algosec

State of Network Security 2026

Marking the start of a consolidation era defined by unification, automation, and centralized control

An AlgoSec report

Table of contents

Executive summary ... 3

Trend 1: The great firewall rebalance ... 4

Trend 2: Cloud firewall strategies prioritize consolidation ... 7

Trend 3: Security becomes the deciding factor in cloud platform selection ... 8

Trend 4: SD-WAN further cements its role ... 10

Trend 5: SASE moves from exploration to standardization ... 12

Trend 6: True zero trust remains elusive ... 14

Trend 7: AI-powered threats and defenses go mainstream ... 16

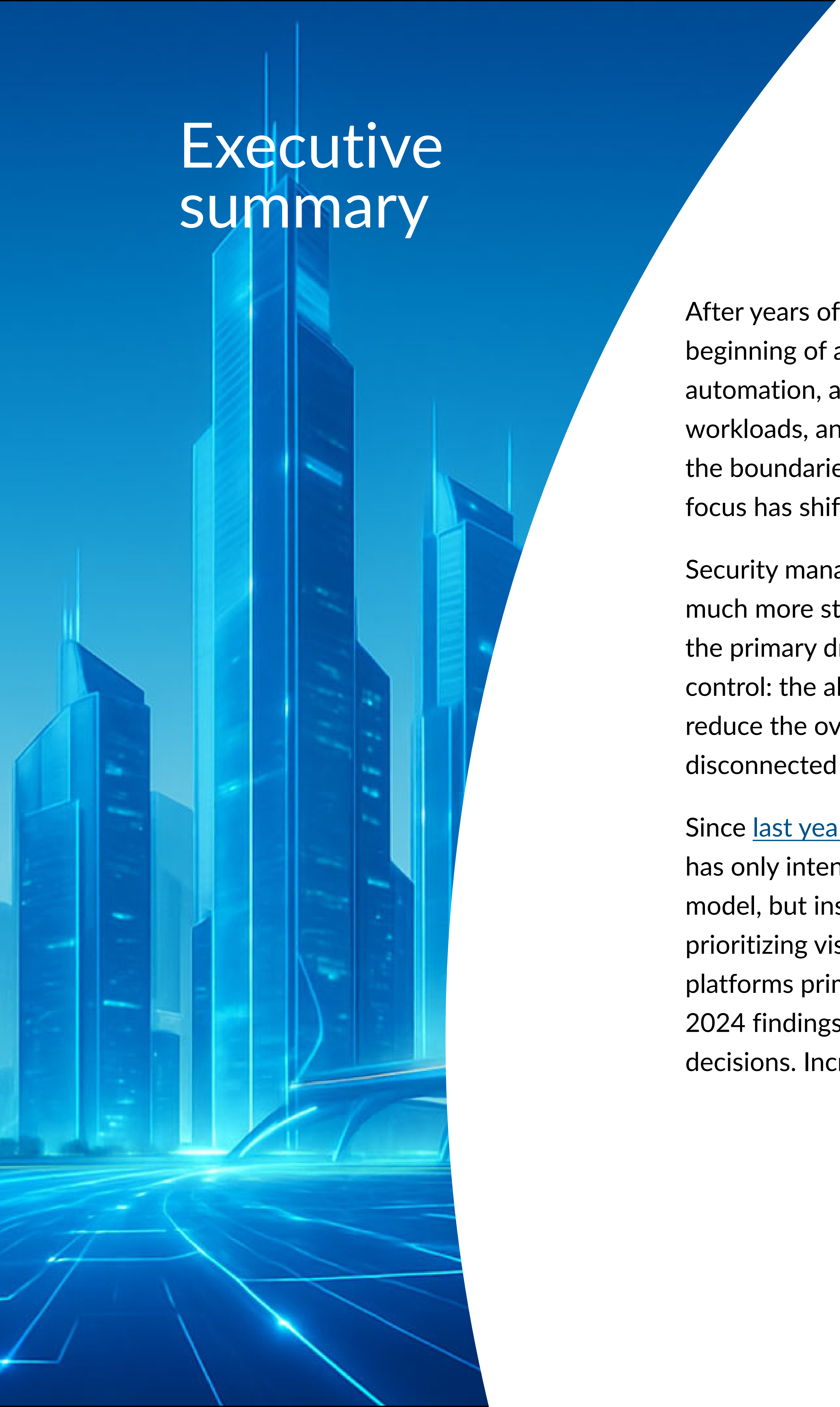
Trend 8: Automation maturity continues ... 18

Trend 9: Consolidation - teams and platforms move toward unified control ... 20

Conclusion ... 22

Methodology ... 23

About AlgoSec ... 24



Executive summary

After years of expansion and tool proliferation, 2026 will mark the beginning of a consolidation period defined by unification, automation, and control. As hybrid architectures, AI-driven workloads, and shared operational responsibilities continue to blur the boundaries between security, cloud, and network teams, the focus has shifted from adding tools to simplifying them.

Security management solutions are now being evaluated through a much more strategic lens. When respondents were asked to identify the primary driver behind their selection, the dominant theme was control: the ability to unify policies, streamline operations, and reduce the overhead that comes from managing multiple, disconnected systems.

Since last year's report, interest in consolidation and simplification has only intensified. Multi-cloud remains the dominant operating model, but instead of seeking scale and breadth, businesses are prioritizing visibility and control. 55% of companies now select cloud platforms primarily based on security, a trend reinforced by Deloitte's 2024 findings that security plays a "major role" in cloud investment decisions. Increasingly, **every cloud decision is a security decision**.

AI is reshaping this environment even further. The priority has shifted from pilot to practice, with teams applying AI to practical, low-risk functions such as hybrid network visibility, compliance enforcement, and rule optimization.

Across all trends uncovered in this research paper, the **unifying thread is consolidation**. This reflects an industry moving from fragmentation to cohesion, simplifying technology stacks, standardizing workflows, and building shared accountability across disciplines that once operated separately.

Based on insights from 504 security, network, and cloud professionals across 28 countries, this year's report offers one of the clearest snapshots yet of this transformation. As the network security landscape enters this new period of consolidation and clarity, one message stands out: resilience now depends less on how many tools an organization deploys, and more on how effectively those tools connect technically, operationally, and organizationally.

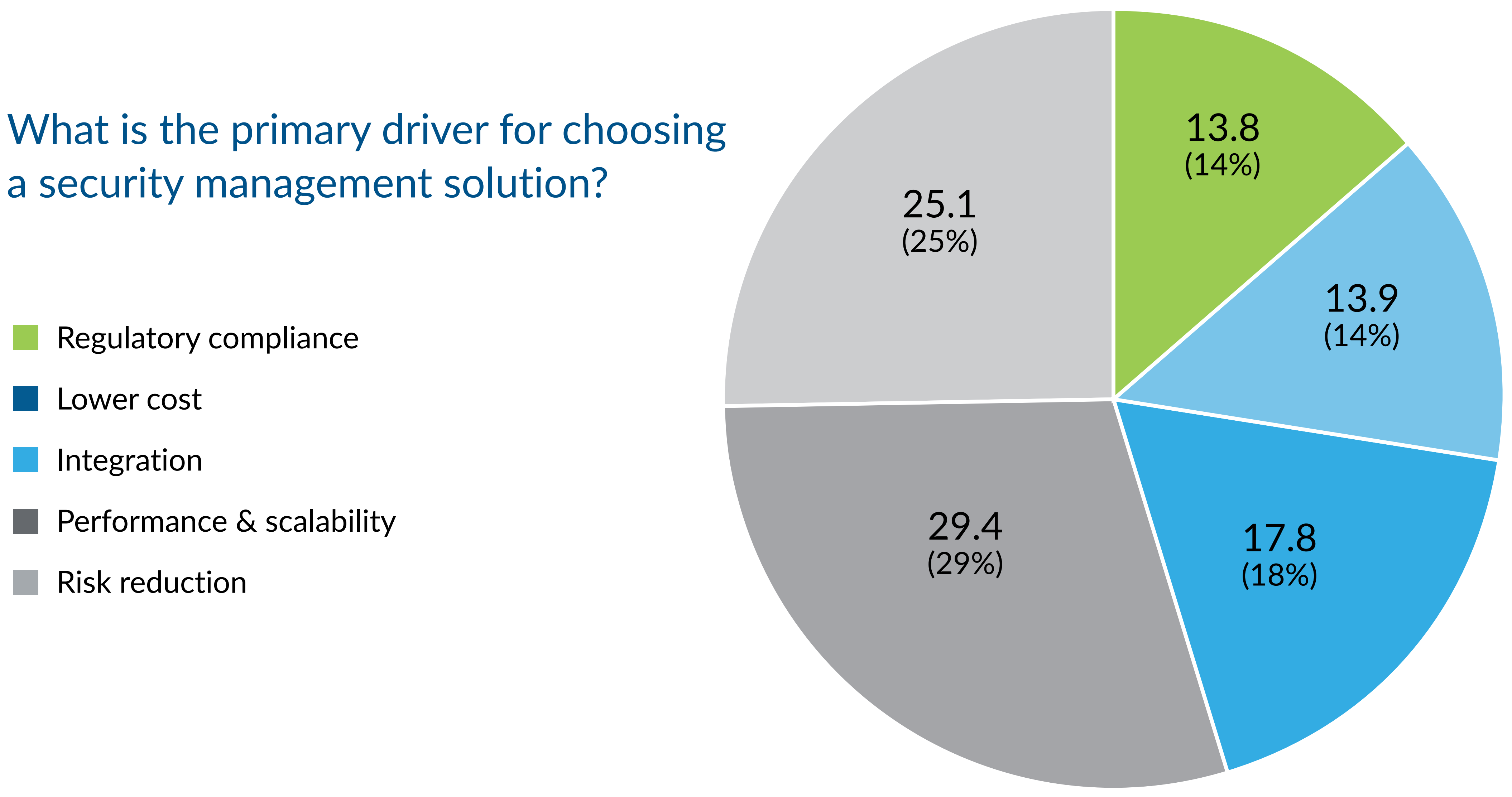
Trend 1:
The great firewall rebalance

Organizations no longer buy tools solely to check boxes for compliance or to deliver incremental improvements. Instead, they are motivated by the need to regain centralized control in the face of sprawling hybrid architectures and increasingly fragmented policy enforcement.

When respondents were asked to identify the primary driver behind their selection, the dominant theme was control: the ability to unify policies, streamline operations, and reduce the overhead that comes from managing multiple, disconnected systems. Performance and cost continue to matter, but they are no longer defining factors with performance and scalability emerging as the top driver at 29.4%. Our findings indicate that organizations are prioritizing platforms that can deliver consistent visibility across hybrid environments, integrate seamlessly with cloud-native services, and support automation at scale. This shift reinforces a broader trend seen throughout the survey – that security teams are consolidating around fewer, more capable management layers that can provide visibility in an increasingly complex network environment.

This strategic shift is tied closely to the broader evolution of the firewall itself. As hybrid and multi-cloud architectures continue to expand, the role of the firewall is undergoing its most significant shift in more than a decade. Firewalls remain a critical enforcement point for securing digital assets, but the way enterprises deploy, manage, and evaluate them is changing rapidly. Rather than treating firewalls as isolated perimeter controls, organizations are increasingly viewing them as part of a distributed, policy-driven security environment that must operate consistently across data centers, public clouds, and emerging application environments.

What is the primary driver for choosing a security management solution?



Trend 1: The great firewall rebalance

This evolution is being driven by the growing complexity of distributed infrastructures and the rising need for unified visibility. With workloads and data now spanning multiple clouds and service layers, security teams are rethinking how firewall capabilities fit into broader governance and automation frameworks. Scalability, interoperability, and centralized orchestration have become as important as raw inspection performance. What's left is a strategic rebalance, where organizations are demanding more flexibility at the edge, more consistency in the middle, and more visibility at the management layer.

Firewall strategies split across three paths

This year's findings report that 30% of respondents plan to expand into multi-vendor environments to maintain flexibility and avoid lock-in, while 24% are actively consolidating. A further 22% intend to maintain their current mix, signaling a period of stabilization after years of expansion. The data suggests that rather than pursuing one path exclusively, enterprises are balancing control and choice, consolidating at the management layer while retaining multi-vendor diversity at the edge.

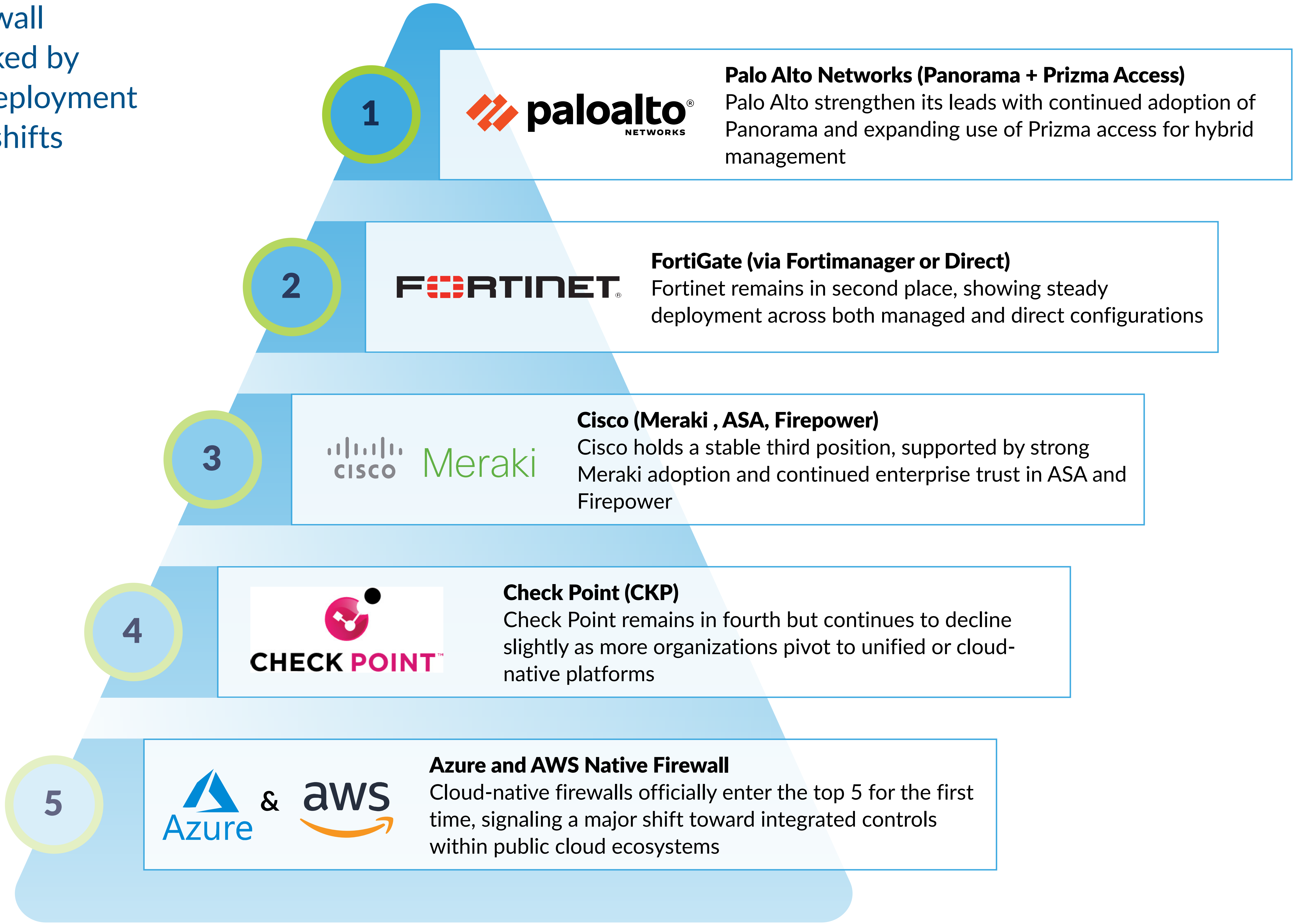
Palo Alto and Fortinet lead a tightening vendor field

Vendor preferences in 2026 highlight consolidation in practice. Palo Alto Networks has reclaimed the top position it lost in 2025, with Fortinet rising from fourth to second, showing the appeal of tightly integrated security and networking under one platform. Palo Alto has gone on the record this year stating that consolidating security data into a single platform will avoid redundant ingestion costs and, with the help of AI analytics, make insights available across the entire security stack[1] Azure Firewall drops to third as organizations rebalance native integration with cross-cloud interoperability. AWS Firewall and Check Point maintain steady adoption, while GCP enters the ranking – perhaps evidence that, even as the market consolidates, ecosystem "fit" can create room for additional players. Notably, Cisco dropped out of the cloud-firewall list entirely, reflecting a maturing market where nearly all organizations now deploy some form of pure cloud-based firewalling.

[1] https://siliconangle.com/2025/03/30/security-palo-alto-networks-sees-reset/

Trend 1: The great firewall rebalance

Top five firewall vendors ranked by enterprise deployment and market shifts



1 **Palo Alto Networks (Panorama + Prizma Access)**
Palo Alto strengthen its leads with continued adoption of Panorama and expanding use of Prizma access for hybrid management

2 **FortiGate (via Fortimanager or Direct)**
Fortinet remains in second place, showing steady deployment across both managed and direct configurations

3 **Cisco (Meraki , ASA, Firepower)**
Cisco holds a stable third position, supported by strong Meraki adoption and continued enterprise trust in ASA and Firepower

4 **Check Point (CKP)**
Check Point remains in fourth but continues to decline slightly as more organizations pivot to unified or cloud-native platforms

5 **Azure and AWS Native Firewall**
Cloud-native firewalls officially enter the top 5 for the first time, signaling a major shift toward integrated controls within public cloud ecosystems

Key takeaway

Firewall strategy is moving into a more deliberate and balanced phase. Rather than expanding indiscriminately or consolidating outright, organizations are adopting nuanced approaches that blend flexibility with control. Multi-vendor diversity remains valuable at the edge, but consolidation at the management layer is becoming essential for achieving consistent policy enforcement and operational clarity. As hybrid environments grow more complex, the enterprises that succeed will be those that rationalize their footprint without sacrificing the adaptability required in a multi-cloud world.

Trend 2:
Cloud firewall strategies prioritize consolidation

As organizations mature their hybrid and multi-cloud environments, 2026 marks an inflection point in firewall strategy. After several years of vendor diversification, the pendulum is swinging back toward consolidation. Businesses are prioritizing unified visibility, simplified operations, and consistency in policy enforcement across complex, distributed networks. In other words, the focus has shifted from expanding coverage to regaining control – reducing sprawl, streamlining management, and integrating security more deeply into cloud architectures.

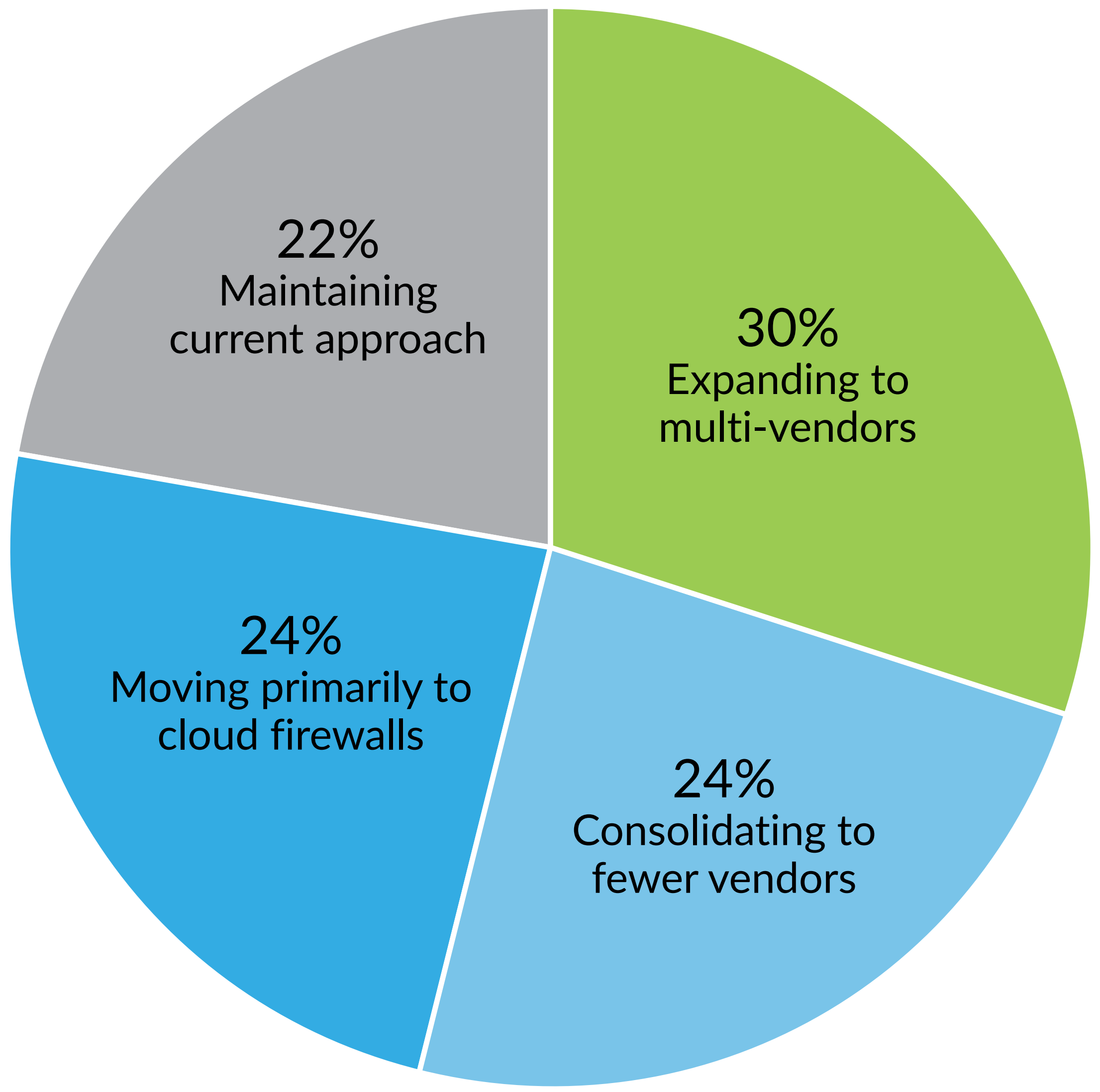
Cloud firewall adoption solidifies as a strategic standard

The move toward cloud-based firewalls continues, but with a change in tone. Rather than experimenting with cloud-native protection, most organizations now view it as essential to enterprise security. 24% of respondents plan to move primarily to cloud firewalls over the next two years, confirming that cloud-native controls are no longer an emerging consideration but a baseline expectation. As hybrid infrastructures become the norm, firewall strategies are being designed to operate seamlessly across both on-premise and cloud environments, enforcing consistent policy without introducing operational complexity.

Hybrid control replaces hybrid compromise

On the face of it, the emphasis on consolidation might signal a retreat from hybrid operations, but it actually represents a new approach to managing them. The question has simply evolved from, “which firewall secures the cloud,” to “which cloud secures the enterprise?” Firewalls are evolving from perimeter defenses into unified control planes for policy orchestration, compliance, and risk management across all environments. As AI workloads and distributed applications proliferate, organizations are standardizing policy and automating enforcement to prevent drift and maintain continuous compliance.

Over the next 2 years, how do you expect your firewall strategy to evolve?



Key takeaway

The firewall market is consolidating around fewer, more integrated vendors. Palo Alto Networks and Fortinet now anchor the field, with cloud-native solutions firmly mainstream and GCP emerging as a secondary player. The dominant priority for 2026 is control: simplifying management, tightening policy enforcement, and building the unified visibility layer that modern hybrid enterprises depend on for resilience.

Trend 3:

Security becomes the deciding factor in cloud platform selection

The cloud has now confidently become the enterprise control layer, where security, data, and consolidation converge. As organizations mature their multi-cloud strategies, the criteria for choosing providers are shifting. Performance and price remain relevant, but they are no longer decisive. In 2026, the dominant priority will be security, confirming that every cloud decision will indeed be a security decision. The rise of AI-driven workloads, compliance requirements, and cross-platform orchestration has made security the critical benchmark for platform selection.

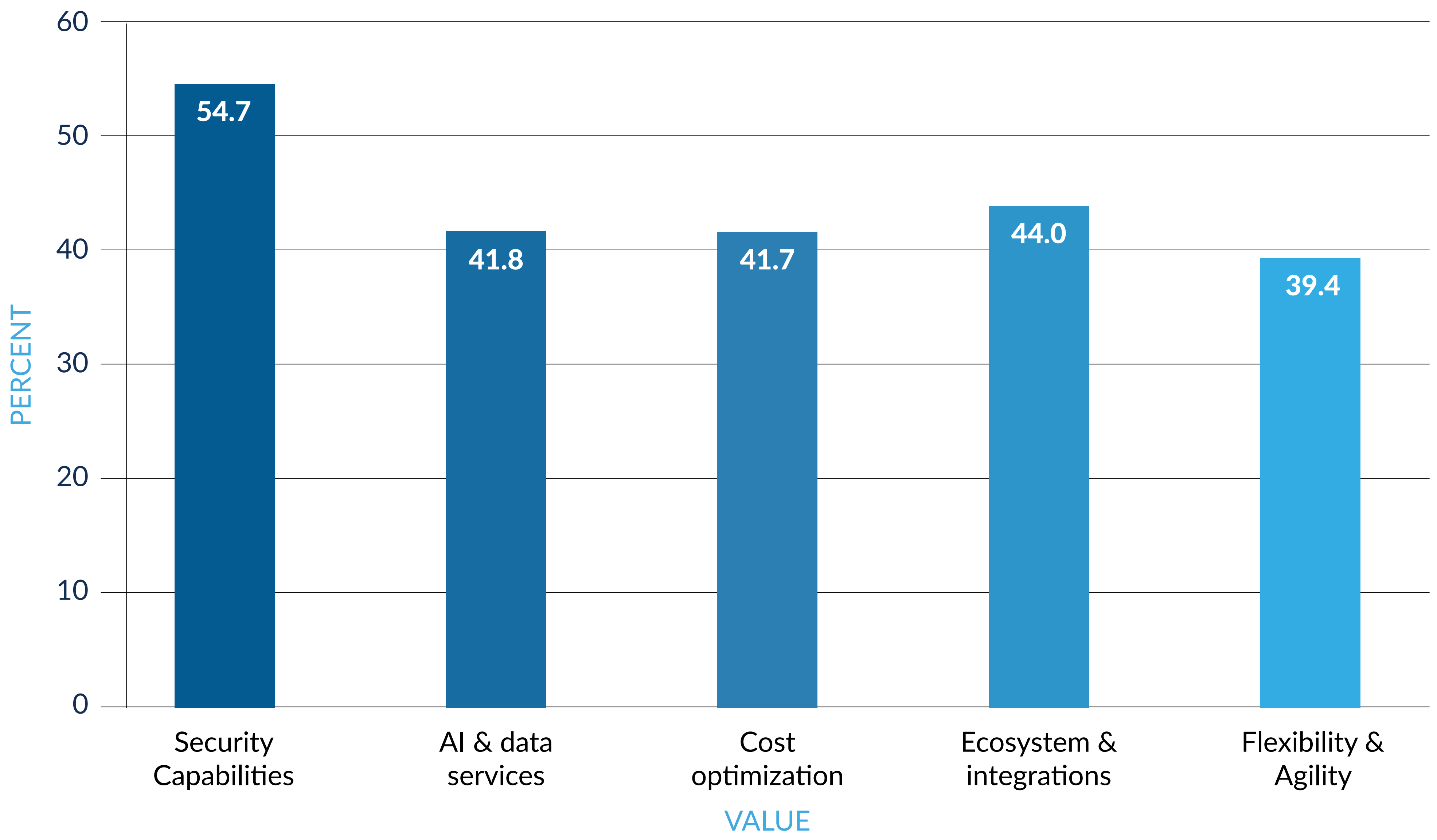
Security leads cloud decision-making

According to Gartner, worldwide end-user spending on public cloud services reached $723.4 billion in 2025 (up from $595.7 billion in 2024)[2]. More than half (55%) cited security as their top consideration, far exceeding any other factor. Ecosystem and integrations ranked second at 44%, while AI and data services (42%) followed closely behind. Collectively, this paints a picture of a market driven by protection, compatibility, and intelligence rather than cost. The finding also underscores a broader mindset shift – enterprises are no longer treating cloud as infrastructure, but as the foundation for secure operations.

Integration and ecosystem strength outweigh price and performance

The emphasis on ecosystem integration reflects how organizations are consolidating around platforms that offer tighter interoperability across security, networking, and data layers. Rather than adopting best-of-breed tools in isolation, businesses are favoring providers that enable unified visibility and shared policy control. This trend echoes the broader consolidation theme observed across firewall and automation data: complexity has reached its limit, and integration has become the differentiator.

When selecting a cloud platform, which factor carries the most weight?



[2] https://www.gartner.com/en/newsroom/press-releases/2024-11-19-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-total-723-billion-dollars-in-2025

Trend 3: Security becomes the deciding factor in cloud platform selection

AI and data services redefine platform value

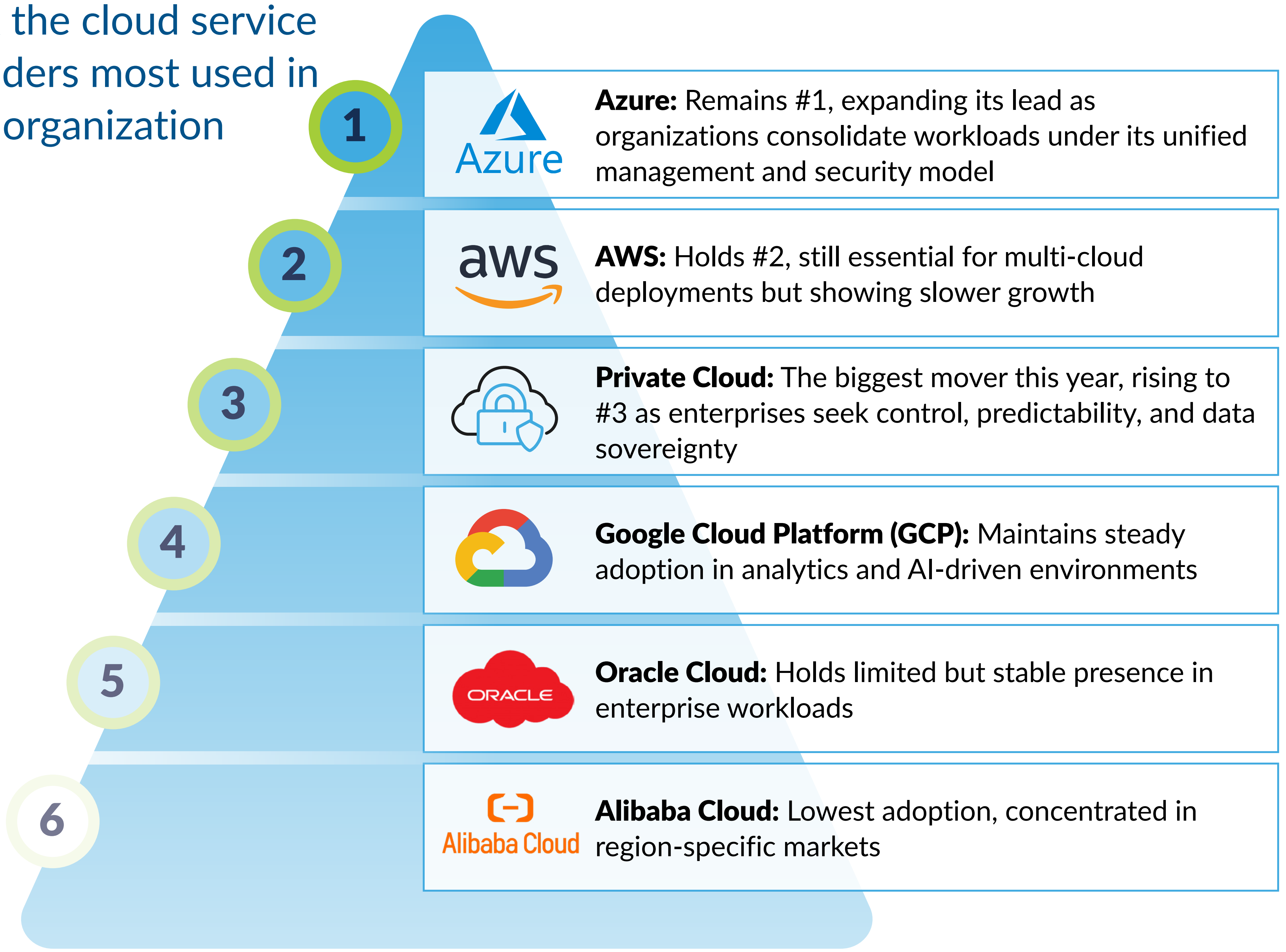
The inclusion of AI and data services among the top selection criteria signals a growing recognition that intelligence is now inseparable from security. Organizations increasingly choose cloud platforms that can support AI-enhanced monitoring, anomaly detection, and compliance analytics within the same environment. The result is a more strategic alignment between where data resides and how it is protected, a shift from infrastructure management to intelligent security orchestration.

Consolidation shapes platform strategy

These findings also reflect a broader pattern of consolidation across cloud ecosystems. While multi-cloud remains the operational norm, the drivers behind it have changed. Rather than spreading workloads for cost or redundancy, organizations are choosing fewer platforms and using them more deeply, consolidating workloads, policies, and visibility tools to reduce friction. The balance of flexibility and control remains key, but the overall gravitational pull is toward simplification.

Consistent policy enforcement overtakes visibility as the top cloud security challenge

The findings from the survey show a notable shift in the challenges organizations face when securing cloud applications. For the first time, maintaining consistent policies across on-premise and cloud environments (58.6%) has overtaken lack of visibility into cloud applications (54.3%) as the number-one obstacle. This change reflects the realities of growing tool sprawl and increasingly mixed deployment models. As businesses consolidate platforms and pursue unified control, the problem isn't identifying what applications exist, but enforcing the right policies for those applications across multiple clouds, networks, and security layers. This also reinforces the broader consolidation narrative, where consistency is key to cloud security.



Rank the cloud service providers most used in your organization

1 **Azure:** Remains #1, expanding its lead as organizations consolidate workloads under its unified management and security model

2 **AWS:** Holds #2, still essential for multi-cloud deployments but showing slower growth

3 **Private Cloud:** The biggest mover this year, rising to #3 as enterprises seek control, predictability, and data sovereignty

4 **Google Cloud Platform (GCP):** Maintains steady adoption in analytics and AI-driven environments

5 **Oracle Cloud:** Holds limited but stable presence in enterprise workloads

6 **Alibaba Cloud:** Lowest adoption, concentrated in region-specific markets

Key takeaway

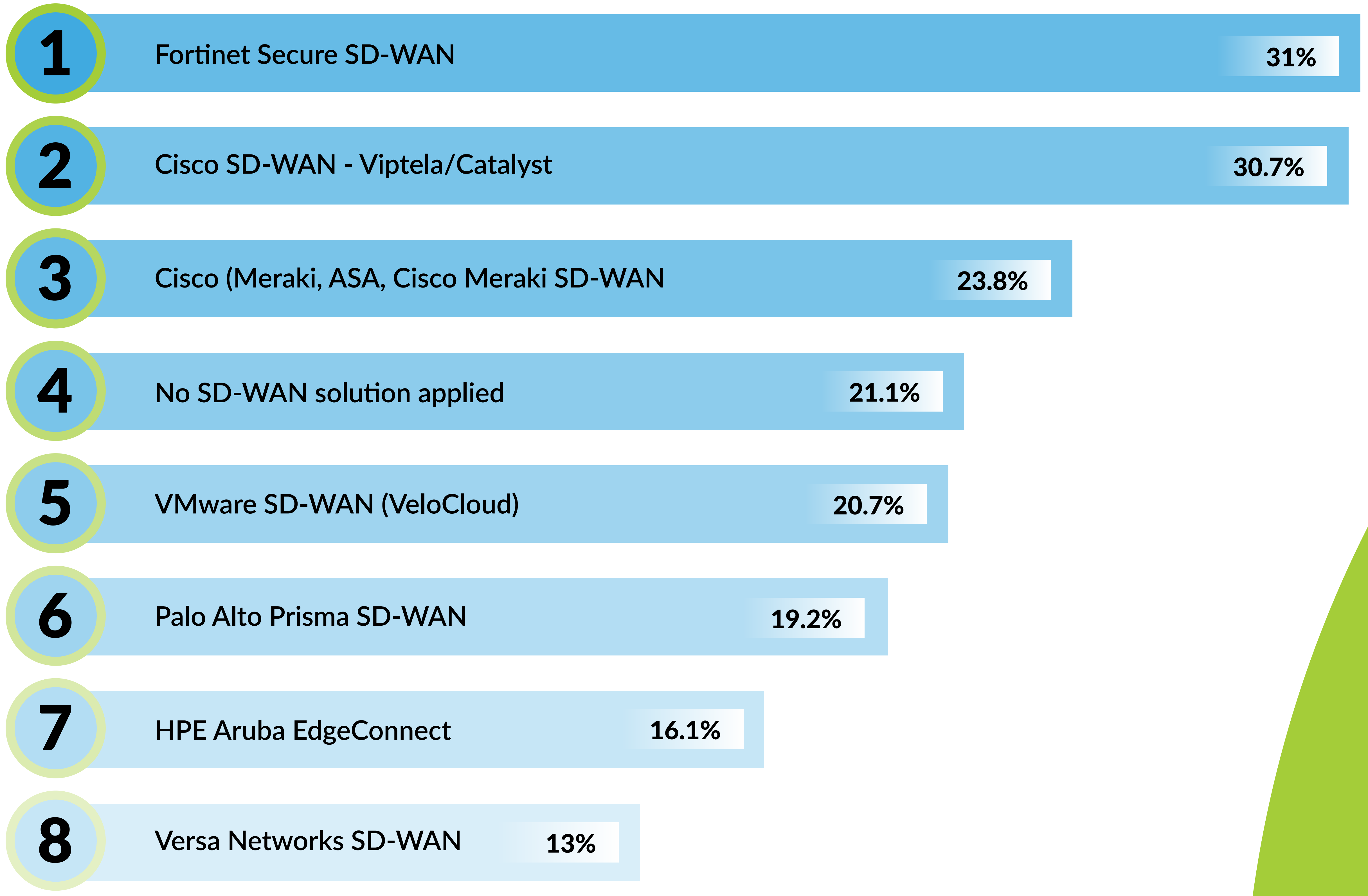
It would be reasonable to say that cloud strategy and security strategy are now one and the same. With more than half of organizations ranking security as the defining factor in provider selection, this year has cemented the cloud's role as the enterprise security backbone. The future of multi-cloud will not be decided by speed or scale alone, but by how effectively each platform can deliver integrated protection, data intelligence, and operational clarity across the entire digital estate.

Trend 4:
SD-WAN further cements its role

The enterprise network edge continues to evolve, with SD-WAN now established as a mainstream capability rather than a specialist solution. As organizations expand their hybrid environments and distributed workforces, the demand for secure, high-performance connectivity has solidified SD-WAN's role as the connective tissue between data centers, clouds, and users. This year's findings show that the market is maturing: adoption is nearly universal, leadership has reshuffled, and the differentiator is no longer deployment speed but the depth of security integration.

SD-WAN adoption reaches maturity

For the first time, SD-WAN can be considered standard practice across most enterprise environments. The share of organizations reporting no solution applied has dropped sharply to 21.1%, confirming that SD-WAN has moved beyond early adoption. Businesses increasingly view it as foundational to hybrid and multi-cloud architectures, providing the visibility and policy control that traditional WAN models lacked. The focus now is on consolidating SD-WAN with broader security frameworks to create unified, adaptive network fabrics.



Trend 4: SD-WAN further cements its role

Fortinet takes the lead in an increasingly competitive market

This year's results mark a significant milestone: Fortinet (31%) has become the most widely used SD-WAN solution for the first time, reflecting its strength in integrating advanced security and networking under one platform. Cisco (30.7%) remains a close second, leveraging both its Viptela and Meraki offerings to address enterprise and distributed site use cases. VMware (20.7%) and Palo Alto Networks (19.2%) maintain consistent adoption, while Aruba (16.1%) and Versa (13%) continue to serve mid-enterprise and service-provider environments. The data suggests a crowded but stabilizing market, with leadership now determined by convergence rather than coverage.

Integration overtakes performance as the new priority

While performance and scalability remain important, the defining value of SD-WAN this year will be integration, particularly its ability to operate seamlessly within consolidated security ecosystems. According to Gartner, by the end of 2026, 60% of new SD-WAN purchases will be part of a single-vendor SASE offering, up from 15 % in 2022.[3] Organizations are no longer viewing SD-WAN as a stand-alone connectivity layer but as a key component of unified network and security orchestration. This trend is reinforced by the parallel growth of Secure Access Service Edge (SASE), where many SD-WAN platforms now serve as the underlying transport for cloud-delivered security functions.

Simplified management drives next-phase adoption

As the market matures, ease of management has emerged as a primary differentiator. Enterprises want simplified, policy-based control that extends across both SD-WAN and security operations. Vendors capable of offering single-pane management, covering traffic routing, segmentation, and threat prevention, are gaining a decisive edge. This shift underscores the industry's pivot from product expansion to platform unification, where value lies in operational simplicity and end-to-end visibility.

Key takeaway

SD-WAN has transitioned from optional to essential. Adoption is near-universal, and leadership now depends on the depth of integration with security and orchestration platforms. Fortinet has overtaken Cisco to lead the market, signaling that convergence, not performance, is the new metric for success. As enterprises strive to unify their networking and security stacks, SD-WAN's role as the foundation of hybrid connectivity has never been clearer.

[3] https://www.fierce-network.com/cloud/gartner-analysis-forces-reshaping-sd-wan-landscape

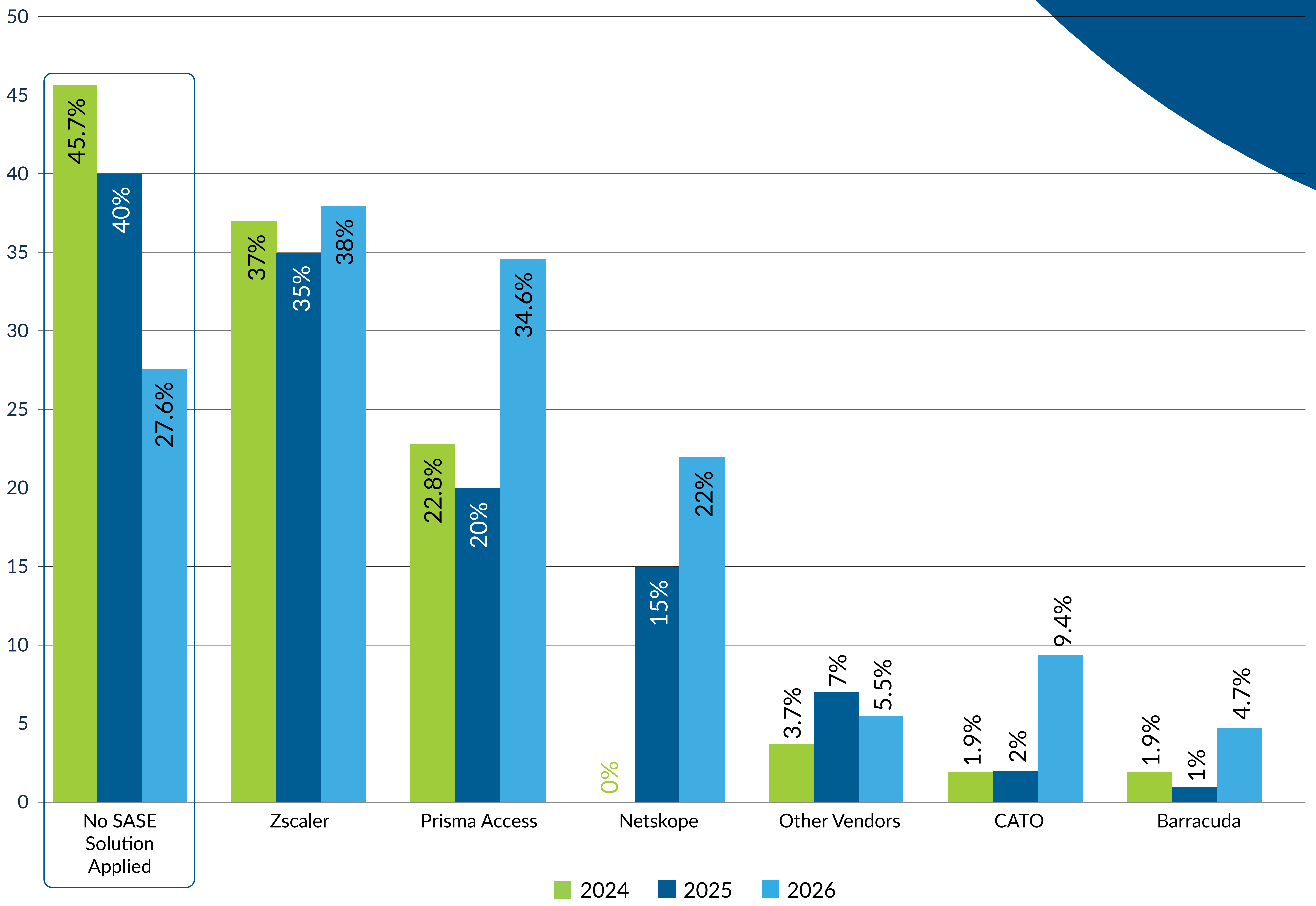
Trend 5:
SASE moves from exploration to standardization

Secure Access Service Edge (SASE) continues its steady progression from a niche innovation to a mainstream framework for unified security and networking. Once viewed primarily as an aspirational goal, SASE is now being operationalized across industries as organizations seek to consolidate connectivity, control, and cloud-delivered protection within a single architecture. This year's findings show a market that has matured beyond experimentation. Adoption is broadening, vendor leadership is stabilizing, and integration with SD-WAN has become the norm.

Non-adoption falls for the third consecutive year

For the third year running, the share of organizations without a SASE solution has declined, down to 27.5% from 40% in 2025. This consistent decrease signals that SASE adoption is no longer exploratory but a planned progression for most enterprises. The increasing prominence of SASE is also reflected by Gartner, who estimate that between 2025 and 2028 the market will have a CAGR of 26% and exceed $30 billion by the end of the decade[4]. As hybrid and remote workforces become permanent fixtures, businesses are embedding SASE as the control layer that secures access, governs data movement, and enforces consistent policy across all environments. The technology's role has shifted from experimental pilot to strategic pillar.

Which SASE platform is your organization using?



[4] https://www.gartner.com/en/documents/6152891

Trend 5: SASE moves from exploration to standardization

Zscaler and Prisma Access maintain leadership amid growing competition

Zscaler (37.8%) remains the market leader in SASE adoption, closely followed by Palo Alto Networks' Prisma Access (34.4%). Both platforms have consolidated their positions through strong ecosystem partnerships and mature policy integration, particularly across large enterprise deployments. Netskope (21.9%) continues its rapid ascent as the fastest-growing challenger, driven by its focus on data protection and multi-cloud visibility. Smaller providers, including Cato (9.3%), Barracuda (4.7%), and other vendors (5.4%), maintain regional or industry-specific footholds where turnkey simplicity and localized deployment remain priorities.

SD-WAN and SASE converge under single-vendor models

According to the Dell'Oro Group, single vendor SASE will grow twice as fast as multi-vendor SASE in the next few years[5]. Organizations increasingly favor single-vendor frameworks that deliver both connectivity and security from the same platform, reducing latency and operational overhead. This reflects the same drive toward consolidation seen across the broader network security landscape to fewer moving parts, shared visibility, and unified control. Last year's Gartner projection that more than half of SD-WAN purchases will be tied to integrated SASE offerings[6] by 2026 appears well on track. In fact, the Dell'Oro Group anticipates single-vendor SASE will make up 90% of the market by the end of the decade.

Implementation complexity gives way to operational consistency

The challenges that once slowed SASE adoption, such as multi-component integration, legacy dependencies, and management fragmentation, are giving way to more standardized deployment models. Enterprises are learning to phase implementation, layering security and access capabilities without disrupting core connectivity. As policy orchestration becomes more automated and AI-assisted, SASE is evolving from a complex project to an achievable operational baseline for hybrid enterprises.

Key takeaway

SASE has crossed the threshold from early adoption to normalization. Zscaler and Prisma Access continue to lead, but Netskope's rapid rise shows that innovation still drives competition. The decline in non-adoption rates confirms that SASE is now the de-facto model for secure, distributed access, valued for its operational simplicity and the consistency it delivers across the modern enterprise network.

[5] https://www.delloro.com/news/single-vendor-sase-to-grow-twice-as-fast-as-multi-vendor-sase

[6] https://www.fierce-network.com/cloud/gartner-analysis-forces-reshaping-sd-wan-landscape

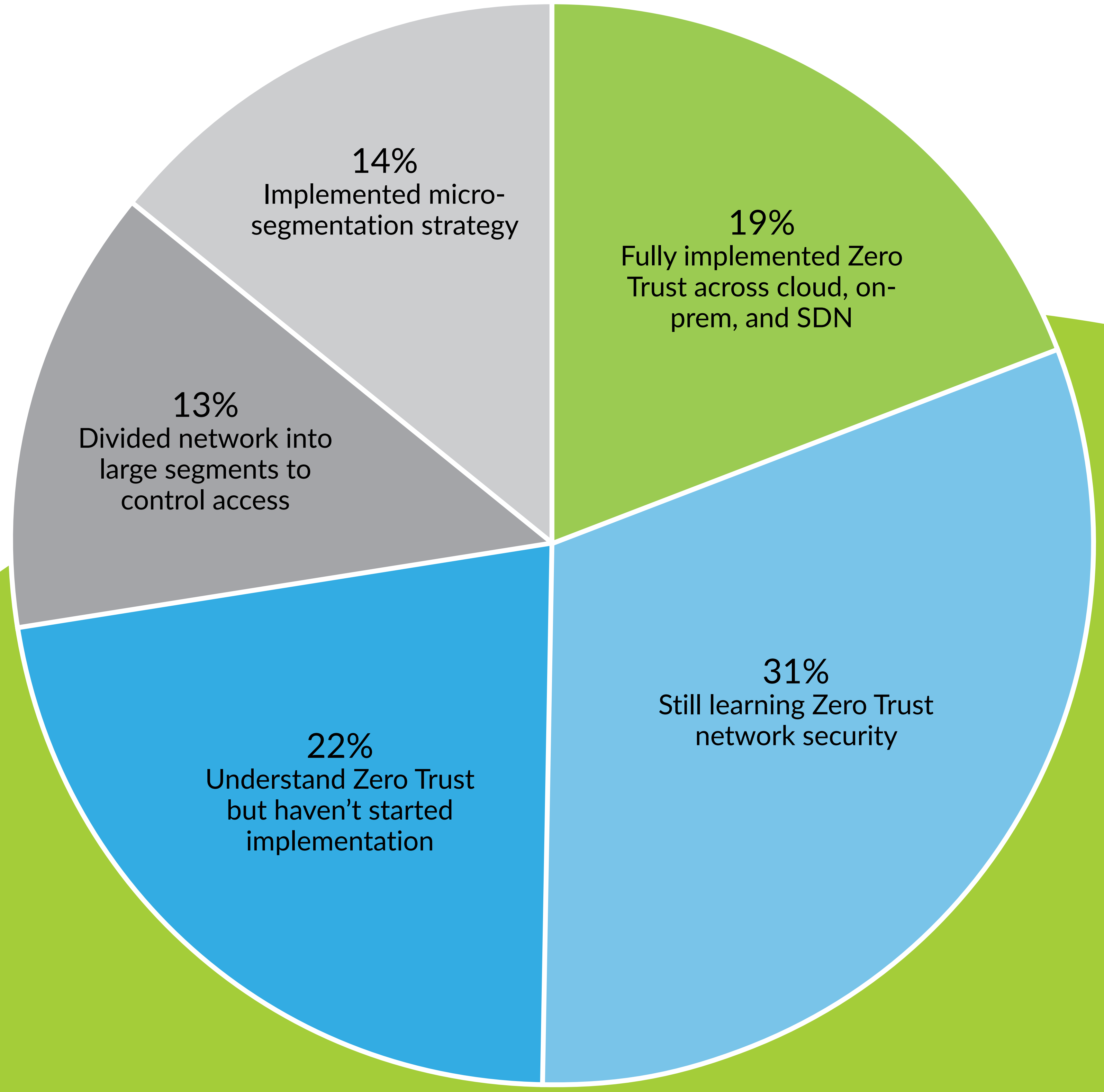
Trend 6:
True zero trust remains elusive

Zero Trust remains one of the most discussed principles in cybersecurity, yet one of the slowest to fully materialize in practice. The philosophy of "never trust, always verify" continues to guide strategic planning, but this year's data reveals that operational progress has stalled. Awareness and intent are high, but implementation maturity has plateaued. Most organizations have laid the groundwork, such as segmentation, identity management, and access control, but few have advanced beyond these initial stages to comprehensive, policy-driven Zero Trust frameworks.

Adoption steady, but forward motion limited

Overall Zero Trust adoption remains consistent at around 55-60%, nearly identical to last year. However, the share of organizations still in the learning phase has increased from 20% to 31%, indicating that while more enterprises are engaging with the concept, fewer are moving to execution. This highlights a widening gap between intent and implementation, where Zero Trust is now universally recognized as the right approach, but practical deployment continues to challenge even mature security teams.

What is your current Zero Trust implementation status?



Trend 6: True zero trust remains elusive

Execution gaps widen as awareness grows

The data also shows that increased awareness has not translated into faster rollout. Many enterprises are still navigating legacy infrastructure, fragmented identity systems, and policy enforcement across hybrid networks. Even organizations that have implemented partial Zero Trust measures, such as micro-segmentation or network division, often lack unified governance models. The result is a growing class of "permanently pilot" deployments that are "active," but not yet integrated or automated. This finding is echoed by Gartner, which revealed that in 2026, only 10 % of large enterprises will have a "mature and measurable" Zero Trust programme in place, up from less than 1 % today[7].

Fragmented approaches slow standardization

The variety of adoption paths available further complicates progress. Some organizations are investing in Zero Trust Network Access (ZTNA) as an entry point, while others prioritize endpoint verification or identity-based access control. This flexibility allows for adaptation but prevents standardization, making it difficult to measure maturity consistently across industries. The absence of a universal framework also leads to uneven tool adoption and inconsistent results, reinforcing the need for clearer guidance and shared benchmarks.

Education becomes the critical barrier

The rising proportion of organizations still in the learning phase reflects a shortage of accessible best practices and practical guidance. Many teams understand the goal of Zero Trust but struggle to translate it into architectural blueprints or measurable outcomes. Training, governance alignment, and vendor-neutral frameworks are now essential to bridge this gap, ensuring that education accelerates adoption rather than replacing it.

Key takeaway

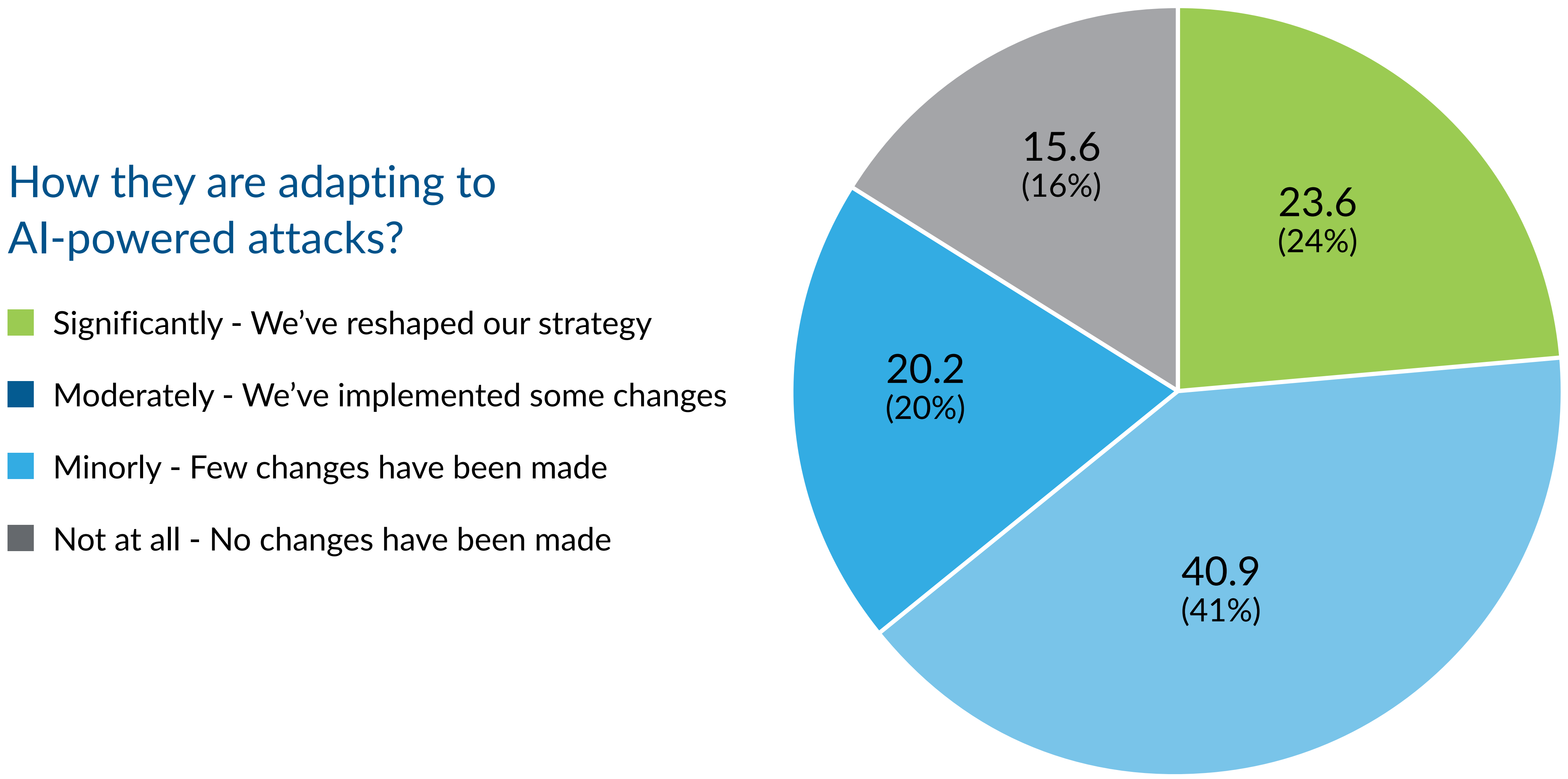
Zero Trust remains the strategic north star for enterprise security, but the journey toward full implementation has stalled. Awareness is at an all-time high, yet maturity has barely shifted. This year's findings highlight an execution gap driven by complexity, fragmented infrastructure, and limited practical guidance. Organizations that focus on education, cross-team alignment, and measurable governance will be best positioned to move Zero Trust from aspiration to operational reality.

[7] https://www.gartner.com/en/newsroom/press-releases/2023-01-23-gartner-predicts-10-percent-of-large-enterprises-will-have-a-mature-and-measurable-zero-trust-program-in-place-by-2026

Trend 7:
AI-powered threats and defenses go mainstream

Artificial intelligence has become both the newest threat vector and the next frontier of defense. According to McKinsey, phishing attacks have surged by 1200% since generative AI went mainstream in 2022, but at the same time, more than 90% of defensive AI capabilities are being outsourced to third parties – showing that businesses are keen to leverage the technology to defend themselves[8].

That trend will continue in 2026, when the conversation around defensive AI will move beyond theory and into practice. Organizations are no longer asking if AI will change their security posture. Instead they want to know how fast they can adapt. Our findings show that while most enterprises are already taking steps to address AI-powered attacks, only a minority have made the deeper structural and procedural changes needed to counter them effectively. The result is a mixed picture - strong awareness, accelerating experimentation, but uneven readiness.



How they are adapting to AI-powered attacks?

Most organizations are adapting, but depth of change varies

The majority (65%) have already adapted their strategies, with 23.6% making major structural changes and 40.9% implementing moderate adjustments. Surprisingly, only 15.6% reported no action at all. This points to an industry that has accepted the inevitability of AI as both an enabler and an adversary. However, while surface-level adaptations are widespread, the transformation of governance, tooling, and training remains in its early stages.

AI investment shifts toward visibility and control

This year's responses mark a sharp contrast to last year. Where last year's priorities centered on real-time notifications and incident response, this year focus has shifted to AI-powered visibility and risk prioritization (39.1%). Organizations are using AI to map hybrid networks, detect policy drift, and surface anomalies faster. AI-driven compliance and policy enforcement (23.7%) has emerged as the next priority, reflecting growing confidence in machine-led governance for structured, repeatable tasks. In essence, enterprises are applying AI where precision matters more than prediction.

[8] https://www.mckinsey.com/about-us/new-at-mckinsey-blog/ai-is-the-greatest-threat-and-defense-in-cybersecurity-today

Trend 7: AI-powered threats and defenses go mainstream

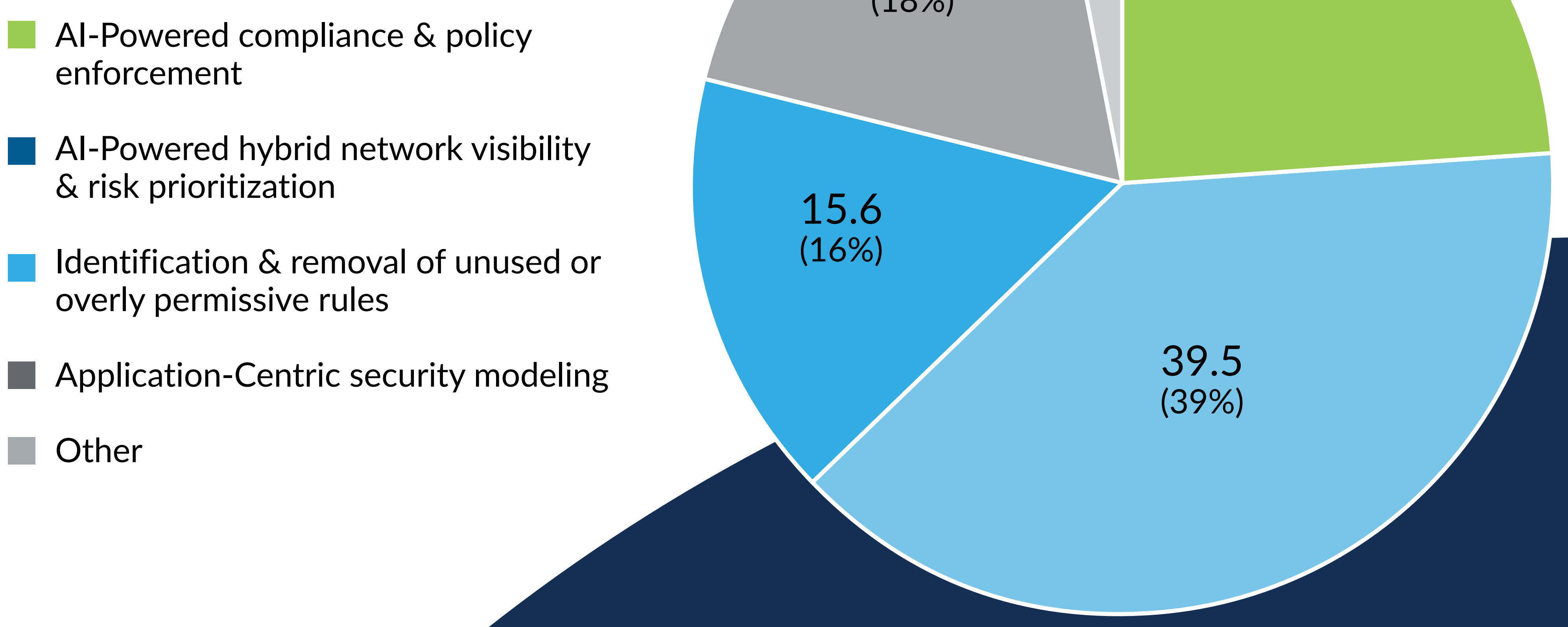
Operational hygiene overtakes experimentation

While generative AI captured early attention, most organizations are deploying AI to improve operational hygiene rather than innovation. Application-centric security modeling (18.4%) and identification of unused or overly permissive rules (15.8%) rank lower but illustrate a pragmatic trend: using AI to clean up, not reinvent. These controlled, low-risk use cases deliver measurable value while avoiding the unpredictability associated with broader AI automation. The preference for predictability over experimentation signals a cautious but maturing stage of adoption.

AI readiness exposes gaps in governance and skills

Despite rising adoption, governance and human oversight remain persistent challenges. Many teams lack formal frameworks to validate AI-driven decisions or ensure accountability when automated systems act autonomously. The gap between AI's technical potential and organizational readiness mirrors the early years of cloud adoption, where enthusiasm outpaced structured implementation. Without parallel investments in training, oversight, and transparent governance, AI-powered defenses risk replicating the same visibility issues they are meant to solve.

Which AI cases will have the greatest impact over the next 2 years?



Key takeaway

AI has become a defining force in network security, driving both threat evolution and defensive transformation. Two-thirds of organizations have already adjusted their strategies, but maturity levels remain uneven. The focus has shifted decisively from detection to visibility, and from experimentation to control. As enterprises refine their governance frameworks and strengthen human oversight, AI will transition from a reactive tool to an operational cornerstone, turning awareness into measurable resilience.

Trend 8:
Automation maturity continues

What began as a gradual shift toward orchestration and policy simplification in previous years has now become a defining operational capability. Our research confirms that automation has matured into a measurable discipline that directly influences efficiency, compliance, and resilience across hybrid networks. Yet while the benefits are increasingly clear, full-scale orchestration across environments remains a work in progress.

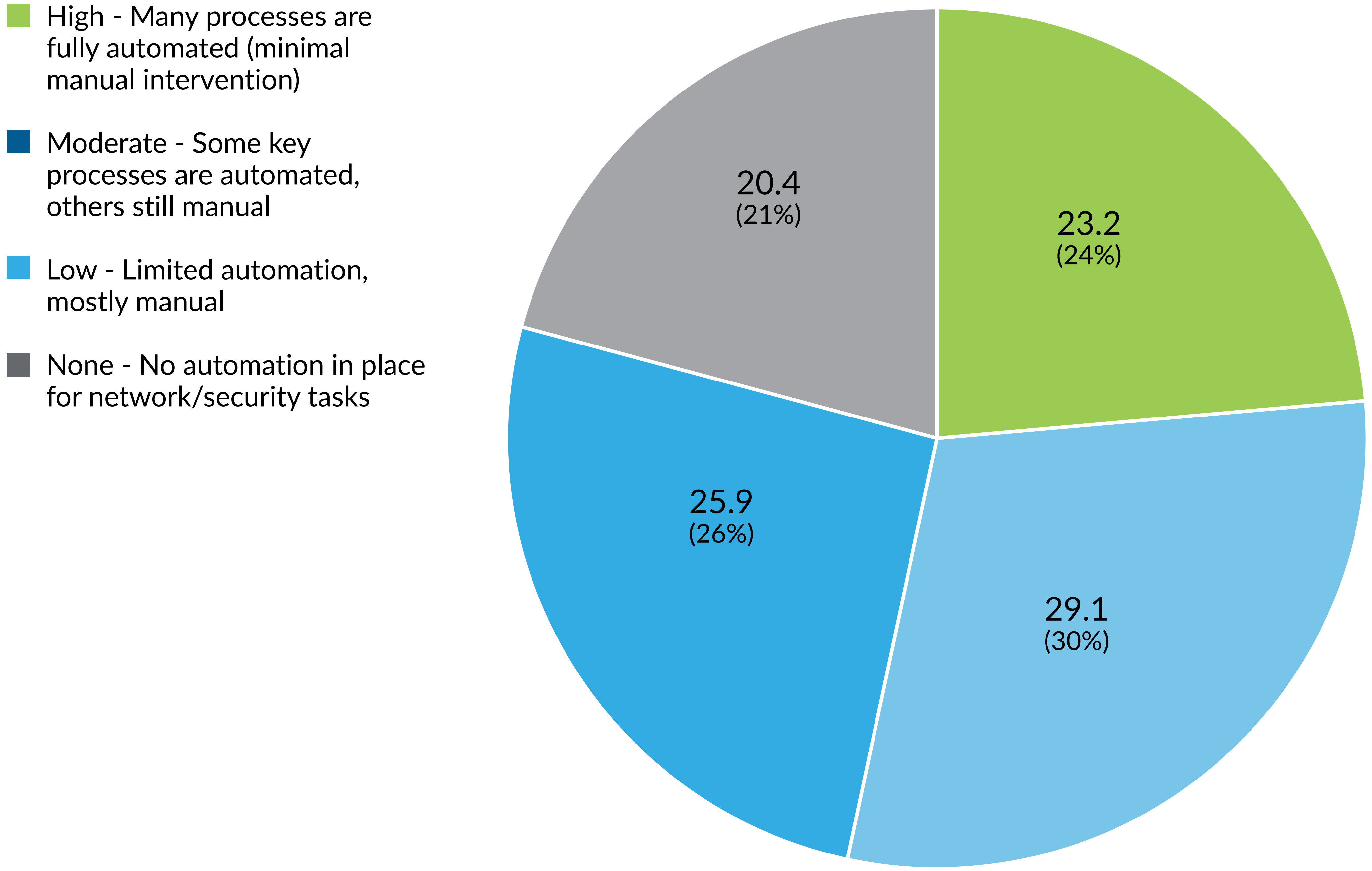
Automation becomes a measurable benchmark

The results show a clear divide: 24% of organizations now operate at a high level of automation, while 30% report moderate automation. Twenty-six percent remain at a low level, and 20% still rely primarily on manual processes. This sprawl validates last year's prediction that automation would become foundational to network security. It also underscores the persistence of a maturity gap between those leveraging automation strategically and those applying it reactively to reduce workloads.

From process acceleration to policy assurance

Beyond accelerating workflows, organizations are now using automation to enforce security policy consistently across hybrid environments. This includes automated risk analysis, change verification, and compliance tracking - all areas once dominated by manual oversight. By shifting from speed to assurance, automation has become central to maintaining reliability and reducing configuration drift, particularly in multi-vendor or multi-cloud architectures where consistency is hardest to achieve.

How would you describe your organization's current level of automation in network security management?



Trend 8: Automation maturity continues

Operational and cultural barriers persist

Despite progress, barriers remain. Many organizations struggle to extend automation across silos, particularly between cloud, network, and application security teams. Legacy approval processes, lack of centralized governance, and limited cross-tool integration continue to restrict scalability. This has resulted in "partial" automation, where specific workflows are automated, but end-to-end orchestration across systems and teams remains difficult to pin down. This mirrors the early adoption curve we saw in cloud migration – progress being built through incremental cultural and procedural change rather than technology alone.

A proving ground for AI-enhanced orchestration

The intersection between automation and AI is emerging as the next frontier. AI-assisted orchestration tools are beginning to optimize rule management, recommend policy changes, and predict the downstream impact of configuration updates. However, confidence in fully autonomous decision-making remains low. For now, organizations are embracing a human-in-the-loop model, where automation handles execution while humans retain control of validation and governance. This balance is shaping a pragmatic, risk-conscious approach to automation at scale.

Key takeaway

Automation has evolved from a strategic ambition into an operational benchmark. Nearly half of all organizations now operate with moderate to high levels of automation, validating its role as a core pillar of network security. Yet maturity remains uneven, with cultural inertia and fragmented governance slowing progress. The next leap will come from convergence and uniting automated workflows, AI-assisted orchestration, and unified policy management to deliver the end-to-end agility and assurance enterprises have long aimed for.

Trend 9:
Consolidation - teams and platforms move toward unified control

As hybrid environments expand and the boundaries between cloud, network, and security responsibilities continue to blur, businesses are rethinking not only what they manage but how they manage it. Our findings reveal an industry shifting toward shared accountability, unified visibility, and integrated control. Consolidation is happening at two levels: teams and platforms, and both are accelerating.

Team structures shift toward shared ownership

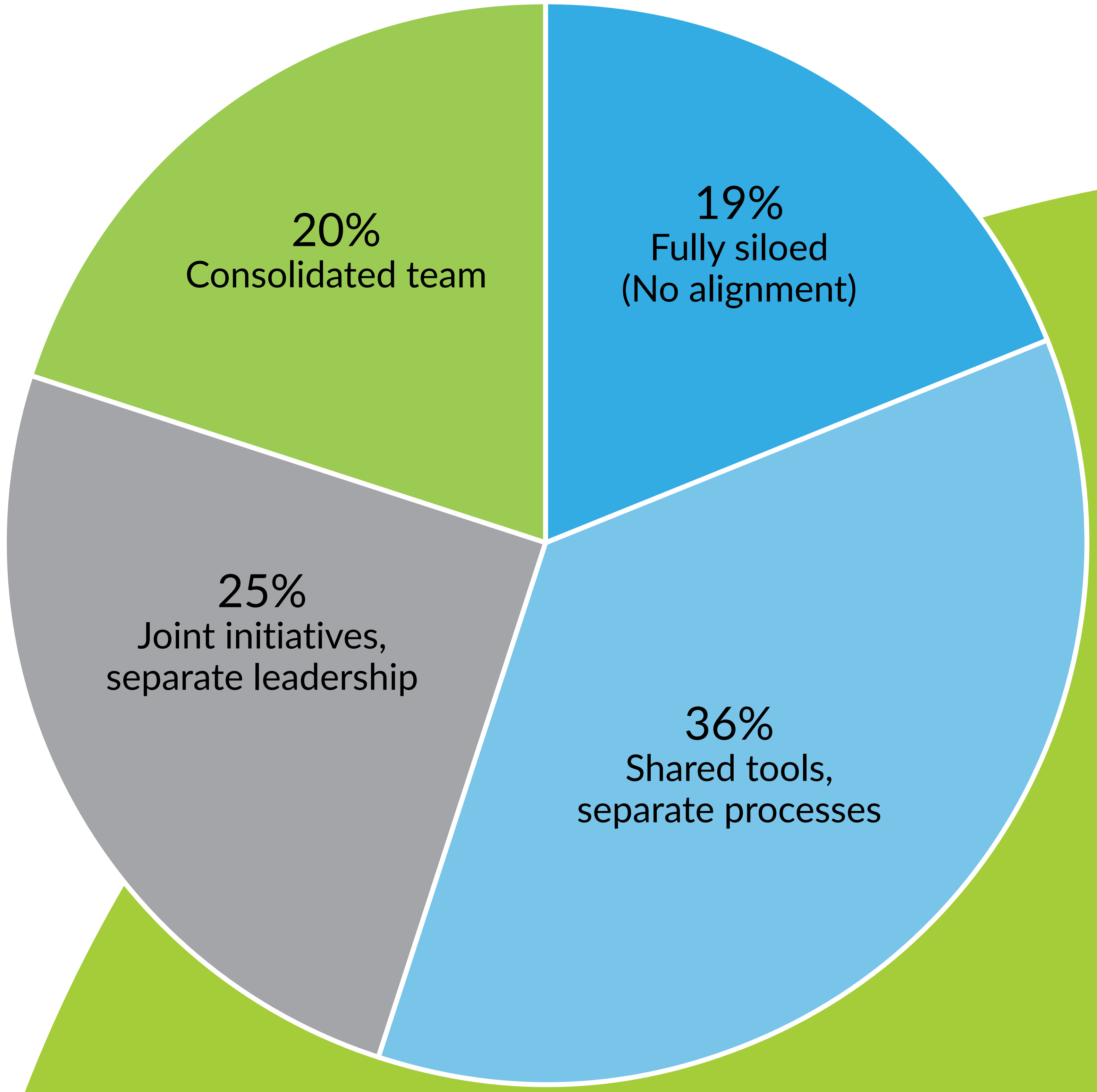
The operational model for security is undergoing a quiet but significant transformation. Organizations are moving away from isolated, domain-specific teams and toward structures that promote shared priorities and cross-functional coordination. The findings show that only 19% are currently working in siloed departments, while 36% of respondents report that their cloud, network, and security teams have consolidated around shared tools. A further 25% of respondents have aligned around shared initiatives and 20% have gone further, operating as fully consolidated teams.

This represents a substantial step toward unified governance. Instead of managing separate workflows or conflicting priorities, teams are aligning around common frameworks for risk, compliance, and service delivery. As AI and automation become more embedded in operations, this collaborative approach is emerging as the new standard for effective decision-making and consistent policy enforcement.

Shared tools become the foundation for cross-team alignment

The rise of shared tooling reflects a deliberate move toward standardization. When cloud, network, and security teams use different systems, visibility fractures and operational gaps appear. But when they converge around shared management layers and shared data sources, collaboration becomes frictionless. This year’s results show that shared tools are now the primary mechanism for team alignment, which is the strongest sign yet that consolidation is being built from the ground up through day-to-day operational workflows rather than top-down restructuring.

How would you best describe the current alignment of cloud & network security teams?

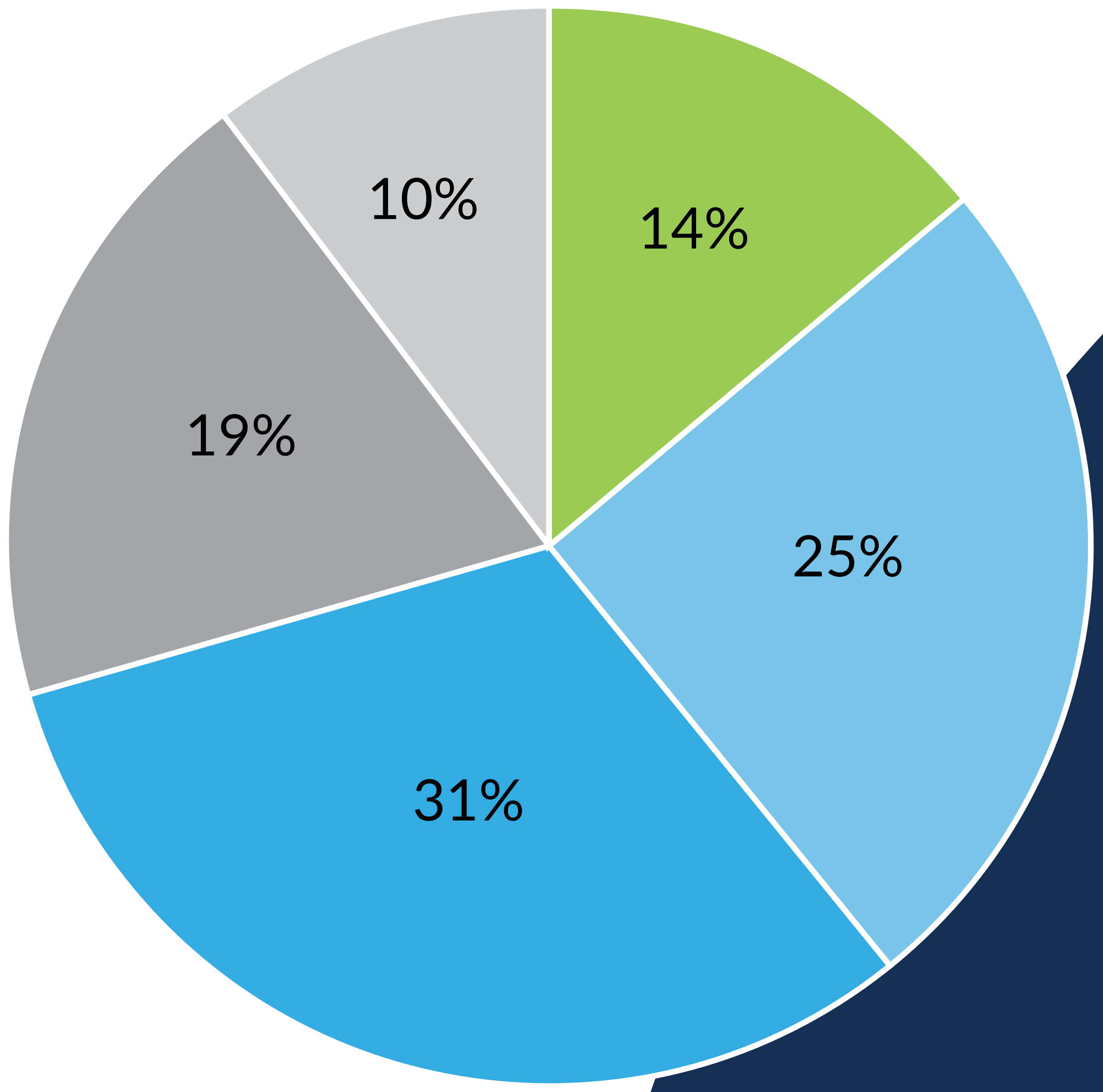


Trend 9: Consolidation - teams and platforms move toward unified control

Platform consolidation accelerates as organizations seek

While team structures are converging, platform consolidation is accelerating even faster. According to our findings, 75% of organizations have consolidated at least some portion of their security tools or policies under a single platform of management layer. While team structures are converging, platform consolidation is accelerating even faster. According to the 2026 findings, 75% of organizations have consolidated at least some portion of their security tools or policies under a single platform or management layer. Around 30% report partial consolidation, 19% say the majority of their infrastructure now sits under one platform, and 10% have achieved full consolidation. Only a quarter still operate with fragmented tooling.

What percentage of your cloud and network security tools are currently consolidated under a single platform or policy engine?



🟩 0%: Completely siloed

🟦 1-25%: Minimal consolidation

🟦 26-50%: Partial consolidation

⬛ 51-75%: Majority consolidated

⬜ 76-100%: Fully consolidated

This reflects a broader desire for unified visibility and simplified operations. As hybrid and multi-cloud deployments grow in scale, point solutions are becoming operationally burdensome. Organizations increasingly want fewer dashboards, fewer approval workflows, and fewer interfaces to manage, instead preferring integrated platforms that are capable of enforcing policy consistently across environments.

Key takeaway

Consolidation is redefining how enterprises operate, both structurally and technologically. Teams are aligning around shared tools, shared responsibilities, and, increasingly, shared governance models. At the same time, platforms are consolidating to provide unified visibility and consistent policy enforcement across hybrid environments.

Conclusion

The state of network security this year is defined by clarity emerging from complexity. After several years of rapid expansion across multi-cloud environments, AI-powered operations, and hybrid architectures, organizations are entering a new phase of consolidation and control. Our survey findings reveal a collective recalibration, with organizations moving away from tool proliferation toward unified management, shared visibility, and measurable automation. Firewalls, SD-WAN, and SASE have all evolved into foundational pillars of a more cohesive network security stack, while Zero Trust and AI continue to mature, bridging the gap between strategy and execution.

Compared to last year, we are now seeing a transition from experimentation to optimization. Where last year's findings reflected a market still expanding in every direction, this year captures a shift toward simplification. The drive for flexibility has given way to the pursuit of consistency, where performance metrics are being replaced by governance and assurance benchmarks. Consolidation of vendors, tools, and even teams, now defines the path forward. Adding layers of protection is not enough – those layers need to operate cohesively.

Looking ahead, the next generation of network security will hinge on visibility, automation, and collaboration, not as separate initiatives, but as integrated capabilities that span every layer of the digital ecosystem. For an industry that has long been dominated by complexity and a "more is better" approach, the next year might be quite surprising. As organizations continue to align their cloud, network, and security teams, the most resilient will be those that embrace simplicity rather than complexity, transforming control into confidence.

Methodology

This report is based on comprehensive research conducted by AlgoSec, gathering insights from security, network, and cloud professionals across a broad range of industries and regions. The data was collected through a global survey carried out in the second half of 2025, designed to capture real-world perspectives on the challenges, priorities, and evolving trends shaping network security in 2026.

Survey scope and participants

The study reflects responses from 504 professionals representing 28 countries. Participants span a diverse set of roles, including security architects, engineers, and analysts (25%); IT and network managers (21%); CISOs and heads of security (13%); consultants and specialists (9%); CTOs, CIOs, and senior IT leaders (6%); business, program, and product managers (7%); DevOps, cloud, and software professionals (8%); and other or undefined roles (11%). This broad representation ensures a balanced view across enterprise, mid-market, and specialist organizations operating within hybrid and multi-cloud environments.

Research objectives

The primary goal of this study was to identify key trends and shifts in network security practice, from strategic priorities to operational realities. The research explores:

- How organizations are consolidating security management across hybrid and multi-cloud architectures
- The evolving role of automation, orchestration, and AI-driven security in modern frameworks
- Adoption trends across firewalls, SD-WAN, SASE, and Zero Trust architectures
- The impact of consolidation on tool selection, team alignment, and visibility
- How enterprises are adapting to AI-powered threats and increasing operational complexity

Data collection and analysis

Participants were asked to provide both quantitative and qualitative feedback on their current deployments, planned investments, and primary challenges in managing network security infrastructure. The survey established new baselines in several areas, including AI-powered attack readiness, automation maturity, and consolidation of tools and teams, while tracking multi-year trends from previous editions of the research. Responses were analyzed to identify correlations, emerging patterns, and year-over-year changes in market behavior.

By leveraging direct insights from practitioners and decision-makers, this study provides an objective, vendor-neutral snapshot of the global network security landscape. Its findings are intended to help organizations benchmark their progress, assess market maturity, and make informed decisions as they navigate the next stage of digital transformation.

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