algosec

# AlgoSec State of Network Security Report 2025

## Unveiling market trends:

Multicloud hybrid networks
in the era of AI

# Table of contents

# Executive summary

Network infrastructure is constantly changing, but the pace of that evolution has picked up dramatically in 2025. As organizations continue to expand their digital footprint across hybrid and multi-cloud environments, the complexity of securing these infrastructures has now become an agenda-topping challenge for businesses – particularly with the rise of AI applications and subsequent workloads. Gartner's claim that there is "no business strategy without a cloud strategy" holds true, yet despite the boom in publicly hosted SaaS applications, 52% of organizations plan to host and deliver their AI-based applications on-premise or through colocation facilities[1].

The real challenge, however, is no longer just about securing data; it's about maintaining visibility and control over a fragmented, fast-moving digital ecosystem. To meet this challenge, organizations are prioritizing automation, orchestration, and risk mitigation as core pillars of their security strategies. Cloud security has become a top priority, and the growing adoption of multi-vendor firewall strategies reflects a need for more flexible, layered security architectures, even as it introduces operational complexity. Meanwhile, the steady rise of SD-WAN and SASE highlights the continued demand for secure, high-performance connectivity across distributed environments. Security and network functions are also converging, blurring the lines between traditionally separate disciplines. Organizations are increasingly looking for solutions that unify security policies, networking infrastructure, and cloud management under a single, cohesive framework. This was also noted in last year's report, and reflects a growing demand for security architectures that reduce complexity, improve interoperability, and enhance real-time visibility across hybrid environments.

This report provides one of the most comprehensive and objective analysis of the network security landscape available today. Gathering insights from 192 security, network, and cloud professionals across 28 countries, it aims to offer a vendor-agnostic assessment of the market across multi-cloud environments and diverse firewall solutions.

Since our 2024 report, multi-cloud adoption has solidified its place as the new standard, with organizations distributing workloads across multiple cloud platforms to optimize performance, mitigate the risks of vendor lock-in, and enhance resilience. Firewall deployments have increased, though organizations are struggling with the complexity of managing multiple vendors. Meanwhile, SD-WAN adoption continues to rise as businesses seek to gain more control over their connectivity, with the market projected to grow at a CAGR of 31% to reach $59 billion by 2032[2]. SASE is seeing incremental growth, but full adoption remains a work in progress due to the inherent complexity of integrating multiple security functions into a single cloud-native service, particularly for those with legacy architectures. AI-driven security capabilities are on the rise, yet operational barriers persist. And while Zero-Trust awareness has increased, many organizations are still in the early stages of implementation.

These highlights point to a fundamental shift: hybrid cloud security is no longer just about protection – it's about integration, automation, and visibility in an increasingly distributed world. By presenting an unbiased view, this report aims to equip organizations with the insights needed to navigate the complexities of modern network security, optimize their infrastructure, and make informed decisions that align with their long-term security and business objectives.

[1] https://datacentre.solutions/blogs/58144/why-companies-are-building-their-ai-applications-outside-of-public-cloud

[2] https://www.snsinsider.com/reports/software-defined-wide-area-network-market-2803

Trend 1:

# The evolving firewall landscape – more vendors, more complexity

As organizations accelerate their shift to multi-cloud and hybrid environments, the role of firewalls in securing digital assets continues to shift. While firewalls remain a critical layer of defense, their deployment is becoming increasingly complex due to multi-vendor strategies, cloud-native architectures, and the growing need for automation. Businesses are now prioritizing scalable, policy-driven security models that ensure consistency across both cloud and on-premise infrastructures. However, managing multiple firewall solutions across distributed environments presents significant operational challenges, requiring centralized orchestration and deeper integration with cloud security frameworks.

## Datacenter firewall deployments continue to expand

As organizations scale their hybrid environments, firewalls in the on-premise datacenters remain critical for securing the infrastructure. businesses are prioritizing firewalls with deeper security integration, advanced threat detection, and automation capabilities. Palo Alto Panorama has taken the lead, reflecting growing trust in centralized security management. Fortinet's next-generation firewall has also gained adoption, as enterprises look for security-driven networking solutions; multi-vendor firewall strategies remain common, but managing them is becoming increasingly complex.

## Multi-vendor firewall strategies offer security but increase complexity

Enterprises are increasingly deploying multi-vendor firewall solutions to enhance security posture and reduce vendor lock-in risks. This approach enables flexibility and layered defense mechanisms, but it also introduces significant complexity. Managing multiple firewall policies across different cloud environments requires robust orchestration tools to prevent misconfigurations, maintain compliance, and reduce operational overhead. Without proper integration, organizations risk policy inconsistencies, security gaps, and increased administrative burden.

| | 2024 | 2025 |
|---|---|---|
| 1 | Cisco | Palo Alto \| Panorama (PAN) |
| 2 | Palo Alto Networks | FortiGate via FortiManager |
| 3 | Fortinet | Cisco (ASA, Firepower, ACI, Meraki, Other) |
| 4 | Check Point (CKP) | Check Point (CKP) |
| 5 | F5 | Palo Alto FW (Direct) |

Top five firewall vendors ranked by enterprise deployment and market shifts

# Trend 1: The evolving firewall landscape – more vendors, more complexity

## Fortinet NGFW gains market share in security deployments

Fortinet's Next-Generation Firewall (NGFW) has gained significant traction, moving up in firewall rankings as adoption increases across hybrid and multi-cloud environments. Its high-performance security processing, AI-powered threat detection, and SD-WAN integration have made it a preferred option for organizations seeking scalable, security-driven networking solutions. Meanwhile, Palo Alto Panorama takes the lead, reflecting the growing trust in Palo Alto's unified security management approach. Cisco remains a dominant force across hybrid and on-prem environments, continuing to be a key player in enterprise security. Check Point maintains its #4 position, while Palo Alto FW (Direct) enters the top five, signaling a shift toward direct and scalable firewall solutions.

## A growing hybrid approach: more organizations retaining on-prem firewalls

Despite the cloud security boom, a surprising trend has emerged – a growing number of organizations are either maintaining or reverting to on-premise firewalls. The percentage of companies reporting "no cloud presence" rose from 7.1% in 2024 to 13.4% in 2025 indicating that regulatory requirements, data sovereignty concerns, and security risks associated with public cloud environments are driving some businesses to retain traditional, on-prem security infrastructures. This shift highlights the need for firewalls that support hybrid deployments, enabling organizations to enforce consistent security policies across both cloud and on-prem networks

### Key takeaway

The firewall landscape is undergoing rapid transformation, with cloud-native solutions gaining ground but also introducing new security management complexities. Organizations are leveraging multi-vendor strategies for added resilience, but without centralized security orchestration, this approach can lead to policy fragmentation and operational inefficiencies. Fortinet's rise in market share reflects a shift toward integrated, AI-driven security solutions, while the increase in hybrid strategies suggests that businesses are carefully balancing cloud adoption with on-premise security concerns.

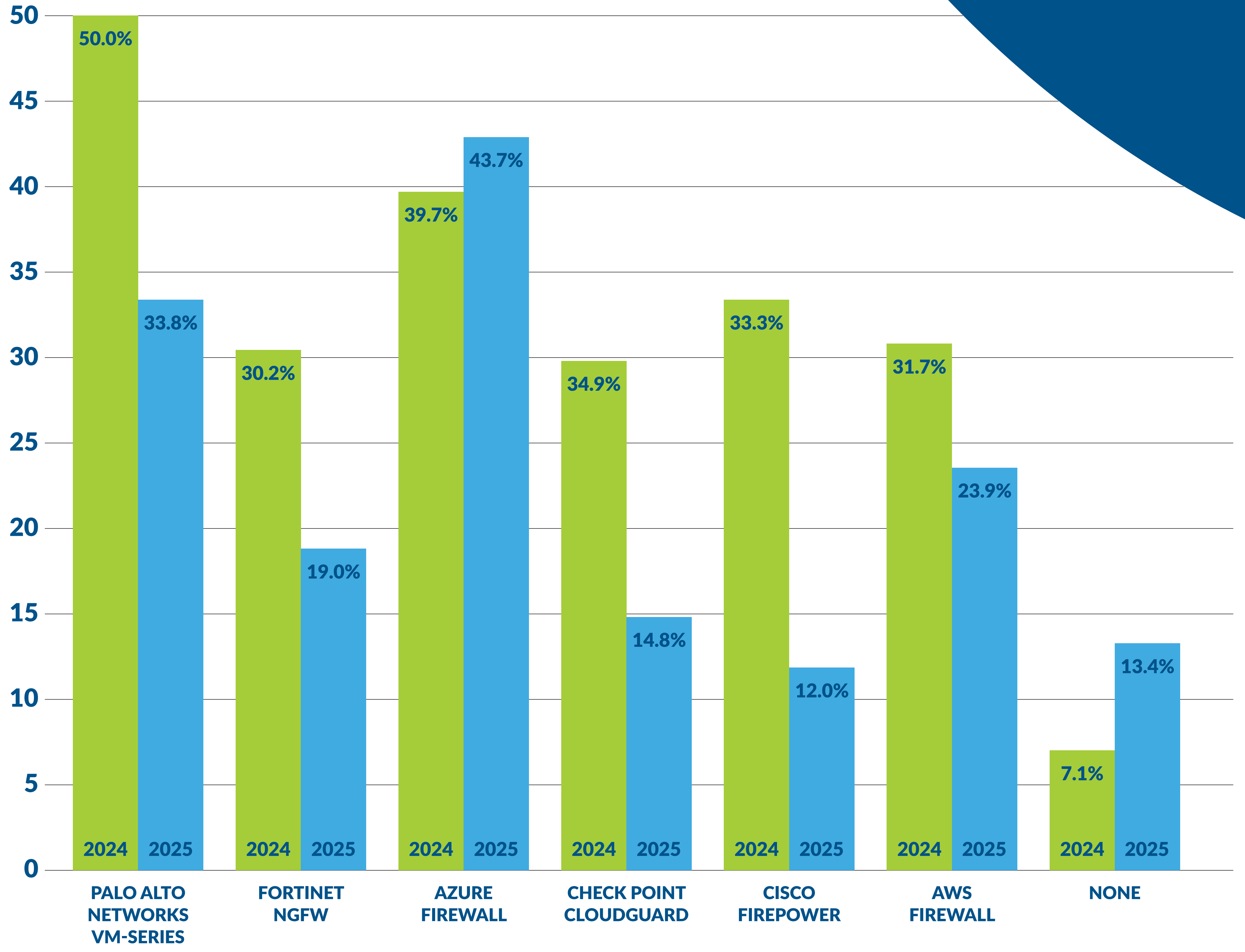
## Trend 2:

# The rise of cloud firewalls as a security standard

Cloud security continues to evolve as organizations expand their reliance on multi-cloud and hybrid environments. As businesses increase their cloud workloads, securing applications, workloads, and data has become a top priority. Traditional network security measures are no longer sufficient, and organizations are increasingly turning to cloud-native firewalls to enforce policies, manage risk, and maintain compliance across complex infrastructures.

### Azure firewall overtakes Palo Alto Networks as the top cloud firewall

Azure Firewall has emerged as the most widely deployed cloud firewall. This shift underscores a growing preference for integrated, cloud-native security solutions that align with existing enterprise ecosystems. Microsoft's ongoing investments in hybrid cloud security, AI-driven threat detection, and compliance automation have made Azure Firewall a compelling choice for organizations that require scalable, policy-driven protection.



Ranking of cloud firewalls by adoption trends and organizational preferences in 2024-2025

# Trend 2: The rise of cloud firewalls as a security standard

## AWS firewall gains market share as confidence in built-in security grows

While Azure leads, AWS Firewall has seen notable growth, climbing to the #3 position in cloud firewall adoption. This increase signals a rising trust in Amazon's built-in security capabilities, particularly among organizations that prioritize scalability, automation, and cost-efficient security solutions. AWS continues to expand its security portfolio, incorporating deep packet inspection, automated threat intelligence, and enhanced integrations with GuardDuty and Security Hub, making its firewall a competitive option for cloud security.

## Multi-vendor firewall strategies add security but increase complexity

With the continued adoption of multi-cloud architectures, enterprises are increasingly deploying multiple firewall solutions to enhance security posture and reduce vendor lock-in risks. However, this approach introduces operational complexity, requiring centralized management, policy enforcement, and automation to prevent misconfigurations and security gaps. Organizations are now looking for cloud-native firewalls that integrate seamlessly across platforms, reducing administrative overhead while ensuring consistent security policies.

## Key takeaway

Cloud firewalls have become a fundamental part of modern security strategies as organizations seek scalable, automated, and policy-driven protection. The rise of Azure Firewall and AWS Firewall adoption highlights the growing need for natively integrated security solutions that align with multi-cloud environments. At the same time, multi-vendor firewall strategies are introducing new management complexities, requiring businesses to invest in better orchestration, visibility, and automation to maintain security across cloud infrastructures.

Trend 3:

# The state of cloud platforms – top choices

Cloud platforms remain at the core of modern enterprise IT, providing the foundation for scalable infrastructure, AI workloads, and multi-cloud strategies. However, while Azure and AWS continue to strengthen their leadership, competition in the cloud security space remains dynamic, with enterprises increasingly diversifying their cloud providers based on workload requirements and security priorities.

## Azure establishes narrow market lead

Azure has become the most widely used cloud platform, in part thanks to its ability to integrate seamlessly with other Microsoft services. Its deep integration with Active Directory, Microsoft Sentinel, and other enterprise tools has made it a preferred option for organizations seeking a unified security and cloud management experience. As AI workloads grow, Azure is also benefiting from its focus on AI-driven security automation, reinforcing its status as a leader in cloud security infrastructure.

| | 2024 | 2025 |
|---|---|---|
| 1 | **AWS** | **Azure** |
| 2 | **Azure** | **AWS** |
| 3 | **Google Cloud Platform (GCP)** | **Google Cloud Platform (GCP)** |
| 4 | **Oracle Cloud** | **Oracle Cloud** |
| 5 | **Alibaba Cloud** | **Alibaba Cloud** |

Ranking of cloud platform adoption and shifts in organizational cloud strategies for 2024-2025

# Trend 3: The state of cloud platforms – top choices

## AWS continues to gain market share in security-driven deployments

AWS has strengthened its position in cloud security, seeing increased adoption among organizations that prioritize flexibility and automation. AWS has expanded its native security offerings, integrating GuardDuty, Security Hub, and identity-based access controls to help enterprises secure cloud workloads at scale. Its continued growth indicates a rising preference for security automation and cost-effective cloud protection, especially among businesses with developer-driven security models.

## Google cloud platform remains a niche player in enterprise security

Google Cloud Platform (GCP) continues to be a strong choice for AI, machine learning, and analytics workloads. It is often used as a specialized cloud provider or as part of a broader multi-cloud infrastructure, complementing other cloud platforms.
As organizations further evolve their cloud security strategies, GCP's growth in security will likely be shaped by its ability to align with enterprise-wide security policies and support comprehensive compliance frameworks.

### Key takeaway

The cloud platform market remains highly competitive, with Azure and AWS leading as enterprises prioritize security, automation, and compliance-driven cloud strategies. Multi-cloud adoption continues to shape cloud platform choices, with organizations balancing performance, security, and integration capabilities. Google Cloud maintains strength in AI-driven workloads. Moving forward, businesses will need to evaluate cloud platforms not just on scalability, but on security capabilities and long-term risk management strategies.

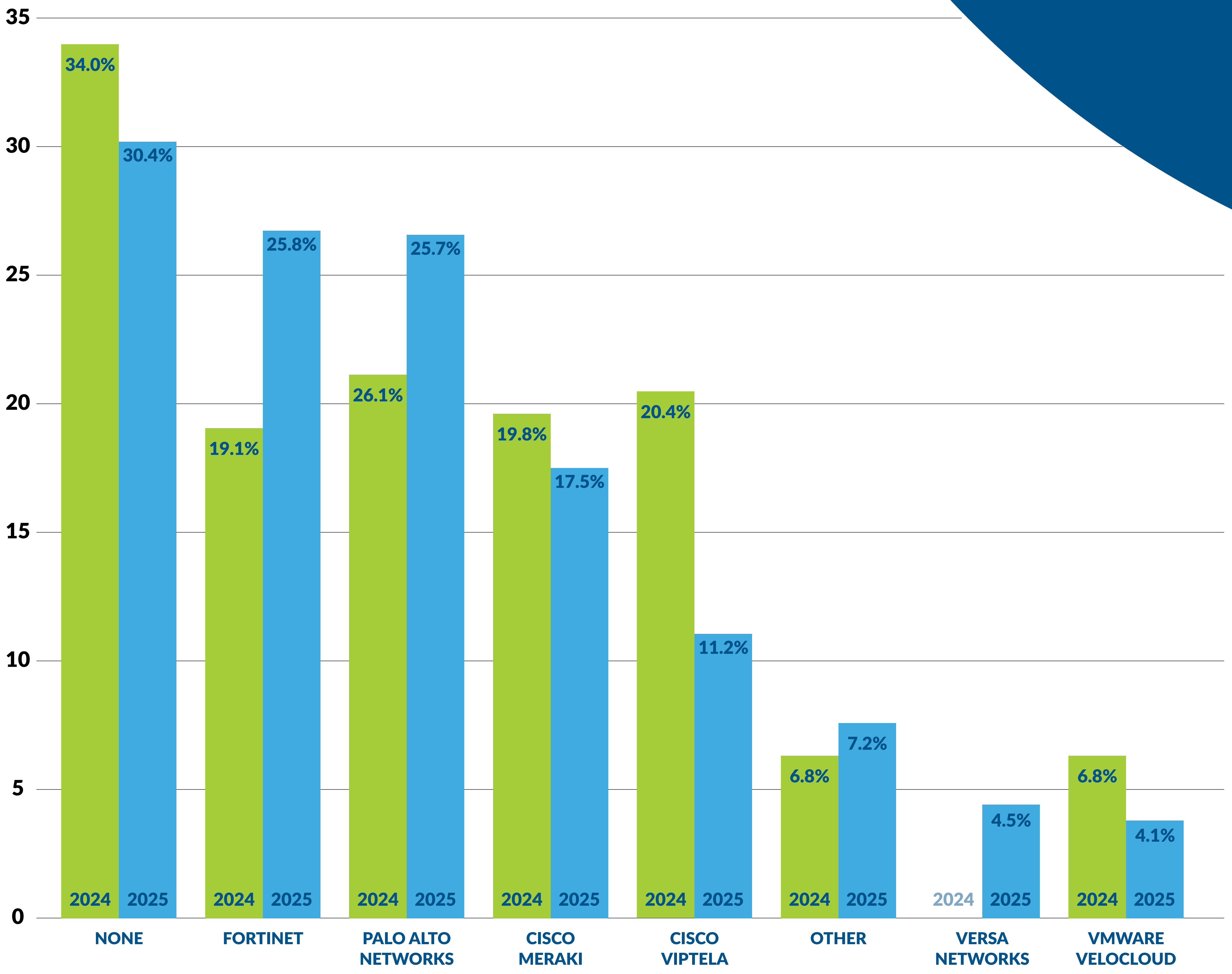
## Trend 4:

# SD-WAN - A shifting competitive landscape

The adoption of SD-WAN continues to rise as organizations seek more secure, scalable, and cost-effective ways to manage their increasingly complex network environments. With the growth of multi-cloud strategies, remote workforces, and edge computing, enterprises are moving away from traditional WAN architectures in favor of software-defined solutions that offer greater agility and security. However, while SD-WAN's value is well understood, implementation challenges remain, and many organizations are still evaluating how best to integrate the technology into their broader network security strategy.

## Top SD-WAN providers - market leaders and trends

While Cisco remains a dominant force in SD-WAN due its Meraki and Viptela solutions, Fortinet has emerged as the leading single SD-WAN provider. Fortinet's success can be attributed to its tight integration of security and networking capabilities, making it a compelling option for organizations prioritizing performance without compromising protection. Its next-generation firewall (NGFW) capabilities, AI-driven threat detection, and built-in SD-WAN functionality have made it particularly attractive to businesses seeking a unified security and networking solution.



Respondents' adoption of SD-WAN solutions and changes in vendor rankings

# Trend 4: SD-WAN - A shifting competitive landscape

## A shift in Cisco SD-WAN preference

Cisco remains a major player in the SD-WAN space. Cisco Meraki is gaining traction, favored by businesses looking for ease of deployment, centralized cloud-based management, and seamless integration with existing Cisco infrastructure. This shift reflects a broader trend toward simpler, scalable networking solutions that can be managed with minimal operational overhead.

## Despite benefits, some organizations remain hesitant

While SD-WAN adoption continues to expand, some enterprises remain cautious about cost, integration complexity, and policy management across distributed locations. Organizations still relying on legacy WAN infrastructure may face operational and technical hurdles when transitioning to SD-WAN, particularly if they lack the in-house expertise to manage policy-based routing and security enforcement effectively. The need for consistent security policies across hybrid environments also remains a challenge, with many organizations still evaluating the best approach to integrating SD-WAN with existing security frameworks.

## SD-WAN adoption accelerates as cloud and hybrid workforces expand

The growing need for secure, high-performance connectivity across cloud environments and distributed workforces continues to fuel SD-WAN adoption. Organizations are increasingly looking for networking solutions that provide greater control, visibility, and security without adding complexity. Analysts project that the SD-WAN market will grow at a CAGR of 31%, reaching $59 billion by 2032, underscoring the increasing reliance on software-defined networking to support modern enterprise connectivity needs.

## Key takeaway

SD-WAN is evolving beyond traditional networking into a security-driven solution, with vendors like Fortinet leading the charge by integrating advanced security capabilities directly into SD-WAN platforms. While demand remains strong, organizations continue to balance complexity, cost, and security concerns when considering deployment. The shift toward simplified, cloud-managed solutions suggests that ease of use and centralized control will be key factors in future SD-WAN adoption. Gartner projects that by 2026, 60% of new SD-WAN purchases will be integrated into a single-vendor SASE offering, up from 15% in 2022[3].

[3] https://www.sdxcentral.com/articles/analysis/gartner-magic-quadrant-reveals-sd-wan-leaders-plus-sase-and-genai-trends/2023/10/

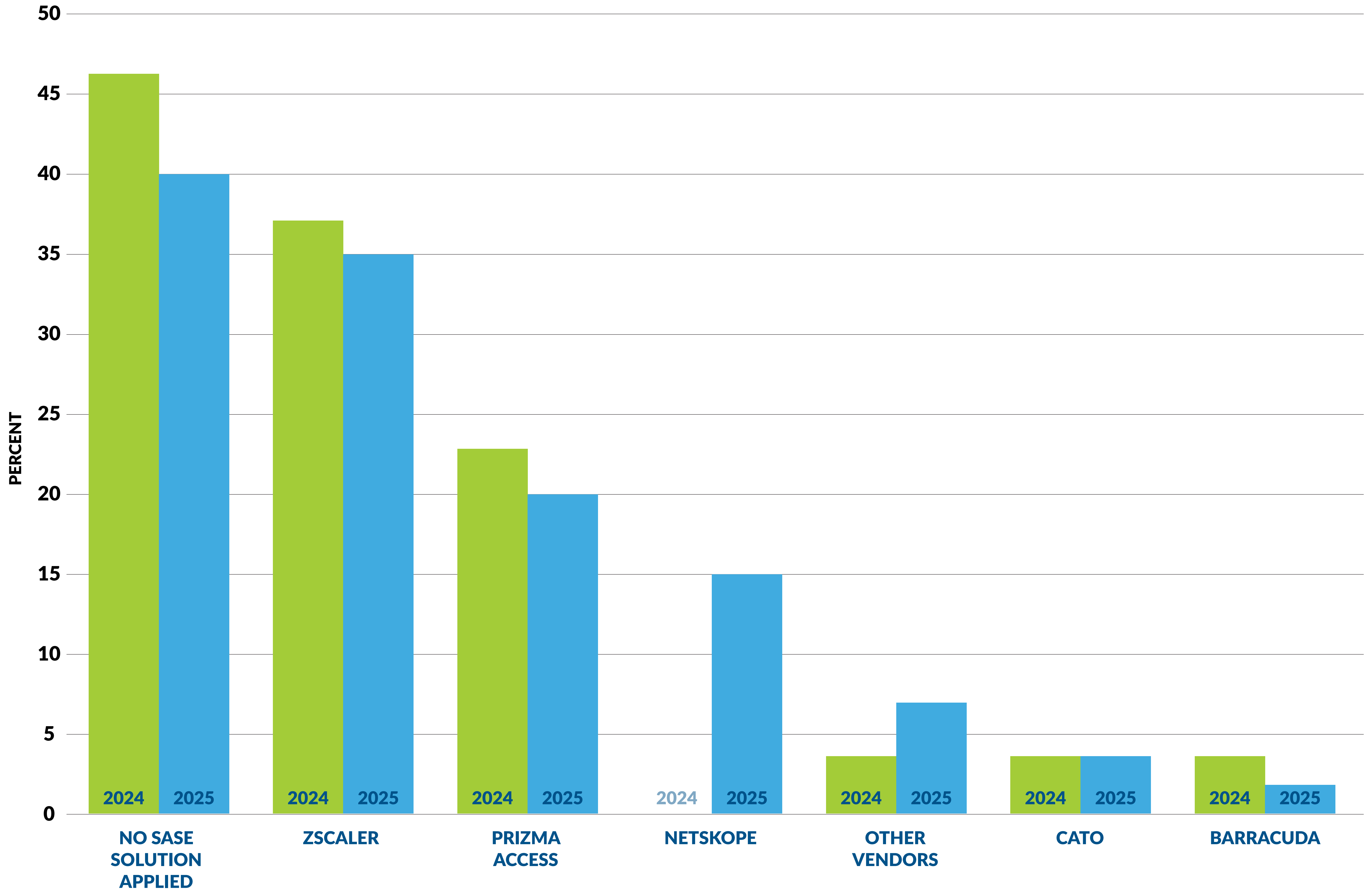
Trend 5:

# SASE adoption – slow but steady growth

Secure Access Service Edge (SASE) adoption continues to grow as organizations seek integrated, cloud-native security solutions that support distributed workforces and multi-cloud environments. By combining network security and wide-area networking (WAN) capabilities, SASE provides a framework for secure, seamless access to cloud applications. However, while awareness of SASE has increased, full adoption remains a slow and deliberate process, as enterprises work to integrate multiple security functions into a single, cohesive architecture.

## SASE adoption continues to grow year over year

A significant number of organizations still have not adopted a SASE solution, with 40% of respondents reporting no deployment – though this marks a slight decline from 45.7% in the previous year. This gradual decrease suggests that while full-scale SASE implementation remains complex, more businesses are starting to explore adoption. The biggest hurdles continue to be integration challenges, legacy infrastructure, and the complexity of merging multiple security components into a single cloud-native service.



Respondents' adoption rates of SASE solutions and vendor market positions in 2024-2025

# Trend 5: SASE adoption – slow but steady growth

## Zscaler and Prisma Access maintain leadership

Zscaler and Palo Alto Networks continue to lead the SASE market. However, changes in their market share YoY reflect increased competition and diversification in vendor selection. These shifts indicate that while leading SASE providers remain strong, enterprises are evaluating alternative solutions to invest in, that align more closely with their unique security and networking needs.

## Netskope emerges as a notable contender

Netskope has gained traction as a relative newcomer in the SASE space, increasing its adoption rate to 15.0% in 2025. This growth reflects a rising demand for data-centric security solutions that emphasize cloud access control and Zero-Trust enforcement. Netskope's ability to secure SaaS applications and enforce granular policies for remote users has made it a viable alternative for businesses prioritizing cloud-native security and compliance-driven architectures.

## Smaller vendors show modest growth as organizations seek tailored SASE solutions

Beyond the leading players, smaller vendors such as CATO and Barracuda have experienced slight increases in adoption. While their overall market share remains relatively low, their steady growth suggests a broader trend toward vendor diversification. As organizations evaluate SASE solutions, flexibility and customization are becoming key factors in vendor selection, with enterprises seeking modular architectures that allow them to integrate security and networking components at their own pace.

## Key takeaway

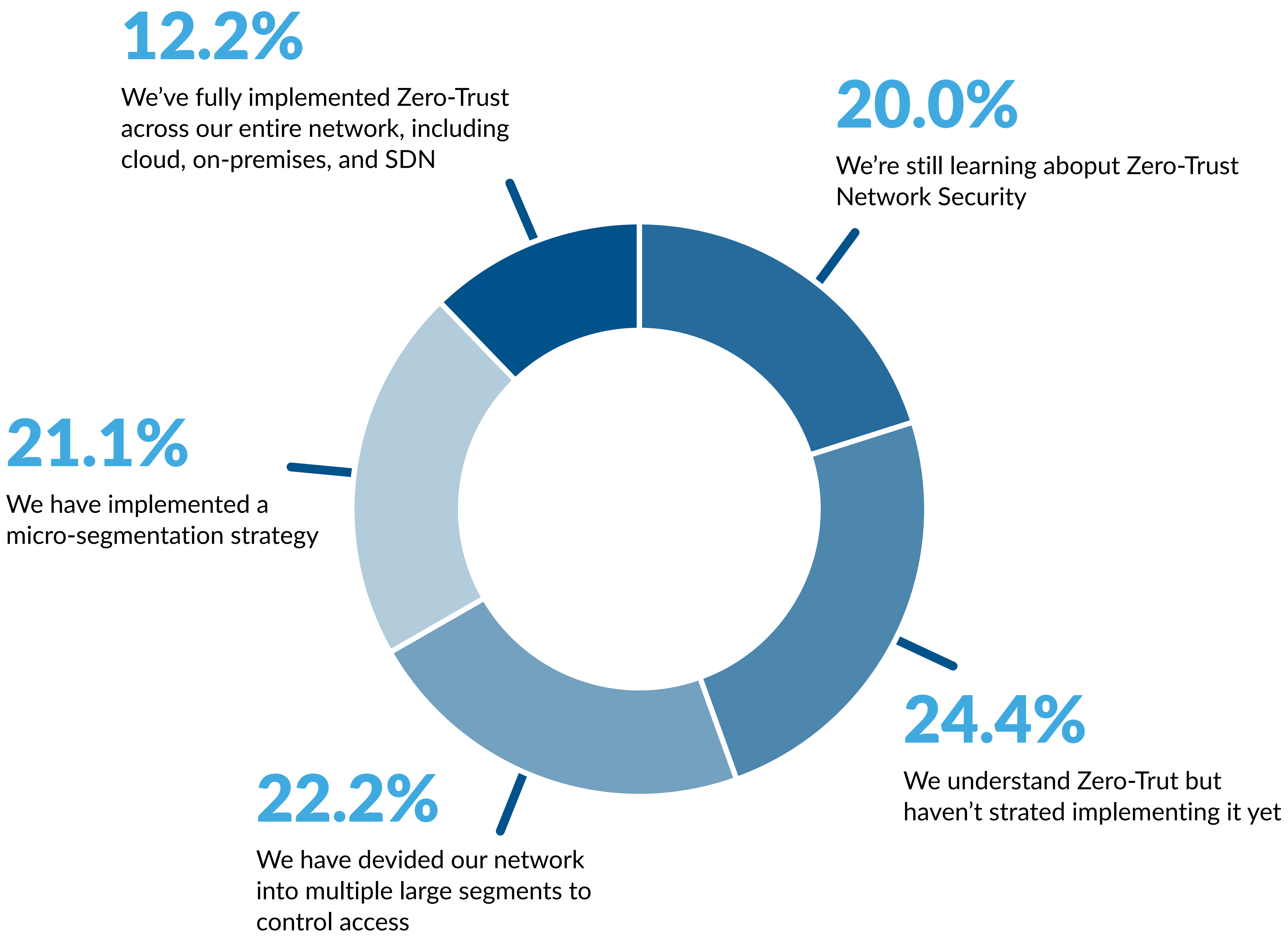
While SASE adoption remains gradual, the market is shifting as organizations move beyond initial exploration toward phased implementation. Leading providers like Zscaler and Prisma Access maintain dominance, but competition is growing as enterprises seek tailored, flexible solutions. The complexity of full-scale deployment continues to be a challenge, but as cloud-first strategies become the norm, SASE is poised for continued, steady expansion.

# Zero-Trust – increasing awareness, slow implementation

Zero-Trust continues to gain traction as organizations seek stronger security postures in response to evolving cyber threats, remote work expansion, and multi-cloud adoption. While the core principle of Zero-Trust – never trust, always verify – is widely accepted, full-scale implementation remains a slow and complex process. Many enterprises are still in the early stages of deployment, grappling with integration challenges, legacy infrastructure limitations, and the need for greater security awareness.

## Adoption of Zero-Trust is growing, but progress is slow

More organizations are adopting Zero-Trust architectures, with 56% reporting some level of implementation. However, most deployments remain partial, focusing on foundational measures such as identity and access management (IAM), network segmentation, and multi-factor authentication (MFA). While these steps mark progress, few enterprises have achieved fully mature Zero-Trust models, as integrating comprehensive policy enforcement across networks, users, and applications remains a challenge.



Percentage of respondents at different stages of zero-trust implementation

# Trend 6: Zero-Trust – increasing awareness, slow implementation

## Lack of understanding and awareness is the biggest barrier

Despite its growing adoption, 20% of organizations report that they are still in the learning phase, highlighting a lack of clear implementation roadmaps and best practices. Security teams often struggle to translate Zero-Trust principles into actionable policies, particularly in complex, multi-cloud, and hybrid environments. This underscores the need for better education, clearer frameworks, and improved tooling to help businesses move beyond basic Zero-Trust principles toward more robust, policy-driven implementations.

## Organizations are taking varied approaches to Zero-Trust

There is no one-size-fits-all approach to Zero-Trust, and enterprises are adopting different strategies based on their security priorities and existing infrastructure. Some focus on micro-segmentation, while others prioritize Zero-Trust Network Access (ZTNA), identity-based authentication, or endpoint security. This flexibility allows businesses to tailor Zero-Trust frameworks to their specific needs, but it also complicates standardization efforts, making it harder to define what “true” Zero-Trust implementation looks like.

## Full Zero-Trust implementation remains rare

Despite the increasing awareness, fully realized Zero-Trust environments remain the exception rather than the rule. Many enterprises are hesitant to overhaul legacy systems or lack the budget and resources to execute a comprehensive Zero-Trust transformation. Instead, most organizations are incrementally adopting Zero-Trust principles within specific areas of their network, such as user authentication or cloud security, rather than committing to a holistic, organization-wide shift.

## Key takeaway

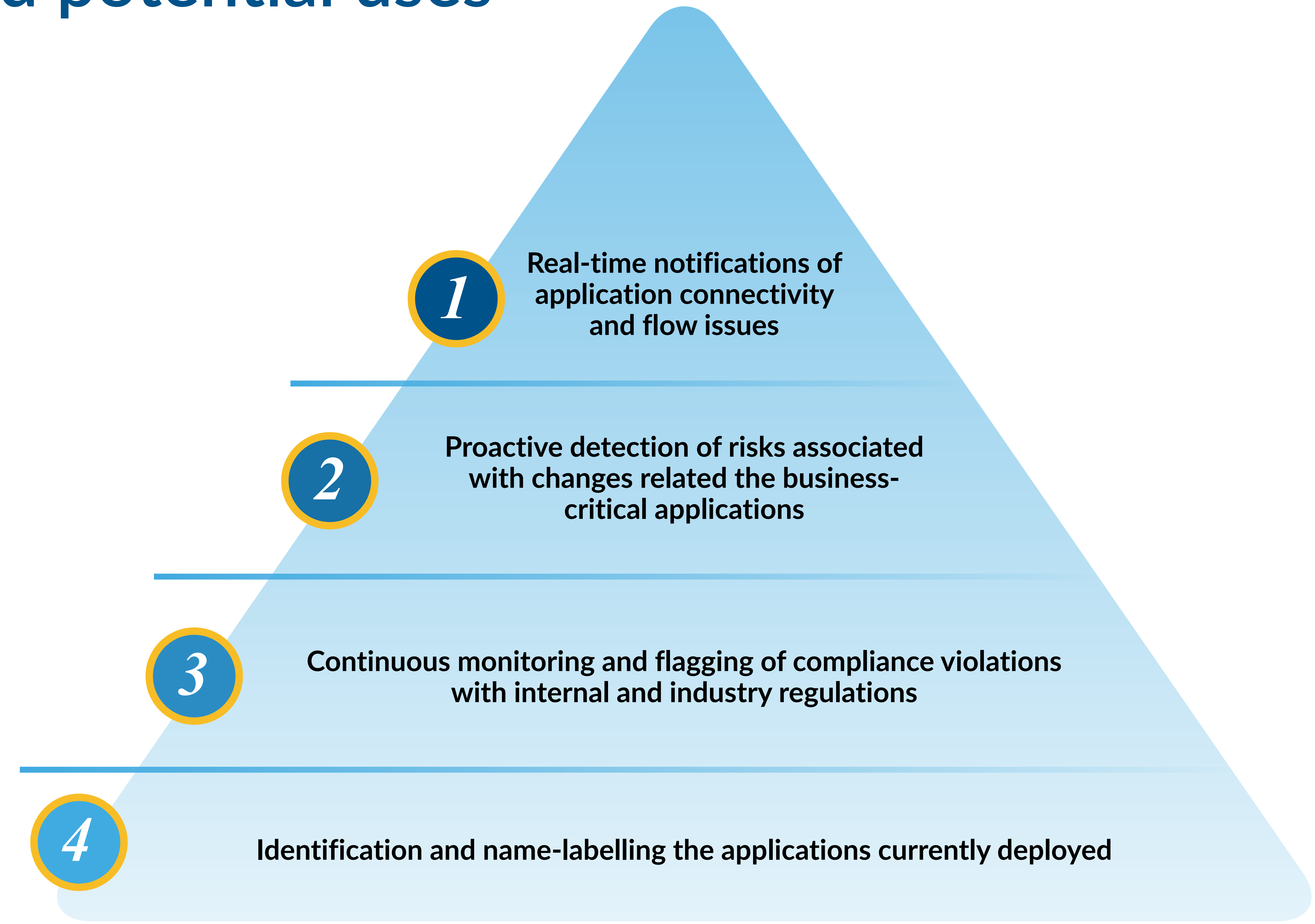
While Zero-Trust awareness is at an all-time high, full adoption still remains a long-term goal for most organizations. The biggest barriers include lack of understanding, integration challenges, and the complexity of applying Zero-Trust principles across diverse IT environments. Companies that take a phased approach – starting with segmentation, access control, and identity verification – will be best positioned to strengthen their security posture over time.

# AI in network security – priorities and potential uses

AI is becoming an integral part of network security, offering the potential to enhance threat detection, automate responses, and optimize security operations. However, while AI-driven security tools are gaining traction, many organizations are still concerned about privacy and sensitive data leaks via GenAI tools[4]. Additionally, organizations still struggle with integration, and real-time risk mitigation. AI in security remains a work in progress, with enterprises prioritizing specific use cases such as risk detection and anomaly identification while continuing to evaluate how best to integrate AI across their broader security strategy.

## Real-time risk notification is a top priority

Organizations are placing a strong emphasis on AI-driven capabilities that deliver real-time security insights. Risk notifications, anomaly detection, and predictive threat analytics have become top priorities for security teams managing multi-cloud, hybrid, and distributed environments. The ability to automate risk detection and provide immediate alerts is seen as a key advantage, helping businesses proactively address threats before they escalate.



1 Real-time notifications of application connectivity and flow issues

2 Proactive detection of risks associated with changes related the business-critical applications

3 Continuous monitoring and flagging of compliance violations with internal and industry regulations

4 Identification and name-labelling the applications currently deployed

Ranking from respondents of which AI-driven capabilities would have the greatest impact on improving organizational security

[4] https://vmblog.com/archive/2025/03/11/new-mimecast-research-reveals-55-of-global-organizations-are-not-fully-prepared-with-strategies-to-combat-ai-driven-threats.aspx

# Trend 7: AI in network security – priorities and potential uses

## Lack of visibility into cloud applications is the biggest challenge

Many enterprises struggle to gain real-time insights into cloud-based applications, making it difficult to identify vulnerabilities and enforce security policies effectively. This issue is particularly pressing in multi-cloud and hybrid environments, where siloed data, inconsistent monitoring tools, and fragmented security frameworks create blind spots that expose organizations to cyber threats. Without better AI-driven visibility solutions, security teams may fail to detect risks in time to prevent incidents.

## AI's role in compliance and data organization is underdeveloped

While AI has the potential to streamline compliance monitoring and data organization, these use cases remain secondary to real-time threat detection and risk prevention. Many organizations acknowledge the long-term value of AI-driven compliance automation, but for now, the primary focus remains on immediate security concerns. As AI security tools mature, compliance automation is expected to play a larger role in regulatory adherence, risk reporting, and governance initiatives.

## Key takeaway

AI is playing an increasingly important role in network security, but its full potential has yet to be realized. Organizations are prioritizing AI for real-time risk detection and anomaly monitoring, while visibility challenges and fragmented security tools continue to slow adoption. As AI capabilities evolve, businesses that invest in proactive threat intelligence and improved cloud visibility will be better positioned to harness AI's full potential in network security.

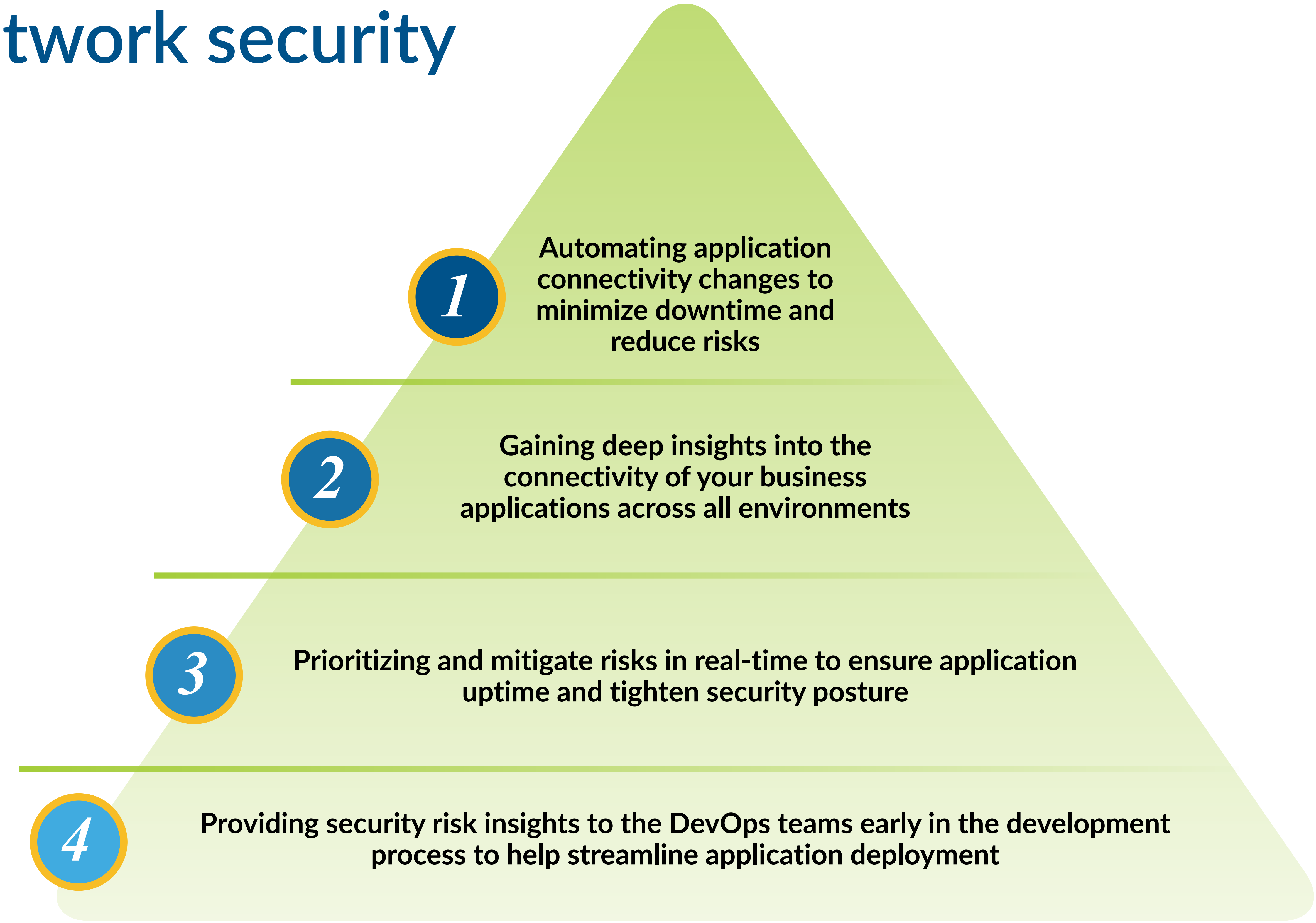
## Trend 8:

# The growing role of automation in network security

As networks become more complex, automation is emerging as a critical tool for security teams to manage risk, enforce policies, and streamline operations. Organizations are increasingly turning to automated security processes to reduce manual workloads, minimize downtime, and improve response times. However, while automation is advancing in policy enforcement and security orchestration, its role in DevOps integration and compliance monitoring remains limited.

### Automation is playing a larger role in policy enforcement and security optimization

Enterprises are investing in automated security tools to improve network visibility, policy enforcement, and risk mitigation. Automated application connectivity management, firewall rule optimization, and security policy orchestration have become key priorities as businesses seek to reduce human error and maintain consistency across hybrid cloud environments. These initiatives help organizations minimize security gaps, improve operational efficiency, and ensure continuous compliance with security policies.



1 Automating application connectivity changes to minimize downtime and reduce risks

2 Gaining deep insights into the connectivity of your business applications across all environments

3 Prioritizing and mitigate risks in real-time to ensure application uptime and tighten security posture

4 Providing security risk insights to the DevOps teams early in the development process to help streamline application deployment

Respondents' ranking of automation features according to priority for network security operations

# Trend 8: The growing role of automation in network security

## Security integration into DevOps remains a lower priority

Despite the benefits of automation, many organizations have yet to fully integrate security into their DevOps workflows. While DevSecOps principles emphasize embedding security into the development pipeline, security automation within CI/CD environments is still in its early stages. Many enterprises continue to treat security as a separate function, rather than embedding automated security checks into code deployments and infrastructure as code (IaC) frameworks. As a result, full-scale security automation across development lifecycles remains a long-term objective rather than an immediate priority.

## Compliance automation is lagging behind other security initiatives

While security teams recognize the value of automation in regulatory compliance, adoption remains slower than in other areas of security. Many organizations still rely on manual compliance audits and risk assessments, limiting the efficiency and scalability of security governance. As automation tools mature, businesses will likely shift toward AI-driven compliance monitoring, allowing for real-time policy enforcement, automated reporting, and continuous compliance tracking.

## Key takeaway

Security automation is becoming a fundamental part of modern network security strategies, particularly in policy enforcement and security orchestration. However, integration into DevOps and compliance monitoring remains underdeveloped. As automation tools evolve, organizations that embrace security automation across operational, compliance, and development environments will be better positioned to reduce risk and improve security efficiency at scale.

# Conclusion

Much like previous years, the state of network security in 2025 continues to evolve at pace, driven by the increasing complexity of multi-cloud environments, the expansion of AI-driven applications, and the ongoing shift toward automation and orchestration. As organizations navigate these changes, they are prioritizing scalability, visibility, and security integration to maintain control over what is becoming an increasingly fragmented digital environment.

This year's findings highlight several key shifts. Cloud platform preferences are evolving, with Azure Firewall as the leading solution, while AWS Firewall gains traction among enterprises. Multi-vendor firewall strategies are becoming more common, but they also introduce new operational challenges, requiring better orchestration and policy management. SD-WAN adoption continues to expand, with Fortinet climbing 3 spots, reflecting the demand for security-driven networking solutions. At the same time, SASE adoption continues to progress slowly as organizations evaluate how best to integrate its multiple security components.

One thing separating this year's State of the Network Report is the increased focus on artificial intelligence and automation, both of which are now playing a much larger role in threat detection and network optimization, despite ongoing challenges around privacy concerns and integration. Zero-Trust has also gained traction as a security framework aspiration, but full-scale implementation remains slightly beyond the reach of most enterprises, mostly due to compatibility issues with legacy infrastructure.

Looking ahead, businesses that embrace proactive automation, centralized security policy enforcement, and risk-based decision-making will be best positioned to navigate the next phase of network security evolution. As organizations continue to adopt hybrid architectures, AI-driven security solutions, and Zero-Trust principles, the ability to adapt, automate, and secure at scale will be critical in ensuring a resilient and future-ready network security strategy.

# Methodology

This report is based on comprehensive research conducted by AlgoSec, gathering insights from security, network, and cloud professionals across a wide range of industries and geographic regions. The data was collected through a survey conducted in Q1 of 2025, designed to capture real-world perspectives on the challenges, priorities, and evolving trends in network security.

## Survey scope and participants

The research includes responses from 192 security, network, and cloud professionals representing 28 countries. The participants span various roles, including DevSecOps engineers, compliance officers, cloud strategy leaders, and security architects, ensuring a broad and representative view of the current state of network security. The study reflects perspectives from both enterprise-level organizations and mid-sized businesses, offering a well-rounded understanding of security strategies across different operational scales.

## Research objectives

The primary goal of this study was to identify key trends and shifts in network security practices, cloud adoption, and security infrastructure deployments. The research explores:

- How organizations are adapting their security strategies to address the growing complexity of multi-cloud and hybrid environments
- The role of automation, orchestration, and AI-driven security in modern security frameworks
- The adoption trends of key technologies, including firewalls, SD-WAN, SASE, and Zero-Trust architectures
- Challenges and barriers faced by security teams in managing policy enforcement, visibility, and compliance

## Data collection and analysis

The survey gathered quantitative and qualitative insights, providing a data-driven foundation for analysis. Participants were asked about their current security deployments, adoption plans, and the biggest challenges they face in managing their network security infrastructure. Responses were then analyzed to identify patterns, emerging trends, and shifts in market preferences, helping to shape the key findings and takeaways presented in this report.

By leveraging first-hand insights from security professionals, this study provides a real-world snapshot of the evolving network security landscape. The findings aim to help organizations benchmark their strategies, identify industry-wide challenges, and make informed decisions as they navigate the future of network security.

# 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 policy across the hybrid network environment.

With two decades of expertise securing hybrid networks, over 2200 of the world's most complex organizations trust AlgoSec to help secure their most critical workloads.

AlgoSec Horizon platform utilizes advanced AI capabilities, enabling users to automatically discover and identify their business applications across multi-clouds, and remediate risks more effectively.  It serves as a single source for visibility into security and compliance issues across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Additionally, organizations can leverage intelligent change automation to streamline security change processes, thus improving security and agility.

Learn how AlgoSec enables application owners, information security experts, SecOps and cloud security teams to deploy business applications faster while maintaining security at www.algosec.com.

For more information, visit www.AlgoSec.com