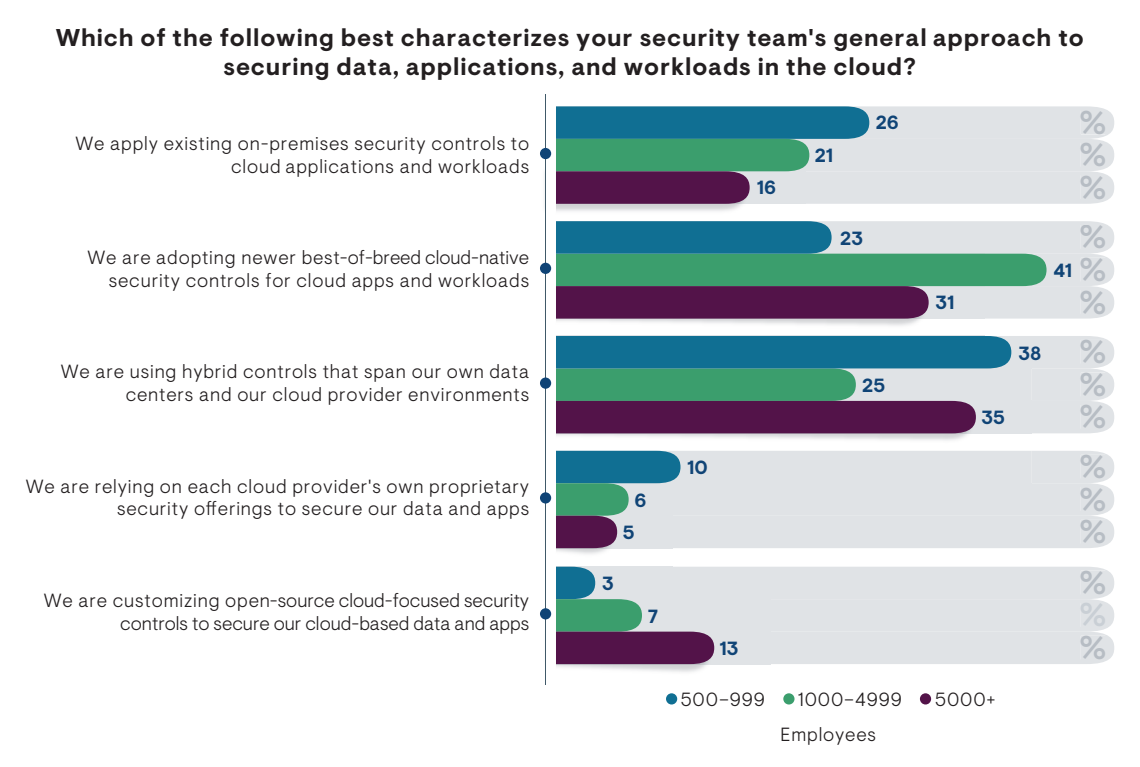


*Figure 5: Types of Security Tools Used to Secure Cloud Assets*

With the growing reliance on cloud-native, best-of-breed security controls, which types of controls are these organizations relying on most often? Out of 14 possible controls, the largest percentage of respondents indicated their organizations were using cloud data security software, cloud security monitoring and analytics, API security software, cloud threat detection and response technology, and cloud file security software. Respondents could select all tools that applied to their organization. Given the large number of selections, it's clear that the days of thinking that a cloud access security broker was all that was needed are long gone. Not surprisingly, the least-used security control is firewall as a service. Adoption of FWaaS is just getting started, although the global pandemic and need to secure users working from home could accelerate that adoption. At the same time, FWaaS is a key ingredient of the emerging secure access service edge architecture.

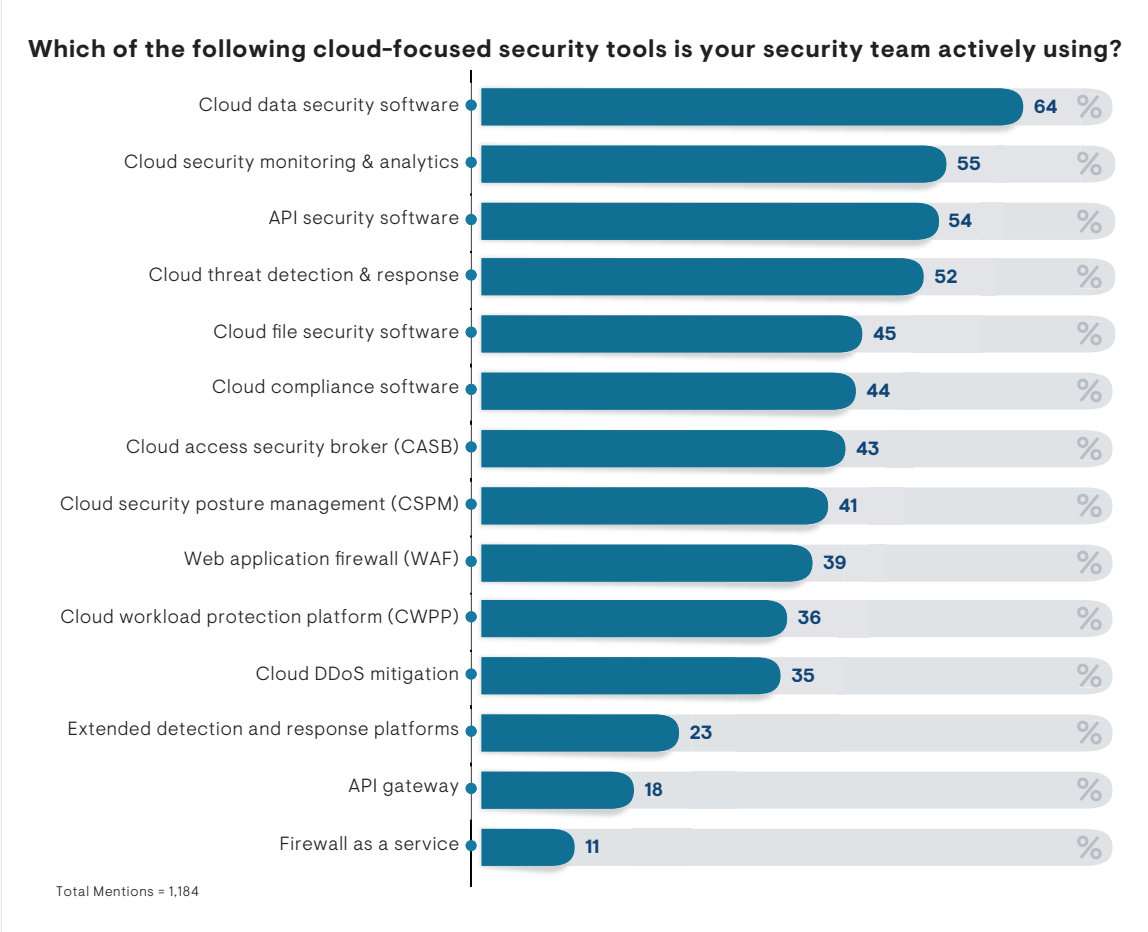


*Figure 6: Cloud-Focused Security Tools in Active Use*

Among respondents who indicated use of cloud-focused security tools, the go-to security tools were fairly common across all three organization size ranges, although large enterprises tend to lean more heavily on cloud security monitoring and analytics products while SMEs turn more frequently to cloud data security software. It's worth noting that as security teams work to detect threats to their cloud environments, a significant majority of respondents indicated that their organizations are using threat intelligence feeds to help identify and secure threats to their cloud environments. Among the 87% who indicated this, most expressed a willingness to boost the threat information they would be willing share with industry peers if it demonstrably improved their own ability to detect cloud threats.

Meanwhile, newer tools (such as cloud security posture management) designed to help identify and fix cloud misconfiguration issues are still not widely used among respondent organizations. Although still a nascent market, CSPM technology is likely to gain much greater attention as organizations come to grips with one of the top cloud threats. Also on the horizon as organizations mature their cloud security capabilities are two other, more nuanced detection and response technologies. With the release of virtual network taps or cloud traffic mirroring by IaaS cloud providers, such as AWS and Microsoft Azure, within the last few years the ability of cloud customers to monitor their own out-of-band cloud traffic became a practical reality. With widespread support among existing network detection and response vendors, IT security practitioners are likely to turn to this cloud security toolset to gain better visibility into their own cloud traffic. In fact, 80% of respondents noted their awareness that NDR technology can be applied to cloud traffic. Among those respondents, 48% see as its primary value the ability to detect threats and anomalies in real time, while 21% see its primary value as facilitating response actions, such as investigation and mitigation.

Another cloud visibility issue that security practitioners may try to tackle as they mature their cloud security function is detecting threats and anomalies in the business logic of cloud applications running in a production environment. Application workload detection and response technology, a subset of the overall cloud workload protection platform market segment, aims to bridge the gap between more static, preproduction application security testing and infrastructure protection in runtime environments by focusing at the application layer, mapping and tracking that environment in real time, learning normal application behavior, and responding to anomalies. Although still in its infancy, ADR was recognized by over 70% of EMA survey respondents. Among those, the largest percentage of respondents believe it offers value in speeding detection of application attacks, providing full attack lifecycle visibility and speeding attack mitigation.

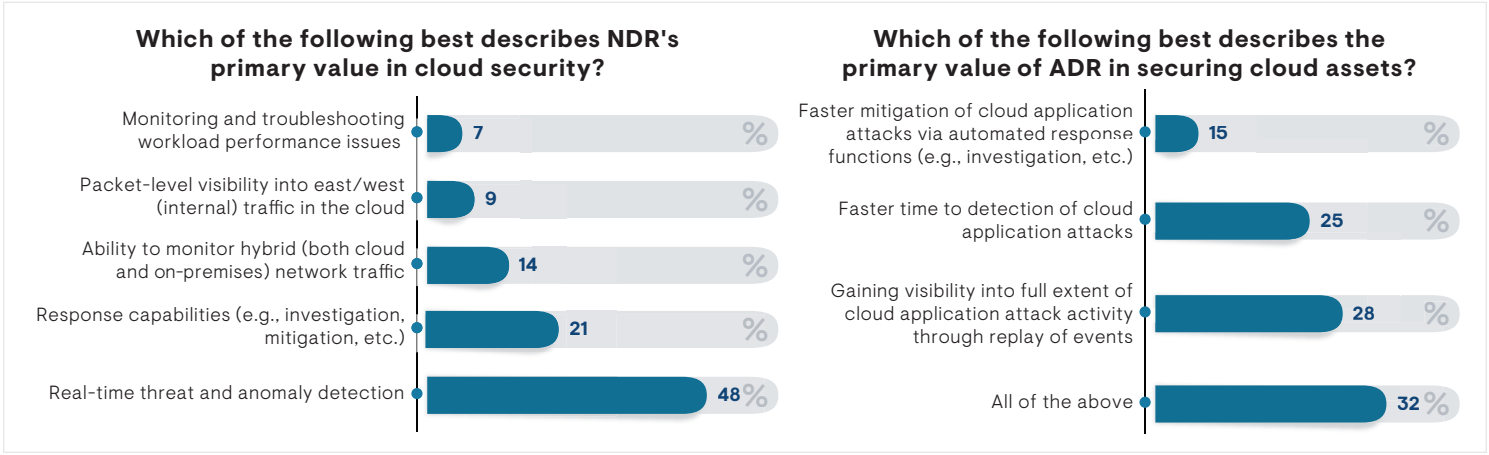


*Figure 7a and 7b: Primary Value of NDR and ADR*

## Why the Disconnect?

EMA sought to gauge what respondents thought of their cloud security practitioners' abilities when it comes to securing cloud assets. Remember, most respondents reported some level of involvement in the acquisition of cloud security solutions, with the largest percentages approving/ purchasing, evaluating, or managing/maintaining such solutions. When asked to rate the level of knowledge that the security team had in specific cloud security requirements, 87% said their practitioners were very or extremely knowledgeable. They also expressed high confidence in their security teams' awareness of all cloud usage and in their ability to learn of and categorize all of the data their organization has stored in the cloud. This is a tall order, especially for large and decentralized enterprises in which different lines of business have independent decision-making power to adopt different cloud services. With all of the attention in the industry given to the reported lack of understanding of the shared responsibility model, respondents nearly universally declared that their security team understands that model either well or very well, with 94% reporting such confidence.

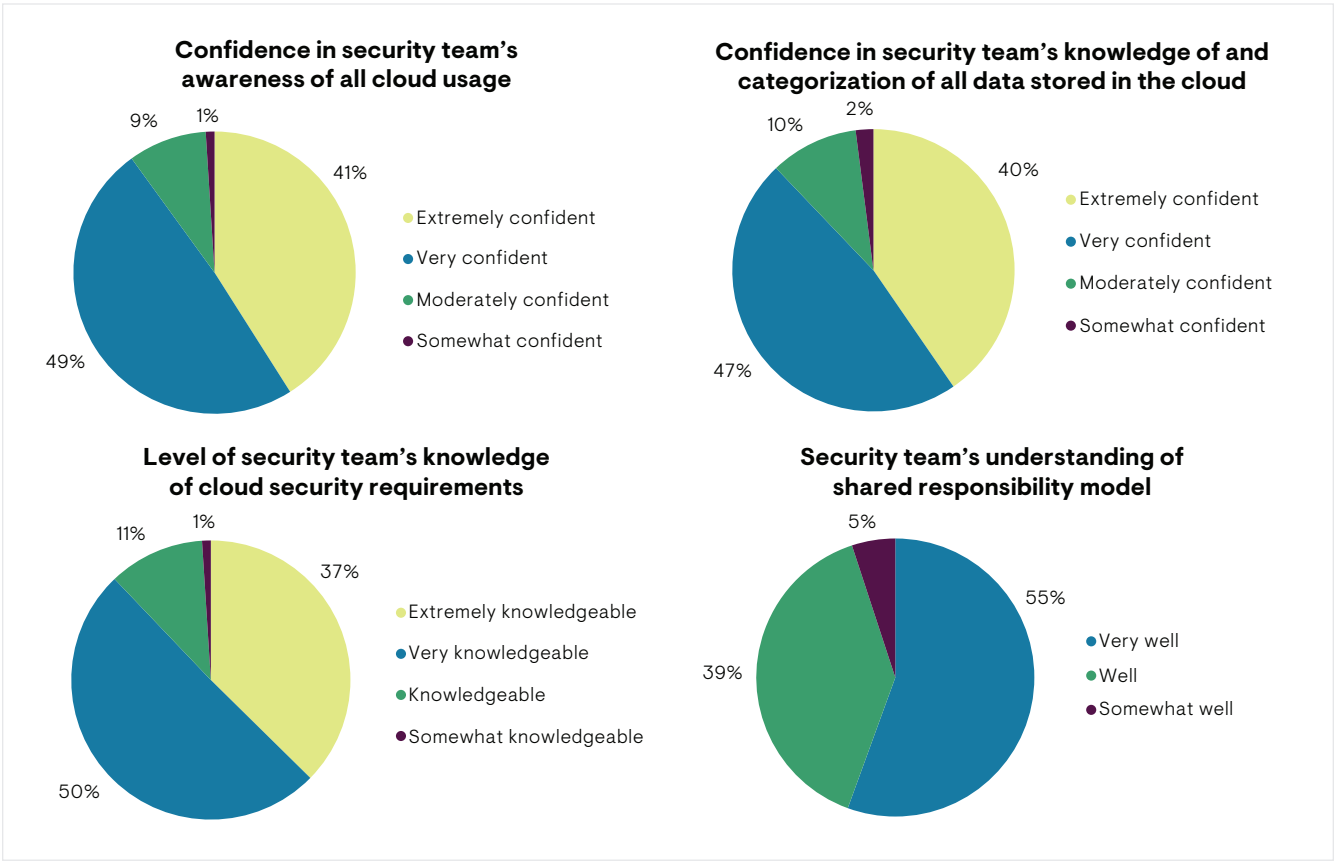


*Figure 8: Rating Cloud Security Ability*

However, in specific questions posed to respondents about their IT security team's level of visibility into their organization's usage of SaaS, PaaS, and IaaS services, such answers did not quite stack up to the high level of confidence expressed generally about cloud usage visibility. For example, when asked to rate the security team's level of visibility into their organizations' SaaS usage on a scale of one to five, with one being the highest level of visibility, only 18% gave it a one and only 27% gave it a two. Another 27% gave it a four. These percentages improved ever so slightly for rating of PaaS usage visibility, then ever so slightly again for visibility into IaaS usage. It should be noted that for each of the three cloud service types, between 11% and 13% gave visibility into usage of those five, but in the more general visibility question, not one respondent indicated that they were not at all confident in their security team's awareness of all cloud usage. This suggests that efforts to improve visibility into the activity surrounding usage of different types of cloud services is a work in progress. Much more is still to be done before IT security teams can declare with any real confidence that they can see what activity is taking place within their different cloud environments.

In looking at awareness of specific types of cloud service usage by organization size, midmarket respondents indicated a significantly greater level of confidence in visibility into SaaS usage and somewhat greater confidence in visibility into PaaS and IaaS usage than the overall sample. With tighter budgets, fewer cloud-based assets, and a longer history of using various cloud services, it makes sense that midmarket organization IT security teams would have greater visibility into usage of different cloud types. Meanwhile, respondents representing SME organizations rated their IT security team's level of visibility into SaaS and PaaS usage fairly poorly overall, while they expressed greater confidence in their security team's visibility into IaaS usage. The largest percentages of respondents representing large enterprises gave their IT teams' visibility into each of the cloud service types either a two or a four. These varying levels of confidence in IT security's visibility into cloud type usage could indicate that differently sized organizations are at different levels of maturity in their cloud security initiatives.

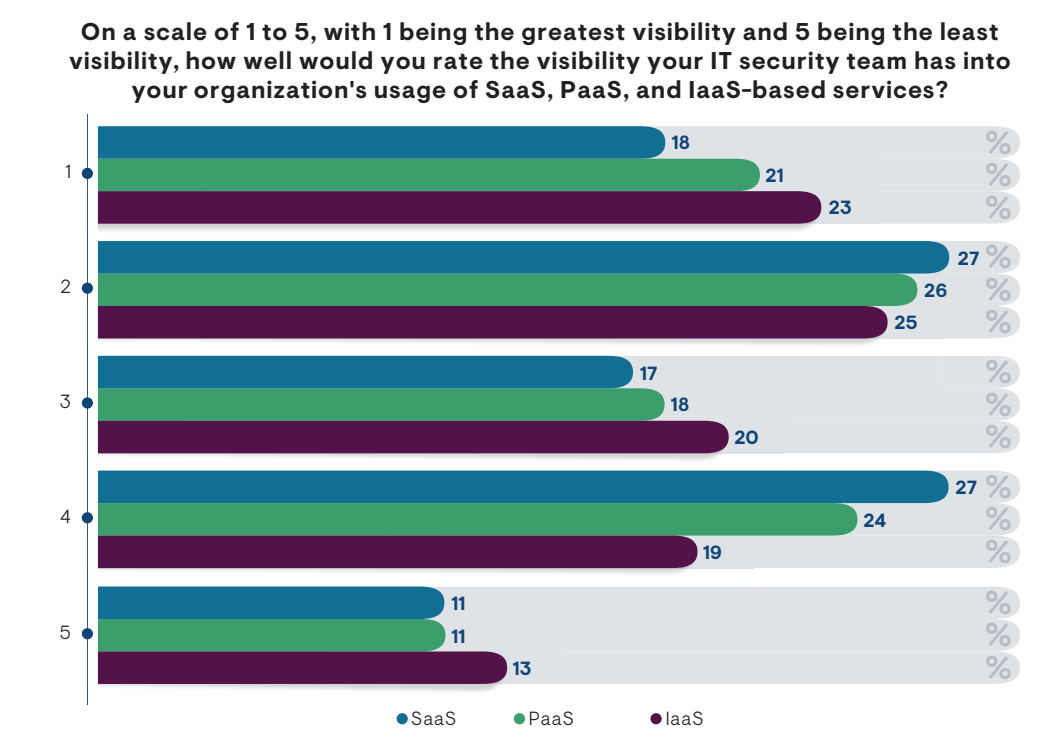


*Figure 9: Rating Visibility into SaaS, PaaS, and IaaS Usage*

## Conclusion

Both enterprise IT security groups and cloud providers have miles to go in creating the right set of controls, the right organizational structure, and the best way to educate users on best configuration and security practices for cloud usage, and in establishing the right culture to achieve the optimum security for cloud-based data, applications, and workloads. The lion's share of enterprise IT security teams have progressed way beyond being the department of no and slow. CISOs and other enterprise security executives have come to understand the need for greater oversight of the processes used to establish cloud usage. As more DevSecOps initiatives are established or as they move forward, progress will accelerate, even as configuration hiccups continue to make headlines

## About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that provides deep insight across the full spectrum of IT and data management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help EMA's clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise line of business users, IT professionals and IT vendors at www.enterprisemanagement.com or blogs.enterprisemanagement.com. You can also follow EMA on Twitter, Facebook or LinkedIn.

---



**Corporate Headquarters:**
1995 North 57th Court, Suite 120
Boulder, CO 80301
Phone: +1 303.543.9500
www.enterprisemanagement.com

4066.020421