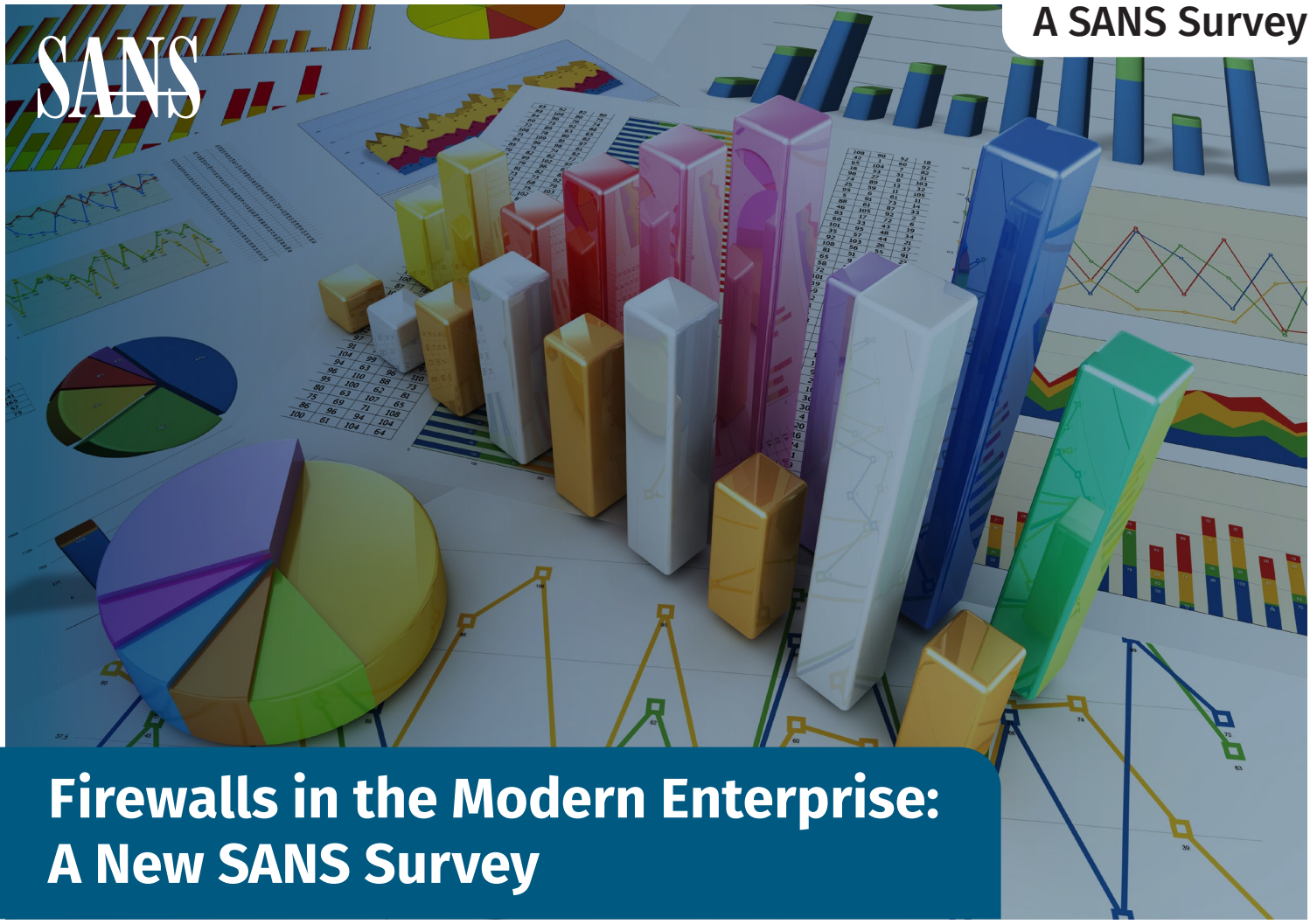
Firewalls in the Modern Enterprise: A New SANS Survey

Matt Bromiley

A SANS Survey



Firewalls in the Modern Enterprise: A New SANS Survey

Written by **Matt Bromiley**

September 2020

Sponsored by:

Palo Alto Networks

Analyst Program

Executive Summary

Each year, it feels as if defending an enterprise network gets more and more complicated. Business entities demand new technologies and capabilities while their users move toward new hardware and software requirements. Looking at most network diagrams, the concept of a local network appears to be stretched further every day. As we continue to see aggressive changes in network infrastructure, we must pause and ask: **Is the security of these networks keeping up with their development?**

In this inaugural survey, we set out to understand how organizations manage network security in these mixed deployments, including on-premises and cloud assets, with complex network structures, such as SD-WAN and global operations. We began by speculating about what the modern enterprise really looks like. For example:

- How many organizations have mixed environments?
- How many organizations are moving to the cloud and away from their traditional hardware models?
- How many are dealing with technologies, such as microservices and/or containerization, that can complicate typical security approaches?

After understanding the makeup of our environments, our focus shifted to securing and protecting these entities. Our survey results confirmed that securing these behemoth, complex networks is no easy task. Key takeaways from this year's survey include:

- More than **64%** of organizations have *six or more* vendors in their security profile, despite nearly **20%** relying solely on their cloud provider.
- Nearly **71%** of respondents utilize centralized network-based management for their security devices.
- The most common security devices in use are firewalls and vulnerability managers, with public cloud inputs and cloud access security brokers the least common.
- Organizations have shifted to "hybrid" or "modern" with the adoption of containers and microservices (**44%**) and implementation of vast cloud infrastructures to support business operations.

For much of the information we solicited, organizations were in a positive or near-optimal state. We can certainly think of times past where security was an afterthought for many organizations. Alas, we still have a good number of participants who responded that they are unsure about critical security questions—indicating that there is still plenty of room to improve.

We explore these complexities and more as we work our way through this year's results. As you work **your way** through this survey—whether you contributed or not—make some mental notes about where your organization lies in comparison to our results. If your organization has a mixed environment, we hope this survey gives you reason to examine your own security posture. We have inserted multiple "Survey Checkpoints," which are quick questions designed to help you focus on an observation from our survey and how it compares to your organization.

A Note on COVID-19: In this survey, we set out to understand some of the complexities of securing large enterprise environments. For many nations around the globe, and thus also our respondent pool, changes in the workforce due to COVID-19 were likely already in full swing. Thus, it's possible our survey results were impacted by reductions in personnel and/or shifts to an entirely work-from-home model. We did not augment our survey to accommodate changes brought to the business landscape by COVID-19, relying instead on our respondents to answer accurately and "in-the-moment."

Geography Matters: This Year's Respondent Pool

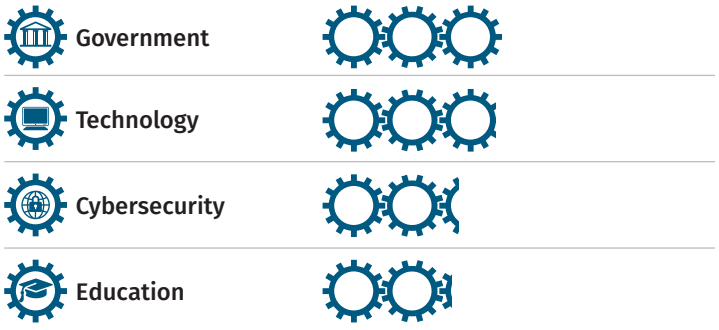
When assessing the security of modern enterprises, our concerns typically begin with geographic region. After all—if your organization is considered a mixed environment—having both cloud and on-premises assets—it may be tough to narrow down how many regions you serve around the globe. Geography also tends to come coupled with regulations on data handling and privacy, such as GDPR. Thus, security concerns may vary based on regions served and/or headquarters location, and we wanted to ensure we captured these differences.

Our respondent pool in this survey was heavily weighted to US-based organizations, coming in at just under 73% with a US corporate headquarters. However, while only 11% are headquartered in Europe, more than 30% have operations in the EU. Canada is in a similar situation, at 5% and 26% for headquarters and operations, respectively. If anything, our survey proves that more organizations are global organizations, and a cloud-based infrastructure helps deliver on that exposure. Figure 1 provides additional details about the demographics of this survey's respondent pool.

Survey Checkpoint #1: Where is your organization headquartered?

Where is your organization headquartered versus where are your operations? Understand the data and regulatory requirements of each, to ensure that your organization isn't falling out of compliance.

Top 4 Industries Represented

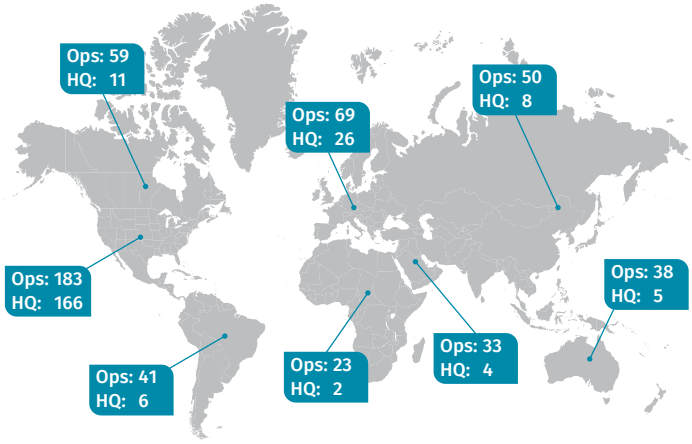


Each gear represents 10 respondents.

Organizational Size

Each building represents 10 respondents.

Operations and Headquarters



Top 4 Roles Represented

Each person represents 10 respondents.

Figure 1. Survey Demographics

When we think about large, complex enterprises, we typically imagine a massive, global conglomerate with tens or hundreds of thousands of employees. Instead, we're seeing the complexities of modern enterprises shared by organizations of all sizes. In fact, an overwhelming majority of our respondents—approximately 70%—have 10,000 or fewer employees. Nearly 89% of that pool has 5,000 or fewer people in the workforce—proving that even "smaller" organizations face the same battles.

Modern Enterprise Infrastructure

Before we examine the complexities that organizations face today, let's discuss what it means to be a *modern enterprise*. Modern infrastructures[1] are typically labeled as *hybrid*, meaning they are using a combination of cloud and traditional, or on-premises, resources. However, it would be a reductionist approach to think of the modern enterprise as simply a switch from on-premises to cloud operations.

Today, enterprises employ a multitude of technologies to provide value to their employees and customers. From containers and microservices to complex SD-WAN networks that bring offices all over the globe together, the simple concept of the client-server infrastructure has changed for the better—or worse! Let's begin by understanding how many of our respondents are taking advantage of the technologies we've mentioned here.

A Place in the Clouds

There are still plenty of organizations and even industries that cannot fully migrate to the cloud within their infrastructure, due to their regulatory requirements, services offered or available resources. As shown in Figure 2, 88% of our respondents indicate they had at least 10% or more of their infrastructure in cloud services, with 31% of all respondents with 50% or more of their infrastructure dependent on cloud services.

A small number of our respondents—a little over 2%—admit to being 100% dependent on cloud-based services. While only a handful of respondents report this level of cloud usage, it's likely a good indication that those organizations were created as cloud-based entities. Going completely cloud-based may be a dream for some, but ultimately it requires significant investment and infrastructure planning, if not done from an organization's inception. We do, however, expect the share of cloud-based services to grow over the next few years as more and more organizations realize the benefits of cloud-based services and are able to adapt their business operations.

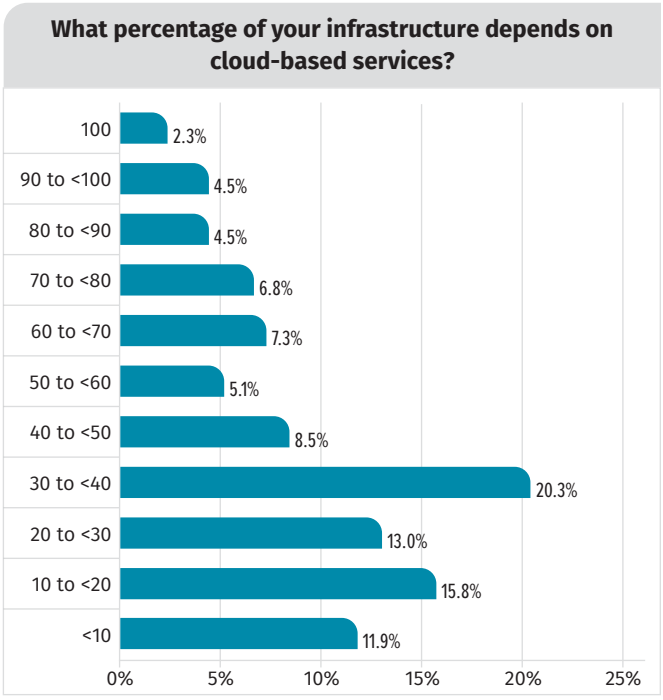


Figure 2. Cloud-Based Service Dependency

[1] Note, we are not implying that an operation with zero cloud-based services is not modern. Instead, we are attempting to signify that many organizations have moved some operations to cloud-based services (as we will see in this survey). This trend certainly isn't new. Cloud services have been around for many years now; for example, organizations have been using cloud storage services and virtualized environments, to name only two, for many years.

Additionally, given the recent changes in business operations due to COVID-19, it is likely that these numbers will continue to rise. The first half of 2020 has made many organizations scramble to replace in-person services with cloud operations, and it's highly likely that these changes will be made permanent in the months and years to come.

Thinking about cloud usage differently, we asked our participants what model(s) of cloud usage they employ: software-as-a-service (SaaS), infrastructure-as-a-service (IaaS) or platform-as-a-service (PaaS). SaaS is certainly the most popular, according to nearly 86% of respondents. Slightly more than 53% report that they use IaaS, indicating that cloud-based storage and systems are quite popular among our respondent pool. See Figure 3.

Understanding the model(s) the organization uses is critical knowledge for the security team. For example, depending on the implementation, security teams may view virtualized systems (IaaS) as another endpoint within the organization's environment and require detection and/or investigative endpoint tools. A SaaS implementation, on the other hand, may remove data storage and runtime capabilities from the environment, lowering the potential risk to the organization. Of course, the risk of a data incident is transferred to the SaaS provider—something we'll discuss shortly (see "Survey Checkpoint #3: Who's responsible?").

Cloud usage models are also crucial in understanding how to properly structure and segment network infrastructure. For example, if an organization moves a critical server over to a cloud service provider, the organization will likely have on-premises systems that still need to communicate with the cloud-based system(s). From a network perspective, this requires teams to establish access to a trusted "external" resource.

Among our respondents who have already moved some of their infrastructure to cloud-based services, a large majority (78%) utilize cloud services for data storage and/or systems alternate to on-premises servers (see Figure 4).

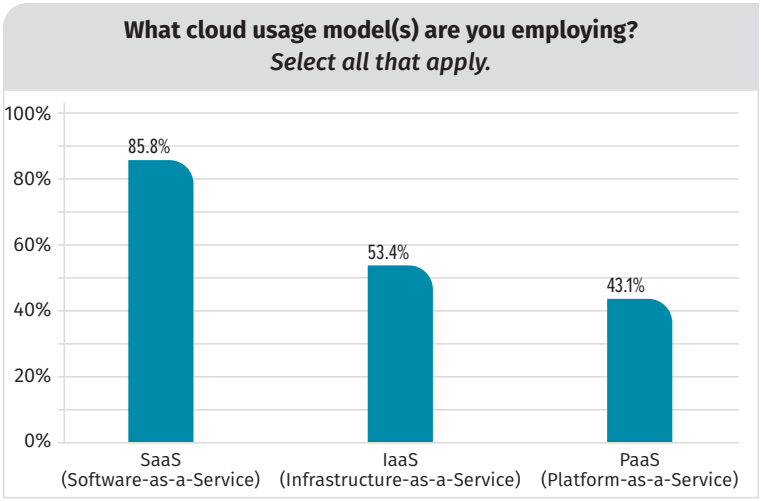


Figure 3. Cloud Usage Models

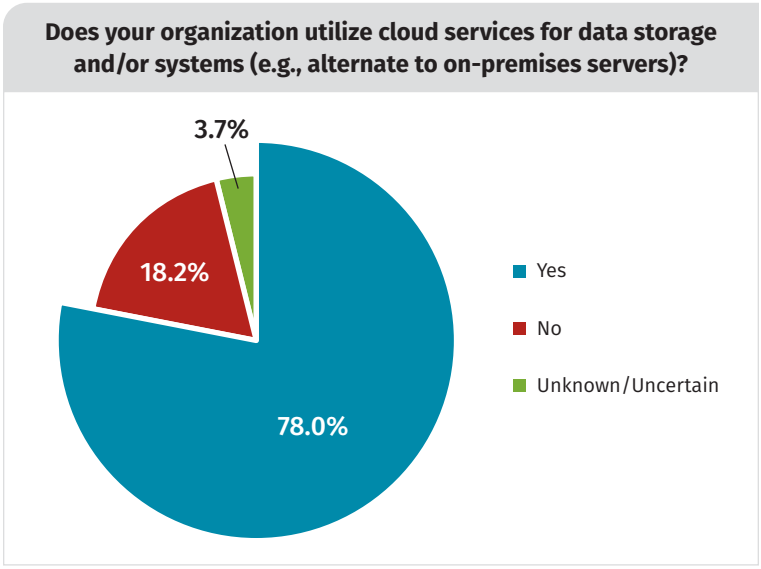


Figure 4. Data Storage and/or Systems in the Cloud

Survey Checkpoint #2: Where does the cloud fit into your organization?

A significant portion of our respondents have at least 20% of infrastructure in cloud-based services, while few have 100% in the cloud. Consider where your organization stands and the services you use. Does your security team know?

We also asked our respondents if they deployed virtualized resources within the cloud. As shown in Figure 5, approximately 59% confirm that they use virtualized resources.

Within this survey, we did not specify the types of virtualized resources. However, our biggest takeaway isn't the use of virtualized resources, it's the lack of knowledge about them. Figure 4, together with Figure 5, presents an additional concern for us: While a tiny minority, just under 4% of our respondents, indicate that they are uncertain how or whether their organization utilizes data storage and/or cloud-based systems, more than double that amount—9%—are unsure whether they use virtualized resources in the cloud. When security professionals admit to a lack of environmental awareness, it always raises concern from a security perspective. Furthermore, there have been multiple data incidents over the past few years that have been the direct result of a lack of cloud asset awareness. To put it simply: Not knowing what you have in the cloud is a significant security risk.

We dug deeper with those who utilize virtualized resources in the cloud to take a look at what technologies they use to secure these devices. A significant majority—65%—use a combination of endpoint and network management. Also shown in Figure 6, approximately 17% of respondents use either endpoint or network management, depending on the device.

Perhaps the most concerning takeaway here is that approximately 7% of our respondents admitted to having virtualized cloud resources without any management whatsoever. We'll explore security next, but this is a consistent trend we see amongst multiple SANS surveys: Organizations deploy and/or take advantage of cloud technologies with little security oversight.

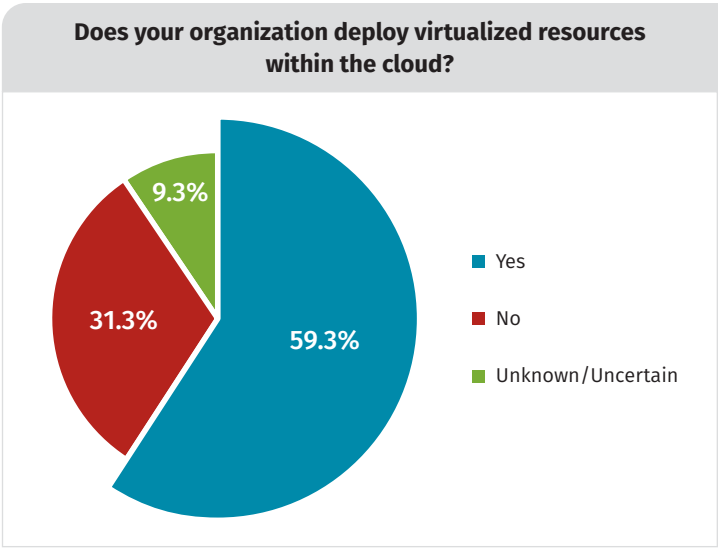


Figure 5. Virtualized Resources in the Cloud

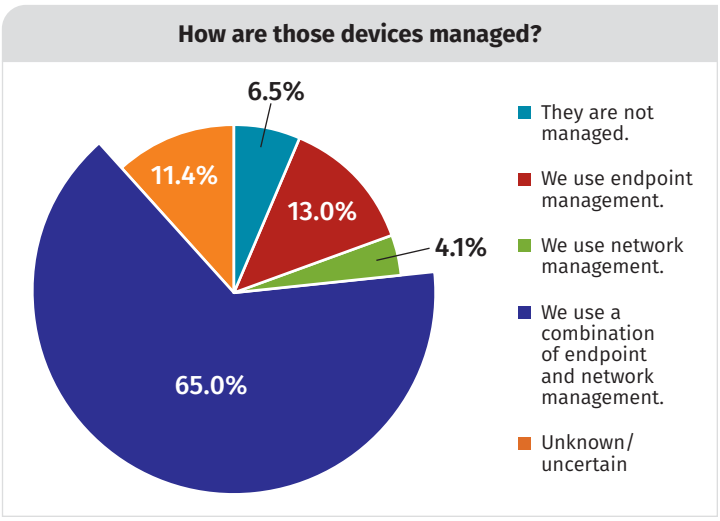


Figure 6. Device Management

Survey Checkpoint #3: Who's responsible?

In the event of a data incident involving one of your SaaS providers, who's responsible for neutralizing the event and investigating the incident? Has your security team considered how your current or future SaaS models impact your network?

Deeper into Network Architecture

Going one-level deeper in network architecture, organizations will often implement segmentation, or micro-segmentation, typically through a software approach. As shown in Figure 7, just about all of our respondents (99%) are aware of their network architecture, with nearly 31% claiming a highly segmented network with micro-segmentation.

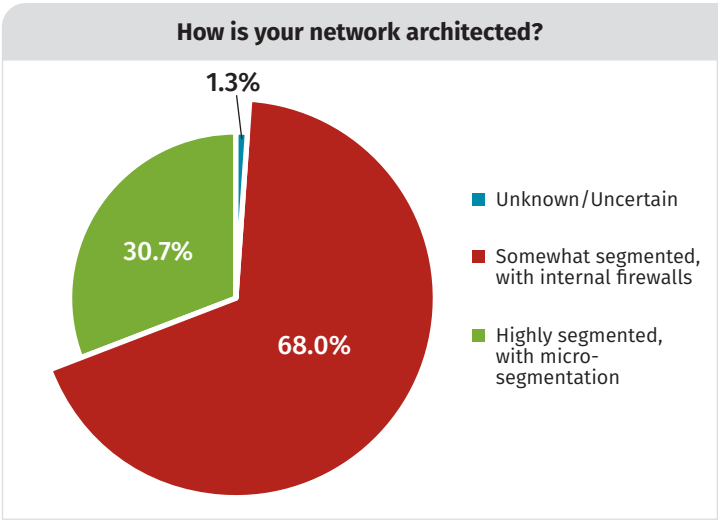


Figure 7. Network Architecture

Keeping network architecture in mind, we asked our survey respondents if they had plans to utilize software- or cloud-based security products in place of current on-premises solutions in the future. As shown in Figure 8, approximately 38% plan to move away from on-premises products.

We encouraged our respondents to elaborate on their answers. The following respondent comments are noteworthy:

- "Hosted SIEM/SOCs ... VMs for most internal tools"
- "Moving endpoint security to cloud ..."
- "Cloud-first direction, including SaaS when we know data can be properly secured."
- "To control and secure endpoints inside and outside the network."

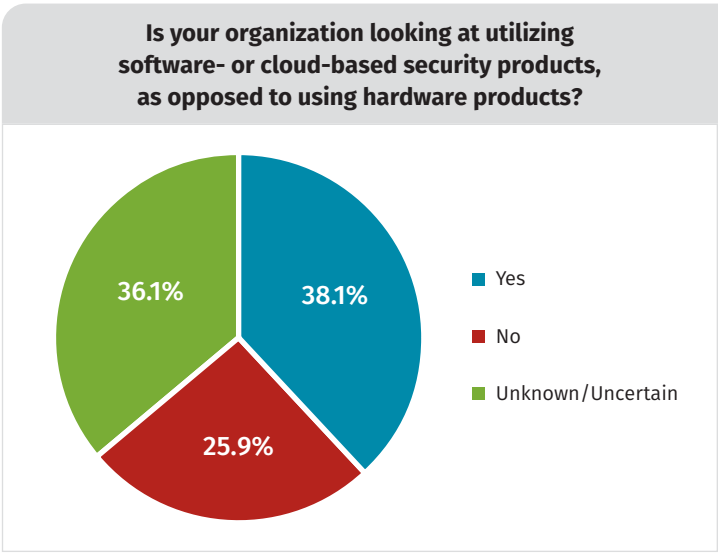


Figure 8. Utilization of Software-Based/Cloud-Based Security Products

Security solutions hosted in the cloud are becoming so common that we're not surprised to see 38% heading in that direction. The 26% of respondents who indicated they are not considering the cloud may be satisfied with their on-premises implementations and see no need for change. This may also include organizations already locked into existing contracts. While they were not looking to the cloud at the time of the survey, they may be migrating in future months or years.

What did catch us off guard was the 36% of respondents who were uncertain about their future use of software- and/or cloud-based security products. We were unable to assess whether these respondents don't have a "seat at the table"—thus are not part of decision-making discussions—or whether the organization has yet to decide the future of their security products.

Complexities in Managing and Securing Modern Enterprises

Understanding the composition of your organization is only half the battle. Providing a means to effectively secure cloud-based assets and services is also crucial to successful cloud integration. For example, as we mentioned in the previous section, the differences between IaaS, PaaS and SaaS are not simply the type of service used. Your breach notification and incident response and handling requirements may differ greatly depending on the types of services you use.

Security in the Infrastructure

We were curious about what technologies our respondents already have in place to secure their infrastructures. Figure 9 shows us that firewalls and vulnerability managers are, without a doubt, the most common types of security devices at 97% and 93%, respectively.

Malware detection, network-based IDS/IPS and hypervisors round out the top five most common security devices. These trends are not new or unique to this survey; firewalls have been a staple in infrastructures and network security for decades. We were happy to see vulnerability managers in the top 2, especially because vulnerability visibility is one of the topics respondents targeted for future spending (see the "Looking Ahead" section).

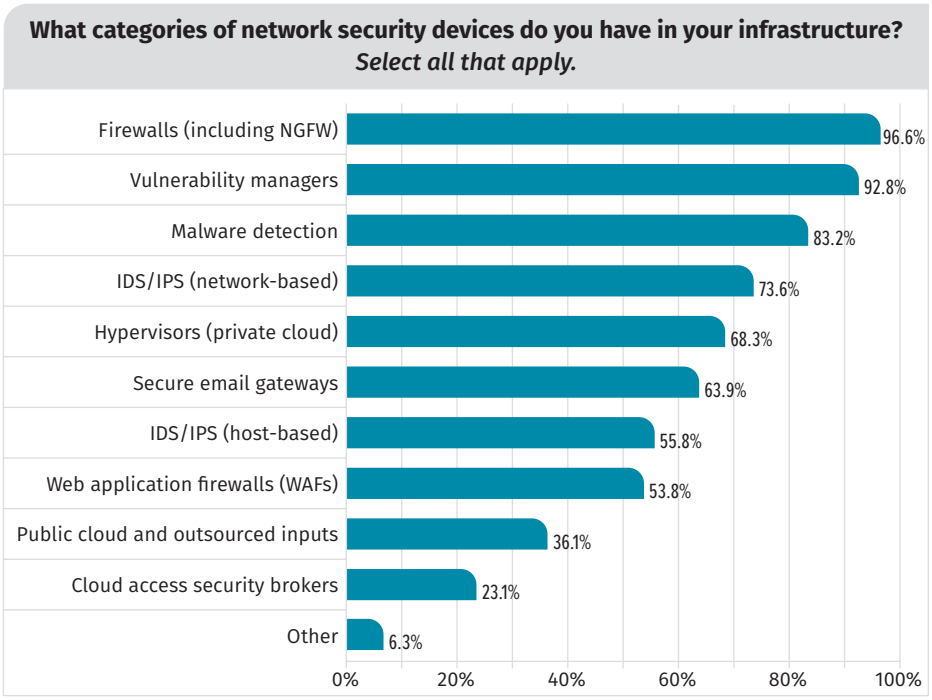


Figure 9. Network Security Devices in Use

Fortunately, even with a plethora of vendors and/or devices, most of our respondents indicated that their organization managed its own devices. A whopping 96% of respondents indicate that they manage their organization's network security devices internally, with only 2% admitting to uncertainty about device management.

Another concern when organizations use multiple network security devices is the number of vendors within an environment and whether their devices are working together. Single-vendor platforms are often tuned to work well together, whereas, although multiple vendor platforms may offer more in-depth, focused security, they may not possess integrated capabilities. Security teams that spend more time combining and correlating data are losing valuable time and resources that they should be spending on investigating threats to the organization.

The number of vendors represented in our respondents' security profiles surprised us significantly. Nearly 65% of our respondents have more than five security vendors, and 30% have *at least 11* vendors represented in their security profile. See Figure 10.

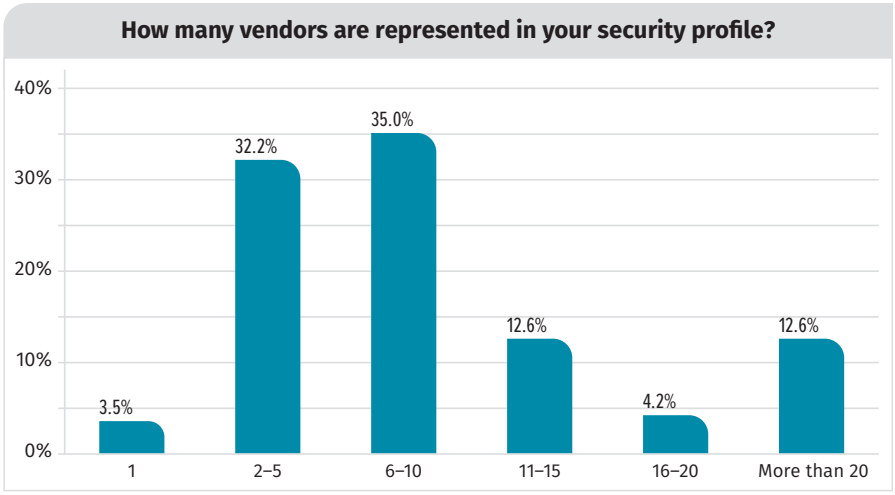


Figure 10. Number of Vendors in Security Profiles

A little more than a third (36%) of our respondents used fewer than six vendors—still a large population to wrangle and manage! Having multiple types of security devices within an organization introduces even more complexities. Managing multiple devices, maintaining complex global rulesets and ensuring devices are up and actively securing the organization can be a full-time job. We asked our respondents if they were utilizing a central management approach. Approximately 71% are centrally managing their networks, while the remaining 29% either are unsure or do not utilize a central approach.

We were happy to see that approximately 78% of those who indicated they had centralized network-based management had security management capabilities (the second highest result for this question). See Figure 11.

The other top features rounding out the top four include network administration, performance monitoring and configuration management. These results didn't surprise us. Typically, organizations choose to use central management to impact these categories. See Survey Checkpoint #4 for more thoughts on central management of network devices.

While it may seem insignificant, how organizations manage their network devices has a direct impact on the organization's ability to secure and protect itself. Multiple vendors and devices can provide granular security, but complex device management processes can prevent even the best devices from effectively protecting users. We asked our respondents directly—how long does it take a security

Survey Checkpoint #4: How do you manage your network security devices?

Central management of network security devices is a game-changer when it comes to securing enterprise infrastructures. The more devices your organization requires, the more deployment, configuration and maintenance your network team will be required to provide. Utilizing a central management platform means your suite of network security products can be updated on the fly.

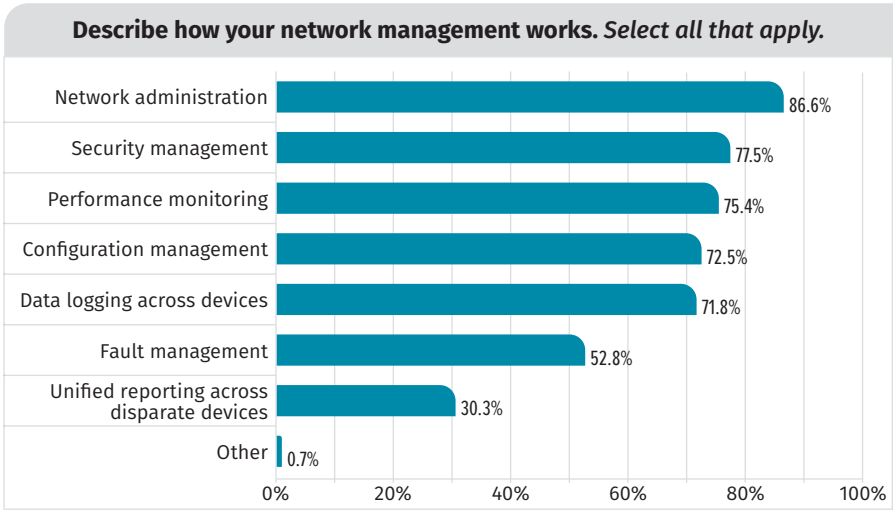


Figure 11. Network Management Types

team to implement firewall changes? As shown in Figure 12, 45% were able to implement changes within less than six hours. Bravo!

Tallied up, approximately 70% of our respondents could implement changes within 24 hours. That's not a bad turnaround, especially when compared to the 5% of our respondents who need at least a week—with almost half of those needing more than two weeks.

What's the roadblock? Often management processes and red tape contribute to the time required. Figure 13 helps illustrate this. A quarter of our respondents have at least three processes to make changes to a firewall, while a staggering 15% *do not know how many processes they need to follow*.

These two questions, concerning the time to make changes to firewalls and the processes involved, represent a critical security finding in this survey. Many organizations are simply unaware of their firewall processes, resulting in changes taking far too long from a security perspective. We should stress: The longer it takes to use a security device for security purposes, the more time attackers have to execute in your network.

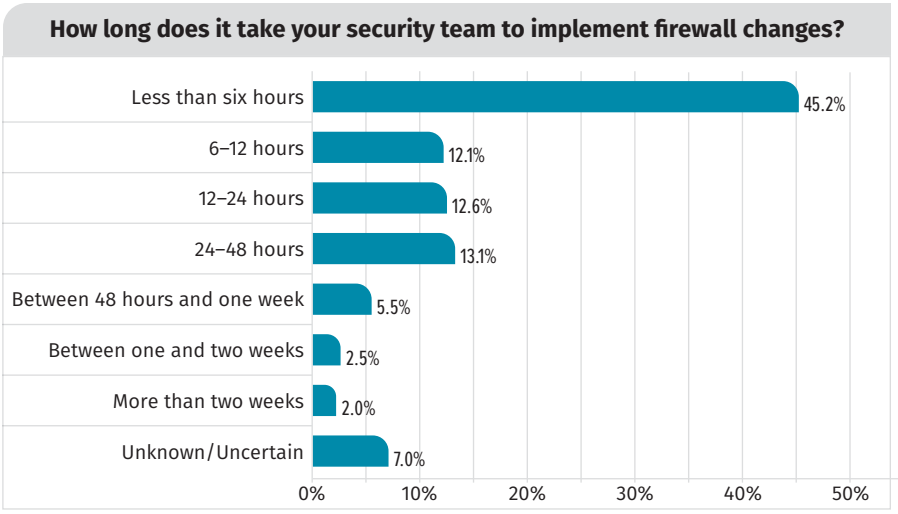


Figure 12. Time Required to Implement Firewall Changes

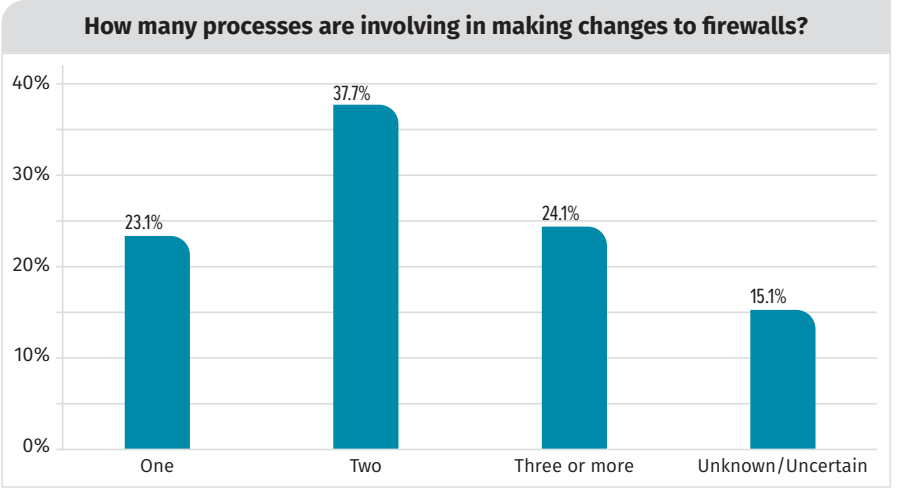


Figure 13. Number of Processes Required for Firewall Changes

Security in the Cloud

Our previous security questions focused on network security devices in general. Keeping with our theme of organizations moving operations to the cloud, we also asked our respondents directly about their use of cloud-based security products. More than half—approximately 60% of our respondents—do use cloud-based products. As shown in Figure 14, only 31% indicated that they do not, but half of those say they plan to.

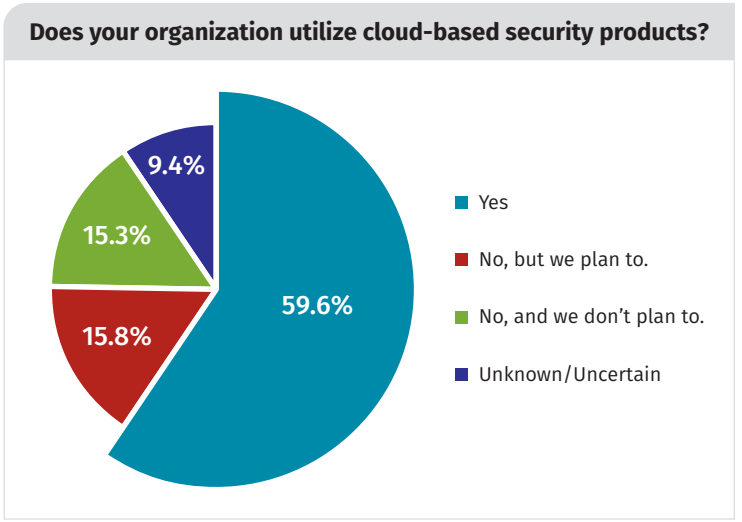


Figure 14. Cloud-Based Security Products in Use

It's worth noting that cloud-based security products do not necessarily imply use of the cloud—for example, many organizations use cloud-based endpoint monitoring for their physical assets. This helps provide security in the event that employees are traveling or off-domain and cannot connect to an internal system. Think again about the changes that COVID-19 has introduced in "normal" client-server architecture.

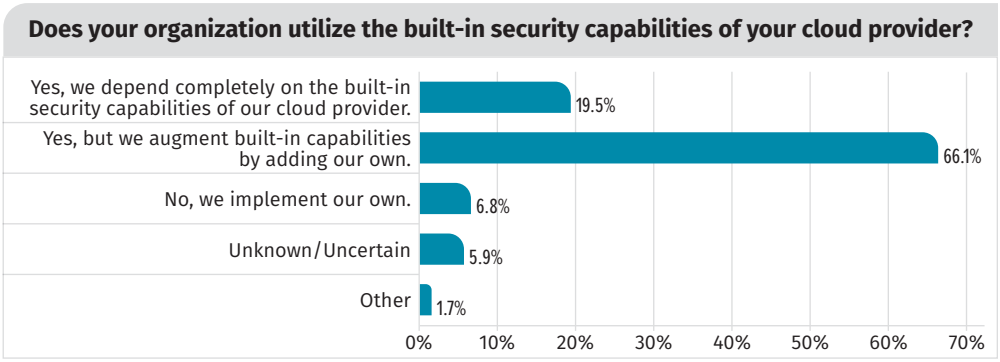


Figure 15. Usage of Built-in Security Capabilities

Shifting the focus to cloud service providers, approximately 86% of our respondents do use the built-in security capabilities of their cloud providers. However, a large portion of that pool indicate that they augment those measures with their own capabilities. See Figure 15.

Only 7% of respondents implement their own security. No respondents elaborated as to why they do or do not utilize built-in security capabilities.

Looking Ahead

Finally, after our assessment of the *current* state of things, we also briefly asked our respondents about their future plans. Regardless of whether their efforts are cloud-hosted or on-premises, our respondents recognize that securing the business comes first. As shown in Figure 16, nearly 21% of our respondents plan to implement preventive security controls, including patch management and application security.

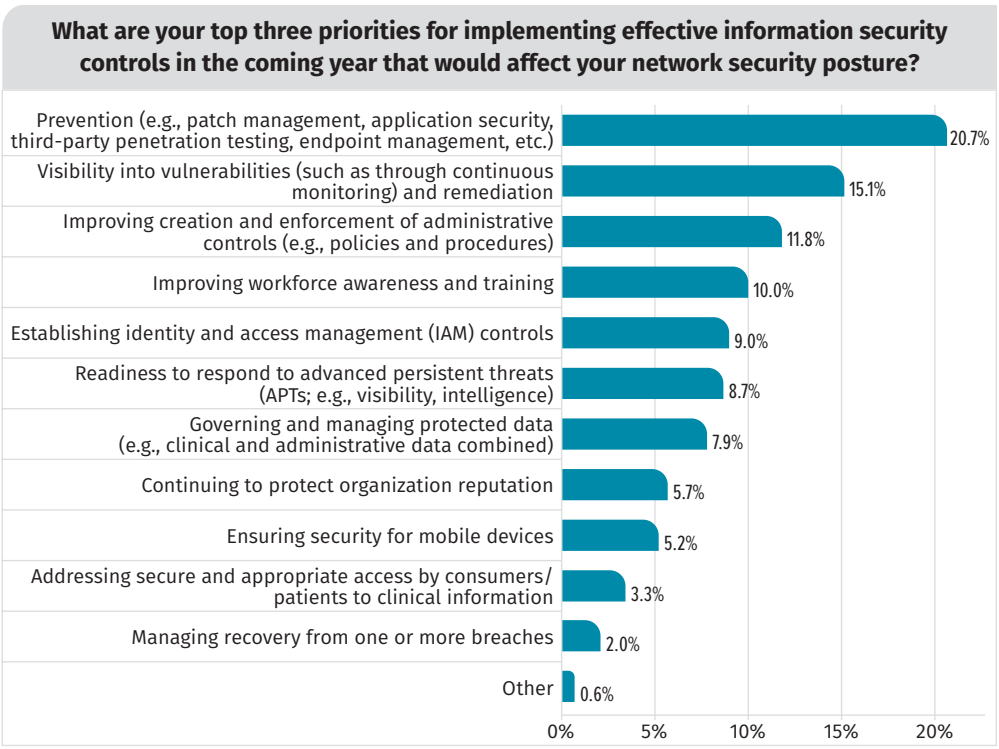


Figure 16. Top Priorities for the Coming Year

Vulnerability visibility and better administrative controls for their assets round out the top three priorities. We were pleased to see preventive measures and vulnerability awareness as the top two results; these will always be our top recommendations in securing any organization.

Closing Thoughts

In this inaugural survey, we spent some time examining the idea of a modern enterprise. The modern enterprise is not necessarily based on size or footprint of operations; instead, a modern enterprise is one that is or has been experiencing a shift of infrastructure and services to the cloud. A majority (88%) of our respondents indicated at least 10% of their infrastructure was in the cloud, confirming our statement that moving to cloud operations is not a new trend. This seems especially true given that a select few of our respondents are 100% based in the cloud.

The core focus of this survey was to examine the security requirements and capabilities of these modern enterprises. After all, it's not infrequent that a business makes moves faster than its security team can keep up. In particular, we explored:

- What technologies are being used by organizations?
- What defense mechanisms are in place, and what does it take to manage them?
- Who protects cloud resources: you or the provider?
- How do subsystem capabilities, such as containerization and microservices, impact an organization's security posture?

Organizations today are building applications and services that are structured around microservices and virtualized, on-demand platforms. Employees, located anywhere in the globe, have access to resources that are hosted in the cloud, creating a truly seamless office experience regardless of the access mechanism. Customers of complex organizations are often unaware that their requests and data may be passing through a multitude of containers, virtual machines and databases, all hosted in secure (we hope) cloud networks. Enterprises with global offices are building SD-WAN networks that allow for extremely granular control over traffic flows around the world. The point being: The modern enterprise is anything but simple, and securing all of this complexity is certainly quite an undertaking.

About the Author

Matt Bromiley is a SANS digital forensics and incident response instructor, teaching FOR508: Advanced Incident Response, Threat Hunting, and Digital Forensics and FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response. He is also an IR consultant at a global incident response and forensic analysis company, combining his experience in digital forensics, log analytics, and incident response and management. His skills include disk, database, memory and network forensics; incident management; threat intelligence; and network security monitoring. Matt has worked with organizations of all shapes and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

Last Updated: October 19th, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS Wellington 2020	**Wellington, NZ**	**Nov 30, 2020 - Dec 12, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**