SANS Institute
Information Security Reading Room

A SANS Survey: Network Security in the Cloud

Dave Shackleford

Copyright SANS Institute 2021. Author Retains Full Rights.

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

https://t.me/learningnets

SANS

Analyst Program

Survey

A SANS Survey: Network Security in the Cloud

Written by **Dave Shackleford**

June 2021

VECTRA®

©2021 SANS™ Institute

https://t.me/learningnets

Executive Summary

Since 2019, our industry has seen a wide range of vulnerabilities in cloud assets, as well as sensitive data disclosure incidents and breaches involving the use of public cloud environments. Some notable examples include:

- In December 2019, Microsoft reported that it had inadvertently exposed a large database of customer support records within Azure, blaming the exposure on "misconfigured security rules" (likely Network Security Group rules or perhaps an identity policy).[1]
- Several Microsoft outages between 2019 and 2020 were significant. The first was an Azure database outage in 2019, caused by DNS configuration changes and some automation scripts failures. And in 2020, numerous Office 365 outages caused many organizations to experience downtime and an inability to access their cloud applications and data.
- In April 2021, cloud and hosting provider DigitalOcean disclosed a breach of customer billing data, without providing any insight into the vulnerability that allowed it to happen.[2]

Additionally, in its 2021 Data Breach Investigations Report (DBIR), Verizon noted that the past year saw external cloud assets involved in more incidents and breaches for the first time.[3]

Despite these types of security issues, more organizations than ever are moving workloads to the cloud, building applications in the cloud, and subscribing to a wide range of SaaS and other cloud services.

This survey, which builds on the SANS 2021 Cloud Security Survey,[4] places an emphasis on how cloud security has changed the enterprise infrastructure in response to the COVID-19 pandemic and an increasingly remote workforce. The key questions we wanted to address included:

- Is the cloud now considered part of the enterprise network?
- How are organizations using network traffic/metadata for detection and response?
- Are organizations now thinking cloud is an integral part of their network? And how has that changed their approach to infrastructure security?

We garnered a significant response across a wide variety of industries and organizations. The top verticals represented include technology firms, banking and finance, cybersecurity, government, education, and healthcare. Survey respondents represented a wide range of workforce sizes as well: Almost 29% have between 1 and 500 employees, roughly 37% have between 500 and 10,000 employees, and the remainder range in size from slightly

---

[1] "Microsoft discloses security breach of customer support database," www.zdnet.com/article/microsoft-discloses-security-breach-of-customer-support-database

[2] "DigitalOcean says customer billing data accessed in data breach," https://techcrunch.com/2021/04/28/digitalocean-customer-billing-data-breach

[3] "2021 Data Breach Investigations Report (DBIR)," www.verizon.com/business/en-sg/resources/reports/dbir

[4] "SANS 2021 Cloud Security Survey," April 2021, www.sans.org/reading-room/whitepapers/awareness/paper/40225

https://t.me/learningnets

more than 10,000 to more than 100,000 employees. More than 50% of respondents hold job titles in information security (e.g., analyst, manager, and architect), while a number of others work in IT operations, executive roles (CIO/CISO), and network engineering. All major geographic regions were represented, with a majority of organizations having a presence in the U.S., Europe, Asia, and Canada. Most organizations have their headquarters in the U.S. (61%) and Europe (19%). See Figure 1.

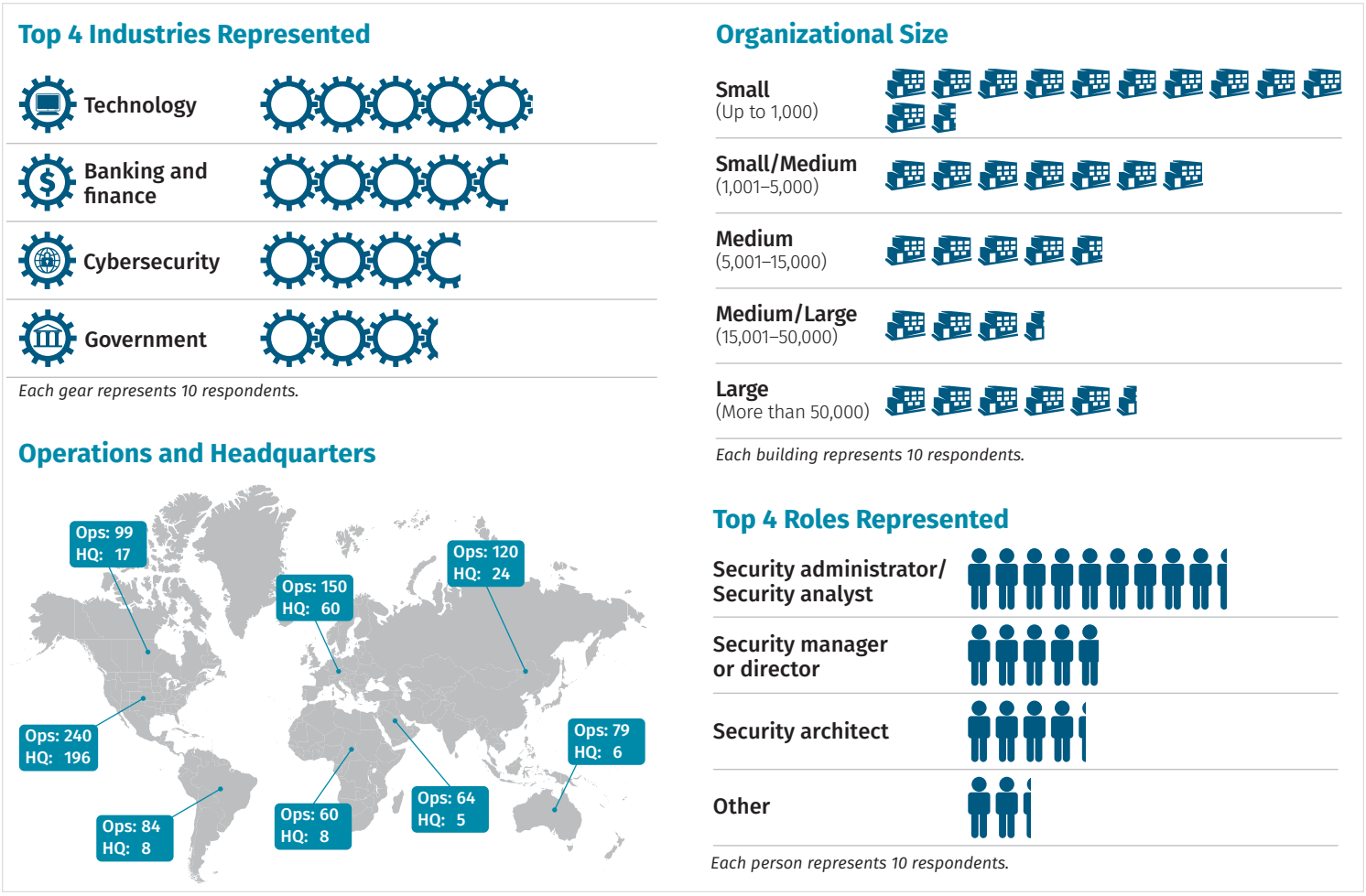

Figure 1. Demographics of Survey Respondents

Here are several highlights of the survey based on feedback from survey participants:

- From 2020 to 2021, the biggest areas of cloud growth came from increased use of workforce and collaboration SaaS services.
- More than 16% of respondents experienced a breach in cloud environments. The top attack vectors seen in these breaches include configuration weakness, credential and account abuse, and shadow IT.
- Sixty-seven percent of organizations consider SaaS, PaaS, and IaaS cloud delivery platforms part of their network scope.
- The top network security controls being used in public cloud environments are web application firewalls (WAFs), network access controls, and network intrusion detection and prevention.

https://t.me/learningnets

Cloud Computing Characteristics

In the past several years, we've observed a significant shift toward more remote workforces, where employees might spend time in the office environment infrequently or not at all. Because traditional on-premises virtual private network (VPN) solutions can be expensive, unwieldy, and difficult to operate and maintain, organizations faced with the prospect of moving their entire company to remote work are considering other options—but all remote access solutions require some degree of investment, both financial and operational. To get a better understanding of how organizations are responding to this challenge, we asked survey participants about the use of cloud services related to the COVID-19 pandemic. Many organizations have prioritized cloud service implementation to facilitate remote work. Fully two-thirds (66%) of respondents stated that COVID-19 brought increased use of cloud services, while 22% said it had not. Another 12% weren't sure.

For those respondents who indicated an increase in their use of cloud services, especially with more remote users, we asked them to identify the types of cloud services they were using already, those they began using with increased frequency, and those they started using for the first time. See Figure 2.

Which of the following cloud services were you already using prior to the WHO declaration of the COVID-19 pandemic on March 11, 2020? Which of these services saw a significant increase in use, with the shift to remote work after this date? Which services did you start using for the first time?
Note: Use March 11 as a benchmark, if needed.

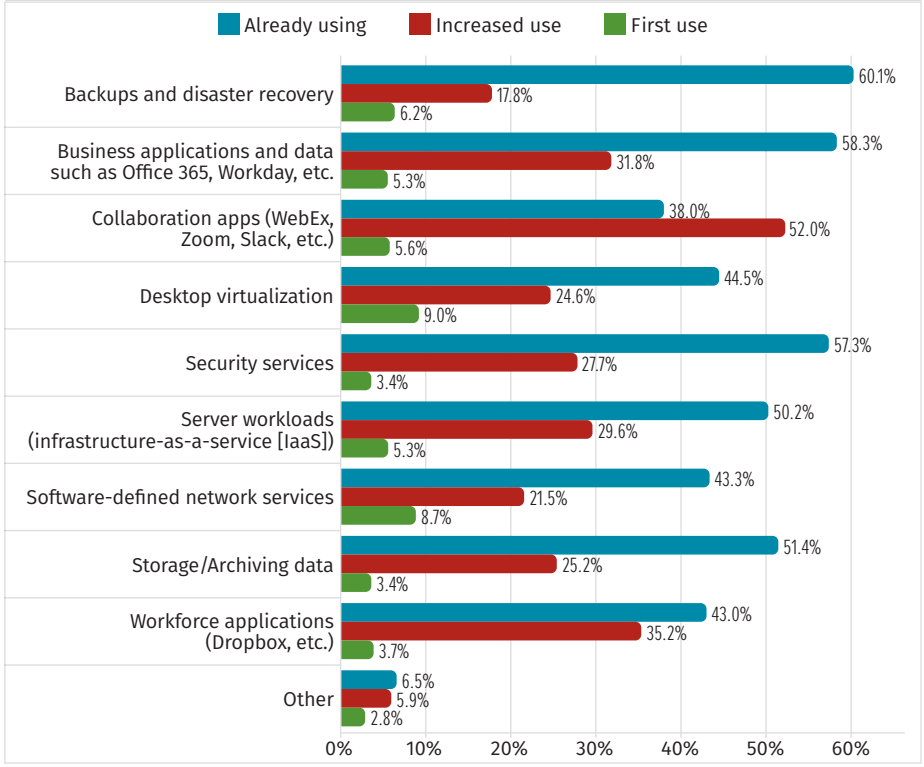

Figure 2. Cloud Service Changes Due to COVID

A significant number of organizations were already using cloud backups, business applications such as Microsoft Office 365, and security services when the COVID-19 pandemic was declared in March 2020. And as these organizations shifted to remote work arrangements, we saw a significant increase in the use of collaboration services such as Zoom and Slack (52%), as well as workforce applications such as Dropbox and other data sharing applications (35%). This makes a lot of sense, because those types of services immediately take the place of in-person meetings and interactions that are now entirely virtual. What is also interesting are the top cloud services being used for the first time, namely desktop virtualization (9%) and software-defined network services (9%). Networking and end-user computing are core operations functions, and these began shifting to the cloud as well—a trend that's likely to continue.

https://t.me/learningnets

How Cloud Security Has Changed with Remote Work

Given that a substantial portion of the workforce is now remote and using more cloud services, it stands to reason that attackers would begin shifting their focus toward remote users and the associated cloud services those users rely on. As we expected, respondents cited a wide range of threats and security issues becoming more pronounced. The top issue is a lack of visibility into what data is being processed in the cloud and where (roughly 50% of responses). Configuration vulnerabilities and lack of security controls for rapidly spun-up applications (41%) and interfaces/APIs (34%) were major concerns as well. Uncertainty about the geographic location of data was another big concern (35%)—and with the possibility of hefty fines under well-known privacy regulations, such as GDPR, this concern is no surprise. Organizations also continued to worry about unauthorized applications and systems, as well as unauthorized access and insider abuse. Figure 3 shows the breakdown of what organizations are growing increasingly concerned about given the onset of a remote, cloud-enabled workforce.

Which of the following security threats or issues have become MORE pronounced as your organization has moved to a remote workforce? *Select all that apply.*

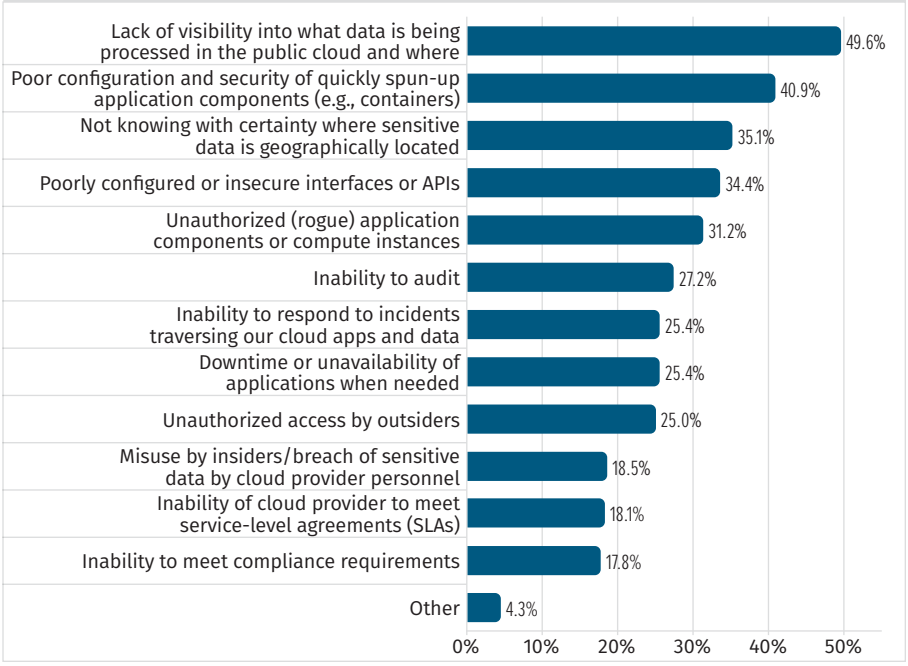

Figure 3. Growth in Security Concerns

Based on experience and industry trends that SANS has observed, lack of visibility into cloud environments and poor cloud configuration settings and controls are exceedingly common issues in many organizations, and these same issues increased with the shift to a more remote workforce.

For those organizations that experienced an attack, what was involved in the attack aligns with these top threats and issues. Misconfiguration of cloud services and assets topped the list at 36% (and insecure or misconfigured APIs wasn't far behind at 27%). Account hijacking came in second at 34%, and shadow IT came in third with 32%. In SANS' opinion, these responses are very much in line with the most prevalent attacks seen in the wild today. There are numerous industry models that describe attack phases, and MITRE ATT&CK® is a mature attack life cycle that includes the following initial stages, now specifically updated to represent the cloud:

- **Initial Access—**Threat actors find an initial means of gaining access to an organization's assets and/or environment. Many of these access points are similar for both on-premises and cloud-focused events, with the exception that attempts to access applications might happen entirely in the cloud, or account hijacking might be cloud user and service accounts (instead of traditional internal accounts).

https://t.me/learningnets

- **Persistence—**This stage involves setting up backdoors and methods to retain access on the system or in the environment over time. With new cloud technologies and services, persistence may now include cloud account manipulation or implantation of containers in a PaaS deployment. Misconfigured systems and settings, as well as shadow resources in the cloud that aren't known to exist, can help attackers set up persistence mechanisms.
- **Privilege Escalation—**Bad actors often use DLL injection and privileged account access to elevate privileges on local systems and gain more thorough control. For the cloud, privilege escalation is usually tied to unauthorized access to and use of cloud accounts and privileges. Twenty-four percent of respondents indicated that privileged user accounts were abused during a breach, which shows that many attackers are successful at gaining access to these credentials.

In later stages of the attack chain, attackers look for new systems to target and credentials that they can leverage to move laterally so they can then attempt to exfiltrate data. In the responses we saw, adversaries pivoted from cloud environments to internal systems in roughly 20% of the incidents reported and exfiltrated sensitive data from cloud applications in more than 19% of incidents. This also likely indicates that attackers are becoming savvier at exploiting and accessing cloud service environments (21% of incidents saw a direct exploit of cloud provider APIs or exposed vulnerabilities), and they are learning how to successfully chart attack paths within cloud ecosystems in a variety of ways. Figure 4 shows a breakdown of attack vectors respondents are seeing.

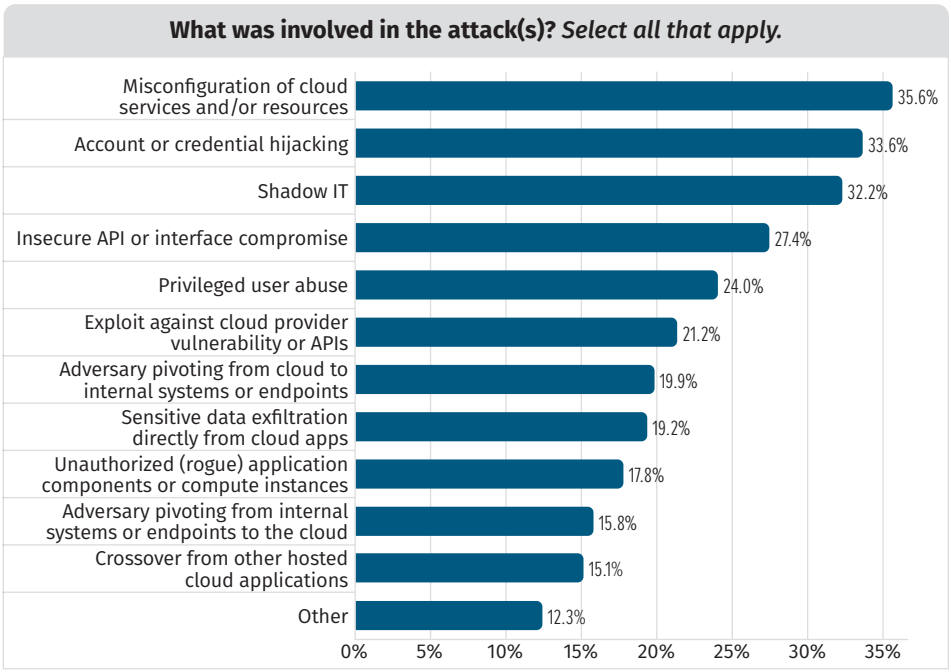

Figure 4. Attack Vectors Noted in Cloud Breaches

Did these attack vectors and issues actually lead to cloud breaches in the past 12 months? Fortunately, the answer for now seems to be "no"—63% of respondents said they are unaware of an actual breach. Further, 11% indicated they did not know, but 17% said they did experience a breach, while 10% said they believed they had but couldn't prove it. This could indicate that more than one-fourth of respondents likely experienced a breach, with another 11% potentially also having experienced a cloud security incident.

https://t.me/learningnets

Network Security in the Cloud

Increasingly, organizations are implementing hybrid connectivity models between traditional on-premises environments and software-defined cloud data centers. With 20% of the reported cloud incidents noting attackers pivoting from cloud environments to internal systems and applications, it stands to reason that more organizations are treating cloud provider environments as part of their networks. And that's exactly what respondents indicated: 67% of respondents indicated that they treat their cloud environments as extensions to their existing networks, 20% do not, and the remaining 12% are unsure.

With the incredible growth in all types of cloud services, it's no surprise that a broad variety of cloud service types and delivery models are included in the network today. About two-thirds (66%) consider software-as-a-service (SaaS) applications to be included in their network scope, while 64% consider both platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) environments (which are often the same provider, such as Amazon Web Services or Microsoft Azure) to be key. Many network and content brokering services are becoming more common as part of the network infrastructure as well, ranging from content delivery networks (CDNs) at 42% to SD-WAN services (34%) and multi-cloud brokers (27%), as shown in Figure 5.

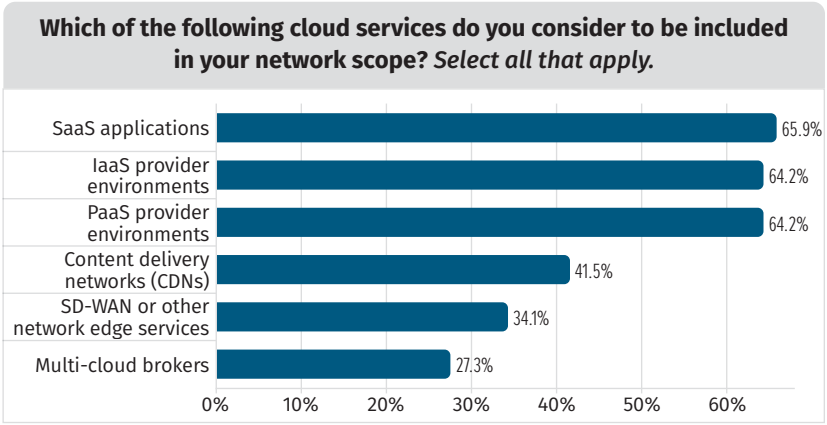

Figure 5. Cloud Environment Network Integration

Adapting network security to the cloud means, more than anything, making some concessions. You really cannot create a model identical to the one built in-house in a cloud environment, although you can develop largely the same types of controls (albeit in a different way).

The main things to consider include the following:

- **Not all vendor products are adapted for the cloud.** While many of the major providers have adapted their products into virtual machine formats that may be available in the cloud, not all have. This means that you may need a new load balancer, firewall, VPN gateway, or whatever other system you are trying to create in the cloud, as well as newer network security tools and services that are purpose-built for cloud traffic and events.
- **Not all product features and capabilities will be available.** Even if a product or service is offered in a cloud format, it may be somewhat limited by the cloud provider environment. Some APIs may not be capable of supporting all features in the cloud, so you should take the time to compare the systems you're used to with those you can get in the cloud.

https://t.me/learningnets

- **Performance is based on software attributes, not hardware.** Many network security platforms rely on specialized chips and hardware, which you won't have (obviously) in most cloud environments. You'll need to provide the appropriate amount of software/virtualized resources, which could get expensive to operate.
- **Some types of monitoring and control may be difficult or impossible without newer tools and services developed purposefully for cloud environments.** For example, east-west traffic control and monitoring are very difficult to do in many cloud environments using traditional tools.
- **You will need to make use of CSP tools and capabilities.** Most organizations will need to use at least some cloud-native access controls and other services, such as security groups, routing, and others.

We asked survey respondents what types of network security controls they had successfully implemented for their public cloud environments. Approximately 61% have successfully implemented WAFs. Respondents are also using network access controls (60%) and network IDS/IPS (58%). More than half (53%) have integrated VPN and/or SD-WAN services, a category in which we noted an increase in new implementations over the past year. Encouragingly, a good percentage of organizations also have implemented network-based anti-malware (49%), network traffic analysis tools (49%), and network data loss prevention (45%). Software-defined perimeter (SDP) technologies are still relatively new; only 22% are using them today. Other technologies included DDoS protection, cloud proxies, and various cloud network brokering solutions. See Figure 6.

Which of the following network security technologies have you successfully implemented to protect sensitive data and access in your public cloud environment(s), whether internally managed and/or in the form of security-as-a-service (SecaaS)? *Select all that apply.*

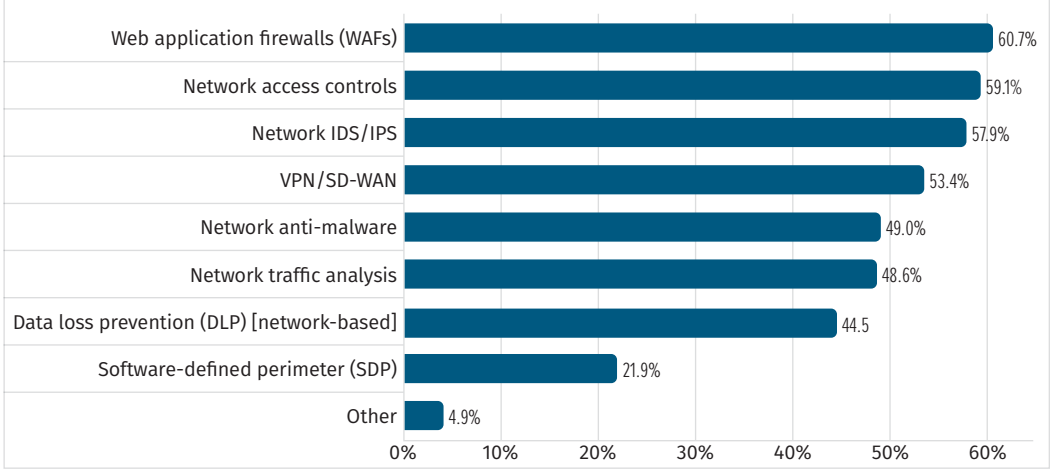

Figure 6. Cloud Network Security Technologies in Use

For many organizations, integrating network security technologies between in-house environments and cloud data centers can make sense for some controls. Benefits of this approach include parity in functionality, existing skill sets and knowledge for operations teams, and central and coordinated management and oversight. Large PaaS and IaaS cloud environments have supported virtual machine workloads for a variety of network technologies for some time (primarily through cloud provider marketplaces), and many network security providers can integrate through service accounts and APIs as well.

https://t.me/learningnets

Many organizations have adapted network firewall technologies to operate in cloud environments with the same providers, so network access controls usually top the list (62% have this in place currently), followed by network malware detection (58%), and then a third-place tie for WAFs and network IDS/IPS (57% each). In many cases, access controls, some malware detection, and IDS/IPS might be integrated into a single platform from leading next-generation firewall (NGFW) vendors. WAF solutions are usually standalone, but leading providers have adapted their solutions to major cloud service provider environments. VPN and SD-WAN solutions are relatively integrated, too (54%). Over the next 12 months, a number of enterprises are planning to implement integrated solutions such as network DLP (30%), SDP (25%), and network traffic analysis (22%) as well. See Figure 7.

Which of the following network security technologies have you been able to integrate between your in-house environment and public cloud? Which are you planning on integrating within the next 12 months? *Select only those that apply.*

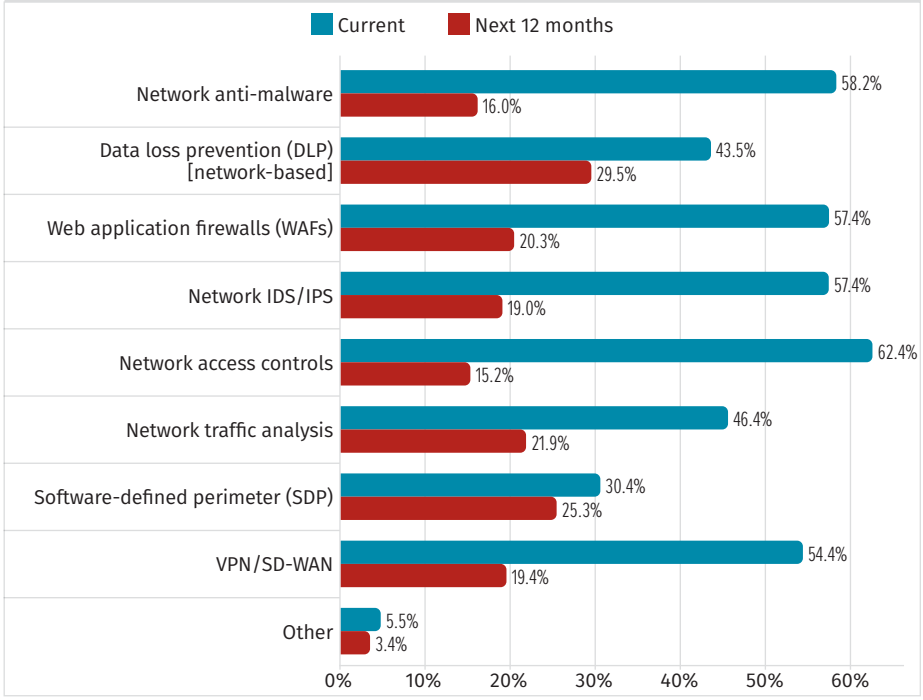

Figure 7. Network Security Technology Integration in Hybrid Environments

Another major consideration for network security in hybrid environments is the ability to unify network security controls integration with a single vendor or solution. Again, the top solutions organizations successfully implemented with a single vendor include WAFs (49%), network IDS/IPS and network malware protection (47% each), and network access controls (41%). This aligns with the previous question in many ways, showing that many solutions from a single provider can bridge both on-premises and public cloud environments in a number of categories. However, it should be noted that none of these control categories were successfully integrated in a single solution by 50% or more of the respondents, which shows there's quite a bit of room for growth and maturity here. Figure 8 shows the full breakdown.

Which of the following network security technologies have you successfully implemented with a single vendor product or control in both your in-house environment and public cloud? *Select only those that apply.*

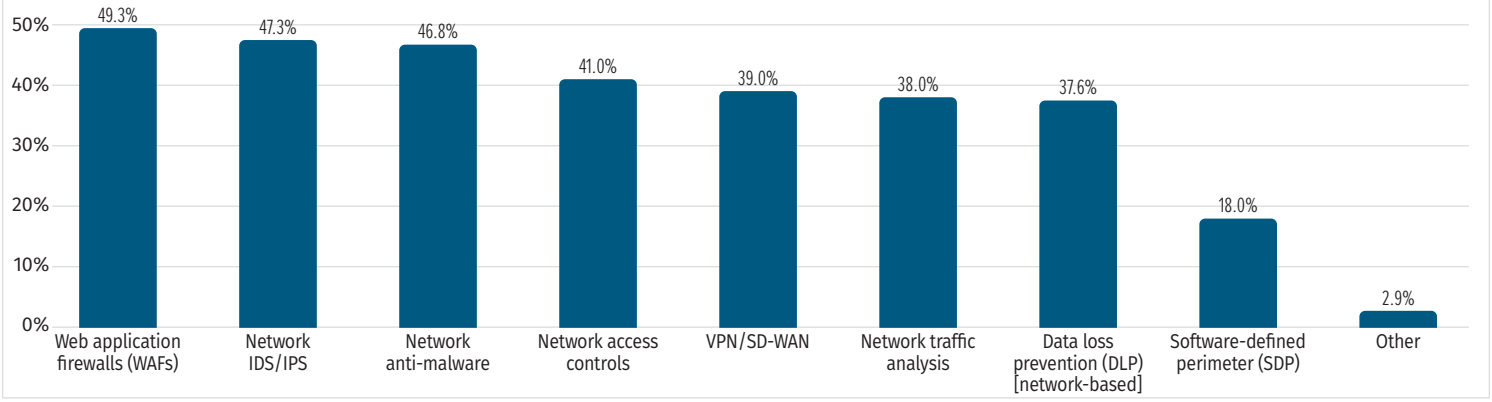

Figure 8. Single Vendor Integration for Network Security

https://t.me/learningnets

One significant area of emphasis for security teams in the past several years has been automation, and leading cloud providers commonly offer a variety of APIs that organizations can leverage to access and automate network security controls. Almost 60% of respondents stated that they're tapping into these APIs today, with 25% stating that they haven't done this yet and 17% indicating they are unsure.

For those respondents who currently are using cloud provider APIs to automate cloud security controls, we sought to understand how respondents are leveraging them for network security automation. Three major use cases emerged:

- **Monitoring—**Some APIs focus on tracking and monitoring network activity and traffic, and this is likely the most prevalent use case overall, particularly with network VPC and cloud log data (something readily available in all major IaaS cloud environments).
- **Data ingestion—**A variety of cloud provider APIs facilitate automated ingestion of network flow and related data, primarily for use with other network detection and analysis tools. This use case was mostly prevalent in network flow data ingestion for monitoring tools, network detection and response, and network analytics (all tools and controls that focus on network visibility and behavior analysis).
- **Network protection—**Additional APIs might allow for automated protection controls, such as automated network access controls blocking malicious or suspicious domains and IP addresses, to take effect. Primary focal areas for protection were centered around access controls and DDoS protection, along with WAF capabilities.

The largest number of responses for monitoring use cases focused on network flow data and behavioral monitoring (67%, or roughly two-thirds of responses), followed by network access control monitoring (50%), WAF traffic processing (47%), and then network detection and response (NDR) at 46%. Network flow monitoring was also a top API scenario for data ingestion (37%), followed once again by NDR and WAFs. In the realm of protection, however, network access controls and DDoS protection were the top use cases for APIs (48% each), followed closely by WAFs (46%). The full breakdown of API usage is shown in Figure 9.

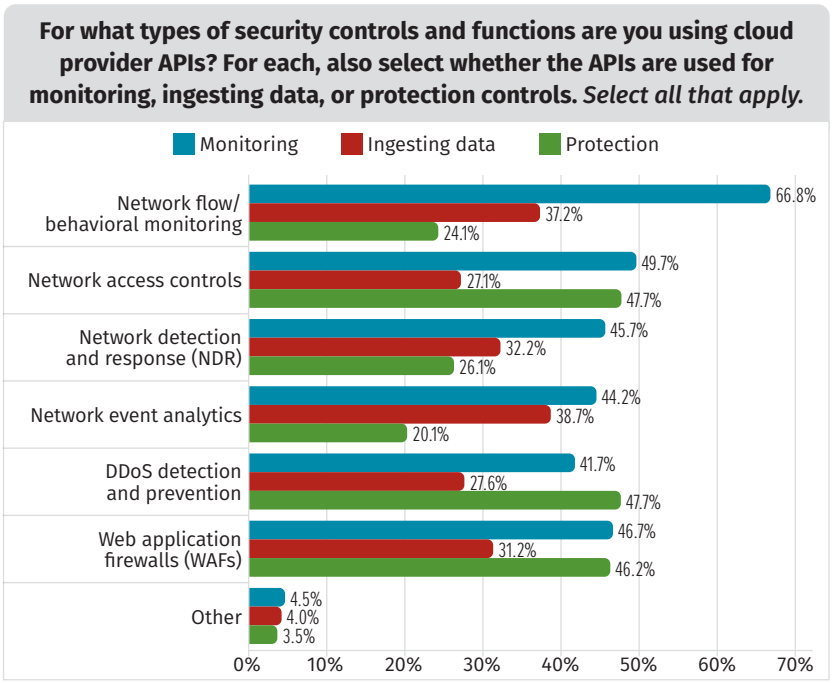

Figure 9. Use of Cloud APIs for Automating Network Security Functions

The final area we focused on for cloud network security was the use of cloud network metadata. Metadata ("data about data") is plentiful in the cloud, and half of respondents stated that they are actively using network metadata to prevent, detect, or respond to threats in the public cloud. Another 30% are not using network metadata, and the remaining 20% are unsure.

https://t.me/learningnets

For those using network metadata, most are collecting and using traditional Layer 2–Layer 4 network flow data (81%), 75% are using application-layer metadata, and 60% are using custom metadata from cloud provider interfaces, objects, and assets. (See Figure 10.)

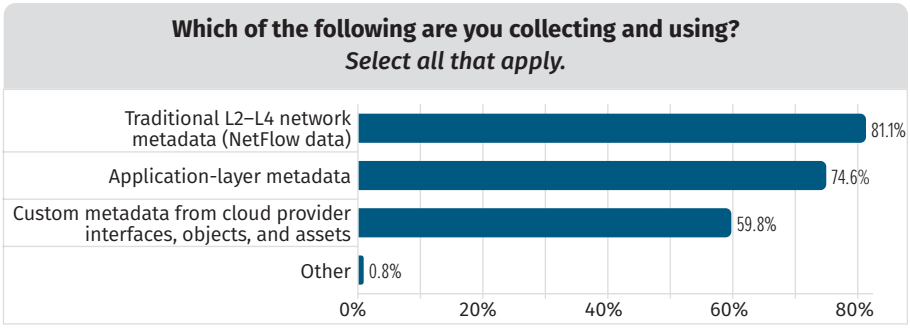

Figure 10. Network Metadata Collection

As more organizations ingest network information via APIs, the number of organizations collecting and using network metadata in the cloud will increase as well. What data is presented via cloud provider APIs is rarely customizable or even flexible, and network metadata is likely the best (and perhaps only) source of consistent API-based information about network activity available in many cloud environments.

For those organizations collecting and using metadata successfully, we asked respondents how they are able to use this information in their own environments. Close to 70% indicated that they could now identify specific network indicators of compromise (IoCs) in the cloud, and 64% stated that they could identify command and control (C2) traffic, as well as rogue/unsanctioned assets and services in cloud environments. Although not as confident, more than half (59%) still believed that metadata helped them identify more advanced tactics, techniques, and procedures (TTPs) and suspicious/malicious patterns in cloud network traffic. See Figure 11.

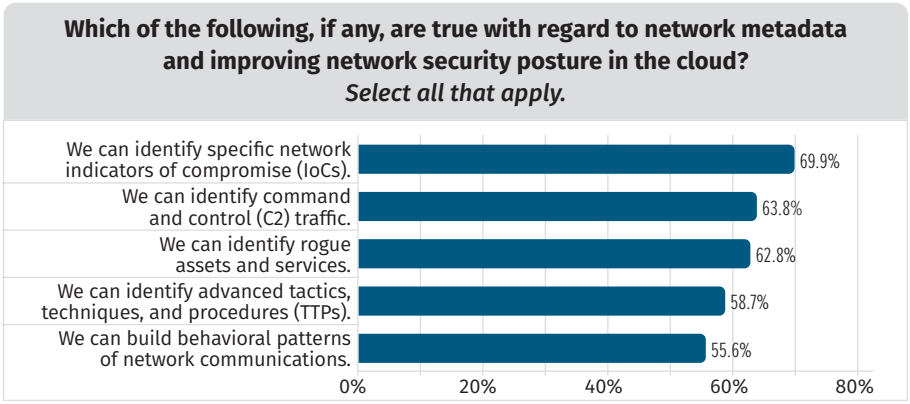

Figure 11. Cloud Network Metadata Security Benefits and Capabilities

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 today. Many respondents mentioned the need for better APIs and automation capabilities to keep pace with the rapidly changing network services in large cloud environments, as well as better centralized tools and services that can be used across more types of cloud service environments. Many security teams noted that network monitoring in the cloud differs significantly from traditional on-premises monitoring, often due to lack of integration and traffic access offered by the providers themselves. There's still the perception that teams aren't getting many needed details about security controls and capabilities from the providers as well.

Overall, we seem to be improving the state of cloud security, albeit slowly. Cloud providers are becoming more open to and accommodating of security data and controls, and more third-party solutions can bridge the gap between on premises and cloud. There's progress and more acceptance of in-cloud network controls and services—but there's room to grow.

https://t.me/learningnets

About the Author

Dave Shackleford, a SANS analyst, senior instructor, course author, GIAC technical director and member of the board of directors for the SANS Technology Institute, is the founder and principal consultant with Voodoo Security. He has consulted with hundreds of organizations in the areas of security, regulatory compliance, and network architecture and engineering. A VMware vExpert, Dave has extensive experience designing and configuring secure virtualized infrastructures. He previously worked as chief security officer for Configuresoft and CTO for the Center for Internet Security. Dave currently helps lead the Atlanta chapter of the Cloud Security Alliance.

Sponsor

SANS would like to thank this paper's sponsor:

VECTRA®

https://t.me/learningnets