SANS

Analyst Program

Survey

Network Security in the Hybrid Cloud Era

Written by Dave Shackleford

October 2023

paloalto NETWORKS

Executive Summary

As more organizations deploy infrastructure in the cloud, many teams are struggling to adapt their controls, processes, and skills to handle this new frontier. Should network security controls and processes used on premises shift into the cloud as well? Should teams adopt cloud-native controls from the providers? Who will manage and oversee these controls and designs? What are some of the top challenges in adapting network security to the cloud? In this survey, we asked the SANS community to weigh in on how network security is changing in the cloud, and where we see it headed.

In this survey, some of the top takeaways include the following:

- Roughly half of organizations are feeling more confident in cloud and security maturity, and there have been noted improvements in team governance and collaboration.
- For organizations deploying next-generation firewall (NGFW) solutions in the cloud, finding and retaining the skills needed to architect these solutions was the primary challenge.
- Most organizations have adapted many on-premises network security controls to the cloud (such as NGFW and network IDS/IPS), but cloud-native network security controls such as DDoS protection and WAF are growing in popularity, too.

Demographics

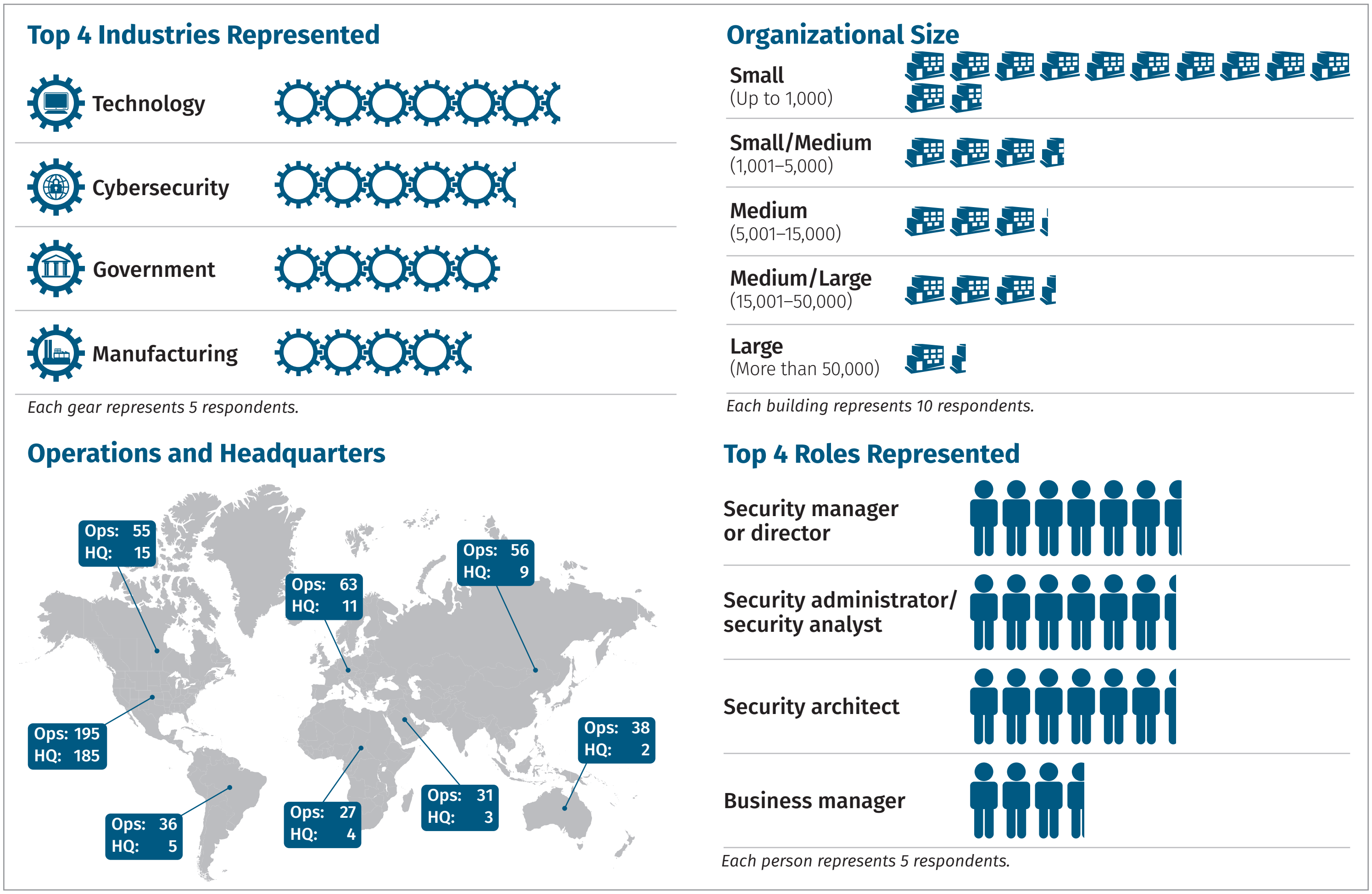

Figure 1. Demographics of Survey Respondents

As shown in Figure 1, almost 14% of respondents were in the technology industry, with 12% in cybersecurity, 11% in government, and 9% in manufacturing. Many other verticals also were represented.

Almost 63% work in smaller organizations (2,000 employees or fewer), close to 20% are in mid-size organizations with between 2,000 and 15,000 employees, and another 21% work in large organizations with 15,000 to 100,000 employees or more.

Forty percent of respondents were security analysts or admins, security architects, and security managers or directors. Other roles represented include CSOs and CISOs, IT managers and directors, and systems admins and compliance analysts. This may indicate a more technical analyst viewpoint in the results when compared with management and compliance-centric roles.

Organizations had operations in most countries, with the United States having the most presence (83%), followed by Europe (27%) and Asia (24%). Respondent organizations' headquarters were mostly in the US as well (79%), with Canada (6.4%) and Europe (5%) rounding out the top three. We also asked survey respondents to indicate which regions they provide support in, with the United States leading with close to 81%, Canada at 17.5%, and Asia and Europe both close to 17%.

Shifting to Cloud Computing

One of the key areas of focus in this survey was to determine what types of cloud deployments were in use and planned across organizations globally, the range of applications and data in use within the cloud ecosystem, and how network security is changing to integrate with cloud deployments. Not surprisingly, almost 55% of respondents indicated that they currently have a hybrid or multi-cloud model in place today, which could include software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS) alongside some on-premises infrastructure. Just over 29% indicated that they are following a "cloud first" deployment strategy, with another 12% only using SaaS now.

Similarly, we asked respondents about the types of deployments they currently had, ranging from cloud-native options like containers, serverless, and Kubernetes to software-defined core infrastructure such as virtual machines and networking. Almost 45% of respondents indicated that they are currently invested in both types of deployments (cloud-native and more "traditional" virtualized software-defined infrastructure), while just over 38% indicated they are in virtualization/software-defined infrastructure only. Just over 17% are using only cloud-native services and applications such as serverless.

We asked the community what cloud applications they were making use of today in the public cloud. Business apps and data topped the list at 66%. Security services were second at 52%, and backups and disaster recovery were the third most popular category at 47%, likely driven by ransomware attacks. Server virtualization, cloud storage, and workforce applications were common, as well. See Figure 2.

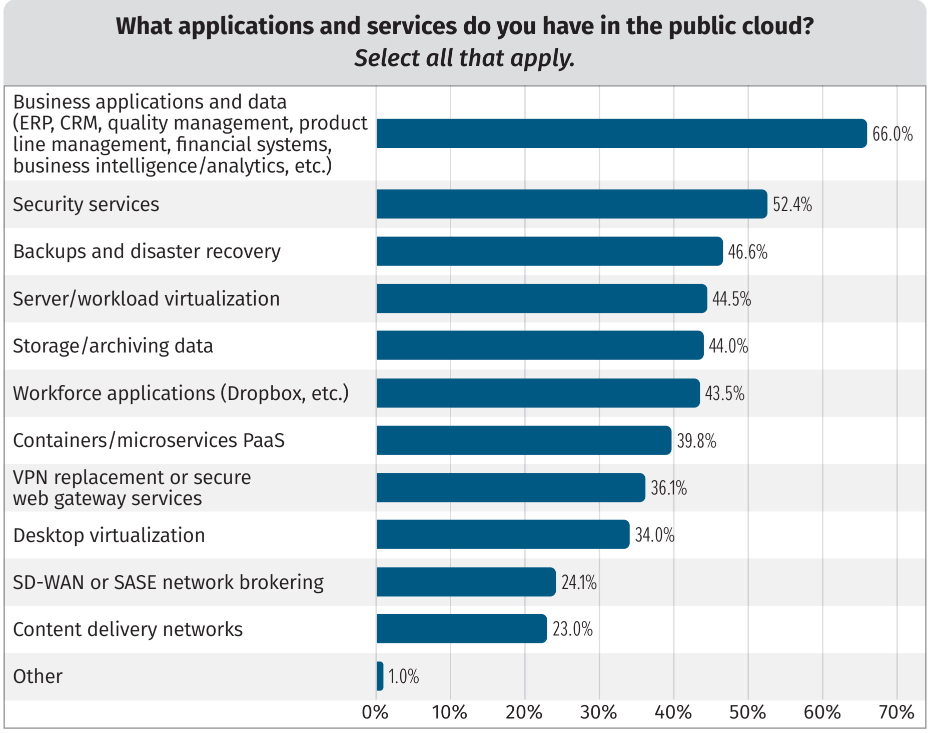

Figure 2. Cloud Applications in Use

This survey also revealed a consistent response in the number of public cloud providers that organizations are using. Based on previous SANS surveys, most organizations have indicated that they are leveraging two to three PaaS/IaaS providers, and that number has stayed consistent in this survey.[1] Smaller organizations are still hesitant to move into multi-cloud deployments, and only a small number of organizations are using more than seven cloud service providers. That some survey respondents admitted to being unsure about the total number of cloud providers in use is telling because it may indicate the presence of shadow IT in the cloud, or simply a lack of insight by the person responding (see Figure 3).

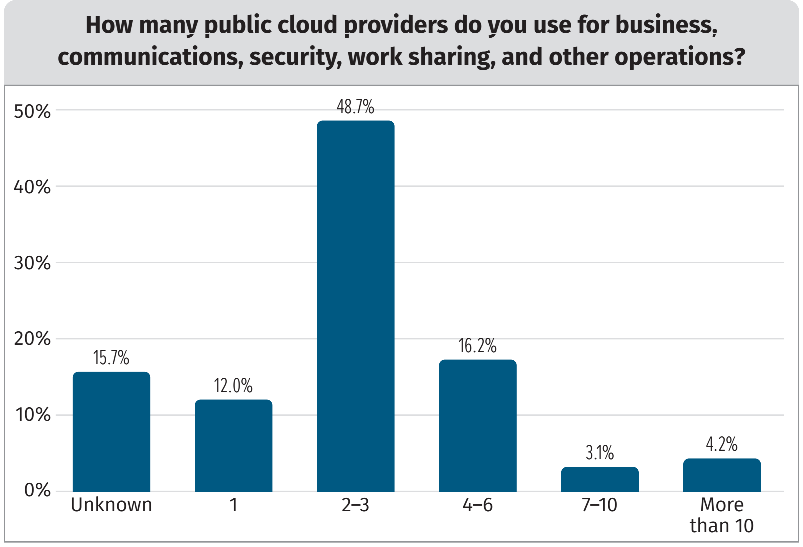

Figure 3. Number of Cloud Providers in Use

[1] "SANS 2022 Cloud Security Survey," www.sans.org/white-papers/sans-2022-cloud-security-survey/ and "SANS 2021 Cloud Security Survey," www.sans.org/white-papers/40225/

As in past SANS surveys focused on cloud security, we asked what kinds of sensitive data organizations were currently storing in the cloud. Business intelligence was first with 47%, followed by business records (financial) at close to 46%, and employee personal information at slightly over 43%. Overall, while the types of data may fluctuate, the general trend here is similar to what we have observed in the past several years: roughly one-half of organizations are willing to put a variety of sensitive data types in the cloud, with lower percentages for those data types that clearly could face enforcement action (customer payment card information was 22%, and employee healthcare records at 30%). See Figure 4.

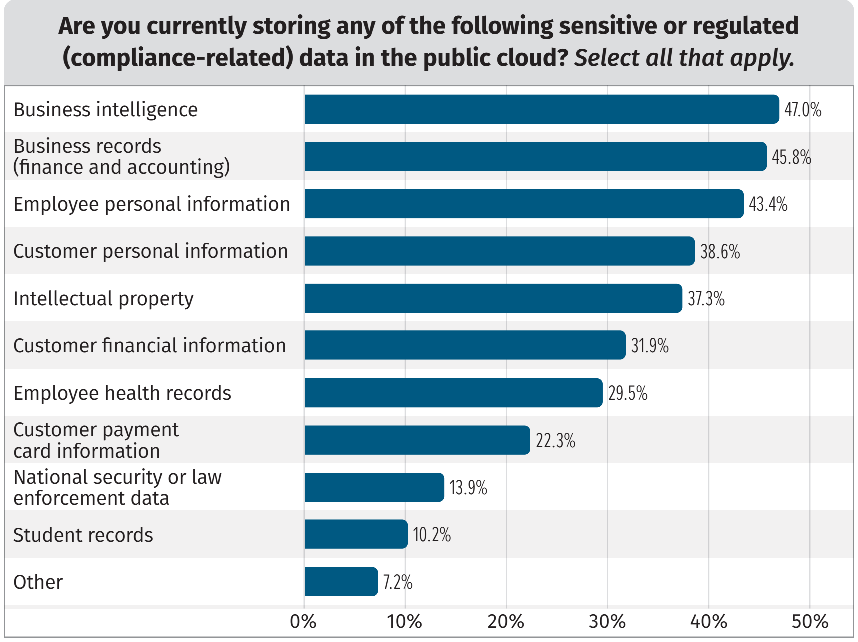
Are you currently storing any of the following sensitive or regulated (compliance-related) data in the public cloud? ***Select all that apply.***

Figure 4. Sensitive Data in the Cloud

With the volume of cloud deployments in place, coupled with significant quantities of sensitive data in the cloud, we wanted to know how comfortable mature organizations feel with their cloud security design, architecture, and operations. Just over 50% felt that their cloud security controls and architecture were "fairly mature," meaning the organization has been building cloud security architecture for some time, and they have implemented some automation and more advanced controls and processes. Just under 29% feel that cloud security is somewhat immature, where the organization knows some basics about cloud security but feels they're behind the curve and have catching up to do. Just under 7% feel highly immature, and another 14% feel highly mature in cloud security. See Figure 5.

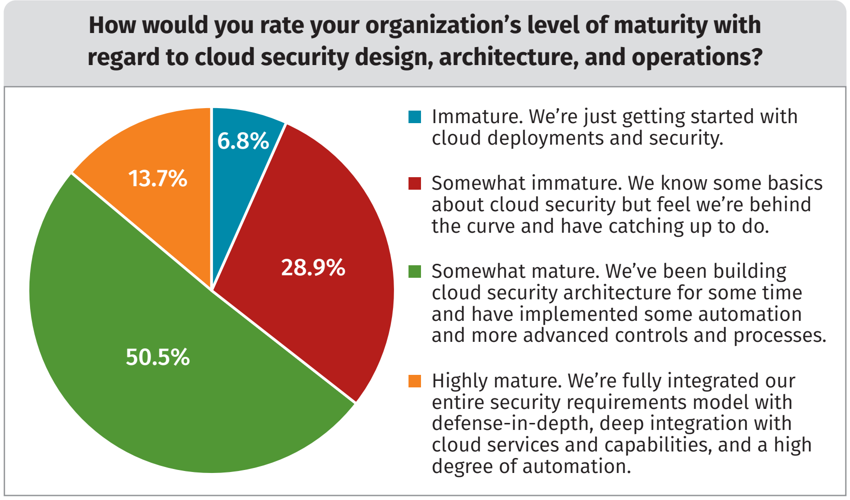
How would you rate your organization's level of maturity with regard to cloud security design, architecture, and operations?

Figure 5. Cloud Security Maturity Levels

These results definitely resonate with what we are seeing as trends in 2023. More organizations are becoming comfortable with cloud security controls and concepts, and information security professionals are learning how to design and build secure cloud infrastructure in most major cloud environments.

Perception Versus Realized

We asked security professionals about their biggest concerns related to the public cloud for business apps, as well as which of those concerns had actually been realized in the previous year. See Table 1 for the full breakdown of those concerns.

Table 1. Concerns and Incidents in Cloud Today

	Perceived	Rank	Realized	Rank
Inability to audit	44.4%	13	37.8%	1
Lack of skills or training within the organization for specific public cloud services	41.7%	15	36.7%	2
Inability to respond to incidents traversing our cloud apps and data	51.1%	3	34.4%	3
Poorly configured or insecure interfaces or APIs	53.9%	2	33.9%	4
Unauthorized access to sensitive data from other cloud tenants	46.1%	9	31.7%	5
Misuse by insiders/breach of sensitive data by cloud provider personnel	48.3%	8	30.6%	6
Unauthorized (rogue) application components or compute instances	58.9%	1	29.4%	7
Unauthorized access by outsiders	49.4%	6	29.4%	8
Lack of visibility into what data is being processed in the public cloud and where	51.1%	4	28.3%	9
Poor configuration and security of quickly spun-up application components (such as containers or serverless workloads, for example)	48.3%	7	27.2%	10
Poor data hygiene or the inability to delete data from the environment	45.6%	11	27.2%	11
Not knowing with certainty where sensitive data is geographically located	50.0%	5	26.7%	12
Inability to meet compliance requirements	42.2%	14	26.1%	13
Inability of cloud provider to meet service levels agreements (SLAs)	44.4%	12	24.4%	14
Downtime or unavailability of cloud services when needed	45.6%	10	21.7%	15
Other	7.2%	16	12.2%	16

This survey found a fairly significant disconnect between perception and realization of concerns. The top two significant concerns among respondents were 1) unauthorized (rogue) application components or compute instances (59%) and 2) poorly configured or insecure APIs and interfaces (54%). The top two concerns realized were 1) inability to audit (38%) and 2) a lack of skills and/or training for public cloud services (37%).

It's not surprising that most organizations feel the biggest realized issues are basic, tactical ones—inability to audit, lack of skills, and issues responding to incidents have consistently come up in numerous cloud security surveys at SANS over the past 10 years. What is potentially more interesting are the unrealized issues—the lingering concerns that haven't necessarily happened yet. Unauthorized components and workloads tops the list, followed by lack of API security and overall lack of visibility and sensitive data tracking. This should not be a shock to security teams, as most organizations are grappling with visibility in the cloud overall, and also a lack of skills and insight into APIs and data tracking. (Most cloud providers have minimal data tagging and tracking capabilities today.) Much of the concern is likely kindled by regulatory or legal requirements: "How will we meet GDPR if we can't track data and don't really know what's going on in the cloud?"

It's worth noting that more than half of respondents (51.1%) are concerned about access to sensitive data, either via cloud provider personnel or insider threats. This concern demonstrates that there is still some overall worry about shared responsibility and transparency with cloud providers, some uncertainty about what is in the cloud, and who has access to the data there.

It's clear that organizations are moving workloads to the cloud and building new applications and infrastructure there as well. It's becoming common for organizations of all types to leverage multiple cloud service providers, and this is leading to gaps in cloud security skills as well as challenges related to visibility, incident response, and audit. With the growing proliferation in cloud deployments, organizations are also becoming more concerned with rogue assets, APIs that may be exposed or vulnerable, and misconfiguration in cloud workloads and other deployments.

Cloud Network Security

Based on responses, roughly 68% of organizations have a dedicated cloud network security strategy in place today. For most enterprises, the NGFW has been a staple of on-premises network security for well over 10 years.

Many organizations have shifted into cloud deployments by bringing NGFW platforms into cloud architecture designs as well (42%). More than 35% of organizations responding stated that they plan to implement NGFW platforms in the cloud, and 23% indicated that they did not intend to install/leverage NGFW in their cloud environments. For many organizations starting out with a "lift and shift" mentality on cloud or using virtual and software-defined servers and infrastructure, building NGFW platforms in the cloud makes the most sense, as network and security teams already know the kinds of traffic control, access control models, and intrusion detection and prevention strategies needed to protect assets (while simultaneously employing well-known centralized management tools for administration).

In fact, 81% of respondents who deployed the NGFW platforms into the cloud stated that they had a centralized way to manage controls across all deployed firewalls, with only 11% stating that they did not and another 8% remaining unsure. These results are not surprising because most IT operations and security teams are struggling to maintain operational continuity in hybrid deployments, while minimizing operational overhead that may arise from deploying entirely new controls and security platforms that teams aren't familiar with.

We decided to delve deeper into the types of centralized management in place for cloud network security controls. Most respondents indicated that they were relying on NGFW provider management utilities and services running in the cloud (69%) and/or on premises (56%). This makes sense because most enterprise teams are already familiar with these tools and would likely want to maintain centralized operations for on-premises and cloud assets. Forty-one percent are also using cloud-native services and controls, which also lines up with what SANS sees in the industry. See Figure 6.

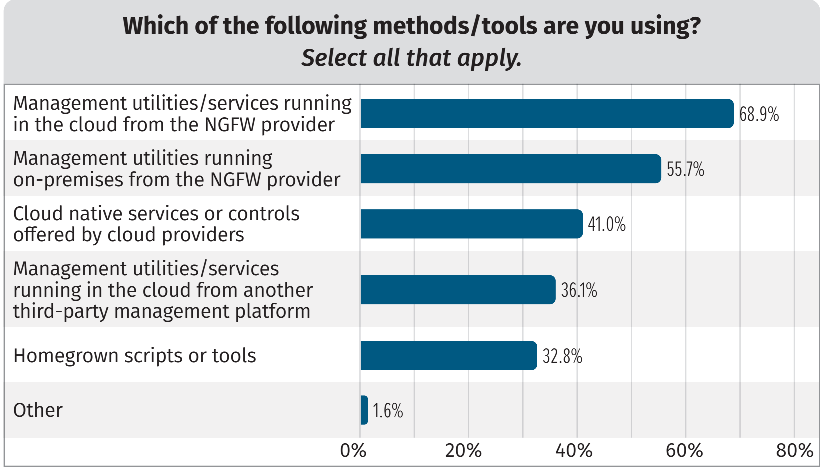

Figure 6. Cloud Network Security Management Tools in Use

Many enterprises have adopted a hybrid network security strategy that employs both cloud provider and NGFW solutions and controls. In fact, almost 68% of respondents stated that they were currently using or planning to use cloud-native network security controls offered by cloud providers, with just under 8% stating that they weren't. Another 25% weren't sure, likely because their cloud strategy is still being developed or evolving. A smaller percentage of organizations is using a different platform from third parties or homegrown scripts and tools for management.

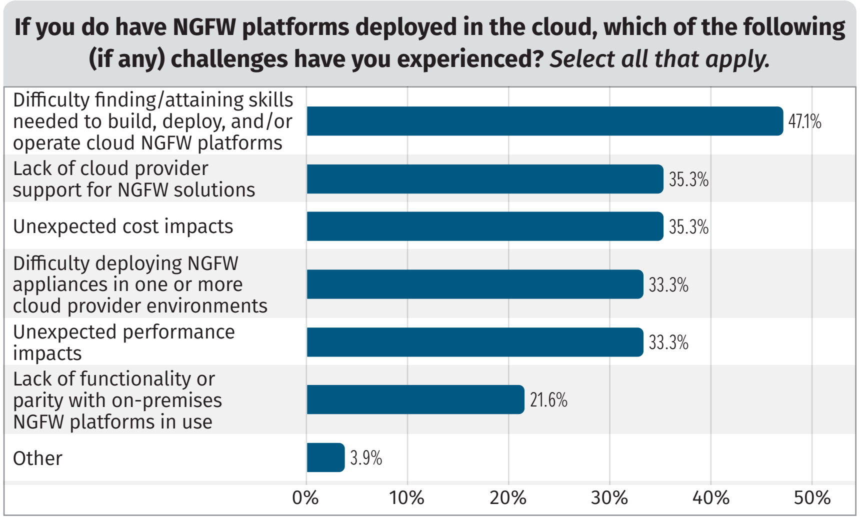

Figure 7. Challenges with Cloud NGFW Deployments

Organizations deploying NGFW technology in the cloud do experience some challenges along the way. The top issue cited, consistent with SANS research related to cloud security, is finding and retaining the skills needed to create, deploy, and manage a cloud NGFW platform or service (47%). Thirty-five percent of respondents also indicated that they'd experienced unexpected costs and had issues with cloud provider support for their NGFW platform of choice. Other issues cited included challenges with implementation, performance impacts, and lack of parity with on-premises NGFW solutions, as well (see Figure 7.

In addition to NGFW platforms, many organizations are building robust, multilayered network security strategies for cloud deployments. In addition to NGFWs (which top the list at just under 62%), the most prevalent technologies in use by many organizations include web application firewalls (WAFs), network intrusion detection and prevention, and VPN, followed by various forms of network access controls.

This network security stack closely mimics many on-premises network security models, and mature technologies are readily available for every one of these controls. Network-based DLP, flow log collection and behavioral monitoring, and network detection and response (NDR) are also becoming more common. Full-packet capture technologies have been notoriously difficult to deploy in the cloud, so it's not surprising that roughly 20% of respondents have this in place. Software-defined perimeter (SDP) technologies are clearly growing for some cloud deployment use cases (and likely will grow more in the next several years). The full list of network security technologies in use is shown in Figure 8.

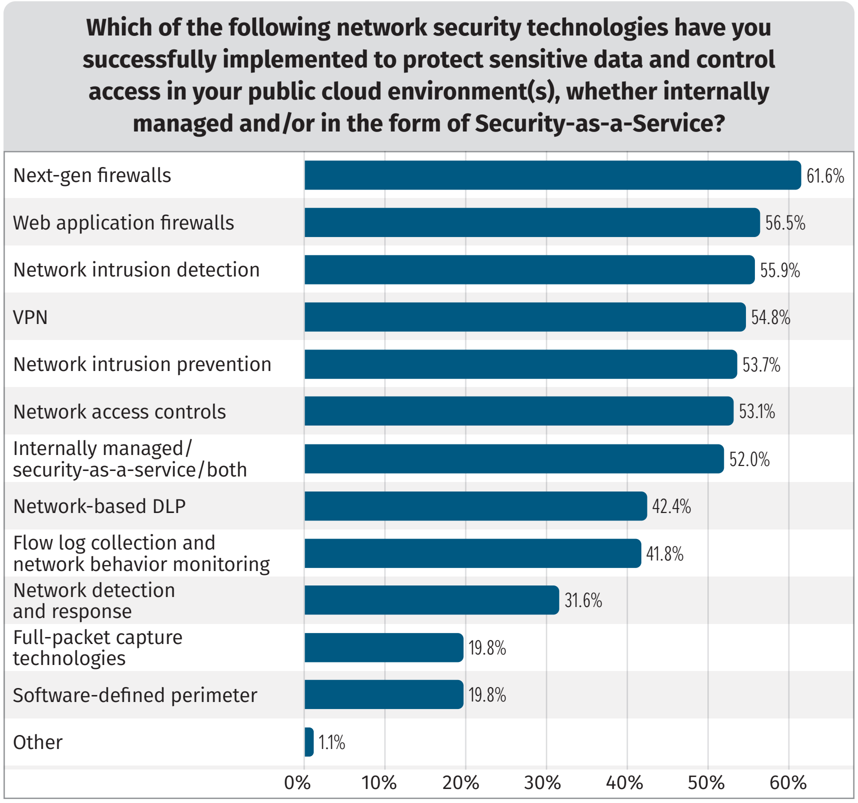

Figure 8. Other Network Security Controls Used in the Cloud

Given that many respondents indicated that they intended to use at least some cloud-native network security controls offered by providers, we asked which controls topped the list. The most popular service among respondents is DDoS detection and prevention (66%). DDoS protection tools and services are notoriously difficult to deploy and manage, and often expensive as well, so it makes sense that many organizations would utilize native offerings within the cloud service environment. More advanced cloud firewall services offered by providers are also popular, along with foundational network access controls such as security groups and network ACLs (both over 60%). Cloud native WAF solutions, network flow log collection, and packet capture rounded out the list (see Figure 9).

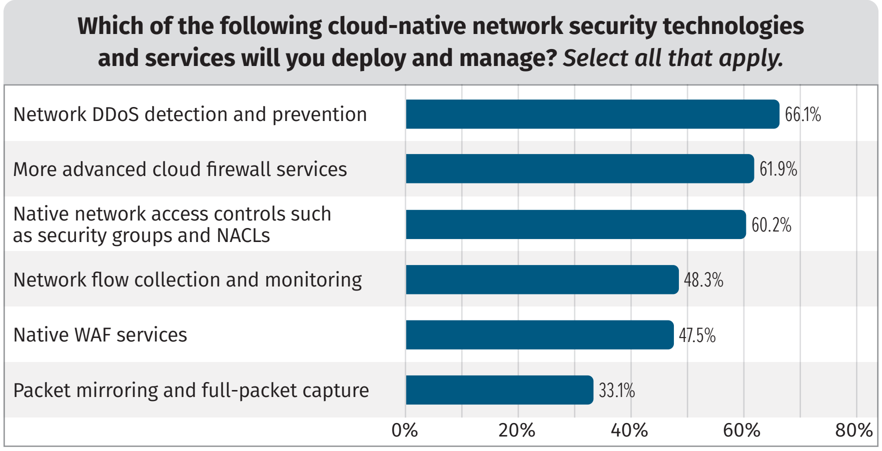
Which of the following cloud-native network security technologies and services will you deploy and manage? *Select all that apply.*

Figure 9. Cloud Native Network Security In Use or Planned

One of the primary drivers for network and security teams in deploying network security controls in the cloud is leveraging cloud provider APIs to improve automation and orchestration, as 60% of respondents indicated. Twenty-three percent stated that APIs weren't currently in use, and another 17% weren't sure.

For those currently using cloud provider APIs in their cloud network security deployments, most (65%) noted integration with other security technologies such as EDR and vulnerability assessments was a leading concern. Network flow log collection and analysis is also a top use case (56%) as is network security event generation and forwarding (53%). Some organizations are leveraging APIs for network segmentation and isolation as well as NGFW management and monitoring. Again, given some of the challenges in capturing packets noted earlier, full packet capture was lower on the list. See Figure 10.

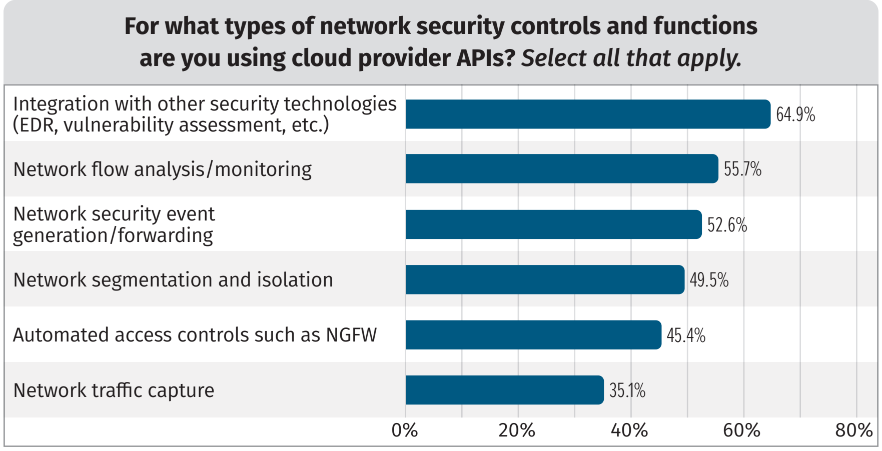
For what types of network security controls and functions are you using cloud provider APIs? *Select all that apply.*

Figure 10. Network Security API Use Cases

Most organizations have a relatively established cloud network security strategy, with most deployments including NGFW solutions and services, primarily managed through centralized tools from the NGFW provider (both in the cloud and on premises). Sadly, this is another area where many security and networking teams are short on skills to properly deploy these technologies in the cloud. In addition to NGFW capabilities, many more teams are capably using WAF, network intrusion detection and prevention, VPN, and network access controls. Also growing is the use of cloud-native network security services, with DDoS protection topping the list, and the use of cloud provider APIs to integrate with EDR, vulnerability management, and other tools.

Teams and Governance: Managing Network Security Solutions in the Cloud

One of the classic balancing acts within IT involves firewall management and administration. Some organizations leave firewall management to the network operations and engineering team while others see this as the responsibility of the security operations and engineering teams. Increasingly, there's some level of involvement from both teams, and this was demonstrated when we asked respondents to indicate who manages internal NGFW platforms today—58%indicated that the network team is involved, while 53% indicated the security team may have some responsibilities here. This balance between networking and security is likely to continue in the future, both for on-premises and cloud deployments. With the advent of cloud, however, we also noted that 32% of respondents have dedicated cloud engineering and security teams involved in NGFW deployment and management. Just under 24% of respondents have dedicated network security teams that would manage NGFWs.

Because cloud deployments require network and security teams to integrate and collaborate with cloud engineering and DevOps teams, we asked organizations whether a clear governance model was in place for definition and oversight of network security in the cloud, with agreed-upon responsibilities in all areas. More than forty percent (43%) of respondents indicated that clear ownership and delineation of responsibility existed, and 18% stated that these were the same team in their organizations. However, 35% indicated that there was little to no role definition and oversight (8%) or that the strategy was currently being developed (27%). Only a small number of respondents were unsure.

In line with this topic, we also asked what types of collaboration and working relationships the network/security and cloud teams had. Most respondents indicated some regular cadence of collaboration, either through regular meetings (26%) or deep, consistent integration across the teams (21%). Unfortunately, roughly one-third of respondents stated that there was little to no interaction or only ad hoc coordination, as shown in Figure 11.

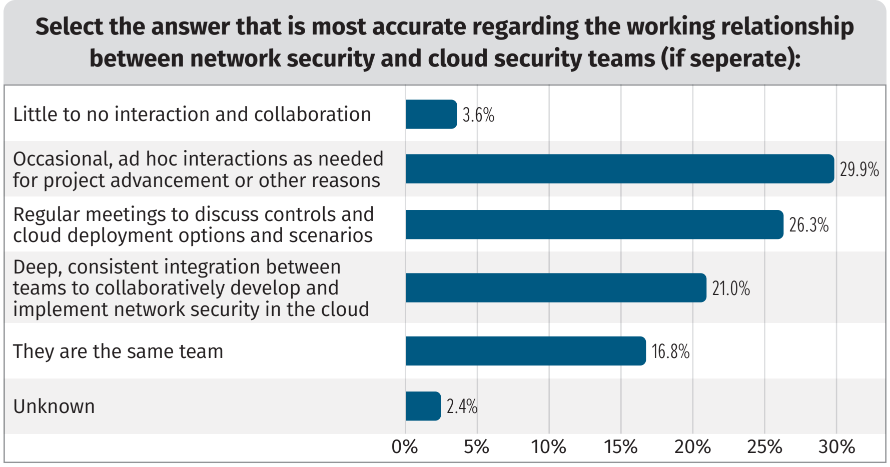

Figure 11. Network/Security and Cloud Team Collaboration

Based on the challenges noted previously about cloud skills for network security (and cloud deployments in general), we asked respondents to tell us about the maturity level of their network engineering/operations and security engineering/operations teams using the following scale:

- **Immature:** Little to no cloud experience and knowledge exists.
- **Limited:** Some exposure to cloud services and tooling has occurred, but skills are still lacking.
- **Comfortable:** The team has invested in training and test environments and understands the core capabilities and services within the cloud.
- **Highly capable:** The team is very cloud-savvy, and can readily design and implement all network platforms, services, and controls in the cloud today.

Based on the responses, most organizations feel that both network and security teams are somewhat limited or reasonably comfortable with cloud security controls and deployment architecture, as shown in Table 2.

Table 2. Network and Security Cloud Skills Maturity

Maturity Level	Network Engineering/ Operations	Security Engineering/ Operations
Immature	4.2%	4.3%
Limited	49.7%	45.1%
Comfortable	30.9%	34.8%
Highly capable	15.2%	15.9%

These responses echo what SANS sees in the community today. While there are still some enterprises just starting in cloud, with a low level of maturity, most have begun working on learning how cloud environments operate, the nuances of deploying solutions within a large PaaS or IaaS cloud, and how to manage security controls and services in cloud infrastructure.

Given that cloud network security touches so many facets of deployments, it's not surprising that both security and networking teams are often involved in developing and implementing network security policies and access controls in the cloud. Although most organizations have clear roles and responsibilities outlined for cloud network security (across security, networking, and DevOps/cloud engineering), many others are still developing their overall governance model. Most teams are becoming more comfortable with cloud network security controls and capabilities, but there is still significant room for growth and maturation.

Conclusion

We concluded the survey by asking participants to provide general feedback on any other trends, concepts, experiences, and issues they've seen in the cloud and network security today, as well as how their organizations were restructuring to meet the needs of the organization with a move to the cloud. Many respondents mentioned the need for better automation capabilities to keep pace with the rapidly changing services offered, as well as better centralized tools and services that can be used across more types of cloud service environments. Especially as we shift toward multi-cloud deployments and cloud environments that are geographically dispersed, more network security services in the cloud will become paramount, which was also noted by several respondents. Many network security teams aren't well-versed in cloud concepts, both in design and operations as well as DevOps/automation tools and tactics. There's a broad mix of approaches to cloud skills and responsibilities too. Some teams are expanding to cover new cloud design and oversight roles, while others are struggling with these "added" responsibilities on existing staff and teams. A general theme we heard from respondents overall, though, was "we are rapidly moving to the cloud no matter what."

Things are improving in cloud network security, both in knowledge level of the managing teams and the tools and services from both providers and vendors in the space. Overall, however, there's a lot of room to grow and mature.

Sponsor

SANS would like to thank this paper's sponsor:

paloalto®
NETWORKS