Enterprise Strategy Group™
by TechTarget

Looking to Modernize Network Security on Public Clouds?

Consider a Cloud-native, Managed Firewall Service

By John Grady, Enterprise Strategy Group Senior Analyst

DECEMBER 2022

ABSTRACT

Nearly all organizations use public cloud services, but many continue to struggle with how best to secure their infrastructure-as-a-service environments. The range of tools available from cloud service providers and security vendors has only complicated the issue. While security and cloud teams have traditionally been forced to choose between ease of use and best-in-class security, managed, cloud-native firewalls from trusted third-party providers can offer the best of both worlds. To deliver this, they must deliver enterprise-grade security, simplicity, and flexibility.

CONTENTS

Introduction

Organizations continue to shift resources to the cloud for a variety of reasons. This creates challenges, including maintaining proper configurations, securing cloud-resident data, and ensuring proper identity management. Yet, from an attack standpoint, attackers continue to use established on-premises tactics to target cloud environments. Thus, despite some questioning the role of network security in a cloud-first world, the firewall remains a foundational component to security strategies.

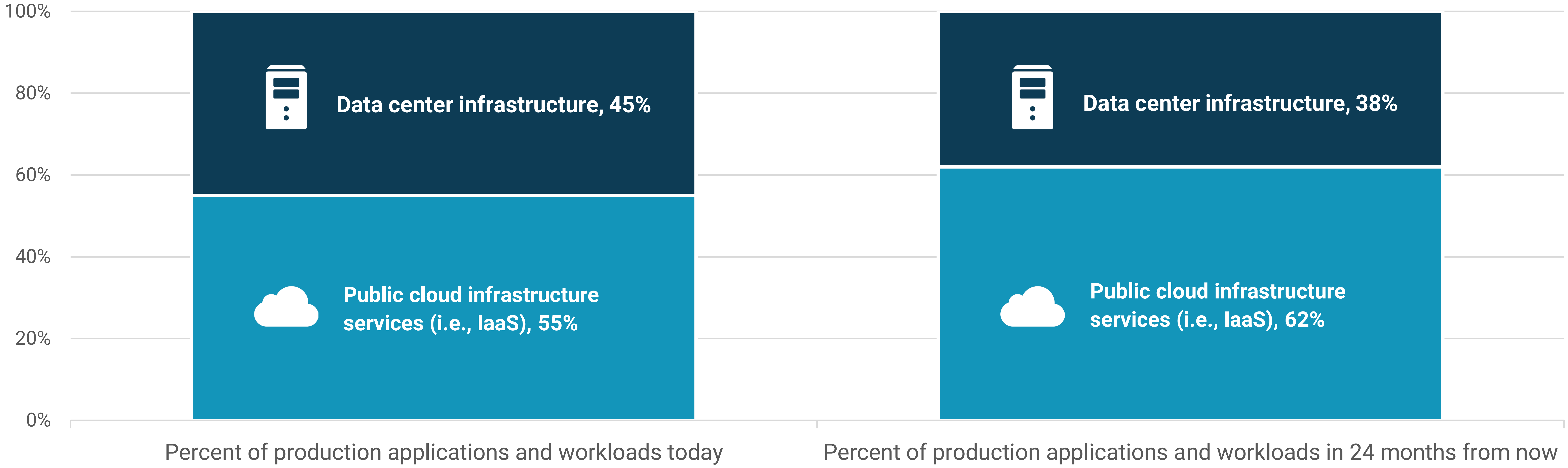
Security teams have typically had two options with regard to firewalls in the cloud: use the virtual machines provided by third-party vendors or use the firewalls offered by the cloud service provider (CSP) themselves. Both options offer benefits as well as drawbacks. Third-party tools are well established from a security perspective but were not purpose-built to scale in elastic environments. Conversely, CSP firewalls are easy to deploy and manage but may not offer the same advanced security options available in on-premises tools. Ultimately, security teams need the best of both worlds to protect modern hybrid cloud environments at scale.

IaaS Security Challenges Persist

Many organizations continue to prioritize the shift to the cloud. Global events of the last few years have forced organizations to emphasize scalability, agility, and resiliency requirements. The need to digitally transform business operations is leading many organizations to adopt cloud-first policies in which new applications are deployed using public cloud services unless there is a compelling case to deploy it using on-premises resources. Research from TechTarget's Enterprise Strategy Group (ESG) has found that 46% of organizations now follow a cloud-first policy.[1]

As a result, the balance of application workloads has shifted noticeably toward the cloud. Specifically, ESG research respondents indicated that 55% of their application workloads run on public cloud infrastructure-as-a-service (IaaS) today, and they expect that to rise to 62% over the next 24 months.[2]

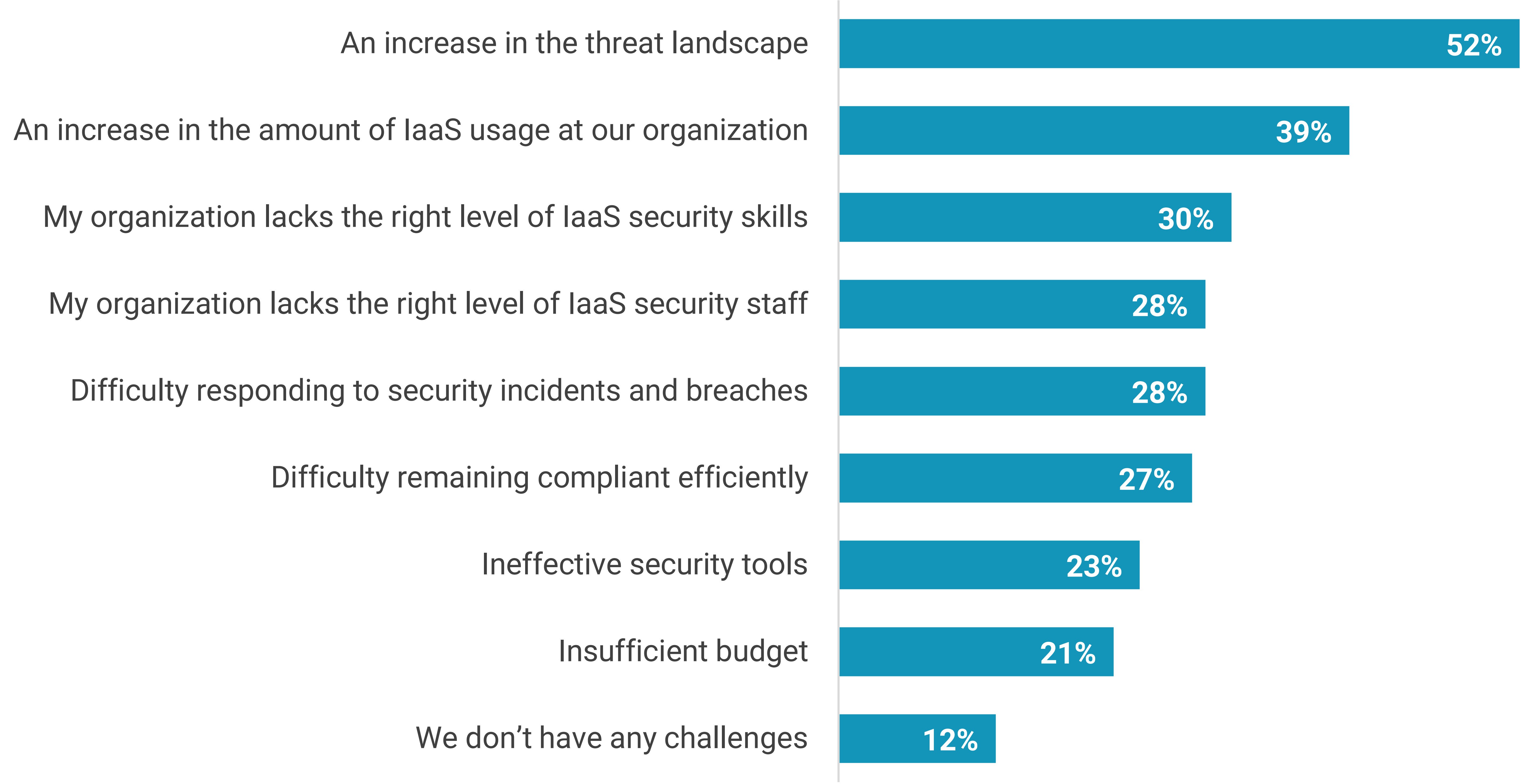
Figure 1. Where Workloads Reside



[1] Source: Enterprise Strategy Group Complete Survey Results, 2023 *Technology Spending Intentions Survey*, November 2022.
[2] Source: Enterprise Strategy Group Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, December 2021.

> “88% of organizations report challenges **securing their public cloud IaaS environments.”**

Figure 2. Public Cloud Infrastructure Security Challenges



While there are obvious benefits to shifting resources to the cloud, this transition does come with challenges, as well. Overall, ESG research has found that 88% of organizations report challenges securing their public cloud IaaS environments.[3] The threat landscape obviously plays a significant role in this, but there are internal issues many organizations must contend with as well. The scale of IaaS usage can become a problem, especially when security is not incorporated from the start. The speed at which IT and development teams operate in the cloud can be difficult for traditional security tools and processes to match. Additionally, the decentralization of control away from the IT organization can leave security teams unaware of corporate resources that are cloud-resident.

Cloud-native architectures drive fundamentally different requirements from a security perspective, and teams that are used to managing on-premises environments can find themselves overwhelmed and unprepared.

Finally, the tools available to secure IaaS environments and their associated cost can pose a challenge. Many security vendors have attempted to shift their existing on-premises offerings to the cloud. The ephemeral nature and specific networking requirements of cloud resources can mean additional configuration and policy management for security teams. At the same time, these tools are often not cost-optimized for cloud environments, which can create issues given budget constraints.

[3] Source: Enterprise Strategy Group Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, December 2021.

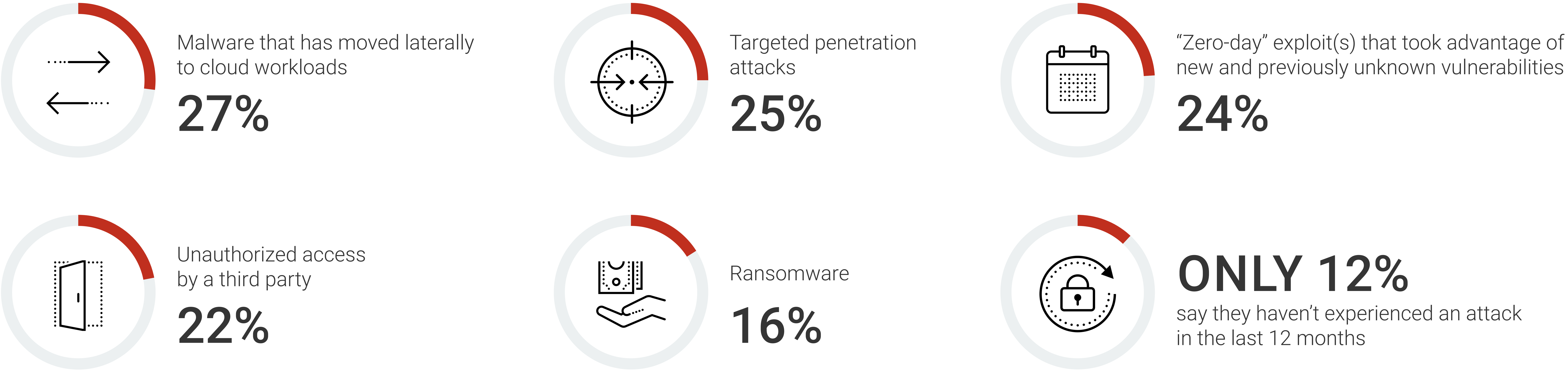
BACK TO CONTENTS

Attackers Target Cloud Environments

As noted, the threat landscape is of particular concern, as attackers have evolved their strategies and begun to exploit gaps in cloud defenses. Overall, 88% say they have experienced a cybersecurity incident specifically related to cloud-native applications and infrastructure.[4] Attacks targeting identities and configurations often receive significant attention when it comes to cloud environments, resulting in a wave of cybersecurity startups focused on these issues.

However, more traditional attacks that target cloud environments remain extremely common, as well. Many attacks continue to rely on malware, and ransomware specifically is increasingly being focused on cloud resources. Similarly, targeted and zero-day attacks remain prevalent. Even foundational issues, such as unauthorized access, continue to occur in cloud environments. So, while, in some ways, IaaS environments are very different from on-premises locations, they do ultimately require many of the same protections historically deployed in the data center.

Figure 3. Threats to Cloud Environments



Malware that has moved laterally to cloud workloads
27%

Targeted penetration attacks
25%

“Zero-day” exploit(s) that took advantage of new and previously unknown vulnerabilities
24%

Unauthorized access by a third party
22%

Ransomware
16%

ONLY 12%
say they haven’t experienced an attack in the last 12 months

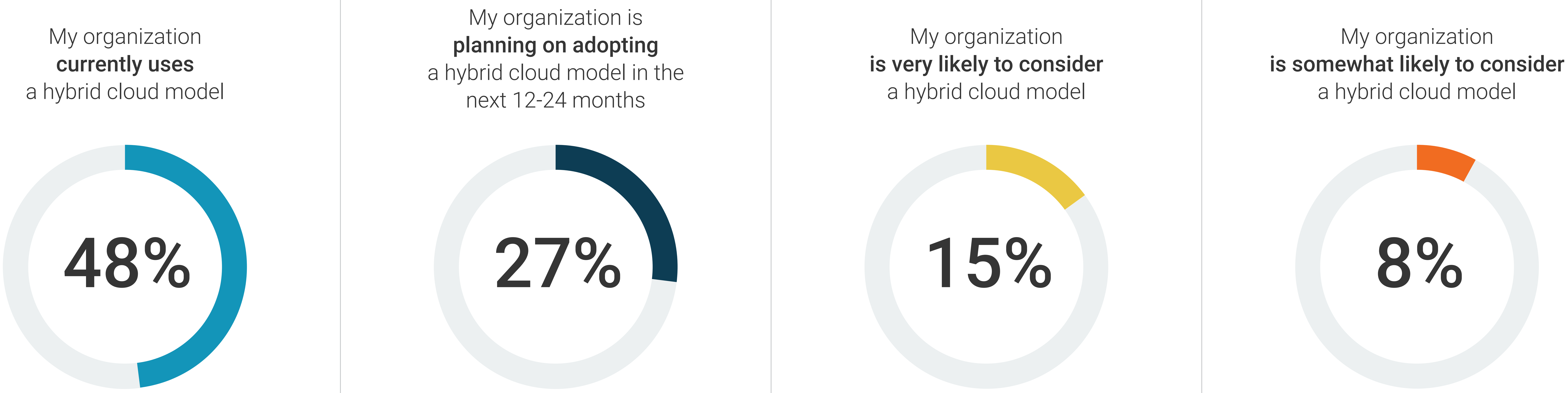
[4] Source: Enterprise Strategy Group Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.

Hybrid Environments Are a Reality for Many, Which Further Complicates the Issue

Even as organizations prioritize the shift to the cloud and the balance of application workloads tilts toward IaaS, the on-premises data center will not disappear. Yet, organizations don't expect to stand pat with existing strategies. Only 12% of organizations reported a desire to get out of the data center business completely, reflecting the fact that some applications and workloads may never make the jump to the public cloud.[5]

However, this is not to say that traditional data center approaches will survive but rather that many organizations will undertake a data center modernization strategy that combines shifting resources to the public cloud and investing to achieve a cloud-like experience on-premises. As this occurs, IT teams need to better integrate these parts of the environment through common management and orchestration. Nearly half of organizations today say they are currently using such a hybrid-cloud model, and an additional 42% are planning on adopting or are very likely to consider adopting one.[6]

Figure 4. Hybrid Adoption

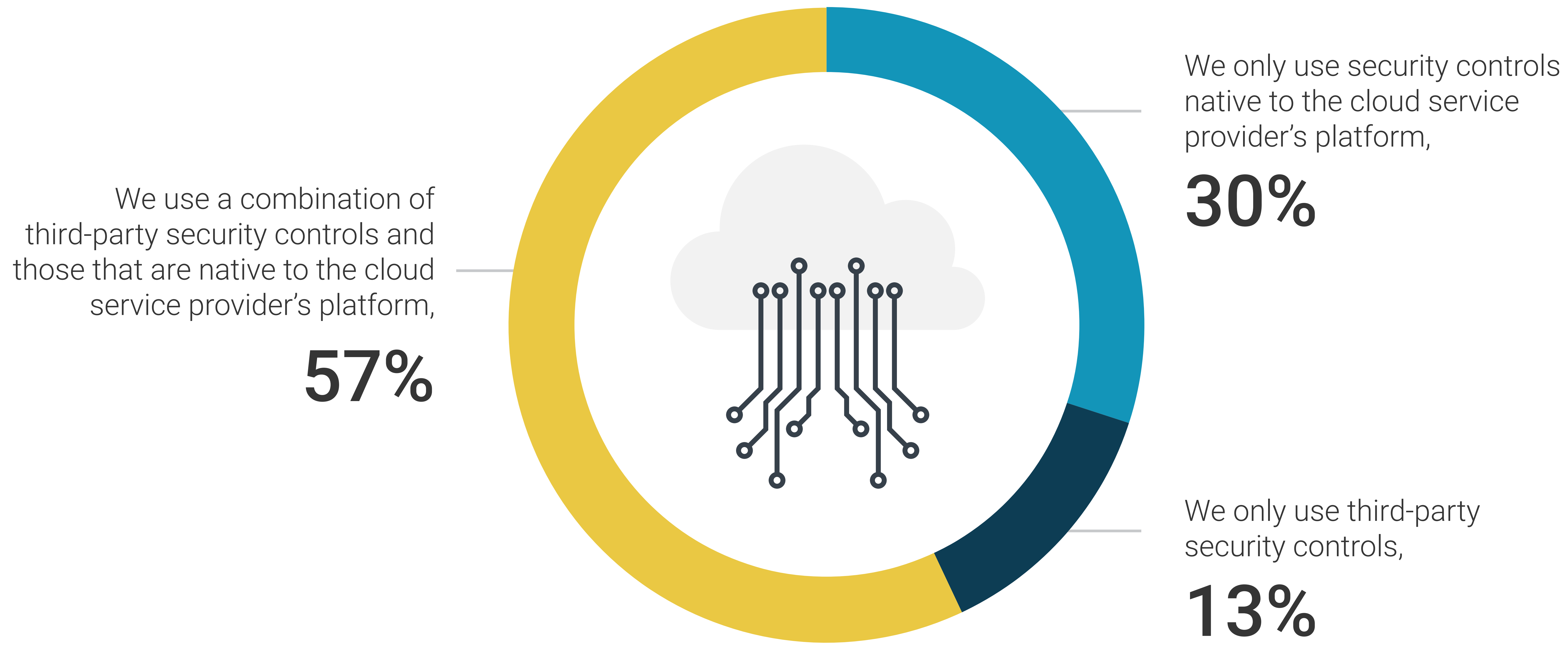


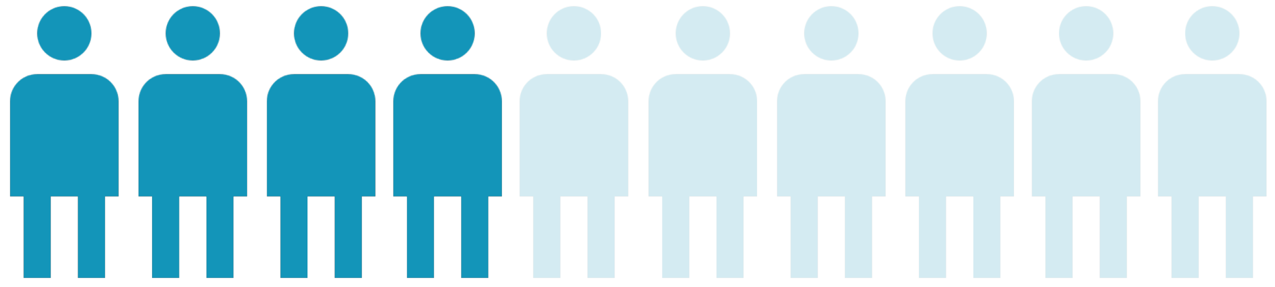
[5] Source: Enterprise Strategy Group Complete Survey Results, *Distributed Cloud Series: Application Infrastructure Modernization Trends*, March 2022.
[6] Source: Enterprise Strategy Group Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, December 2021.

BACK TO CONTENTS

Yet, while general orchestration and management across hybrid environments may be improving, security coordination often lags. Organizations that are very heavily weighted toward either centralized security oversight or a developer-led approach may lean toward a specific type of tool. Organizations with more centralized security oversight may have deployed virtual firewalls, while organizations that are more developer-led may be more likely to utilize CSP tools. However, the majority of organizations report using a combination of both third-party and CSP tools. This creates additional challenges, with 40% of Enterprise Strategy Group research respondents indicating that the use of multiple cybersecurity controls resulted in increased cost and complexity.[7]

Figure 5. Controls to Secure Cloud-native Applications





40%

of Enterprise Strategy Group research respondents indicated that the use of **multiple cybersecurity controls resulted in increased cost and complexity.**

[7] Source: Enterprise Strategy Group Survey Results, *The Maturation of Cloud-native Security: Securing Modern Apps and Infrastructure*, June 2021.

CSP Firewalls Can Offer Benefits but Do Have Limitations

Enterprise Strategy Group (ESG) has found that 66% of research respondents use network firewalls from cloud service providers to protect their public cloud infrastructure environments. There are clear reasons why some organizations prioritize these tools over traditional third-party virtual firewalls. Some of the most significant reasons include:[8]

1. EASE OF USE

Many cite ease of use as a reason for using CSP network security tools. Specifically, 48% use these tools due to their ease of management, and 46% use them for ease of deployment. Because they are native to the CSP, these firewalls are tightly integrated into the cloud infrastructure and management stack. Management often occurs directly in the cloud console, and policy may dictate that firewalls be deployed as new resources or virtual private clouds (VPCs) come online.

2. SCALABILITY

Closely aligned with ease of use is the scalability CSP firewalls offer, which was cited by 41% of organizations as a reason for using CSP tools. CSP firewalls are typically offered as a managed service, which automatically provisions infrastructure as needs change and firewall requirements expand.

3. ORGANIZATION AND SKILL ALIGNMENT

Organizations can sometimes struggle to manage third-party tools as they restructure to support more cloud-centric and cloud-first models. If cloud operation and infrastructure teams are responsible for security provisioning, they may be more comfortable with cloud-native tools over third-party options. Nearly half of ESG research respondents (44%) cited alignment with organizational structure as a reason for using CSP firewalls.

[8] Source: ESG Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, December 2021.

BACK TO CONTENTS

Limitations

At the same time, CSP firewalls do have three key limitations:

1. LIMITED SECURITY

CSP firewalls are often focused more on access control than threat prevention. They operate at Layer 4 with rules based on source and destination IP addresses, ports, and protocols. Typically, these firewalls do not offer intrusion prevention (IPS), sandboxing, or advanced malware detection functionality. Even when they do, custom work is required to maintain up-to-date signatures for effectiveness.

2. SINGLE CLOUD FOCUS

As discussed, most organizations are managing infrastructure across multiple locations. CSP firewalls provide control over their own cloud environment and do not secure on-premises or multi-cloud deployments. This may be less of an issue for organizations that have standardized on a single cloud provider or have a limited on-premises footprint, but for other organizations, this fact can contribute to tools sprawl and lead to additional complexity.

3. COST

Pricing models can be complex and expensive. Users often must pay for one or more firewall instances for every cloud virtual network they operate. In addition, they are charged for the time the firewall instances are operational, as well as the amount of traffic processed by those firewall instances.

BACK TO CONTENTS

Requirements for Third-party, Cloud-native Firewalls

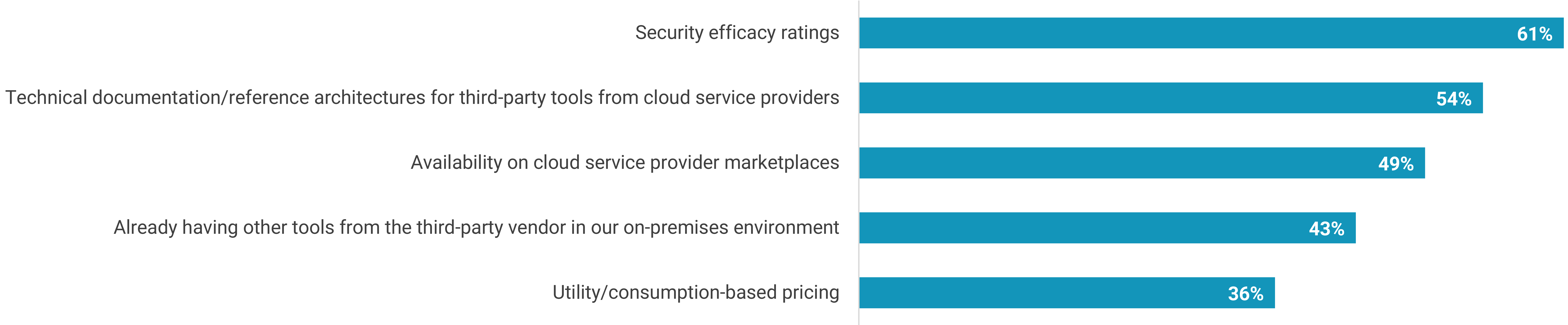
To this point, organizations have had to make choices and tradeoffs when it came to cloud network security. What security teams need is the best of both worlds: the security and consistency provided by third-party firewalls, paired with the ease of use and simplicity of CSP firewalls. This requires enterprise-grade security, simplicity, and adaptability.

As the lines between different parts of the infrastructure have blurred and attackers have increasingly targeted cloud resources, security teams require the same level of functionality and efficacy in the cloud as they do on-premises. The ability to accurately block advanced attacks in the cloud is now foundational.

At the same time, third-party tools must be deeply integrated with CSP management consoles and infrastructure to simplify management and improve scalability. Availability on the CSP marketplace is also critical to streamline procurement.

Finally, third-party firewalls should offer the adaptability to address different needs and use cases. Rather than just filtering inbound and outbound traffic, third-party cloud-native firewalls should offer east-west protection, as well, to protect against threats moving between VPCs. Further, third-party firewalls should follow the same consumption-based pricing model that the cloud itself provides so that organizations only pay for the security they actually use. Lastly, one of the key benefits of using third-party tools is the integration across different parts of the environment. Yet, while this can help ensure consistent security and a lower total cost of ownership (TCO), supporting both centralized and cloud-native management options can help ensure that different roles have the tools they need to operate successfully.

Figure 6. Considerations For Third-party Solutions[9]



[9] Source: ESG Complete Survey Results, *Network Security Trends in Hybrid Cloud Environments*, December 2021.

Fortinet FortiGate Cloud-Native Firewall Service on AWS

Fortinet has long offered virtual instances of its FortiGate next-generation firewalls on AWS. Its recent release of the FortiGate Cloud-Native Firewall (FortiGate CNF) provides a managed Firewall-as-a-Service (FWaaS) option for organizations that currently use FortiGate NGFWs on-premises or in the cloud and want a cloud-native option or cloud-first organizations that have been hesitant to add third-party firewalls to their environment. FortiGate CNF provides advanced network protection at any scale and at an optimized cost without any infrastructure management on AWS Cloud. Key benefits of FortiGate CNF include:

ADVANCED SECURITY

FortiGate CNF offers the same NGFW protection as existing FortiGate products. It provides Layer 7 protection and includes URL and DNS filtering, intrusion prevention, IP reputation, and botnet/command and control protection. The service is supported by FortiGuard Lab's Global Threat Intelligence, which leverages artificial intelligence and machine learning, along with Fortinet's global threat visibility to help block advanced attacks.

EASE OF USE

In addition to advanced security capabilities, FortiGate CNF supports ease of use in a variety of ways. The solution is available on AWS marketplace, making procurement simple and straightforward. FortiGate CNF is also a managed service, which offloads the need for security teams to coordinate provisioning and update activities. Further, integrations with AWS Gateway Load Balancer provide auto-provisioning and auto-scaling, while a single FortiGate CNF instance can support multiple availability zones and VPCs in an AWS region across multiple AWS accounts. From a policy perspective, Adaptive Security policies abstract away network dependencies, which makes the solution well suited for elastic workload environments.

FLEXIBILITY

To help organizations consume the service in the way that best suits their needs, FortiGate CNF provides three key areas of flexibility. First, the solution provides broad coverage by addressing the three main cloud network security use cases: inspecting outbound traffic, inspecting inbound traffic, and inspecting east-west traffic. Additionally, FortiGate CNF offers three management options. Security teams can use the FortiGate CNF console for both service and security policy management on AWS or use FortiManager for consistent security policy management across on-premises and AWS environments and use the FortiGate CNF console for service management. Another option is to use the FortiGate Console for security policy management and use AWS Firewall Manager to automate service management with cloud workflows. Finally, organizations can choose between annual or on-demand pricing options. In the on-demand model, users pay only for the specific hours of operation and amount of traffic that is scanned by each inspection engine. This offers a substantial difference over alternatives that charge based on the capabilities that are available, rather than what is actually used.

The Bigger Truth

Every organization is different, which often means that broad, sweeping recommendations are not actionable for many users. Yet, in some cases, even when these differences are accounted for, the recommendation can remain relevant for the majority. The case for third-party, cloud-native firewalls is certainly an example of this. Regardless of whether an organization is a multi-national corporation with a significant hybrid cloud footprint, a large cloud-first enterprise, or a smaller born-in-the-cloud organization that prioritizes security, third-party, cloud-native firewalls are an attractive option.

Nearly all companies struggle with skills, staffing, and maintaining efficiency. Security teams across all company types also must support different use cases and stakeholders. Cybersecurity is now a business imperative with executive oversight. All these factors highlight the need for network security options in the cloud that offer enterprise-grade security, simplicity, and flexibility. Fortinet's FortiGate Cloud-Native Firewall delivers on these needs, providing advanced network protection at any scale.

LEARN MORE

FORTINET®

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.