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

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

Sponsored by:

ExtraHop

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

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

Table of Contents

EMA

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

Executive Summary

Trying to gauge where organizations are in their journey to secure cloud-based assets is akin to answering some of the basic questions necessary in a news story: the who, what, when, where, how, and why of cloud security.

Who. In research EMA carried out in late 2020 of North American IT practitioners and executives, those who are responsible for securing cloud assets include IT security teams, with 46% of respondents reporting that group as leading the charge. Also responsible are separate cloud operations groups, with 28% reporting that approach, and another 9% reporting network operations as handling cloud security. As more workloads and applications are migrated to the cloud, organizations are expanding the number of IT security practitioners dedicated to cloud security. For organizations with between 500 to over 20,000 employees, the mean number of dedicated cloud security practitioners is 292.

How organizations approach cloud security engagements appears to be coalescing around a handful of options, with the most common approach relying on a central infrastructure team that provides a tooling/orchestration layer for developers to use to get to cloud infrastructure, with just over half of all respondents reporting that paradigm. The next-most common approach is to employ decentralized DevSecOps with distributed teams dominated by developers, but including embedded security engineers or close support from a central security team, with 23% of respondents reporting that approach. IT security teams or practitioners collaborating well with their colleagues in the application development organization is critical to ensuring the security of applications as they are migrated to the cloud. While that level of collaboration has improved, there is still more work to be done. When asked to rate the level of collaboration between application developers and the security teams on a scale of one to five, with one being extremely collaborative and five being not at all collaborative, 28% of respondents gave it a one, while 26% gave it a four.

What. Based on a list of 14 different threats to cloud-based assets, 16% of respondents ranked data loss/exposure due to misconfigured cloud infrastructure as the biggest risk to their organization's cloud usage. This was followed by 14% of respondents who thought their biggest cloud risk was data exfiltration by malicious outsiders. The types of tools organizations are applying to the task of protecting cloud-based assets have evolved away from trying to apply existing security tools and technologies to cloud assets. Instead, 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%.

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

Methodology and Demographic Overview

In late 2020, EMA surveyed 211 IT executives and contributors whose organizations largely serve customers in North America, although many had a secondary presence in other geographies. Most respondents worked within the IT organization, although just under 10% worked within a separate cybersecurity/fraud/risk/compliance organization. The largest percentage of respondents held IT Director-level positions at 34%, followed by IT Manager-level positions at 21%, and 9% were CIO/CTO/IT VPs. Despite the range of titles, a clear majority of respondents indicated that their primary role was in IT/information security at 73%, and the rest had some secondary responsibility for IT security.

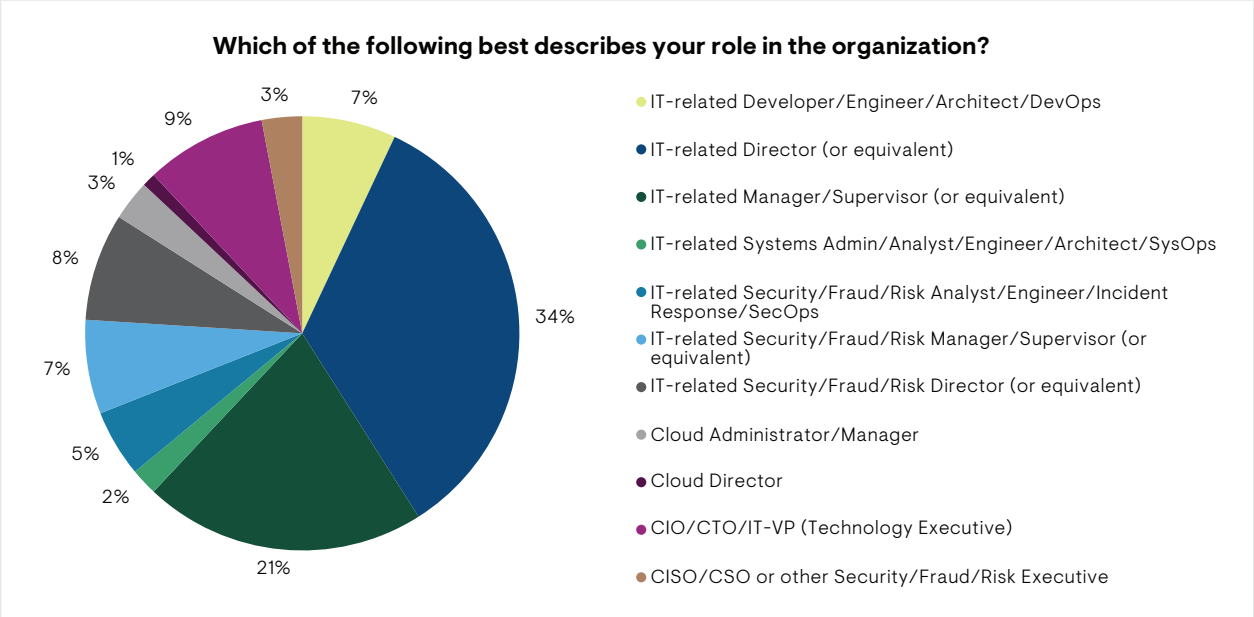

Figure 1: Respondent Roles

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.

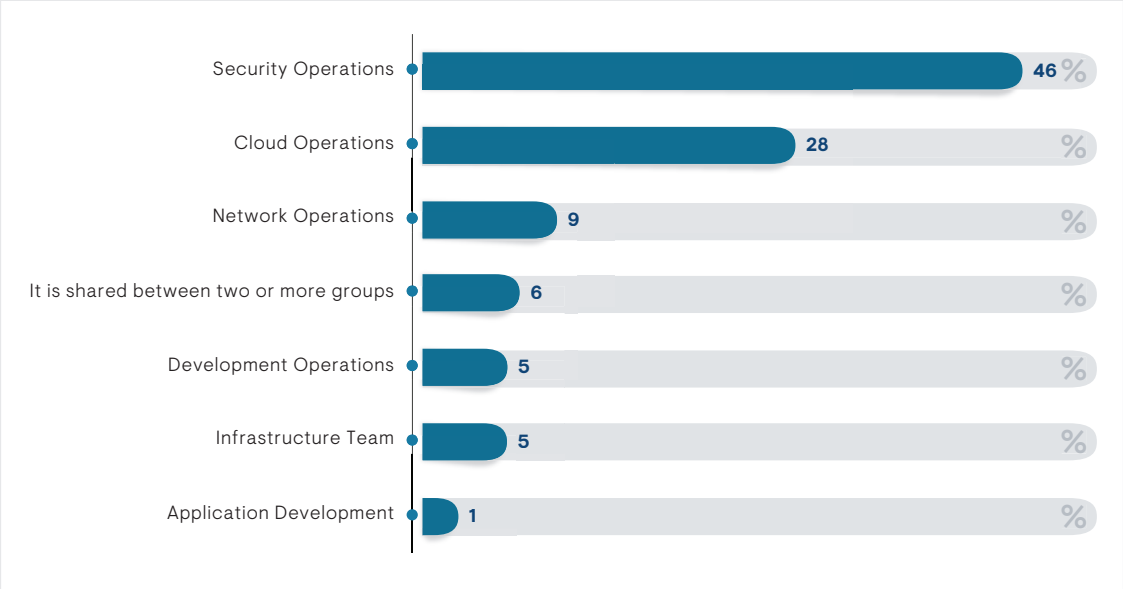

Figure 2: Who is Responsible for Cloud Security?

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.

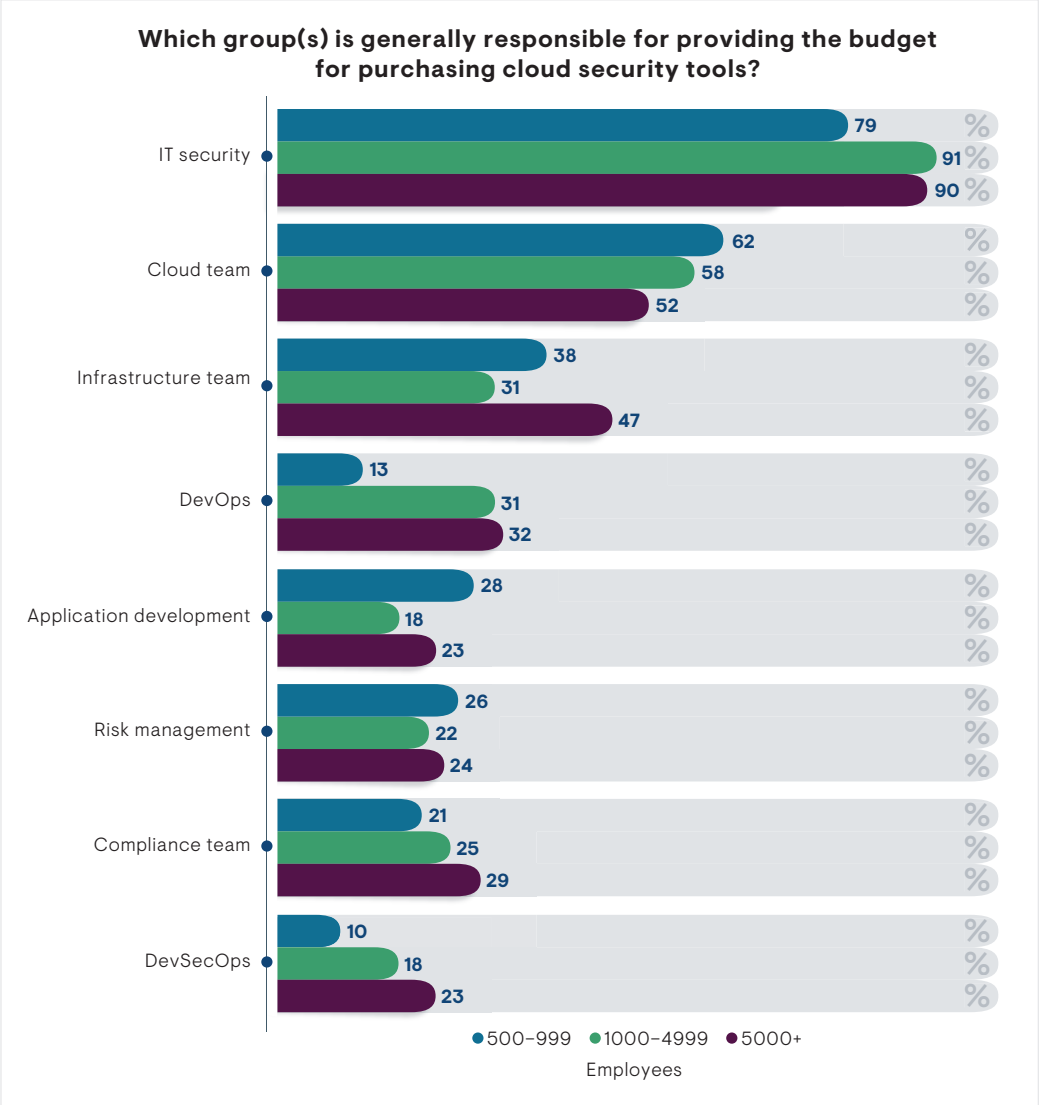

Figure 3: Who Buys Cloud Security Tools Varies by Organization Size

The *How* of Cloud Security

With the advent of continuous integration and continuous delivery methods of application development, the tension between developers and those responsible for ensuring the security of new applications running primarily in the cloud has risen to new levels. Security teams are struggling to keep up with the ship fast/run anywhere mode of code development, and it's more critical than ever for security and development teams to work together effectively to test for, identify, and fix vulnerabilities before they are exploited by bad actors. How well are these two teams with differing goals collaborating to assure the security of new code before it goes into production? Survey respondents were asked to rate the level of collaboration between application developers and the security teams on a scale of one to five, with one being extremely collaborative and five being not at all collaborative. Among all respondents, 28% gave it a one, but another 26% gave it a four. However, in looking at those answers according to the size of the organization respondents represented, there were interesting differences. Among those representing large enterprises, only 15% gave the level of collaboration a one, while the majority of those respondents gave it either a two or a four. This is despite the fact that the largest percentage of large enterprise respondents reported that those responsible for application security meet with developers on a daily basis at 37%, followed by 31% that meet on a biweekly basis. Meanwhile, those representing small to medium-sized enterprises were relatively evenly split between a one and a four in rating the level of collaboration they observed between application developers and the security team. Clearly, there is more work to be done to better align application development and security teams in hardening new code, and organizations of different sizes are at different points in their journey to evolve and automate code testing processes to meet the challenge of keeping pace with faster CI/CD development pipelines.

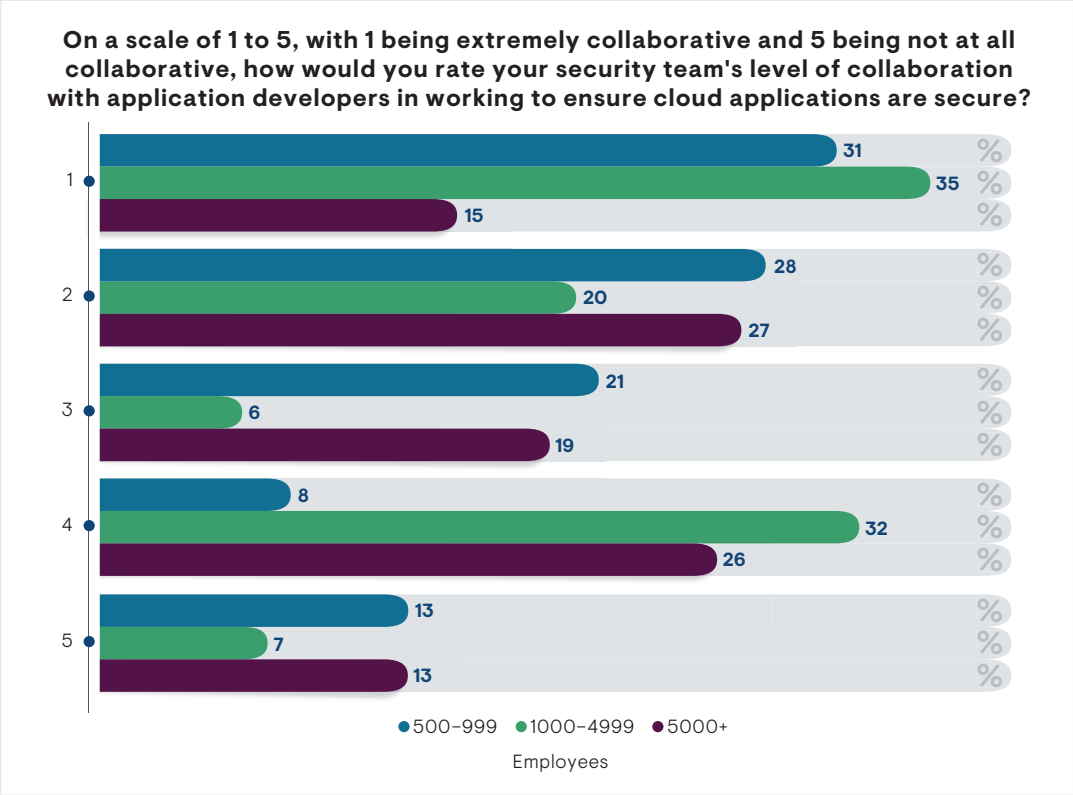

Figure 4: Level of App Dev and Security Team Collaboration Varies by Organization Size

How organizations approach cloud security engagement has been a topic of discussion for years within the IT security industry. Some pundits and those further along in their journey to better secure cloud usage advance the notion that security champions should be embedded within the application development organization to help ensure more secure cloud code is created. Much of the discussion among security practitioners focuses on the need for a cultural shift that requires a new approach and different tools than what were used in the past. Some organizations found that what worked best for their organization was to have the application development team hire its own application security engineer, who then collaborated with the CISO's security team to help guide what needed to be done to assure cloud security. Having that role enables the necessary channels of communication and can help progress the necessary cultural shift. Other CISOs counsel their peers to embrace cloud computing tools and practices to leverage the agility they can provide.

Well-respected CISO Phil Venables, now Google's CISO but formerly a long-time IT security executive at Goldman Sachs, has observed four distinct approaches to cloud security engagement in networking with peers. Two of those include an ad hoc, developer-led team or group that follows cloud provider recommendations or uses cloud provider default security, and a decentralized DevSecOps with distributed teams dominated by developers but including embedded security engineers or close support from a central security team. Another of the four approaches includes a central infrastructure team that provides a tooling/orchestration layer for developers to use to get to cloud infrastructure. In this approach, the orchestration layer provides security defaults and gates for security tooling to validate deployments. The last approach uses a corporate cloud orchestration platform with independent control plane validation and security team-owned cloud security posture management in place to validate the effectiveness of the orchestration platform. In the research project, EMA presented respondents with these four approaches to learn how common each is and whether any other approaches are used. The most common approach among all respondents relies on a central infrastructure team that provides a tooling/orchestration layer for developers to use to get to cloud infrastructure. This is especially the dominant approach used by midmarket companies and large enterprises, where respectively 59% and 58% took that approach. The next-most common approach for all three organization size ranges is the decentralized DevSecOps with developer-dominated teams. The least selected approach among all organization sizes is the ad hoc, developer-led team relying on cloud provider recommendations. Although respondents were given the option to describe another approach to cloud security engagement outside the four defined, none did so.

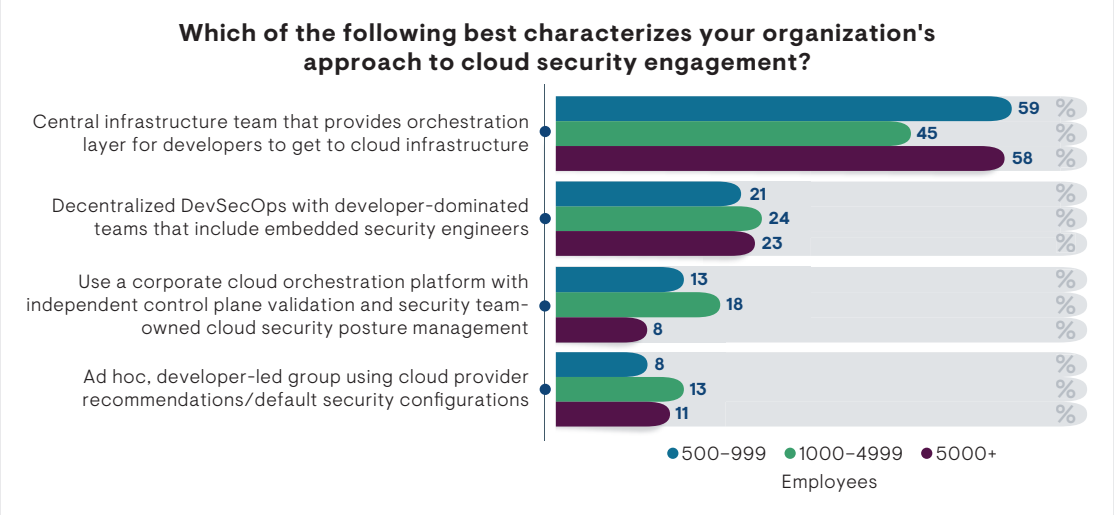

Figure 5: Four Primary Approaches to Cloud Security Engagement

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.

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 6: 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.

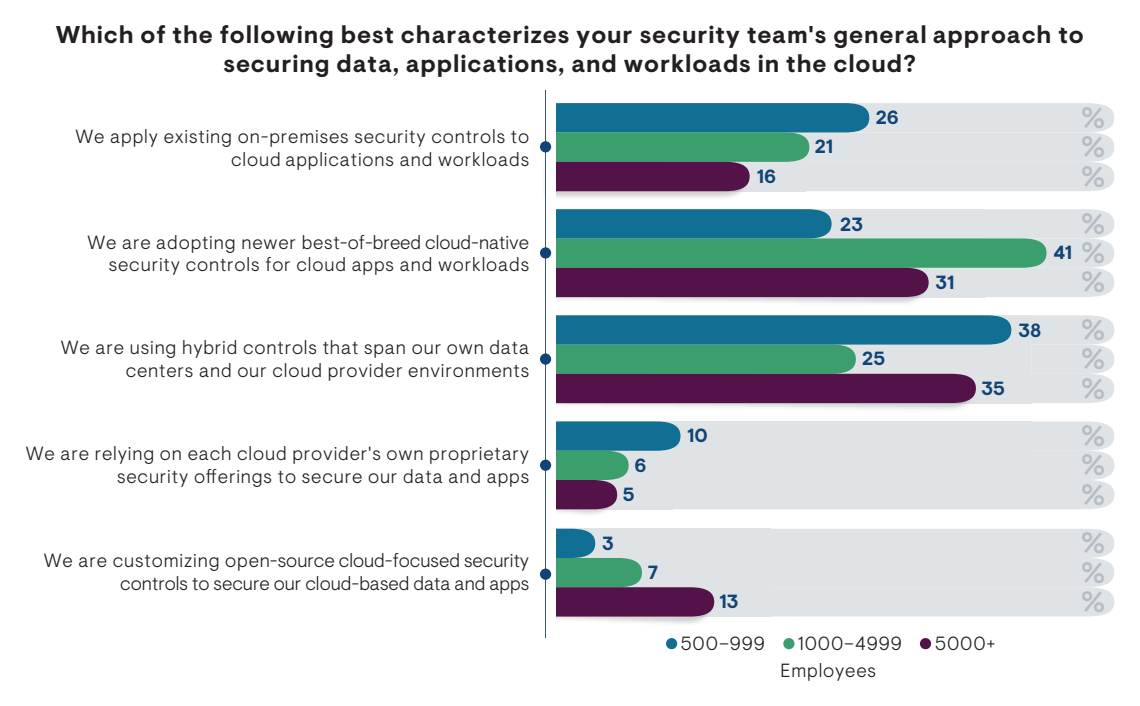

Figure 7: Types of Security Tools Used to Secure Cloud Assets

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.

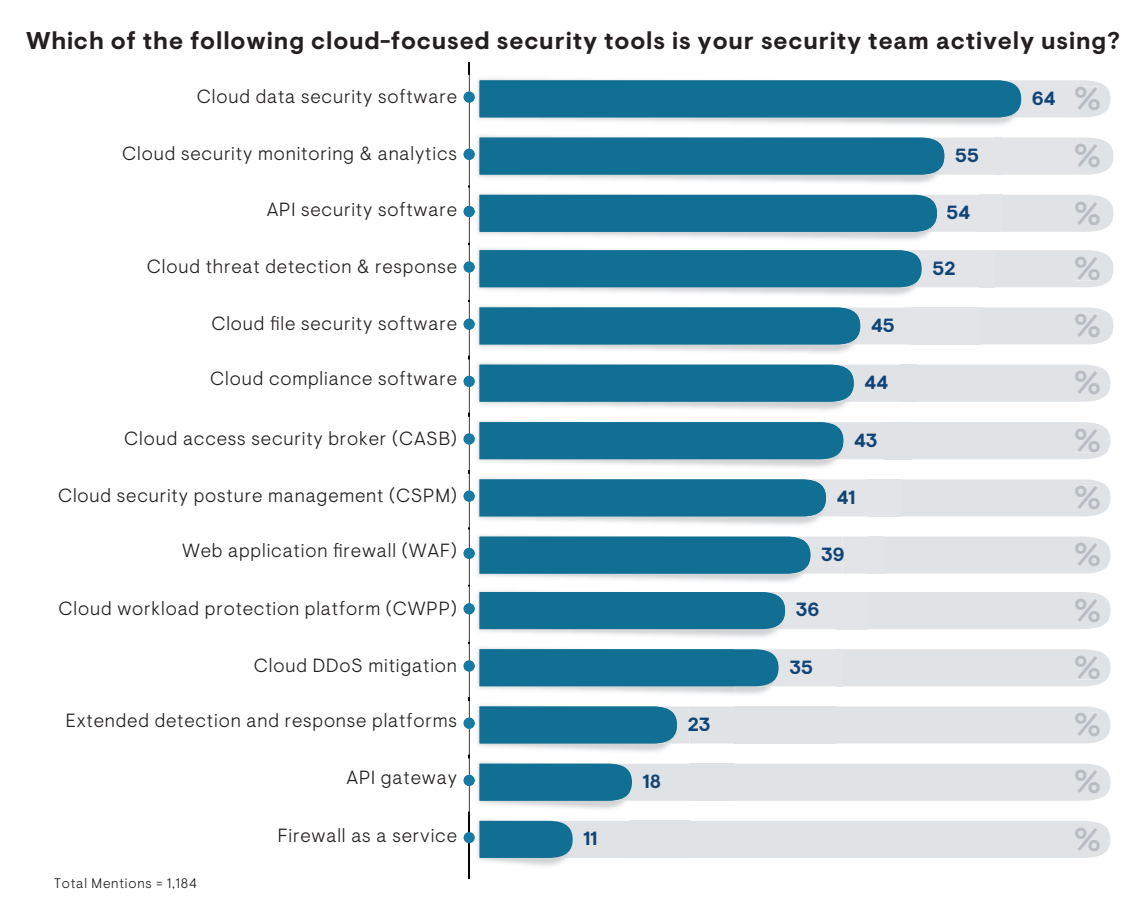

Figure 8: Cloud-Focused Security Tools in Active Use

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.

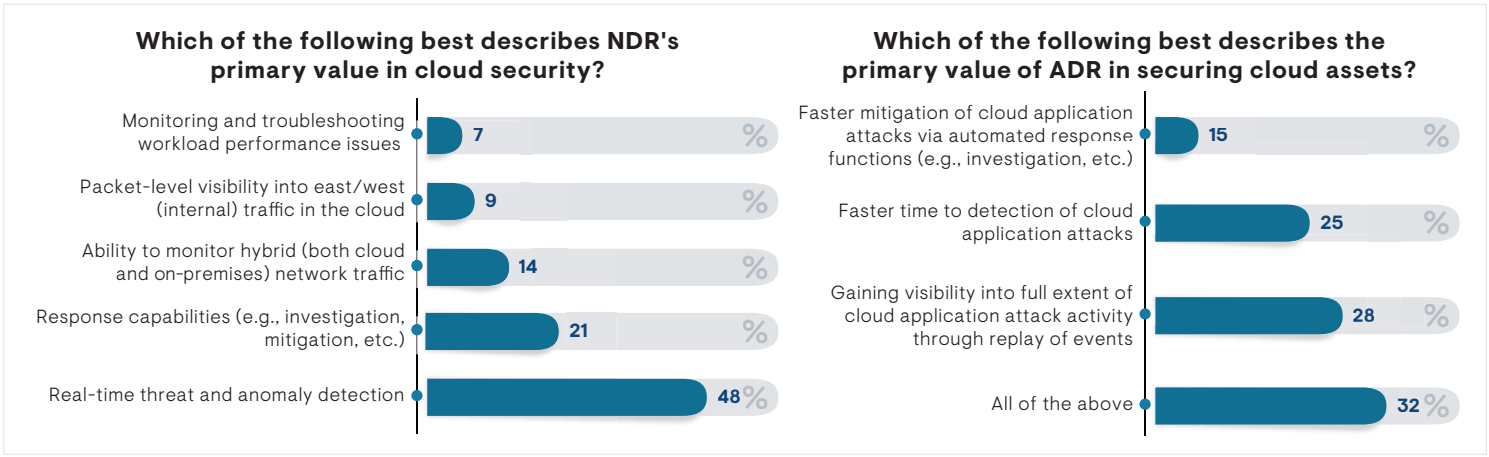

Figure 9a and 9b: Primary Value of NDR and ADR

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

4066.020221