Enterprise Strategy Group™ by TechTarget

The Evolution of Network Security

What Security Teams Require From Firewalls in a Cloud-centric World

John Grady | Principal Analyst
ENTERPRISE STRATEGY GROUP

JUNE 2024

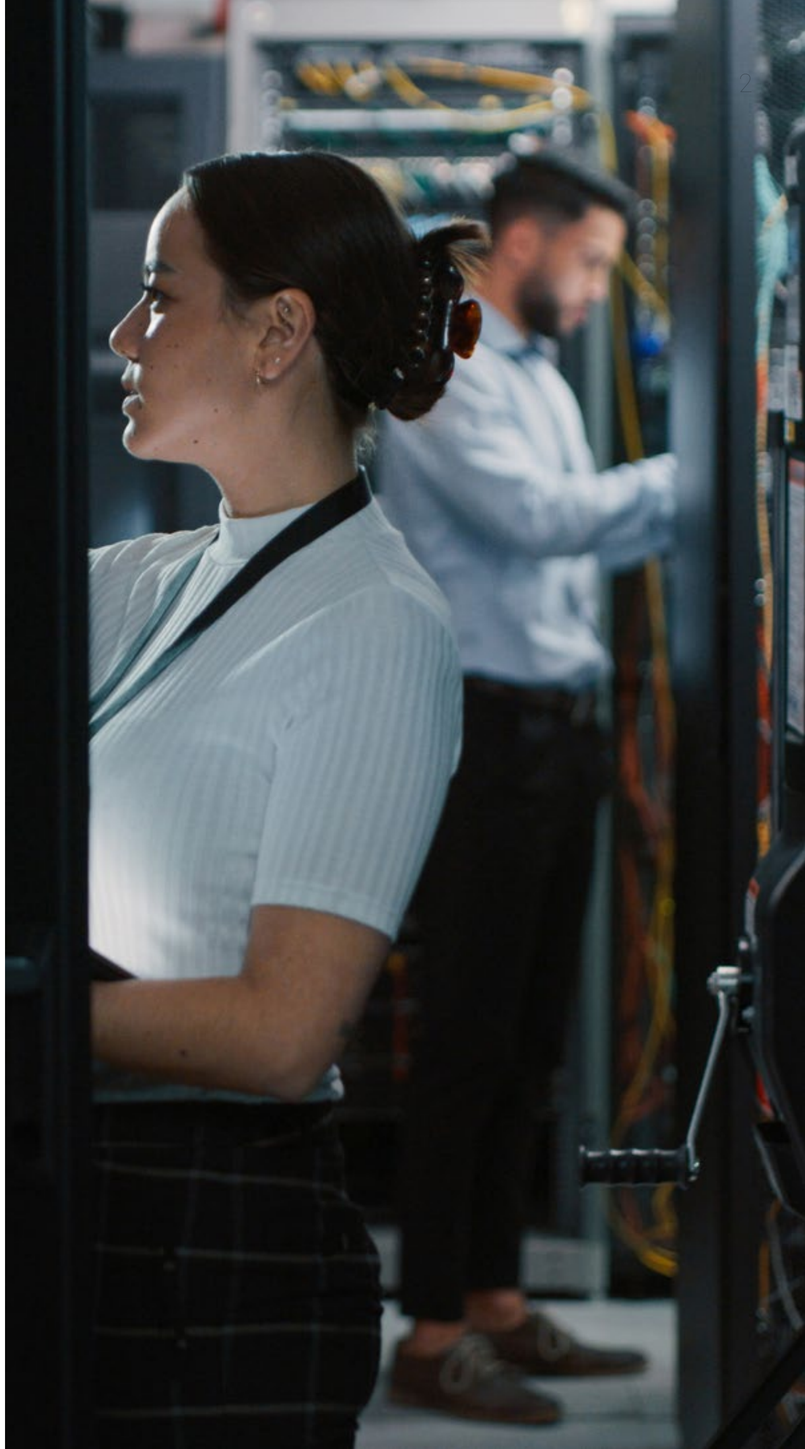
Research Objectives

As IT environments have grown more distributed and diverse, network security tools generally and firewalls specifically have become fragmented. The availability of CSP firewalls, cloud-native firewalls, and firewall capabilities from networking tools has created confusion in the market. Historically, the choice between many of these options boiled down to ease of use and efficiency versus functionality and efficacy. However, organizations can no longer make tradeoffs. They require the best of both worlds and need help understanding their options for network security and the best fit for the use cases they need to support.

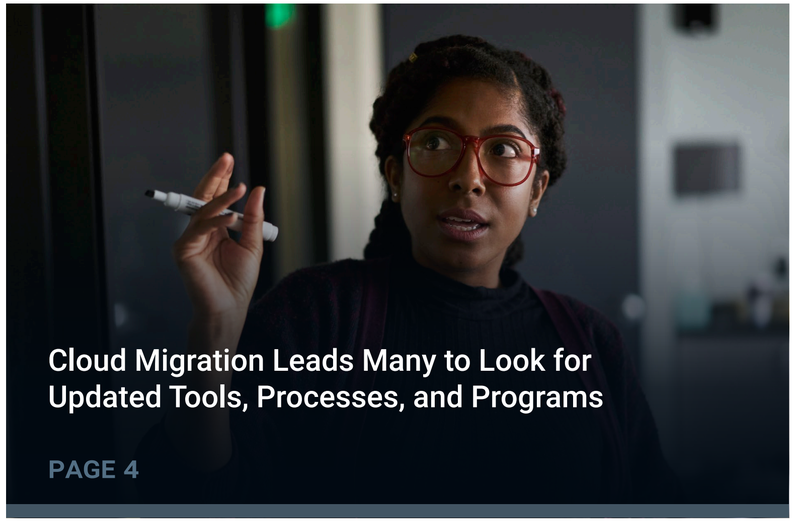
To gain insights into these trends, TechTarget's Enterprise Strategy Group surveyed 358 IT and cybersecurity professionals in North America (US and Canada) involved with network security technology and processes at their organization.

THIS STUDY SOUGHT TO:

- **Understand** the tools network security teams currently use and their reasons for prioritizing them.
- **Explore** the top challenges teams face and frequency of both attacks and downtime.
- **Determine** how modern application architectures impact network security practices.
- **Assess** the level of collaboration around network security and the teams involved in firewall buying decisions.

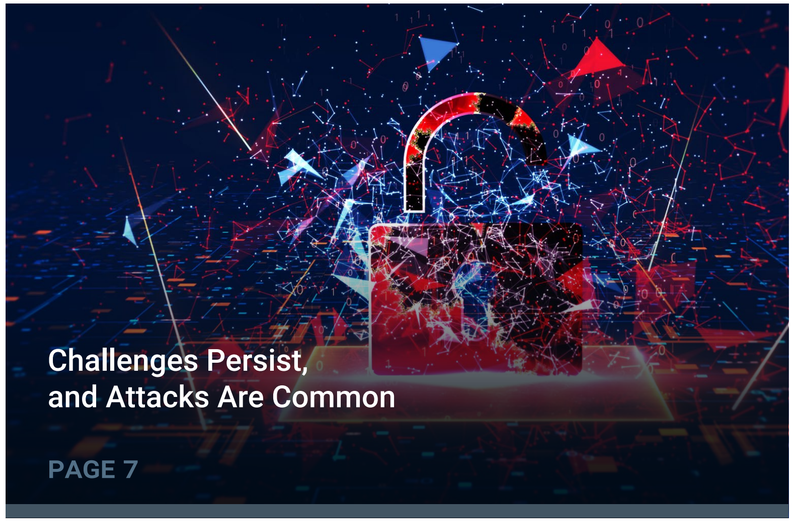


Key Findings



Cloud Migration Leads Many to Look for Updated Tools, Processes, and Programs

PAGE 4



Challenges Persist, and Attacks Are Common

PAGE 7

Organizations Are Prioritizing Securing the Use of AI and Using AI for Security

PAGE 10

Most Use Multiple Tools, but Improved Ease of Use Would Move the Needle Toward Third-party Vendors

PAGE 13

Spending Increases Are Expected Across Many Tools, but Firewall Vendor Consolidation Is a Focus

PAGE 18

Public Cloud Network Security Is Cross-functional, and Most Are Working to Improve Collaboration

PAGE 21

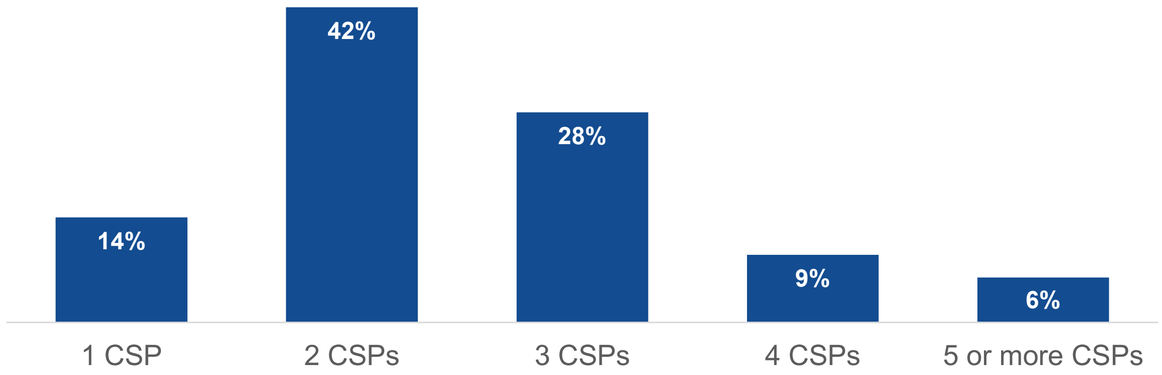
Cloud Migration Leads Many to Look for Updated Tools, Processes, and Programs

Cloud Migration Continues, Creating Complex IT Environments

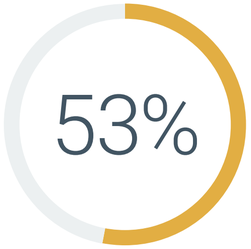
Most organizations continue to prioritize moving their applications to the cloud to achieve better scale, flexibility, and resiliency. For many organizations, this journey ultimately results in the introduction of multiple cloud service providers (CSPs) into their environment. Among survey respondents, 85% indicated they use at least two CSPs, with 43% using three or more.

While this can occur unintentionally over time due to merger and acquisition activity or lines of business going around the IT department, the use of multiple CSPs is increasingly becoming a purposeful, strategic decision. In fact, 42% of the respondents using two or more unique CSPs indicated they use multiple CSPs equally as primary providers, while 5% said they use multiple CSPs in a meaningful way and do not have a primary CSP. Finally, the use of cloud-native application architectures, and containers specifically, continues to grow.

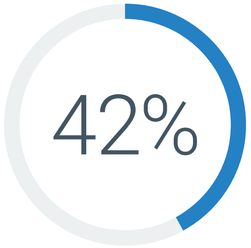
Number of unique CSPs in use.



Approach to multi-cloud usage.



We use **one CSP** as our primary provider and use other CSPs on a secondary basis



We use **multiple CSPs equally** as primary providers and use other CSPs on a secondary basis

We use **multiple CSPs in a meaningful way** (i.e., we don't have a primary CSP)

BACK TO CONTENTS

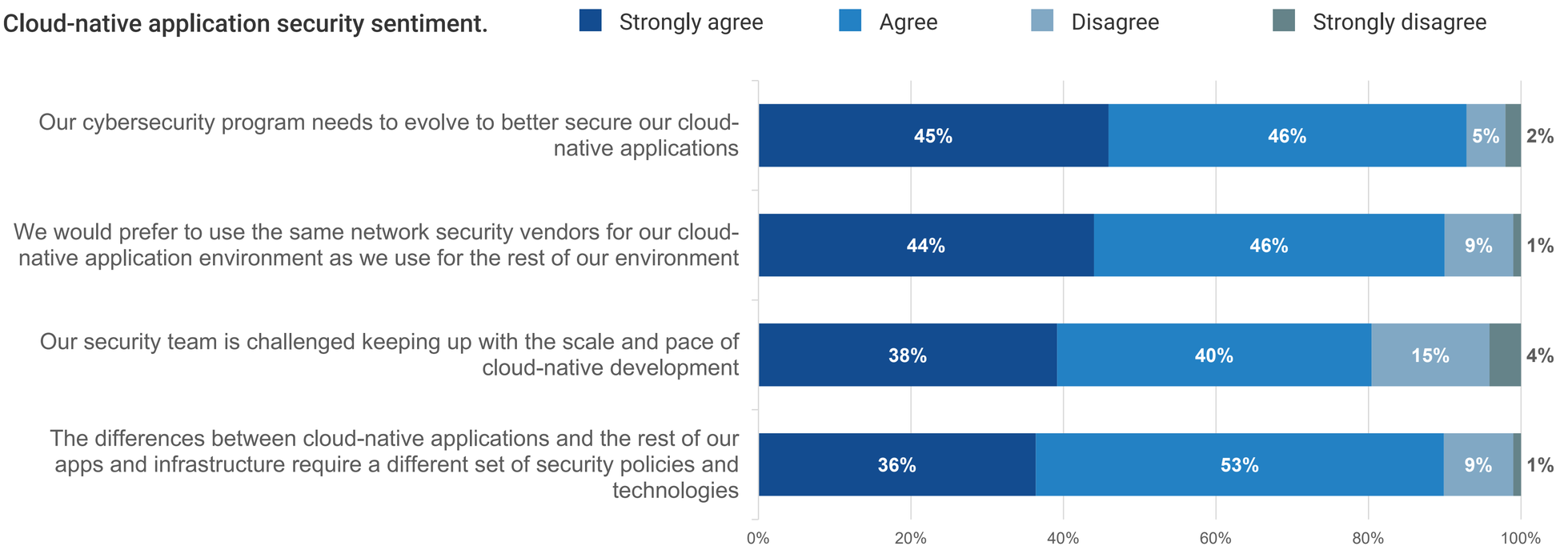
Most Agree an Evolution Is Needed, but Specific Opinions Vary

As a result of these environmental changes and the adoption of cloud-native application architectures, nearly all respondents (91%) agree their cybersecurity program needs to evolve. Fewer but still a strong majority (78%) indicate their security team is challenged keeping up with the scale and pace of cloud-native development.

Unsurprisingly, 89% agree that the differences between cloud-native applications and other applications and infrastructure require a different set of security policies and technology. Manually deploying and configuring network security tools as a new virtual private cloud (VPC) or virtual network (VNet) spun up in AWS or Azure slows operations down and creates a bottleneck that most businesses will not accept.

Yet at the same time, 90% of respondents say they would prefer to use the same network security vendors for their cloud-native environments as they do for the rest of their environment. This is an intriguing finding and highlights the desire to reduce the tool and vendor sprawl that has been created over the years.

Cloud-native application security sentiment.



"Nearly all respondents (91%) agree their **cybersecurity program needs to evolve**."

BACK TO CONTENTS

Challenges Persist, and Attacks Are Common

There Are Many Challenges Securing Hybrid Cloud Environments

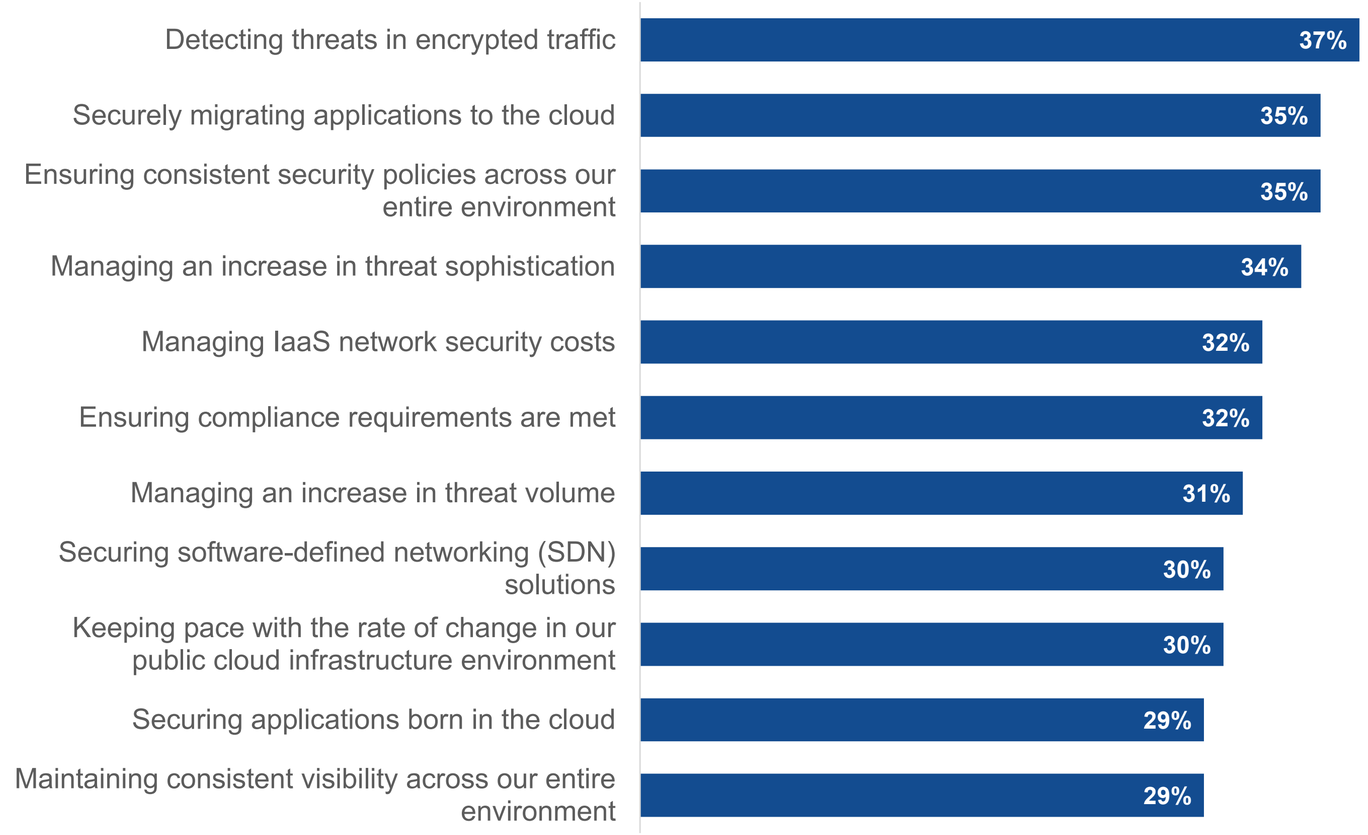
While the focus on cloud infrastructure is important, protecting on-premises infrastructure remains important as well. Respondents report an almost even split of applications residing on premises (51%) and on public cloud infrastructure (49%).

A variety of challenges securing these hybrid environments were cited. Unsurprisingly, the threat landscape ranks highly, with 37% citing the difficulty of detecting threats in encrypted traffic, 34% saying they have trouble managing an increase in threat sophistication, and 31% having trouble with threat volume.

Consistency is also important. More than a third (35%) say ensuring consistent security policies across the entire environment is a challenge, while 29% point to maintaining consistent visibility across the entire environment. Securing application migration to the cloud (35%) and managing IaaS network security costs (32%) were also called out as challenges.

Given the prevalence of these cloud-centric challenges, it makes sense that nearly half (47%) say securing cloud environments is more difficult than on-premises infrastructure.

Top ten network security challenges of hybrid cloud.

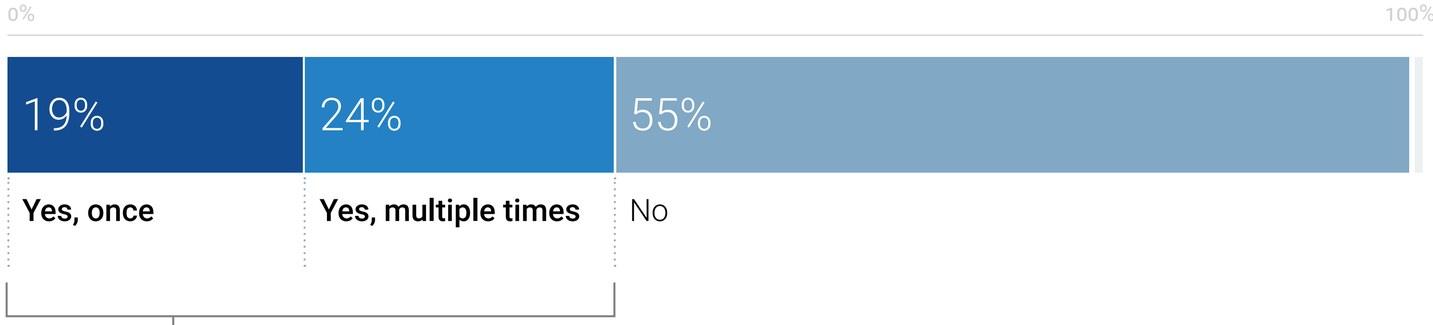


BACK TO CONTENTS

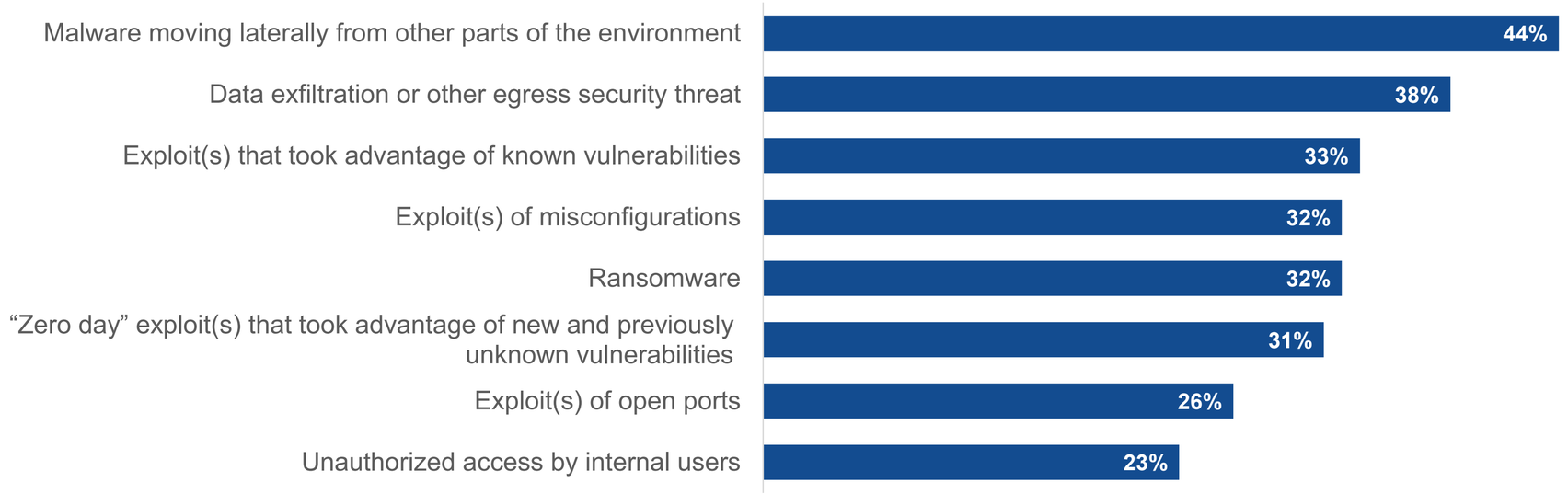
Public Cloud Attacks Are Common Across a Variety of Vectors

More than four in ten organizations have experienced an attack on their public cloud infrastructure within the last two years, with 19% having suffered one attack and 24% reporting being victimized by multiple attacks. The types of attacks varied, but the most common was malware moving laterally from other parts of the environment (44%). This would seem to justify the concerns around maintaining consistent security policies and visibility across the environment. Among the attacks seen were data exfiltration or other egress security threats (38%), exploits of known vulnerabilities (33%), exploits of misconfigurations (32%), ransomware (32%), and “zero day” exploits (31%). The wide range of attacks experienced highlights the fact that security efficacy cannot be compromised and should be a priority attribute in any network security tool protecting public cloud infrastructure.

Have organizations suffered attacks on their public cloud infrastructure environment over the last 24 months?



Types of attacks organizations experienced.



BACK TO CONTENTS

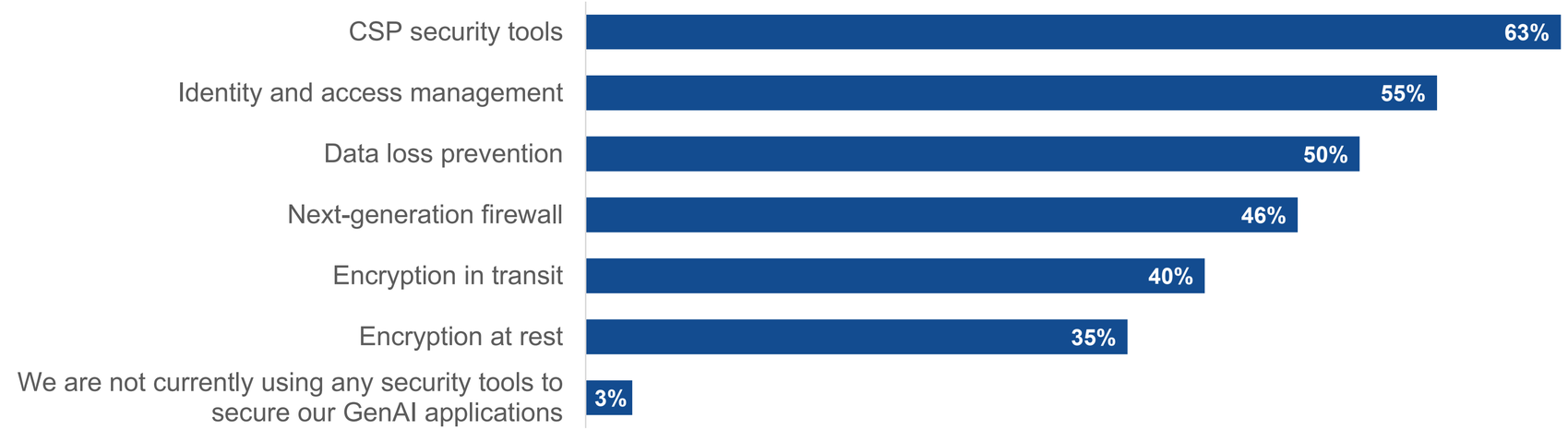
Organizations Are Prioritizing Securing the Use of AI and Using AI for Security

A Variety of Tools Are Used to Protect AI Applications

AI receives a lot of attention in the market, and for good reason. It has the potential to help organizations deliver better and more efficient services to their users but also represents a significantly different threat vector. When discussing AI and security, it is important to delineate between securing the *use of* AI applications and capabilities and *using* AI to enhance the effectiveness of security tools.

For the first use case, 89% of respondents say they are currently developing or running applications using generative AI technologies. Examples of this may include customer-facing support bots, internal chatbots, or multimedia content generation. Nearly all (97%) are using security tools to protect these applications, and most are using multiple tools. While many are focused on CSP tools, identity and access management, and data loss prevention solutions, nearly half (46%) are using next-generation firewalls to ensure the generative AI capabilities of both internal and external-facing applications are protected from abuse. Similar to the finding that many would prefer to use the same network security vendor for cloud as on-premises environments, this shows that many organizations do not want to add tools to address emerging use cases and ideally would extend the coverage of what is already in place.

Security tools used to secure generative AI applications.



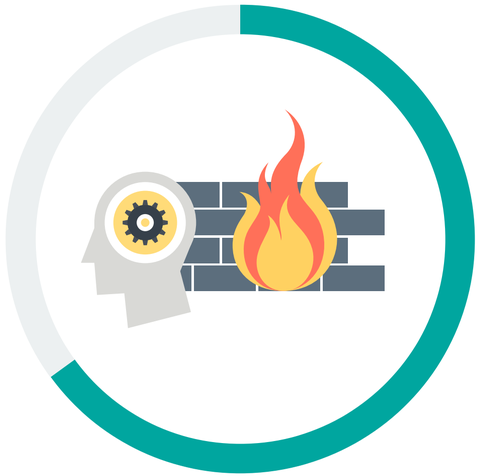
"89% of respondents say they are **currently developing or running applications using generative AI technologies.**"

BACK TO CONTENTS

Use of AI for Policy Management Is Yielding Tangible Benefits

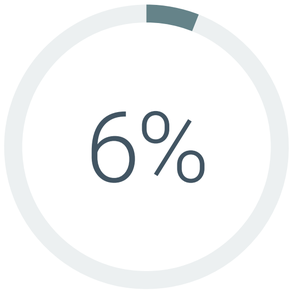
For the second use case for AI and security, 65% of respondents say they currently use generative AI technology as part of their infrastructure for firewall policy management. More importantly, this is paying dividends, with 92% saying this has saved them at least six hours per week on firewall policy management, with an average savings of roughly 20 hours per week.

Security organizations continue to be challenged by the cybersecurity skills shortage. Across the board, operational efficiency is a top IT priority. Solutions that help security teams do more with less resources to create cycles for more proactive tasks should be prioritized. With firewalls, AI can help administrators write policies, avoid rule conflicts, ensure proper configuration, and more, which saves time, effort, and ultimately, money.



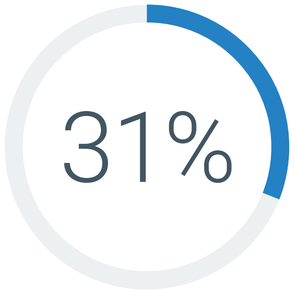
We use generative AI technology as part of our infrastructure for firewall policy management, 65%

Estimated hours per week organizations save using generative AI for firewall policy management.

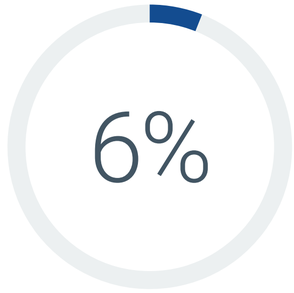


Up to 5 hours

6 to 20 hours



21 to 40 hours



More than 40 hours

BACK TO CONTENTS

Most Use Multiple Tools, but Improved Ease of Use Would Move the Needle Toward Third-party Vendors

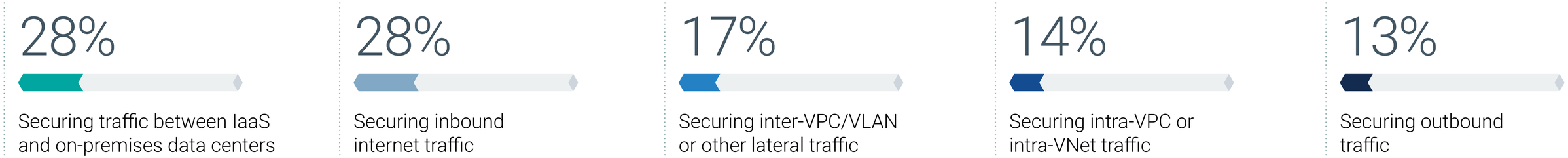
Top Use Cases for Protecting Public Cloud Infrastructure

There are a handful of use cases organizations need to think about when securing their public cloud infrastructure: inbound traffic, outbound traffic, and east/west traffic. Within the east/west category, additional use cases include securing traffic between IaaS and on-premises data centers, traffic flowing from one VPC or VLAN to another VPC or VLAN, and traffic flowing within a VPC or VLAN.

The use cases rated as most important were securing inbound internet traffic, which was ranked #1 by 28% of respondents, and securing traffic between IaaS and on-premises data centers, also ranked #1 by 28% of respondents. These are more traditional, perimeter-focused use cases, so it makes sense organizations are prioritizing here.

There is less focus on internal public cloud east/west use cases. Only 17% said securing inter-VPC/VLAN traffic was most important, and only 14% pointed to securing intra-VPC/VNet traffic. Considering the number of attacks respondents saw moving laterally, these numbers should be higher.

Most important use cases for network security tools.



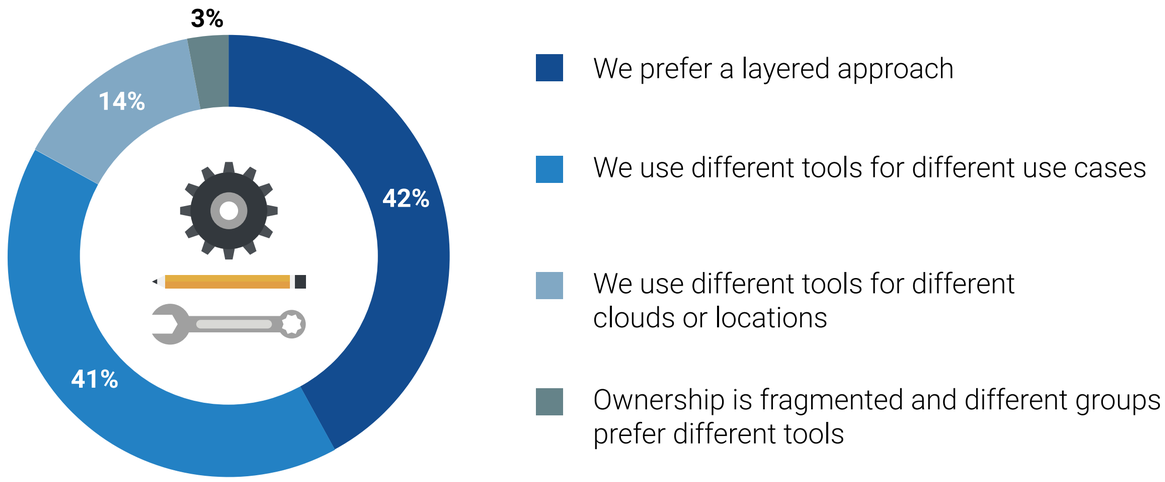
BACK TO CONTENTS

Most Use Multiple Tools

To address these use cases, most organizations are using multiple tools. Specifically, 90% said their organization uses more than one network security tool. The most common tools used by respondents were network firewalls from CSPs (79%), security groups from CSPs (68%), and network firewalls from third-party vendors (59%). Proxies (34%) and microsegmentation tools (28%) saw less usage.

Somewhat surprisingly, this tool sprawl is often by choice. Specifically, 42% said they prefer a layered approach, 41% said they use different tools for different use cases, and 14% said they use different tools for different clouds or locations.

Reasons organizations use multiple tools to protect IaaS/PaaS environments.



Network security tools currently used to protect IaaS/PaaS environments.

79%
Network firewalls from cloud service providers

68%
Security groups from cloud service providers

59%
Network firewalls from third-party vendors

34%
Proxies

28%
Microsegmentation

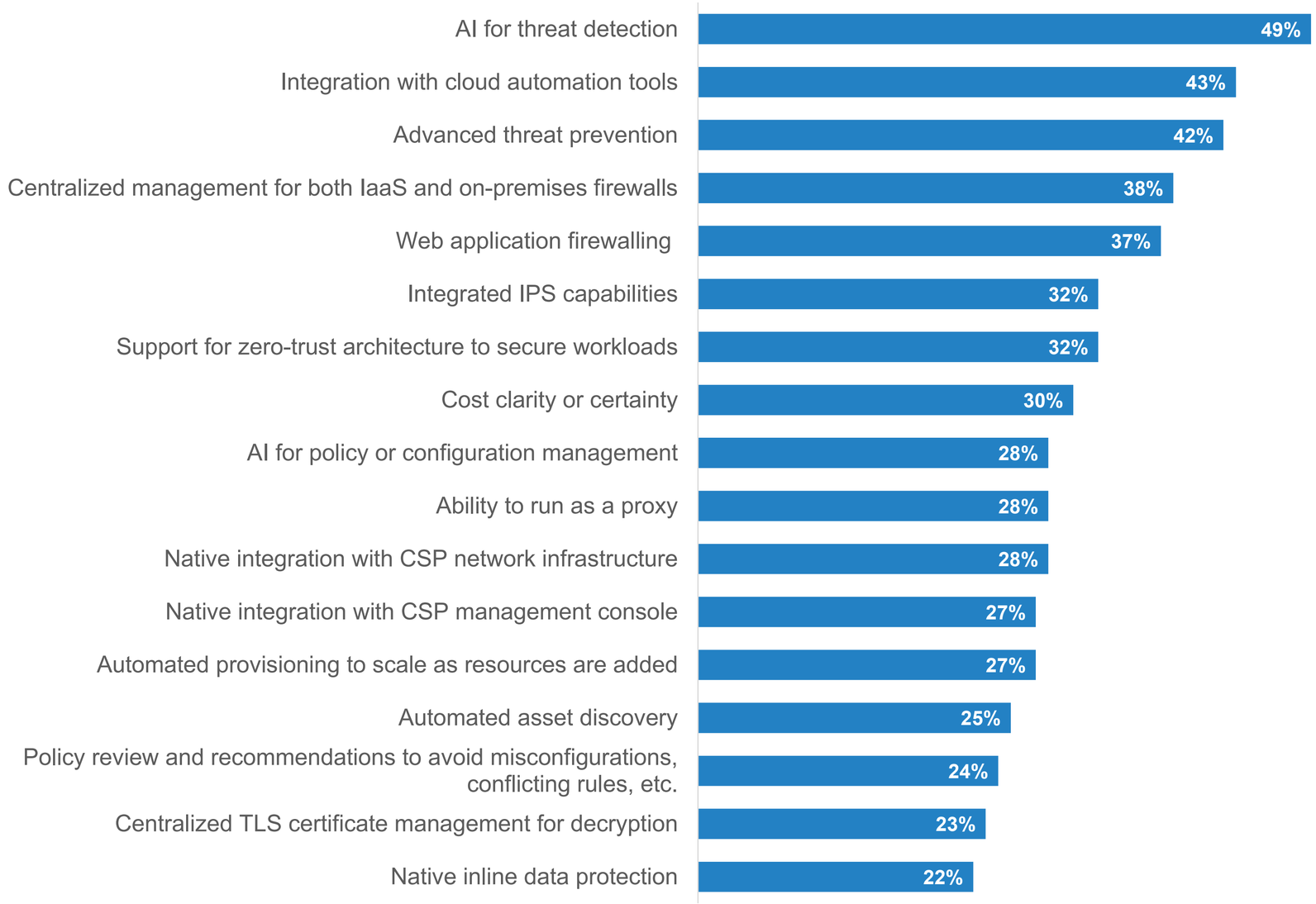
BACK TO CONTENTS

Top Attributes for Network Security Tools Protecting Public Cloud Infrastructure

While there is a long list of attributes respondents look for in network security tools protecting public cloud infrastructure, two key themes stand out. First, security is critical. Nearly half (49%) wanted AI for threat detection, 42% cited advanced threat protection, 37% selected web application firewalling, 32% noted the importance of integrated IPS, and 28% valued the ability to run as a proxy.

At the same time, usability is important. Integration with cloud automation tools was cited by 43% of respondents, centralized management for both IaaS and on-premises firewalls by 38%, and AI for policy or configuration management by 28%. Additionally, native integration with CSP network infrastructure was cited by 28%, native integration with CSP management consoles by 27%, and automated provisioning by 27%.

Important capabilities for network security tools protecting public cloud infrastructure environments.



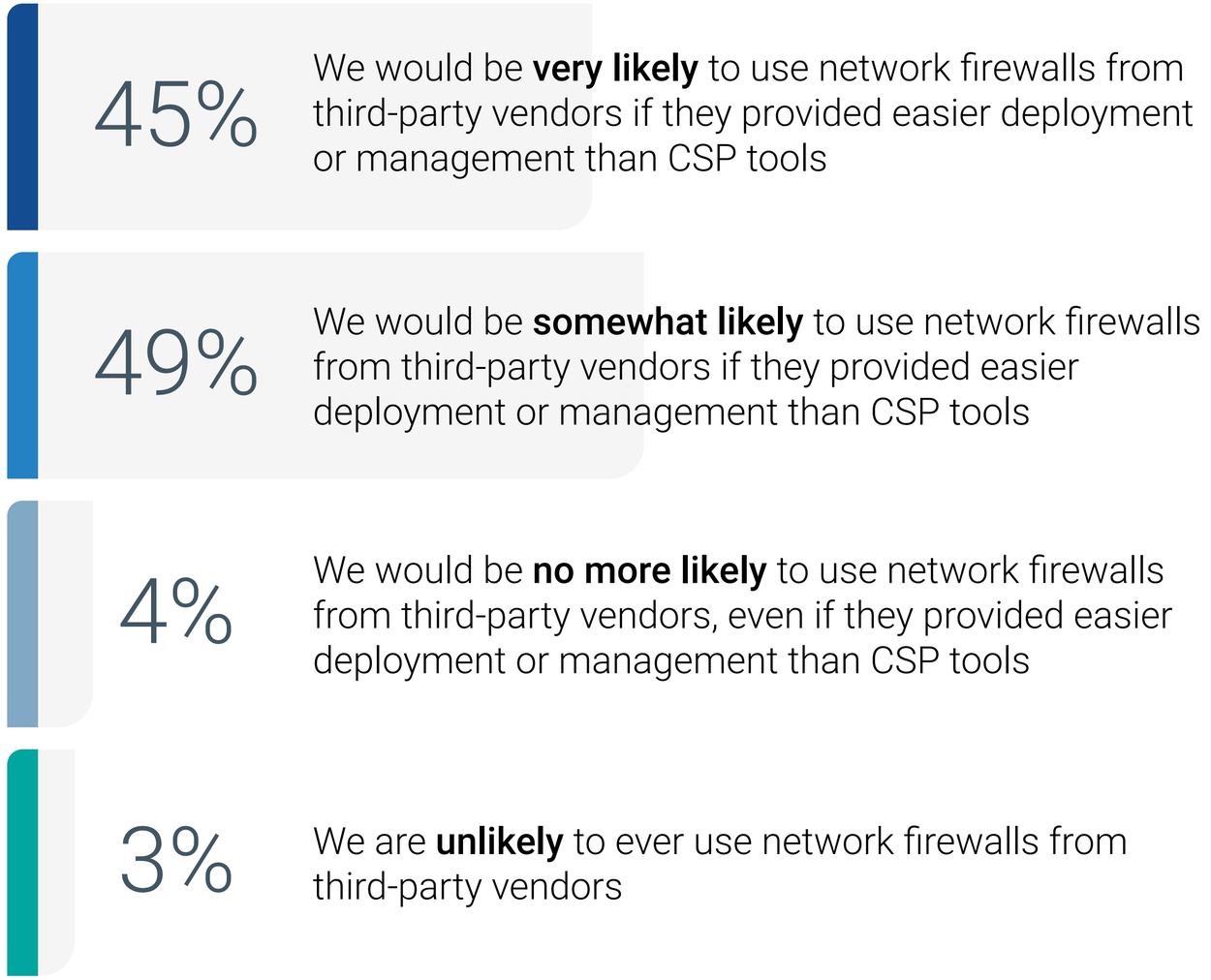
BACK TO CONTENTS

Strong Agreement That Ease of Use Would Drive More Usage of Third-party Firewalls

Historically, one knock against using third-party firewalls for securing public cloud infrastructure was the need to manually provision, configure, and deploy the firewall and supporting infrastructure, such as load balancers. In comparison, because CSP firewalls are natively integrated with the underlying infrastructure, the provisioning, configuration, and deployment is much more automated.

However, based on the top firewall attributes previously discussed, strong security is clearly a priority. As a result, there was near universal agreement among respondents not currently using third-party firewalls on the impact better ease of use would have on their firewall preferences. Specifically, 45% said they'd be very likely to use network firewalls from third-party vendors if they provided easier deployment or management than CSP tools, while 49% said they would be somewhat likely to use them under those circumstances. Only 3% said they are unlikely to ever use network firewalls from third-party vendors, so there does appear to be a desire for coupling ease of use and strong security.

Likelihood of using third-party vendors for network firewalls.



BACK TO CONTENTS

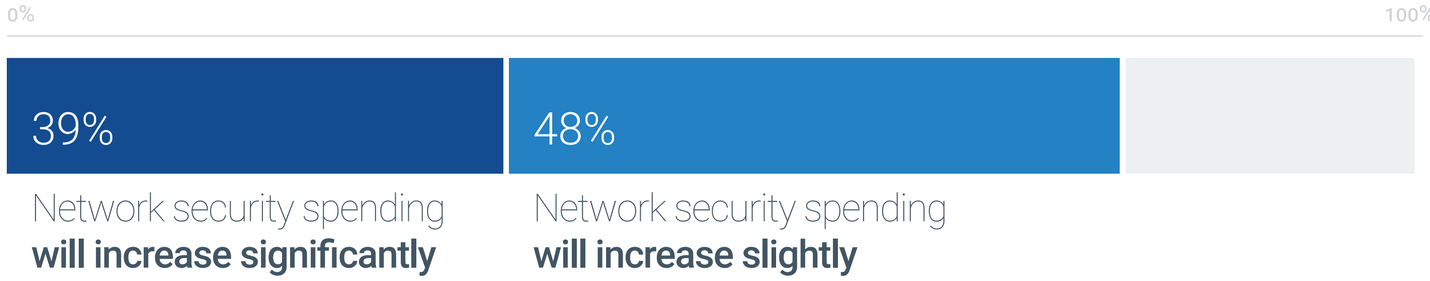
Spending Increases Are Expected Across Many Tools, but Firewall Vendor Consolidation Is a Focus

Cloud-native Firewalls Expected to See Spending Increases

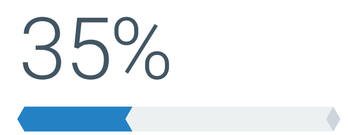
Overall, spending for network security technologies, services, and personnel for on-premises data center and public cloud infrastructure is expected to increase over the next 12-18 months. More than a third of respondents (39%) expect spending to increase significantly, while 48% expect spending to increase slightly. No respondents believe spending will decrease.

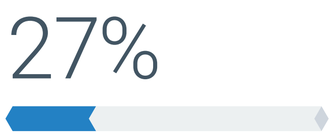
Of the many areas respondents foresee increased spending in, cloud-native firewalls were at the top of the list (44%). Cloud-native firewalls are fairly new, but because they solve some of the top challenges organizations face with public cloud infrastructure security, interest is high. They are powered by third-party providers to offer strong security capabilities but are natively integrated into the CSP infrastructure and management console to allow faster deployment, auto-scaling, and automated infrastructure provisioning.

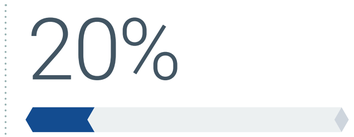
Firewalls from CSPs (41%), from third-party vendors (35%), and for container environments (34%) are also expected to see spending increases as security teams work to secure both cloud-resident and cloud-native applications.



Network security controls earmarked for increased spending over the next 18-24 months.







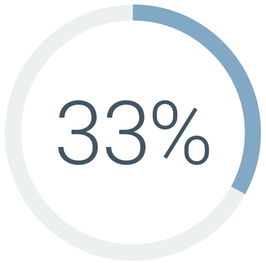
BACK TO CONTENTS

Firewall Consolidation Is Top of Mind

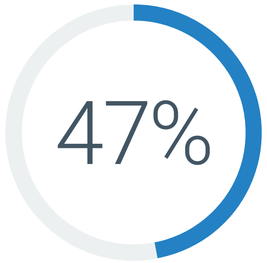
While no single firewall technology clearly stands above the rest in terms of use or anticipated spending, respondents clearly relayed the importance of firewall vendor consolidation. One-third indicated that consolidating firewall vendors is a critical priority, and 47% said it is an important priority.

With hybrid, multi-cloud environments now a reality for the majority of organizations, vendors that offer tools that can provide strong security, ease of use, and consistency across multiple CSPs and on-premises data centers are critical.

Importance of consolidating the number of firewall vendors across hybrid cloud environments.

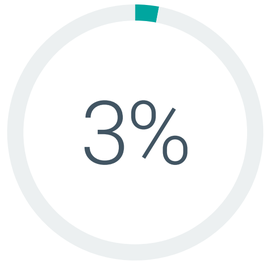


Consolidating firewall vendors is a critical priority



Consolidating firewall vendors is an important priority

Consolidating firewall vendors is an action we will take but is not a priority



Consolidating firewall vendors is not something my organization is considering

"One-third indicated that **consolidating firewall vendors is a critical priority**, and 47% said it is an important priority."

BACK TO CONTENTS

Public Cloud Network Security Is Cross-functional, and Most Are Working to Improve Collaboration

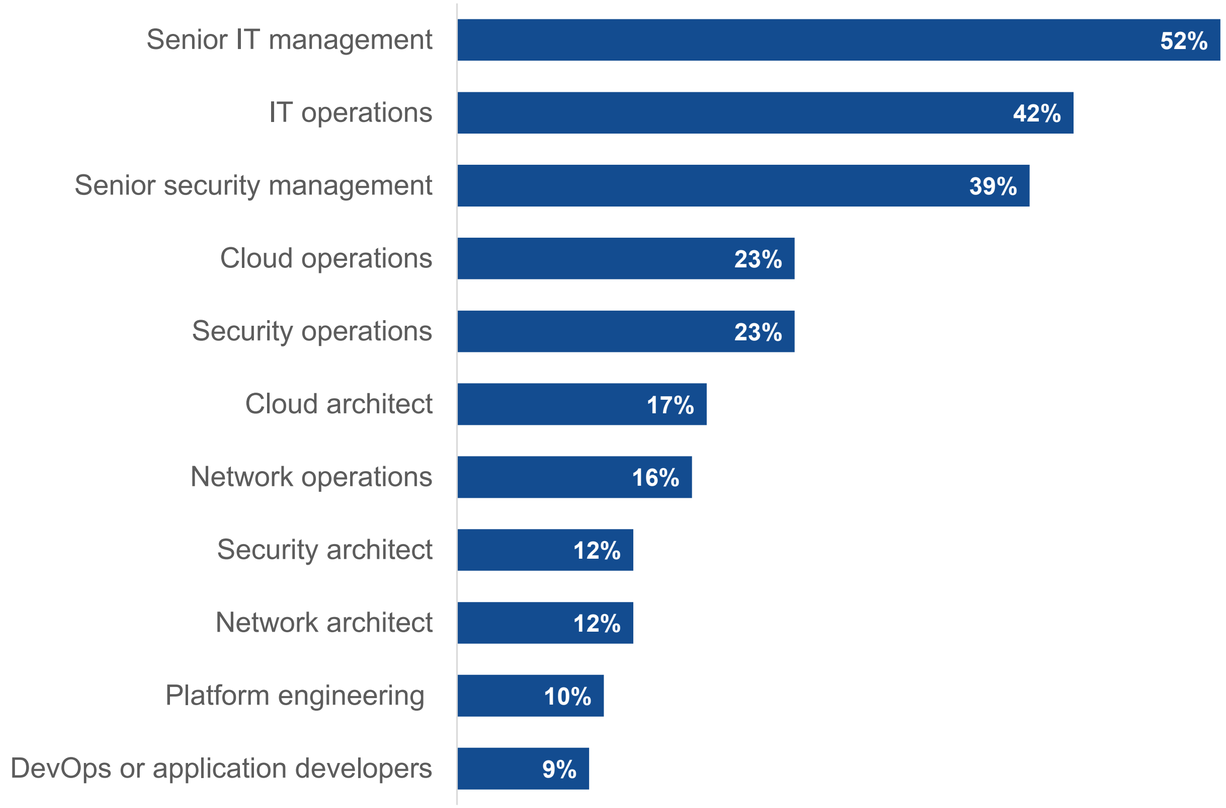
A Variety of Roles Are Expected to Become More Involved

As always, cybersecurity is about more than tools. From a people perspective, respondents provided somewhat conflicting thoughts on their organizations. Nearly nine in ten (89%) said the team responsible for public cloud infrastructure network security is the same team that is responsible for on-premises data center and private cloud network security.

At the same time, other roles are expected to have more input into public cloud infrastructure network security decisions over the next 12-24 months. IT operations (42%), cloud operations (23%), and cloud architects (17%) were some examples. Additionally, while 60% of respondents said their organization has a platform engineering practice, only 10% believed this team would have more network security input moving forward.

The team most responsible for our organization's public cloud infrastructure network security is also responsible for on-premises data center/private cloud network security

Roles expected to have more input into network security decisions for public cloud infrastructure over the next 12-24 months.



BACK TO CONTENTS

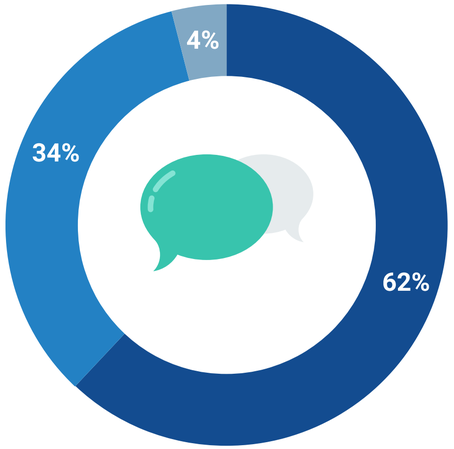
Collaboration Is Strong, but Most Are Taking Multiple Steps to Improve

The good news is that most respondents (62%) rate the level of collaboration on network security for public cloud infrastructure as very good, working most of the time. Yet they continue to strive to improve. Only 4% of respondents said they were taking no steps to improve collaboration on public cloud infrastructure network security.

Among the organizations that are working to improve, a number of steps are being taken. These range from process optimization and better alignment to organizational changes. Specifically, more than half (54%) said they are improving workflows, 51% are increasing meeting and collaboration frequency, and 43% are aligning goals and KPIs.

On the other hand, 37% are creating hybrid roles that span disciplines, and 36% are staffing a multifunctional center of excellence or CloudOps team. While these steps may not be necessary for every organization, it can be beneficial to understand the type of changes others are making.

Effectiveness of collaboration between the different groups responsible for evaluating and selecting network security tools for public cloud infrastructure.



- Very good, works most of the time
- Good, works some but not all of the time
- Fair, works OK but there are known problems

Steps being taken to improve collaboration across the teams and roles responsible for network security.

54%

Improving workflows for collaborative processes

51%

Increasing the frequency with which these teams meet and collaborate

43%

Improving alignment of goals and KPIs

37%

Creating hybrid roles that span disciplines

37%

Improving compensation alignment

36%

Staffing a dedicated multifunctional cloud center of excellence or CloudOps team

BACK TO CONTENTS

ABOUT

Cisco has long established itself as the networking leader, while building an open, integrated portfolio of cybersecurity solutions along the way. Cisco Security is built on the principle of better security, not more. We deliver a streamlined, customer-centric approach to security that ensures it's easy to deploy, easy to manage, and easy to use — and it all works together to increase your resilience. Because people and our customers are at the heart of what we do, Cisco Security empowers the security community with the reliability and confidence that they're safe from threats now and in the future.

We help leading organizations around the globe protect what's now and what's next with the most comprehensive, integrated cybersecurity platform on the planet. Learn more about how we simplify experiences, accelerate success, and protect futures at cisco.com/go/secure.

Cloud Visibility Report

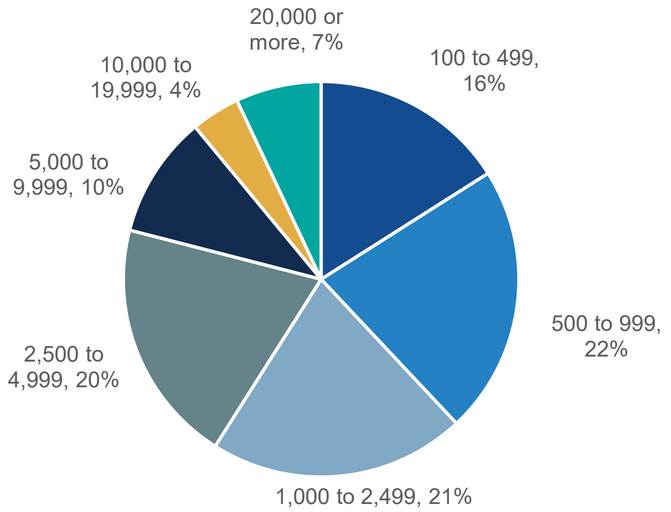
Cisco Secure Firewall

RESEARCH METHODOLOGY AND DEMOGRAPHICS

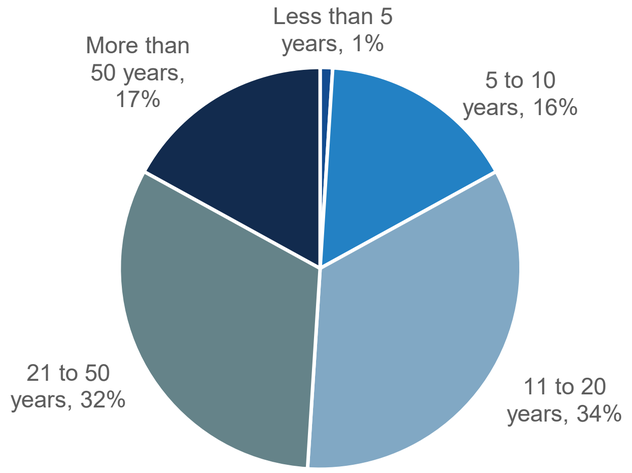
To gather data for this report, TechTarget's Enterprise Strategy Group conducted a comprehensive online survey of IT and cybersecurity professionals from private- and public-sector organizations in North America between April 18, 2024, and May 17, 2024. To qualify for this survey, respondents were required to be involved with their organization's network security technology and processes. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 358 IT and cybersecurity professionals.

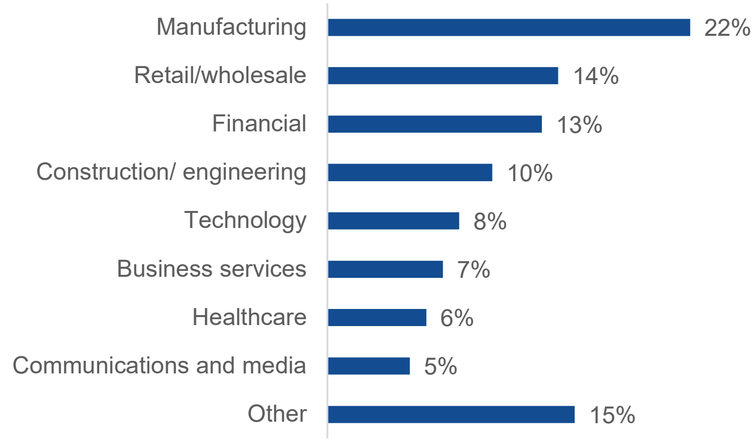
Respondents by number of employees.



Respondents by age of organization.



Respondents by industry.



BACK TO CONTENTS

Enterprise Strategy Group™
by TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm providing market intelligence, actionable insight, and go-to-market content services to the global technology community.