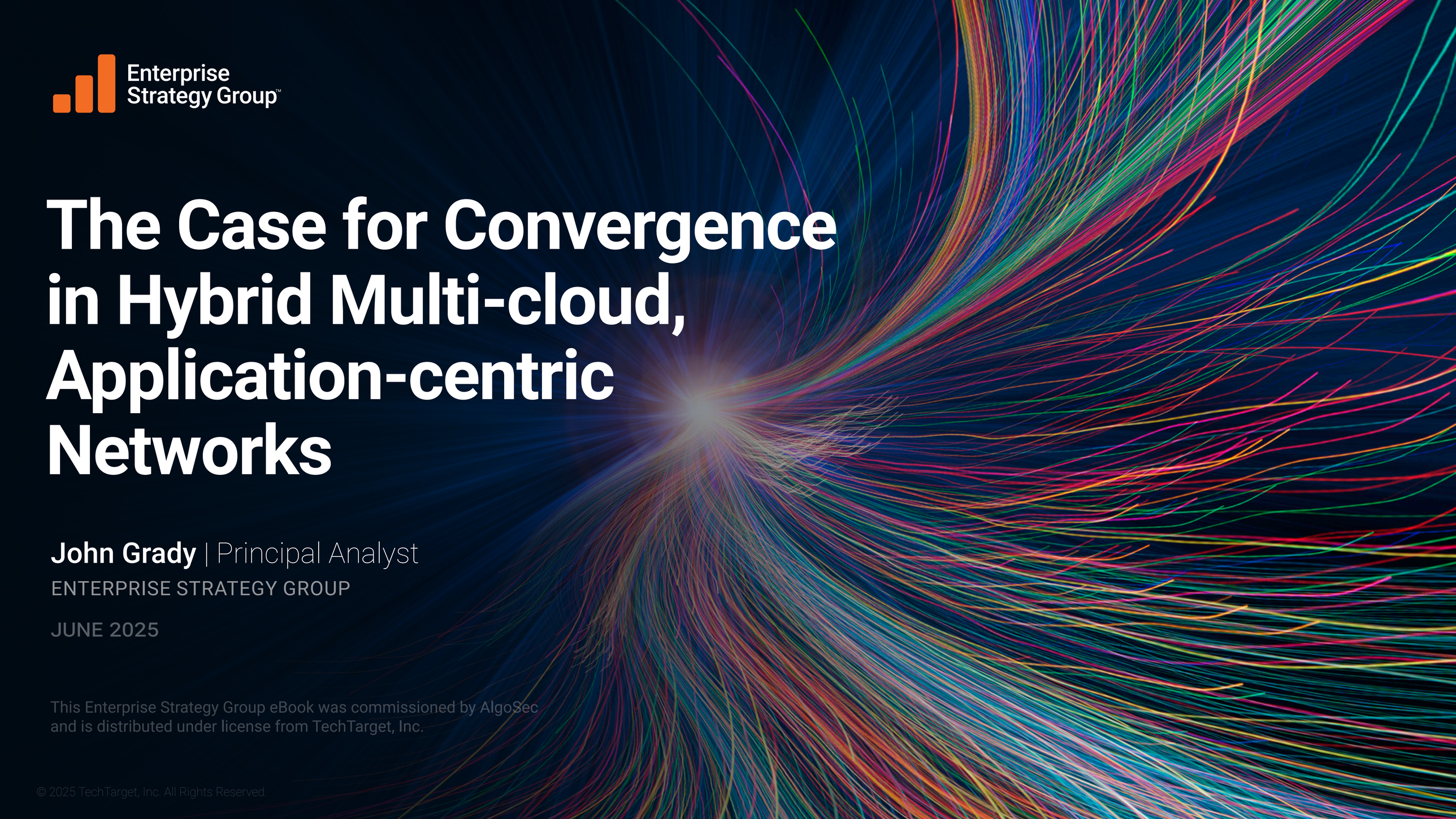


Enterprise Strategy Group™

The Case for Convergence in Hybrid Multi-cloud, Application-centric Networks

John Grady | Principal Analyst

ENTERPRISE STRATEGY GROUP

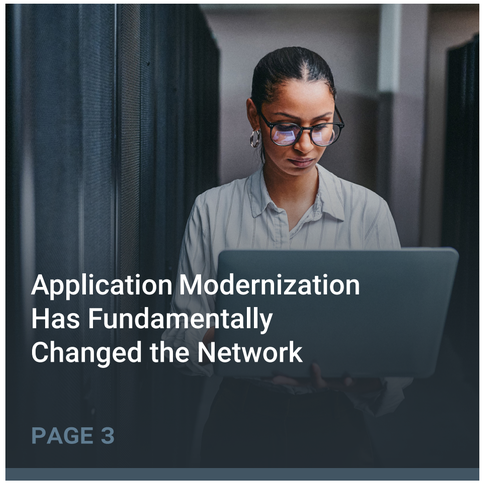
JUNE 2025

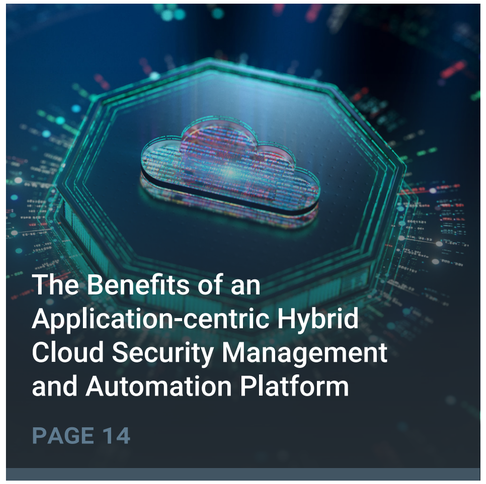
This Enterprise Strategy Group eBook was commissioned by AlgoSec and is distributed under license from TechTarget, Inc.

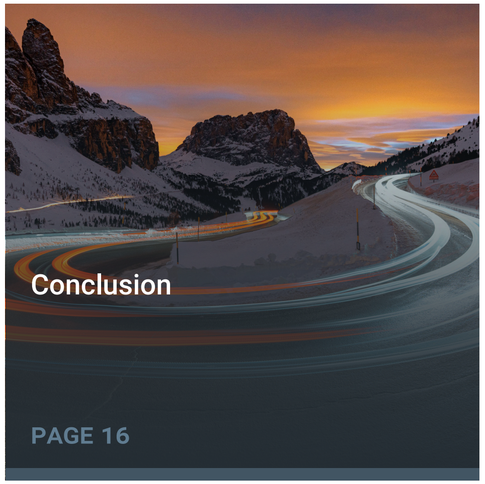
Introduction

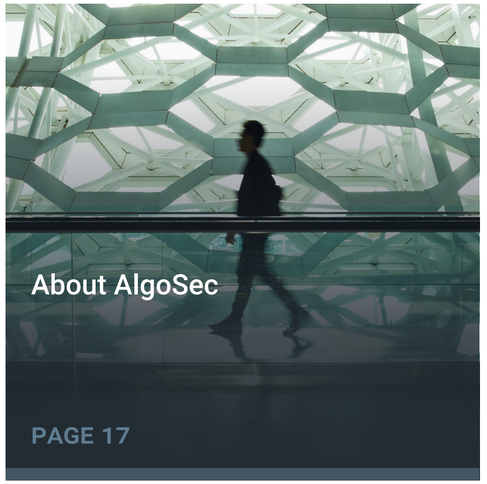
Modern enterprise IT environments are more distributed and dynamic than ever before, with resources spanning on-premises data centers and multiple cloud providers. The traditional silos between cloud and on premises from a security tool, team, and process perspective no longer meet the realities today's enterprises face. As security responsibility has begun to be distributed across different groups, it has become imperative to converge the technology and teams charged with ensuring network security. With applications now being central to many, if not most, business processes, and the network serving as a delivery mechanism for these applications, taking an application-centric, converged hybrid multi-cloud network security approach can help security teams realize both their security and business objectives.

CONTENTS









BACK TO CONTENTS

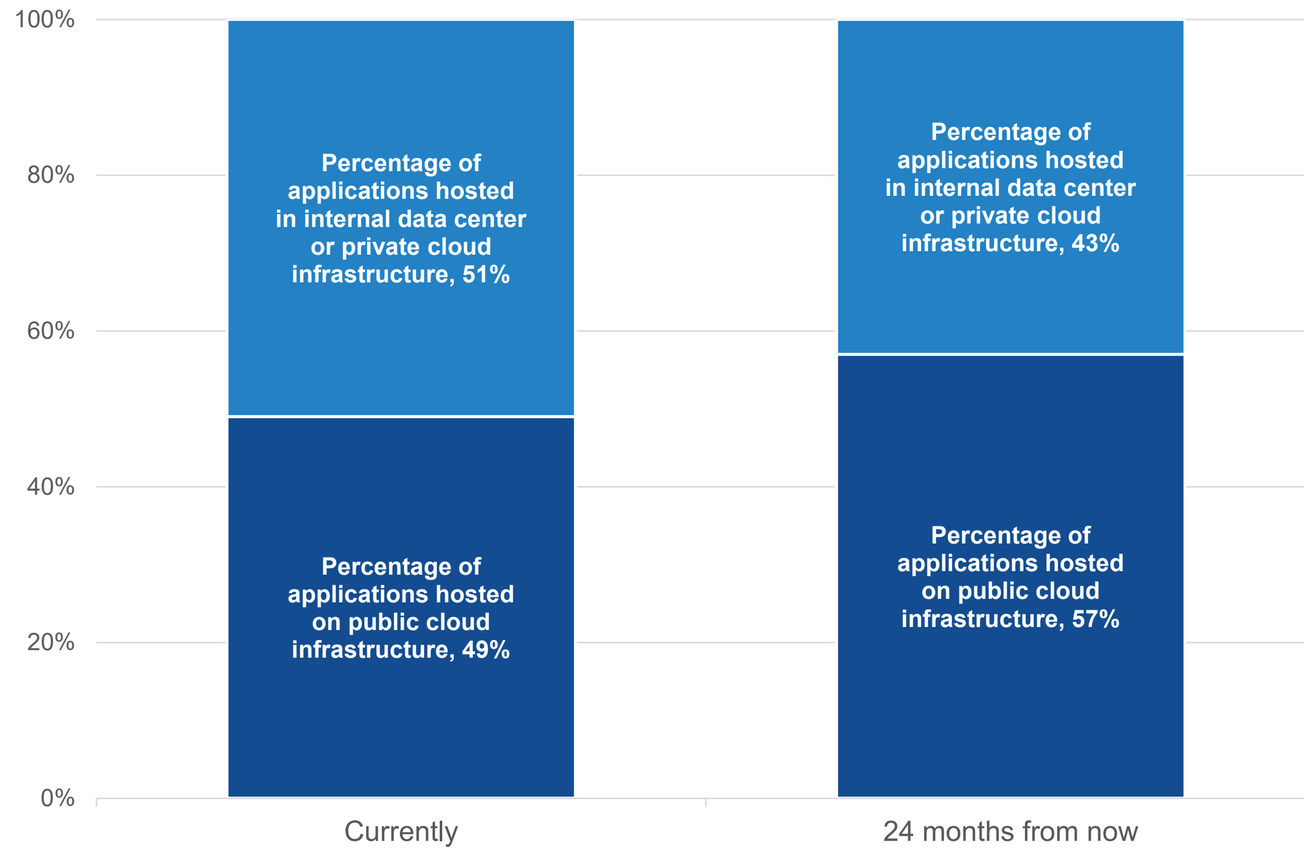
Application Modernization Has Fundamentally Changed the Network

Applications Are Numerous and Distributed Across Hybrid Environments

Applications have become central to how many organizations operate. Whether they are used for internal purposes, external engagement with customers or partners, or direct revenue generation, applications are now critical to a variety of business processes. As importance has risen, the number of applications used has as well. According to Enterprise Strategy Group research, 60% of organizations reported using at least 250 total production business applications across their environment.[1]

Developers continue to rely on cloud infrastructure to support this scale, optimize costs, and increase agility. As a result, many organizations have come to use multiple cloud service providers (CSPs). Enterprise Strategy Group research found that 85% of organizations reported using two or more CSPs.[2] Yet, while many organizations might follow a cloud-first policy, where new applications are deployed in the cloud rather than on premises by default, there remain those that take a case-by-case approach depending on the application and use case. Further, many on-premises applications, either due to their composition or the resources the organization has at its disposal, are expected to remain in traditional data centers for the foreseeable future. As a result, while the percentage of cloud-based applications is expected to grow from 49% to 57% over the next 24 months, 43% of applications will remain on premises. Subsequently, this leaves many organizations in a position where they must secure hundreds of applications across a distributed and diverse hybrid, multi-cloud environment.

Percentage of Applications Deployed on IaaS vs. On Premises.



[1] Source: Enterprise Strategy Group Research Report, *Application Modernization and the Role of Platform Engineering*, October 2024.
[2] Source: Enterprise Strategy Group Research Report, *The Evolution of Network Security*, October 2024. All Enterprise Strategy Group research references and charts in this eBook are from this report unless otherwise noted.

BACK TO CONTENTS

"Even when looking only at public cloud infrastructure, most organizations use **multiple tools from either CSPs, third-party firewall vendors, proxy vendors, or microsegmentation providers."**

Security Tool Fragmentation Complicates the Issue

For most organizations, the tools used to secure network infrastructure and applications are different, as are the tools used to secure on-premises data centers and public cloud infrastructure. Specifically, 89% of organizations agreed that the differences between cloud-native applications and the rest of their applications and infrastructure require a different set of security policies and technologies. At the same time, 90% said they would prefer to use the same network security vendors for cloud-native application environments as the rest of their environment.

Unfortunately, this is not realistic, in large part due to the different teams and personas involved across the organization. Even when looking only at public cloud infrastructure, most organizations use multiple tools from either CSPs, third-party firewall vendors, proxy vendors, or microsegmentation providers. The issue of policy consistency was raised earlier and becomes clearer as this picture of tool fragmentation comes into focus. It would be difficult for security teams to maintain consistency across one tool, let alone multiple tools across multiple clouds and applications, especially in the cloud, where application developers or cloud teams are likely to be responsible for configuration and security rule changes.

Tools Used to Protect Public Cloud Infrastructure.

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 tools

BACK TO CONTENTS

Hybrid, Multi-cloud Environments Create a Variety of Security Challenges

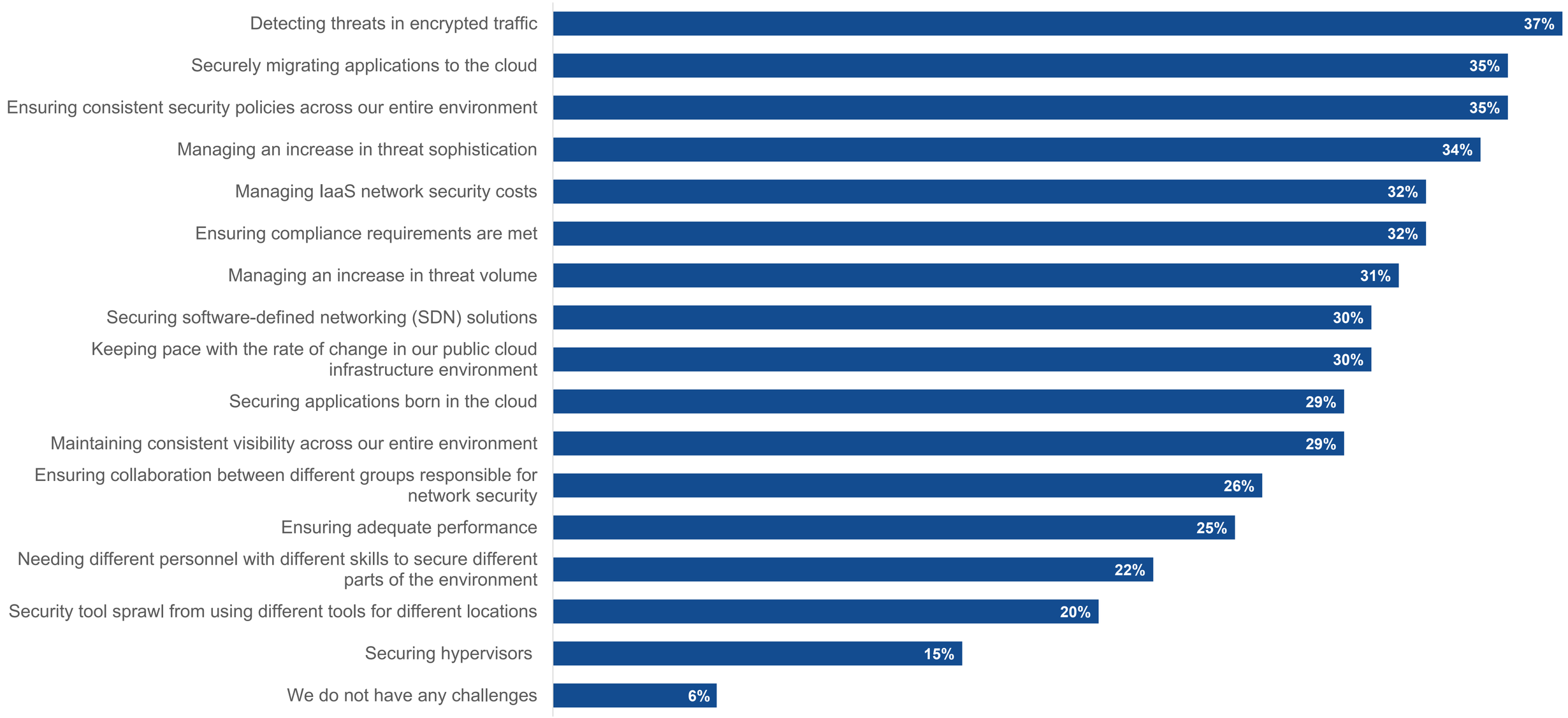
Security has never been easy. However, it can be argued that when all an organization's applications were centralized in a data center, the security team at least had an idea of what it needed to protect and more control over the infrastructure that applications were deployed on. In today's environment, the security team often does not have complete visibility into everything it needs to protect. Developers are often distributed throughout the lines of business, sometimes have the ability to deploy applications outside the purview of IT or security, and operate at a much faster pace than ever before.

From a security perspective, this leads to a variety of challenges. The threat landscape, both in terms of threat sophistication (34%) and threat volume (31%), remains among the top concerns for many organizations. But beyond that, there are a variety of challenges cited that highlight the issues security teams face with securing applications across hybrid multi-cloud environments. These include:

- **Securely migrating applications to the cloud (35%).** As noted, there is a steady stream of applications being moved to the cloud in many enterprise environments. Confidence in the ability to secure these applications as they are deployed plays a large role in how quickly organizations are willing to move.
- **Consistency of policies (35%) and visibility (29%).** As environments sprawl and different security tools are added, maintaining policy consistency can become very difficult. Similarly, aggregating and centralizing visibility data to understand the resources, traffic, and threats affecting entities across hybrid multi-cloud environments is difficult to scale when done manually.
- **Ensuring compliance (32%).** The global regulatory environment continues to grow in complexity. Maintaining and showing compliance across different locations and cloud providers can be incredibly burdensome and difficult if security and governance, risk, and compliance teams don't have a full view of where resources reside.
- **Keeping pace (30%).** Foundationally, security teams struggle to keep up with their cloud and application counterparts. Both tools and processes play a role in this, requiring security teams to think differently than they do in on-premises use cases.
- **Enabling collaboration (26%).** Relatedly, security responsibility has become distributed across not just the security team, but cloud, networking, and application teams as well.
- **Ensuring performance (25%).** While security teams are most concerned with preventing threats, they do (typically) understand that they can't impact the business. Ensuring that security solutions do not impact performance, which can degrade user experience, should be on the radar for all security teams, but only some cited it as a challenge.

BACK TO CONTENTS

Hybrid Cloud Security Challenges.



BACK TO CONTENTS

Many Organizations Are Experiencing Attacks

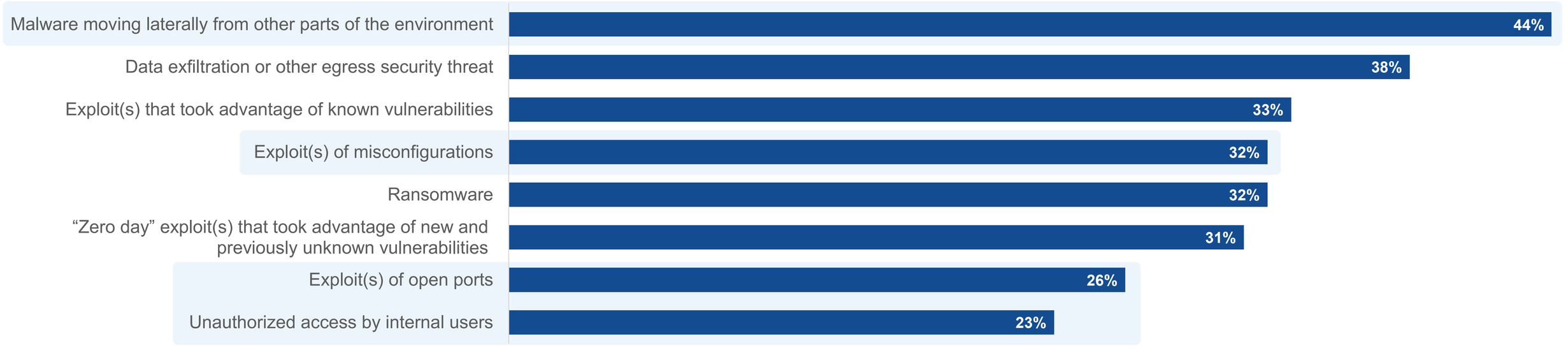
These issues are important not because of hypothetical threats but because organizations are being compromised. Specifically, 43% of organizations indicated they had experienced an attack on their public cloud infrastructure in the last 24 months. Nearly one-quarter (24%) indicated it occurred multiple times. Among the most common attacks experienced were:

Malware moving laterally from other parts of the environment (44%). This highlights the fact that attackers do not think in silos. They find the easiest point of entry and work their way to something of value. Weakness in any part of the environment can lead to a compromise elsewhere, especially if proper segmentation or zero-trust principles are not followed.

Exploits of misconfigurations (32%) and exploits of open ports (26%). Unforced errors are unfortunately an all-too-common cause of compromise. As discussed, the rate of change in modern environments and decentralization of security controls make it more likely that something will be missed, leaving an opening for attackers.

Unauthorized access by internal users (23%). Finally, while external threats are often top of mind, curious and malicious insiders also represent a risk. Ensuring least privilege is enforced and application access is limited to what is needed to perform one's role are best practices but can be difficult to implement at scale given all the issues previously mentioned.

Types of Attacks on Public Cloud Infrastructure.



BACK TO CONTENTS

How to Update Network Security Practices to Keep Pace

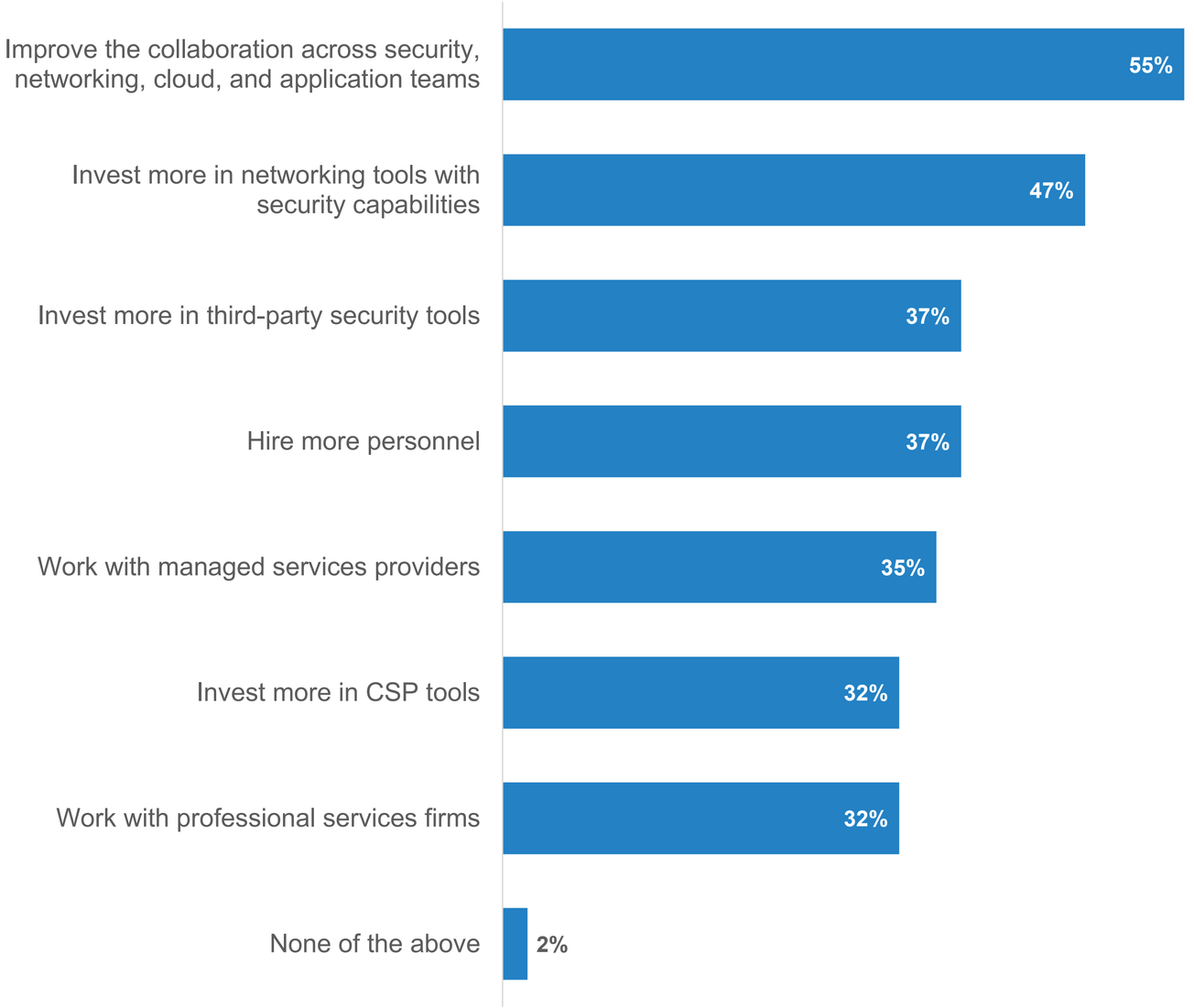
Why Cloud and Network Security Convergence Is Important

With all this in mind, how should organizations think about network security in a hybrid multi-cloud world? First and foremost, the traditional silos across teams and tools responsible for on premises and cloud must be broken down. Historically, as new locations and threat vectors have been introduced, additional tools have been added, often with different personas responsible for management. As the lines between on premises and cloud blur and truly hybrid environments become the norm, with the different components of an application spanning different locations, these artificial barriers begin to cause more problems than they solve. The good news is that many organizations are moving forward with this transition. Nearly nine in ten organizations (89%) said that the team most responsible for public cloud infrastructure network security is the same team that is responsible for on-premises data center/private cloud network security.

Yet, while this is a good step in the right direction, it does not fully address the fact that security responsibility is distributed across many teams and personas, and tools remain fragmented. When asked about their top priorities for hybrid cloud network security moving forward, more than half (55%) indicated that improving collaboration across not just the network security team, but also the networking, cloud, and application teams, was one of the actions they planned to take. This indicates there is still work to do with regard to convergence organizationally outside of the core network security team.

At the same time, there was no clear consensus on the technology to be used for hybrid cloud network security, with 47% planning to invest more in networking tools with security capabilities, 37% planning to invest more in third-party security tools, and 32% planning to invest more in CSP tools. So even as teams begin to work more closely together, there could remain issues attaining consistency from a tool perspective.

Top Priorities for Hybrid Cloud Network Security.



BACK TO CONTENTS

Aligning Goals and KPIs Is Critical

Facilitating organizational convergence requires more than just changing reporting alignment or team structure. It requires team members to think about their responsibilities in different ways. Cloud, networking, and IT teams must have some consideration for security as they make decisions, and security teams must take into account business priorities. To achieve this, some of the specific steps organizations should take include:

- Better aligning on goals and KPIs, as security teams are more focused on reducing risk and preventing incidents, while cloud and developer teams are assessed on uptime, performance, and similar metrics. Cross-pollenating these goals across the different groups can help them become aligned and work toward common outcomes.
- Reviewing and optimizing workflows across network security, cloud, and application teams to ensure security teams are not slowing things down and application teams are addressing security concerns early in their process.
- Ensuring these teams communicate and meet on a regular basis to keep one another apprised of issues and concerns or to build on what's working well.

Steps to Improve Collaboration.

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

4%

We are not taking active steps to improve collaboration

BACK TO CONTENTS

Organizations Should Prioritize Tools That Bridge the Gap and Offer an Application-centric Approach to Network Security

While organizational dynamics and processes are important, ultimately, the tools in use must be able to support these new models. When it comes to network security, tools that converge capabilities covering hybrid multi-cloud environments, with a focus on application visibility, are critical to ensure the secure application connectivity across the environment.

Ultimately, the network's core function is to deliver the applications that power the business. In the past when applications were monolithic and lower in number, taking a port, protocol, IP address view of the network made more sense. As more and more traffic has become application-based, and applications have become fragmented, the need to understand the relationships between those applications and application components has grown. Essentially, securing the network has become securing application connectivity. Simply accepting that security tools might negatively impact availability is no longer acceptable, making an application focus even more important.

Some of the key attributes to prioritize include:

- **Integration with cloud automation tools (43%).** More and more cloud and development teams are adopting infrastructure as code to accelerate deployment, improve consistency, limit errors, and enhance efficiency. Security must follow suit but should be plugged into these workstreams so that it can be incorporated as infrastructure and applications are deployed, rather than bolted on after the fact.

- **Centralized management (38%).** Most organizations have supported cloud infrastructure and on-premises data centers for years. In many cases, there were cleaner lines of demarcation in terms of the applications and workloads residing in each. As those lines have blurred and truly hybrid environments have become more common, the need for consistent management across all clouds and on-premises locations has grown.

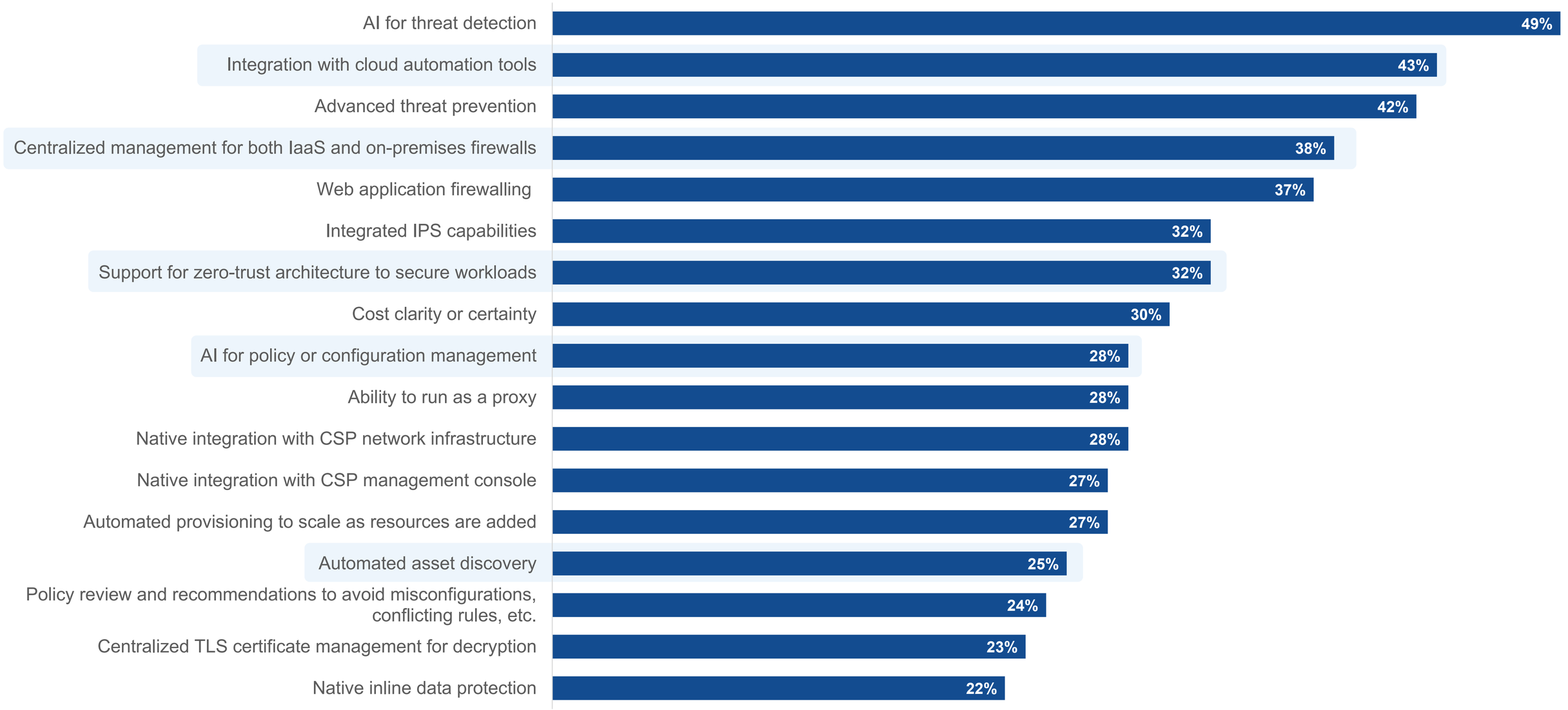
- **Support for zero trust (32%).** Whether they have a broad, formally defined zero-trust initiative in place or not, every organization would be well-served by beginning to implement some zero-trust tenets across their environments. Among the most important of these are least privilege and a more dynamic, risk-based policy construction. Tools that help teams understand what entities should have access to what resources, limit access to the bare minimum needed to perform required business tasks, and continually assess risk to limit access as that changes can help, but an application-centric view is necessary to achieve this. Otherwise, the context needed to apply these granular policies is missing.

- **AI for policy/configuration management (28%).** As the speed of application and cloud infrastructure deployment accelerates, security policy and configuration management must keep pace. The hype around AI can be overwhelming at times, but policy and configuration management is one foundational area where AI can help immensely. Providing policy recommendations, reviewing the impact of rules before they are actively deployed, and cleaning extensive rule lists to remove duplicate or conflicting rules are some ways AI can help.

- **Automated asset discovery (25%).** While applying zero trust is important, security teams must understand what assets are in the environment. Manually tracking down every workload and application in place would be impossible for most organizations today. Tools that automate this process so that network security teams have the context they need to confidently deploy firewalls without fear of breaking valid application connections can speed time to value and help improve security.

BACK TO CONTENTS

Key Network Security Capabilities for Hybrid Cloud Environments.



BACK TO CONTENTS

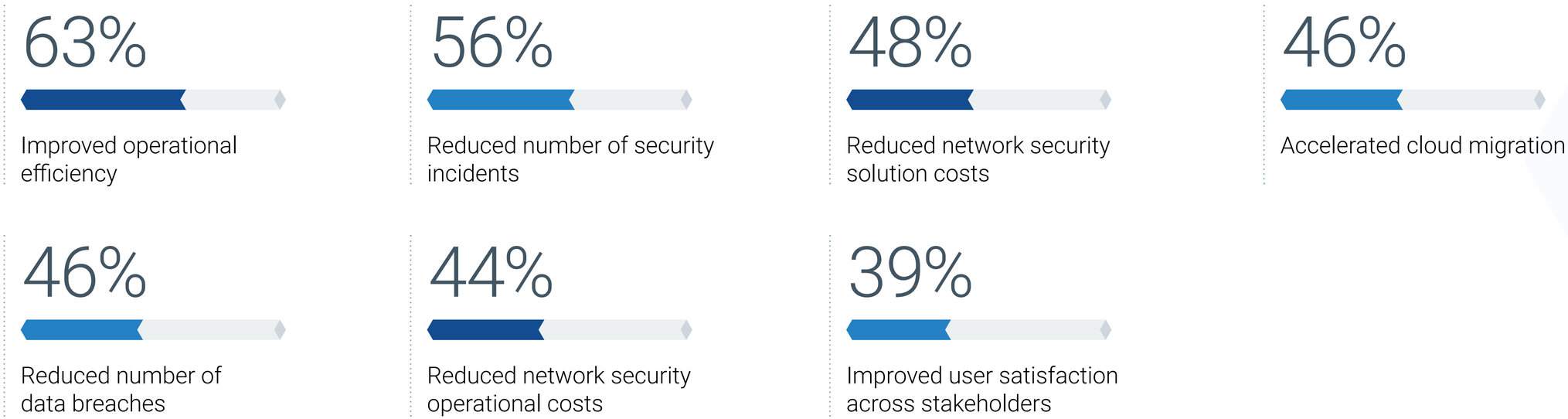
The Benefits of an Application-centric Hybrid Cloud Security Management and Automation Platform

Organizations Expect Both Security and Business Benefits From Hybrid Cloud Network Security

Ultimately, whether they actively realize it or not, network security teams have been moving in this direction for some time now. While limiting incidents and preventing data breaches are still critical metrics, many security teams are pivoting to focus on driving business outcomes as well. Improving operational efficiency (63%), reducing costs (48%), accelerating cloud migration (46%), and improving user satisfaction (39%) are some of the top benefits organizations expect from their network security approaches.

To achieve these goals, network security teams have to broaden their focus and view the network through a different lens than they have typically been accustomed. Applications are the foundation of most businesses, and the network provides the connectivity to ensure they are accessible. That connectivity must be secured, which requires a deep visibility and understanding at an application level, with converged support for hybrid multi-cloud environments. Teams and programs must be converged as well, but tools can act as an enabler, and solutions that support a converged, application-centric approach to network security can help accelerate the transition from legacy to modern network security.

Expected Benefits From Hybrid Cloud Network Security.



BACK TO CONTENTS

AlgoSec Horizon

AlgoSec Horizon is the industry's first application-centric platform, empowering CISOs and security teams to streamline application delivery without compromising security.

Focused on securing and automating connectivity of business applications, AlgoSec Horizon was uniquely developed for enterprises with complex hybrid network environments, bridging cloud and on-prem data centers.

The platform utilizes advanced AI capabilities to automate discovery and identifiction of the deployed business applications. It serves as a single source for visibility into security, and enables security teams to work more efficiently at scale with greater automation, context-aware risk management, and compliance assurance.

Conclusion

Cloud security receives a lot of attention, and with good reason. In the broad scheme of IT, cloud is still relatively new, and many organizations have struggled with implementing effective security in the cloud. However, focusing solely on cloud and neglecting the reality that many applications currently and will continue to reside on premises is a recipe for failure. It is impossible to look at network security through the lens of on premises or cloud when an application spans both locations. Organizations must rethink their network security technology, strategy, and team structure and adopt a more converged approach. This requires tools that offer application-centric, hybrid multi-cloud coverage to support network security and cloud teams as they modernize their security program.

BACK TO CONTENTS

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to securely accelerate application delivery up to 10 times faster by automating application connectivity and security policies across the hybrid network environment. With two decades of expertise securing hybrid networks, over 2,200 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads.

LEARN MORE

Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.