



AlgoSec State of Network Security Report 2024

Unveiling market trends in the shifting sands of connectivity

Table of contents

Executive summary.....	3
Trend 1: The persisting relevance of hybrid networks.....	4
Trend 2: Security, continuity, and compliance drive cloud platform selection	5
Trend 3: The increasing importance of firewalls in securing cloud estates	6
Trend 4: The growing adoption of SD-WAN.....	7
Trend 5: The rise in SASE adoption	8
Key findings	9
Conclusion	10
Methodology	11
About AlgoSec	12

Executive summary

The next generation of networks is here. In recent years, the connectivity landscape has evolved from traditional data centers to the cloud, with technologies like SD-WAN and SASE gaining traction in the pursuit of seamless and secure connectivity. As networks grow more complex with numerous endpoints, cloud artifacts, applications, and digital estates to manage, the security risks and potential vulnerabilities associated with these assets have also increased significantly. Gartner predicts that by 2027, 50% of critical enterprise applications will reside outside of centralized public cloud locations,¹ underscoring the ongoing expansion, evolution, and complexity of today's network infrastructures.

To navigate this landscape effectively, the importance of visibility, automation, orchestration, and application-based security cannot be overstated. The booming deployment of SD-WAN is testament to this necessity, providing secure, direct connectivity to the internet and cloud applications, expected to grow at a CAGR of 14.6%,² reaching \$8 billion by 2026. Similarly, the rise of SASE highlights the demand for secure remote workforce solutions, with the market projected to grow at a CAGR of 29%, reaching over \$25 billion by 2027.³ These advancements illustrate the critical role of advanced network security solutions in modern enterprise environments.

This research, conducted with a diverse group of security, network, and cloud experts, offers valuable insights into the current network security landscape. The purpose of this report is to shed light on key market trends, highlight which solutions and technologies are in demand and why, and ultimately help organizations navigate the complexities of modern network security. Our findings are based on comprehensive surveys conducted throughout 2022 and 2023, reflecting the views of security engineers, IT managers, and network advisors and architects.

Among the key trends identified, the report highlights the increasing adoption of multi-cloud solutions, the growing complexity of firewall deployments in cloud environments, and the significant rise in SD-WAN and SASE implementations. These trends underscore an ongoing shift towards more integrated, automated, and application-centric security strategies. By understanding these trends, businesses can better prepare for the future of network security and ensure their infrastructure remains resilient and secure amidst the rapidly changing technological landscape.

¹ <https://www.gartner.com/en/newsroom/press-releases/2023-10-30-gartner-says-50-percent-of-critical-enterprise-applications-will-reside-outside-of-centralized-public-cloud-locations-through-2027>

² <https://www.sdxcentral.com/articles/feature/6-sase-and-sd-wan-trends-to-watch/2024/01/>

³ <https://www.sdxcentral.com/articles/feature/6-sase-and-sd-wan-trends-to-watch/2024/01/>

The persisting relevance of hybrid networks

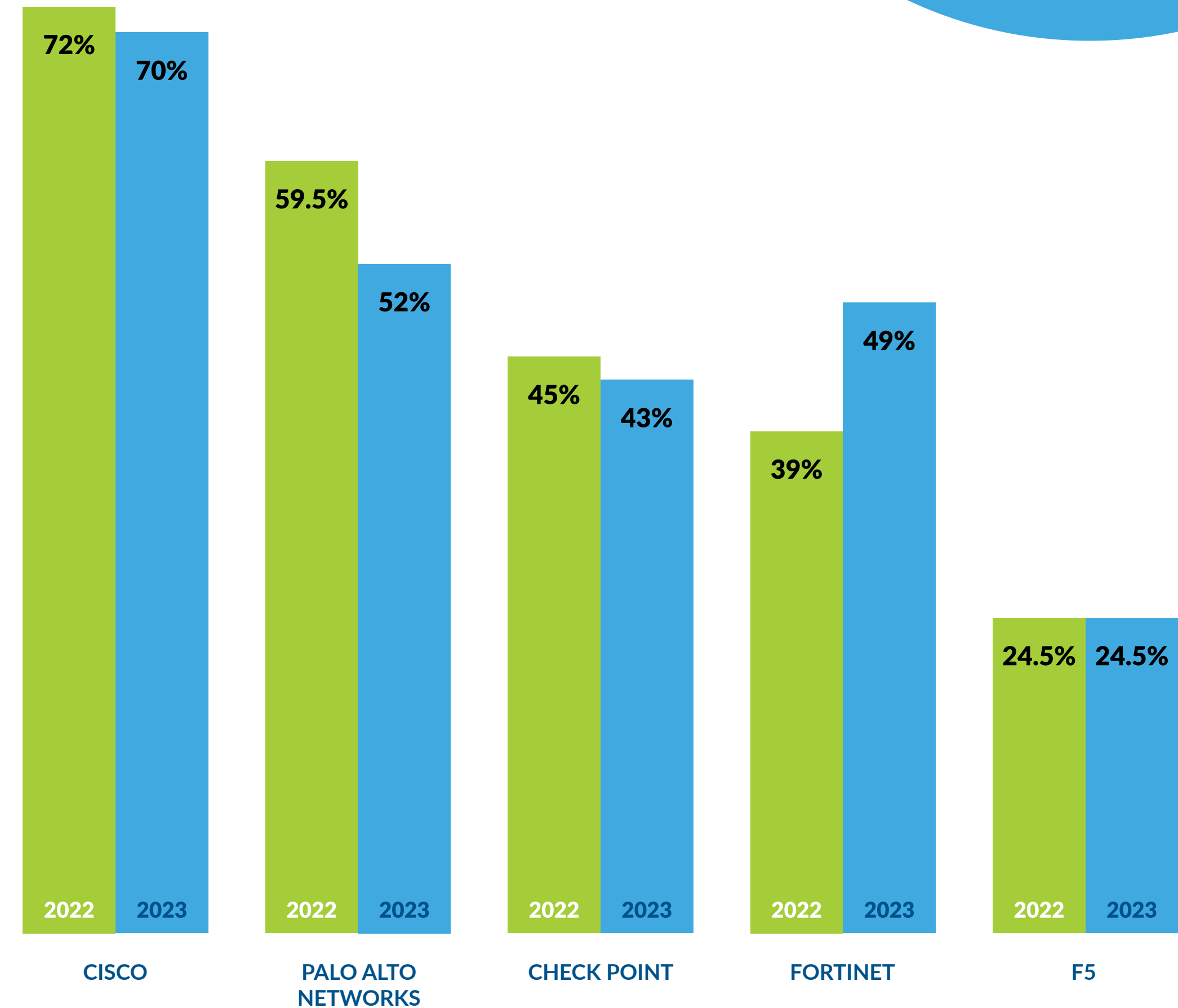
As organizations undergo digital transformation and expand their presence in the cloud, the complexity of network environments continues to increase. Despite the shift towards cloud infrastructure, on-premise data centers remain a critical component of many businesses' network strategies. This hybrid approach necessitates the management of both cloud and on-prem environments, adding layers of complexity and security considerations.

Cisco remains the most widely deployed brand in this landscape, with Palo Alto Networks following closely behind. Cisco's comprehensive range of networking hardware, including routers, switches, and security devices, has been integral to the build-out of corporate data centers for decades. Its integrated ecosystem includes not only hardware but also software solutions and services tailored specifically for on-premise environments. This extensive product range and integration capabilities make Cisco a preferred choice for many organizations managing on-premise data centers.

The enduring popularity of Cisco indicates a persistent need to manage on-prem data centers and devices. Although the number of user-controlled on-prem data centers has dropped from 60% to 40% over the past five years,⁴ they remain a significant feature of the network landscape. This decline highlights the shift towards cloud solutions but also underscores the continued importance of on-prem infrastructure for specific applications and workloads that require stringent control and security.

Key takeaway

On-premise data centers and device rollouts remain highly relevant. Organizations are increasingly factoring security and threat prevention into their decision-making processes, as much as they consider performance and throughput. This focus on security is crucial as it ensures that both on-prem and cloud environments are protected against the ever-evolving threat landscape, maintaining the integrity and reliability of their overall network infrastructure.



⁴ <https://www.datacenterdynamics.com/en/opinions/on-prem-data-centers-arent-dead/#:~:text=The%20smaller%20%22retail%22%20colocation%20sites,to%20only%2040%20percent%20now.>

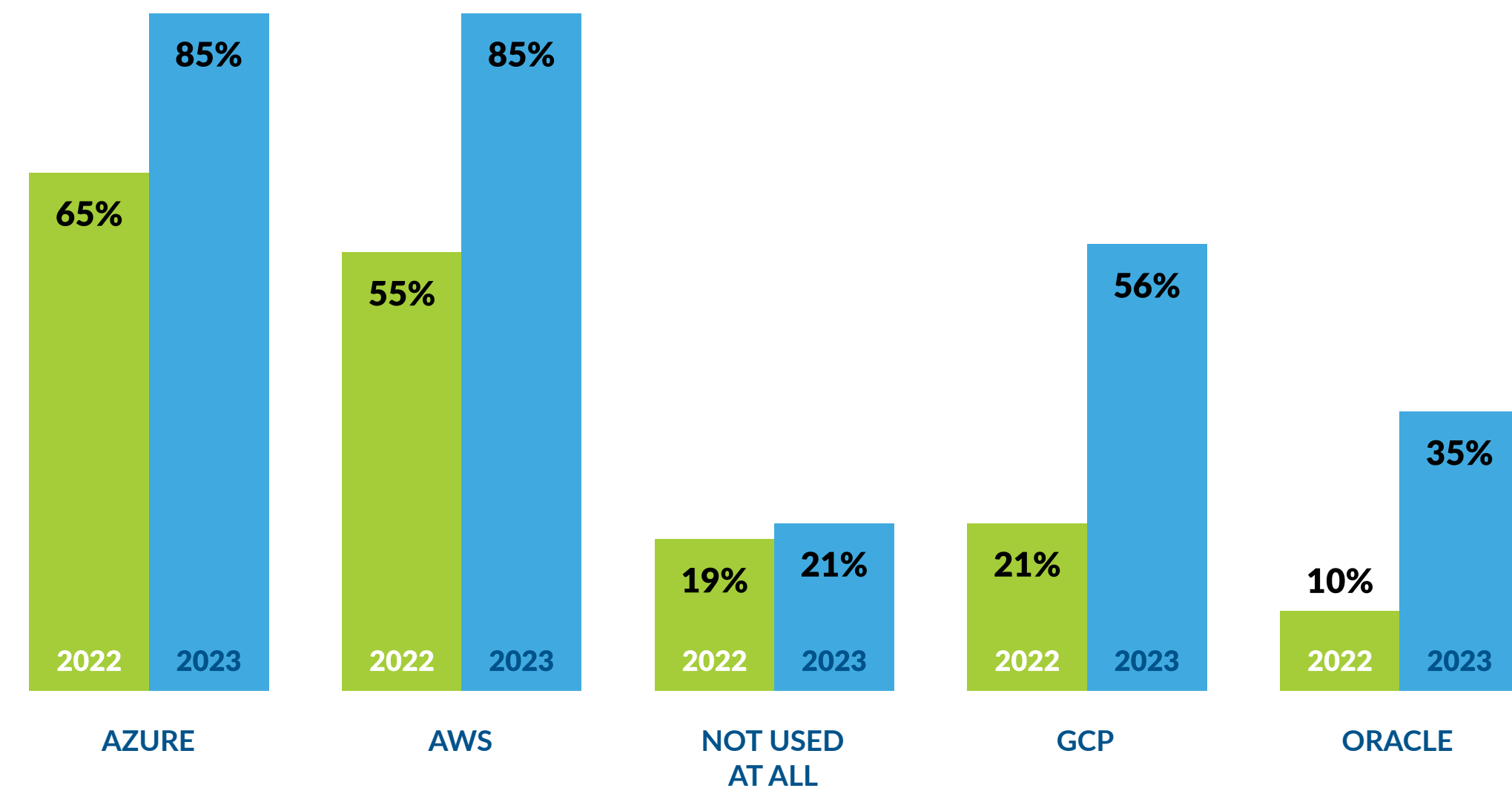
Security, continuity, and compliance drive cloud platform selection

Cloud platforms are booming in popularity with continuity, compliance, and security now key differentiators. The robust security features inherent in leading cloud platforms, such as advanced threat detection, data encryption, access control, and adherence to security compliance protocols, are critical for protecting data and applications in a constantly evolving threat landscape.

According to a 2022 survey, 89% of organizations use more than one cloud for storage and workloads, with only 9% relying on a single public cloud and 2% using a single private cloud solution.⁵ This multi-cloud strategy allows organizations to leverage the strengths of different cloud providers, enhancing their overall security posture and operational resilience.

AlgoSec's research highlights that while the overall adoption of cloud platforms has grown, the ranking of different vendors has remained relatively stable. Azure continues to be the most widely used platform, closely followed by AWS, which has shown the fastest pace of growth. Google Cloud Platform (GCP) and Oracle Cloud also remain significant players in the market. Azure's continued dominance can be attributed to its seamless integration with Microsoft products like Windows Server, SQL Server, and Active Directory, making it a preferred choice for businesses seeking an easy transition to cloud technologies. Azure's robust hybrid cloud solutions also allow organizations to maintain some data and applications on-premises, catering to the needs of hybrid deployments.

On the other hand, AWS is gaining traction due to its scalability, competitive pricing, and innovation. AWS's global infrastructure ensures high performance and reliability, which, coupled with cost-effective solutions, attracts a wide range of businesses from startups to large enterprises. Its extensive developer tools and ecosystem support further enhance its appeal to technology-driven companies looking to leverage advanced computing capabilities.



Key takeaway

Organizations now prioritize seamless integration, compliance, and robust security features when choosing cloud platforms. Azure's popularity reflects a preference for continuity and ease of transition, while AWS's rapid growth underscores the demand for scalable, innovative solutions. This trend highlights the critical role of cloud platforms in supporting modern business operations and the ongoing evolution of network security strategies.

⁵ <https://aag-it.com/the-latest-cloud-computing-statistics/#:~:text=Cloud%20Adoption%20Statistics,a%20single%20private%20cloud%20solution.>

The increasing importance of firewalls in securing cloud estates

With the accelerating shift to cloud infrastructure, organizations are facing unprecedented challenges in securing their digital assets. Firewalls have emerged as a crucial component in this defense strategy, providing a robust barrier against external threats by meticulously controlling access and filtering traffic based on sophisticated security policies.

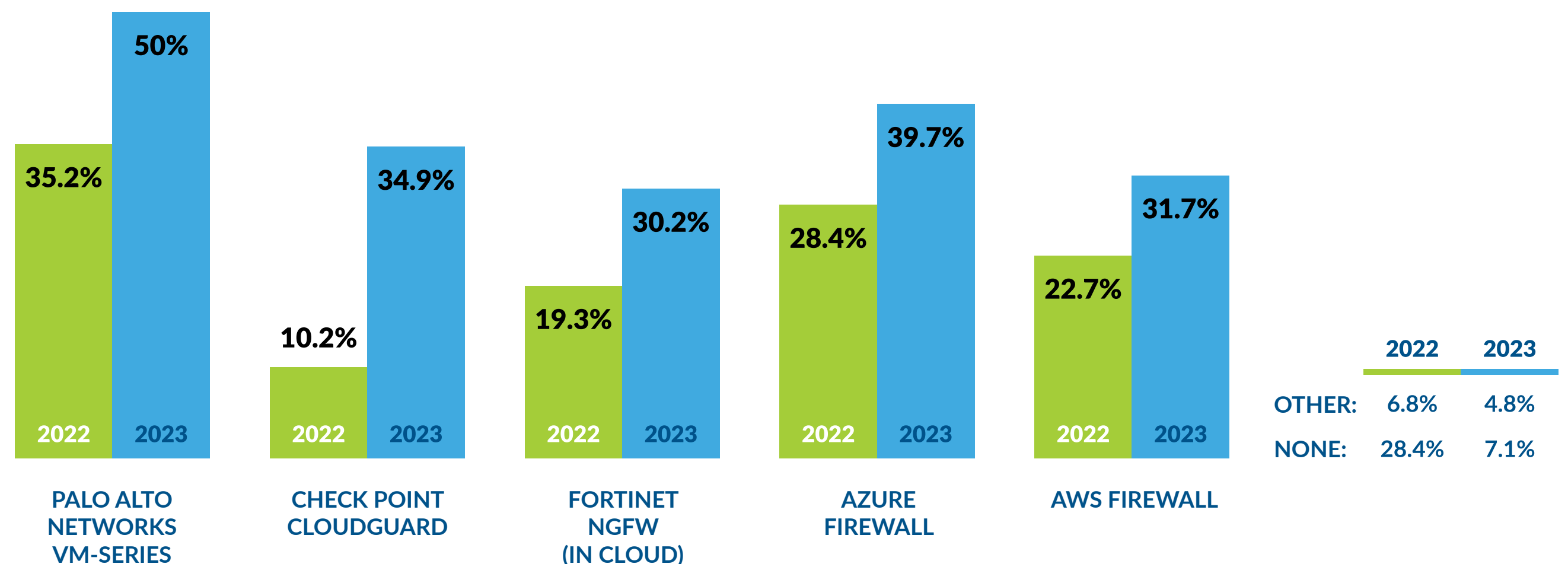
These findings underscore a significant uptick in the deployment of firewalls within cloud environments. Leading the charge is Palo Alto Networks, whose VM series firewalls are renowned for their advanced threat prevention and comprehensive security features. Azure Firewall also commands a strong presence, owing to its seamless integration within the Azure ecosystem. Other key players such as Check Point CloudGuard, Cisco FirePower, and AWS Firewall are making substantial contributions, each bringing unique strengths to the table.

The increasing implementation of firewalls in the cloud reflects their essential role in safeguarding application security, preventing downtime, and mitigating cyber threats stemming from network vulnerabilities. Organizations are increasingly adopting multi-vendor firewall strategies to bolster their security posture, despite the additional complexity this approach introduces.

Palo Alto Networks continues to dominate traditional firewall deployments, leveraging its well-established reputation and robust security capabilities. Its advanced threat detection and prevention features offer comprehensive protection across both on-premises and cloud environments. Meanwhile, the rapid growth of Azure Firewall adoption underscores its effectiveness in providing integrated security solutions within the Azure cloud platform, making it a preferred choice for businesses scaling their cloud infrastructure. The rise of Cisco FirePower in the rankings signifies Cisco's successful adaptation of its on-premises security expertise to meet the demands of cloud-focused security solutions.

Key takeaway

The cloud security landscape is increasingly dynamic and complex, requiring solutions that offer integration, reliability, and advanced protection. Organizations are turning to firewalls to secure their cloud estates, recognizing the critical need for proactive threat prevention and the benefits of orchestration and automation in managing multi-vendor security environments.



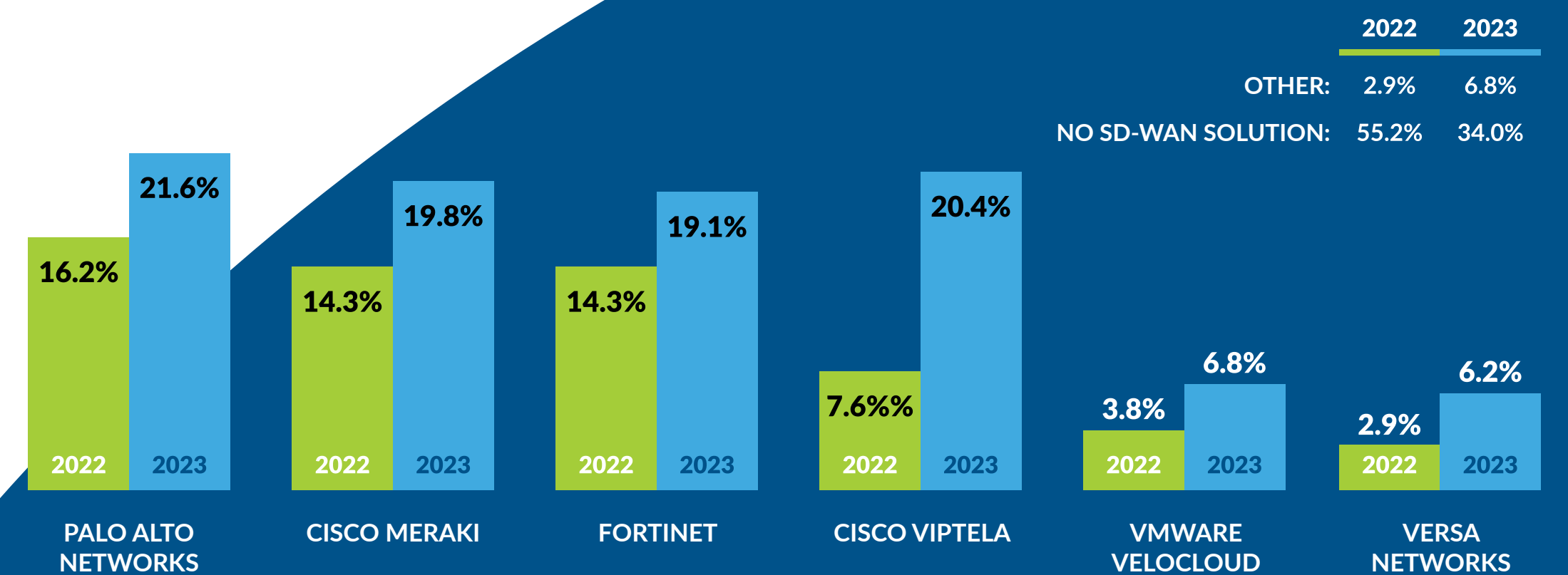
The growing adoption of SD-WAN

The adoption of Software-Defined Wide Area Network (SD-WAN) solutions is experiencing significant growth as organizations seek to enhance connectivity and security across geographically dispersed locations. SD-WAN is pivotal in modern network security, providing optimized traffic routing, improved application performance, and robust security features such as encryption, intrusion prevention, and consistent policy enforcement.

Our research highlights the substantial increase in SD-WAN deployments in 2023. This surge is largely driven by the ongoing shift towards remote work and cloud computing, necessitating more flexible, reliable, and secure network management solutions. Palo Alto Networks remains the leading single provider of SD-WAN solutions, renowned for its strong integration of security and network performance. However, when considering combined solutions, Cisco's Viptela and Meraki take the overall lead, reflecting their strategic advantage in offering diversified solutions tailored to varying enterprise needs.

Palo Alto Networks' position as the leading single provider of SD-WAN solutions underscores its reputation for robust security features, seamless cloud integration, and overall reliability. These qualities are critical for organizations aiming to securely manage their network traffic and protect against sophisticated cyber threats. On the other hand, Cisco's dual approach with Viptela and Meraki caters to a broader market segment, from small businesses to large enterprises. Cisco Viptela is recognized for its advanced routing and comprehensive network management capabilities, suitable for large enterprises with complex network requirements. In contrast, Meraki appeals to smaller businesses or those requiring quick deployment with minimal configuration, thanks to its simplicity and ease of use.

The evolving nature of network management is evident in these trends, where versatility in product offerings and the ability to provide integrated, secure networking solutions determine market leadership in the SD-WAN space. Organizations are increasingly turning to SD-WAN to ensure secure, reliable connections across dispersed locations, enhancing both network performance and security in a cost-effective manner.



Key takeaway

The trend here is clear: SD-WAN remains crucial to modern network security, but only for those who need it. As businesses continue to embrace digital transformation and remote work models, perhaps with dispersed branches across different locales, SD-WAN's integrated security features and optimized connectivity solutions are essential for maintaining agility and protecting against cyber threats. This trend highlights the need for versatile, scalable solutions that can adapt to the diverse and evolving demands of today's sprawling network environments.

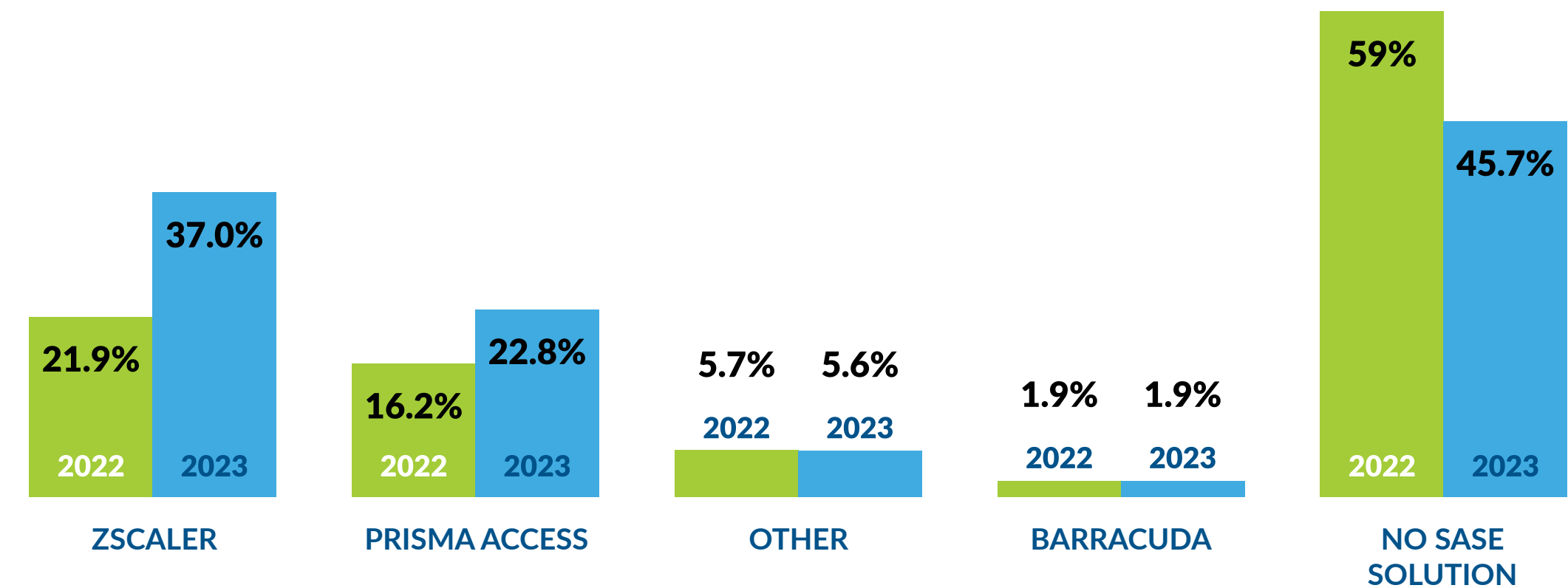
The rise in SASE adoption

The emergence of Secure Access Service Edge (SASE) as a prominent network architecture is transforming the way organizations manage security and connectivity. SASE combines WAN capabilities with cloud-native security services, including secure web gateways, cloud access security brokers (CASB), firewalls, and zero-trust network access. This integrated approach offers seamless, secure access to network resources regardless of user location or device, which is crucial in today's increasingly mobile and remote workforce environment.

We've discovered that SASE adoption has grown significantly between 2022 and 2023, with Zscaler and Prisma Access (Palo Alto Networks) leading the pack. This growth can be attributed to SASE's alignment with the shift towards cloud-based resources and the need for organizations to support secure, efficient access for distributed users. SASE simplifies traditional network security management by consolidating multiple security functions into a single, unified cloud service, reducing complexity, and improving performance.

As a pioneer in the cloud security space, Zscaler has developed a robust global cloud infrastructure capable of handling large volumes of encrypted traffic efficiently. This extensive infrastructure allows Zscaler to provide high-performance services, crucial for organizations with significant cloud operations and global reach. Similarly, Prisma Access by Palo Alto Networks leverages the company's strong security foundation, offering comprehensive protection and seamless integration within cloud environments.

Managing network security in a SASE environment requires prioritizing risk, maintaining compliance, and managing all aspects from an application-centric view. The ability to consolidate various security functions into a single framework enhances visibility and control, allowing organizations to proactively address security threats and ensure compliance with regulatory requirements. This approach not only improves security posture but also streamlines operations and reduces the burden on IT teams.



Key takeaway

The key takeaway here is the runaway strategic advantage offered by SASE in securing modern, distributed networks. As businesses continue to embrace digital transformation and remote work models, the integrated, scalable nature of SASE makes it an ideal solution for securing network access and protecting data across dispersed locations. This trend underscores the importance of adopting comprehensive, unified security solutions that can adapt to the dynamic needs of today's enterprise environments.

The research uncovered several critical trends reshaping the network security landscape:

Brand trends in network security:

- Cisco remains the most widely deployed brand, with Palo Alto Networks following closely.
- The persistent need for managing on-prem data centers and devices underscores the ongoing relevance of traditional networking hardware alongside cloud solutions.

Cloud platform adoption:

- Azure continues to be the most widely used cloud platform, though AWS is growing rapidly.
- Multi-cloud strategies are prevalent, with 89% of organizations using more than one cloud provider.

Firewall deployments:

- The deployment of firewalls in cloud environments has increased, with Palo Alto Networks, Azure Firewall, and Check Point CloudGuard being the top choices.
- Multi-vendor firewall strategies are common, introducing additional complexity but enhancing security resilience.

SD-WAN adoption:

- There has been significant growth in SD-WAN adoption, driven by the need for secure, flexible, and reliable network management for remote and dispersed locations.
- Palo Alto Networks leads as the single provider, while Cisco's combined solutions (Viptela and Meraki) take the overall lead.

SASE adoption:

- The adoption of SASE solutions has grown, with Zscaler and Prisma Access (Palo Alto Networks) at the forefront.
- SASE's integrated approach to security and connectivity aligns with the demands of modern, distributed workforces.

Conclusion

The state of network security is witnessing a remarkable transformation as organizations grapple with the complexities of modern, interconnected environments. This report has explored the significant trends that are redefining how businesses approach network security, emphasizing the critical need for robust, integrated solutions to protect against evolving threats.

Throughout the research, several key trends have emerged. Despite the surge in cloud adoption, the relevance of on-premise data centers persists, highlighting a hybrid approach that balances traditional and cloud-native strategies. Cisco remains a cornerstone in the network security landscape, with its extensive range of networking hardware and integrated solutions continuing to dominate the market. Meanwhile, cloud platform adoption is at an all-time high, with Azure and AWS leading the charge, driven by their robust security features and seamless integration capabilities. The deployment of firewalls has surged, underscoring their critical role in preventing application downtime and safeguarding against cyber threats. The rise of SD-WAN adoption reflects the need for secure, reliable connectivity across dispersed locations, with solutions from Palo Alto Networks and Cisco's Viptela and Meraki leading the market. Finally, the adoption of SASE solutions, led by Zscaler and Prisma Access, is transforming network security by integrating WAN capabilities with comprehensive cloud-native security services.

In conclusion, the insights from AlgoSec's research highlight the dynamic and ever-evolving nature of the network security landscape. As organizations continue to navigate digital transformation, the adoption of integrated, automated, and application-centric security solutions will be crucial. The need for a unified connectivity management solution across on-premise, cloud, SD-WAN, and SASE environments is also more apparent than ever. By embracing these trends and leveraging advanced security strategies, businesses can effectively protect their critical assets and ensure resilience in an increasingly complex digital world.

Methodology

The insights presented in this eBook are derived from comprehensive research conducted by AlgoSec, encompassing surveys carried out in the second half of 2022 and 2023. The surveys gathered responses from a wide range of professionals, including security engineers, network engineers, managers, advisors, architects, and other experts in security, network, and cloud technologies. This diverse group of respondents provided a holistic view of the current network security landscape, reflecting the experiences and perspectives of those at the forefront of the industry.

Survey scope and participants

- 2022 Survey: Included 100 respondents from 27 countries.
- 2023 Survey: Expanded to include 160 respondents from 34 countries.

The participants represented a broad spectrum of industries and organizational sizes, ensuring that the findings are both comprehensive and representative of the global market.

Research objectives

The primary goal of the research was to identify key trends and shifts in network security practices, cloud adoption, and the deployment of security solutions. By analyzing the data collected, AlgoSec aimed to provide actionable insights that organizations can leverage to enhance their security strategies and adapt to the evolving digital landscape.

Data collection

The surveys included a variety of questions designed to capture detailed information about:

- The types of security solutions and platforms currently deployed.
- The frequency and nature of security incidents experienced.
- The strategic priorities and challenges faced by security and network teams.
- Preferences and trends in the adoption of cloud platforms, firewalls, SD-WAN, and SASE solutions.

About AlgoSec

AlgoSec, a global cybersecurity leader, empowers organizations to secure application connectivity and cloud-native applications throughout their multi-cloud and hybrid network.

Trusted by more than 1,800 of the world's leading organizations, AlgoSec's application-centric approach enables to securely accelerate business application deployment by centrally managing application connectivity and security policies across the public clouds, private clouds, containers, and on-premises networks.

Using its unique vendor-agnostic deep algorithm for intelligent change management automation, AlgoSec enables acceleration of digital transformation projects, helps prevent business application downtime and substantially reduces manual work and exposure to security risks.

AlgoSec's policy management and CNAPP platforms provide a single source for visibility into security and compliance issues within cloud-native applications as well as across the hybrid network environment, to ensure ongoing adherence to internet security standards, industry, and internal regulations.

Learn how AlgoSec enables application owners, information security experts, DevSecOps and cloud security teams to deploy business applications up to 10 times faster while maintaining security at www.algosec.com.

For more information, visit