NCR ATLEOS

Debunking 4 common myths about Secure Access Service Edge (SASE)

An essential guide to network challenges and SASE enterprise transformation capabilities

start

Table of contents

Introduction

Businesses today are keeping up with a lot, from balancing customer experience and security to embracing AI to optimize efficiency and cost, all while ensuring minimal disruption in the network. While adapting and evolving to enhance business operations, ensuring your network infrastructure stays in top form becomes crucial. The most common causes of network outages continue to be related to networking and connectivity issues, along with IT software- and configuration-related issues.[1]

In a study conducted by NCR Atleos and Technology Business Research, Inc. (TBR), executives consider network security (48%) and the complexity of network management and monitoring (46%) to be the primary challenges of enterprise networking.[2] When it comes to security, the threats that businesses face worldwide have become more challenging, with AI triggering more complex and frequent attacks.

Now, tech leaders and CISOs must not only focus on information security but also on ensuring that networks are highly protected with proactive security measures. In cloud environments, the complexity increases with legacy networks and security practices often working in silos that cannot meet the needs of the organization.

Network challenges for today's businesses

Organizations today face critical network challenges that can significantly impact coverage and availability. Some of these challenges are outlined below.

Secure cloud connectivity: As data continues to migrate to the cloud, enterprises must ensure that connectivity to cloud resources is not only seamless but also secure. Cloud environments introduce new vectors for cyberattacks and require sophisticated security controls that can adapt in real time.

Hybrid work: With the rise of hybrid and remote work, there is an amplified need for reliable connectivity. Employees, vendors and other stakeholders located across different regions require secure access to centralized applications and databases without the constraints of traditional VPNs. This drives the need for solutions that ensure consistent delivery and security across all access points.

Escalating cybersecurity threats: Today's cyber threats are no longer just basic malware attacks but highly orchestrated AI-driven attacks that target vulnerabilities in real time. Hackers are smarter and more persistent, and organizations need the ability to preemptively mitigate risks. To quickly identify and neutralize threats, there is a heightened need for enhanced visibility into network traffic.

Network complexity: Enterprises today rely on multiple networking solutions from several vendors. This can lead to complex management issues, increased operational costs and inefficiencies that impact proactive network monitoring and control. For businesses to be successful, simplified and consolidated systems are necessary to reduce complexities and lower risk.

User experience: Poor network performance, whether due to latency, bandwidth constraints or misconfigured security protocols, can directly impact employee productivity and customer satisfaction. The need to ensure that every touchpoint—from internal applications to customer-facing platforms—functions seamlessly is a constant challenge.

Cost efficiency: Managing disparate tools and systems not only drives up costs but also dilutes focus from core business objectives. Enterprises need scalable technology solutions that can grow with their needs while offering the simplicity and cost-savings that come from operational consolidation.

48% of executives consider network security to be the primary challenge of enterprise networking.

SASE: A hero for network security

Secure Access Service Edge (SASE) is a framework or architecture that unifies SD-WAN and security capabilities into a single, cloud-delivered framework, which results in simplified WAN deployments, improving efficiency and security.

The SD-WAN and SASE market has seen significant expansion since 2023 and will continue to grow exponentially, reaching a predicted market size of $8B by 2026 (according to Gartner) and $7.5B by 2027 (according to IDC).[3] Businesses are realizing the complexities associated with multiple platforms and want to ensure management of access policies is not the cause of disruptions.

The integration and operation of these platforms also cause higher costs due to the increasing need for capacity and bandwidth, in addition to security and limiting visibility of the network in its entirety. Expectations are also high for these environments and technologies to work efficiently in hybrid, in-office and remote work settings. Often, these projects can result in disjointed teams and processes, and SASE is considered the Holy Grail.

SASE projects lead to collaboration between networking and security teams in areas such as vendor selection, implementation, operations and budget allocation. This collaboration can be a significant advantage for businesses, resulting in benefits like:

- Reduced complexity and cost due to consolidated disparate security and network tools
- Increased business agility to quickly adapt to changing business needs and seamlessly scale your network with cloud-native flexibility
- Enhanced security that seamlessly integrates network and security functions for comprehensive protection and optimized network performance

Therefore, SASE is critical to improving network performance and bandwidth optimization by enhancing traffic flow, minimizing latency and simplifying management to improve user experience and network performance. In cases where businesses are expanding into new regions, establishing and managing connectivity is the most critical factor to ensure a smooth and successful global expansion. Hughes and Cybersecurity Insiders found that 39% of IT leaders and cybersecurity professionals are confident of SASE's ability to enhance network performance and optimize bandwidth.[4]

39% of IT leaders and cybersecurity professionals are confident of SASE's ability to enhance network performance and optimize bandwidth.

Debunking SASE myths

Business and technology decision-makers usually adopt an innovation to achieve growth and progress. With any new concept comes an array of doubts, misconceptions and myths. SASE is growing in popularity, but misconceptions may cause hesitation. Here, we debunk four common myths to clarify SASE's real capabilities.

1. SASE solutions are the same across all vendors

The Myth

Many assume that every SASE solution available on the market is essentially identical, leading to the belief that vendor choice is inconsequential.

The Facts

SASE is a framework, not a one-size-fits-all solution, providing networking flexibility. The key SASE technologies include software-defined wide area networking (SD-WAN), zero-trust network access (ZTNA), firewall-as-a-service (FWaaS), secure web gateway (SWG) and cloud access security broker (CASB). Together, these components form a SASE architecture where security and networking converge in a cloud-based platform that supports cloud migrations and a distributed workforce. Vendors offer various components, enabling organizations to tailor solutions to their specific needs. The choice between single or multiple SASE vendors depends on the business goals driving its adoption.

By the end of this year, 65% of enterprises are expected to consolidate individual SASE components into one or two SASE partners.[5] If simplifying management, reducing complexities and lowering costs are the goals, partnering with a vendor that specializes in all these components could prove more beneficial in the long run.

back

next

2. SASE adoption is complex and time-consuming

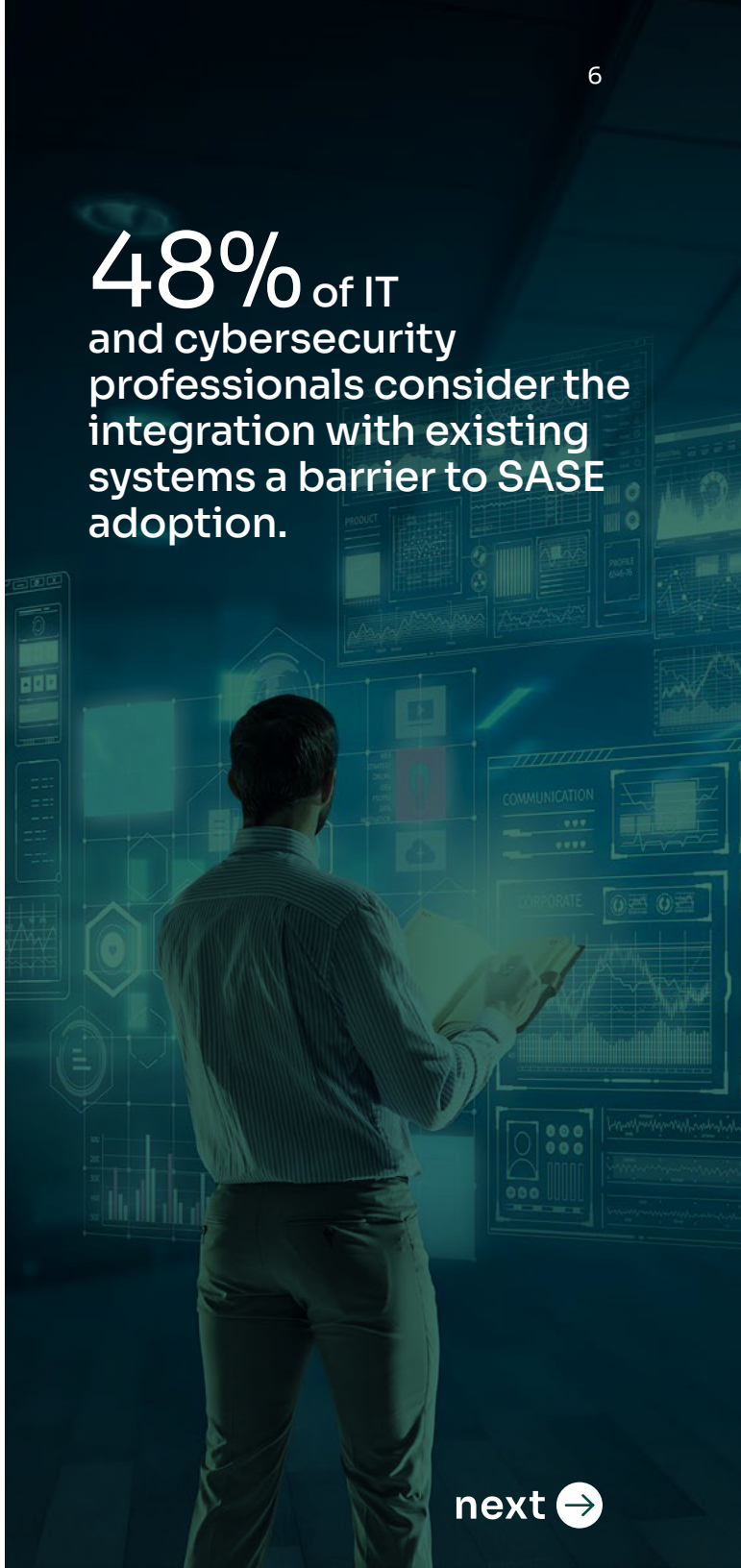
The Myth

There is a common perception that implementing SASE is an arduous process, fraught with integration issues and lengthy deployment timelines.

The Facts

Realistically, SASE implementation is complex not because of the solution itself but because of what is required for a successful deployment. From network and security teams working collaboratively to the integration of different SASE components with existing and legacy infrastructure, it requires involvement of multiple teams and technologies.

Research has found that 48% of IT and cybersecurity professionals consider the integration with existing systems a barrier to SASE adoption.4 The convergence of network access and security requires a mature cloud environment which could impact SASE implementation. On the other hand, managing security policies and controls in SASE without an expert team can pose a significant struggle. With multiple vendor engagement, it may be challenging for organizations to gain visibility into the ongoing activities in SASE and cloud infrastructure. That's why the expertise of a managed SASE partner is beneficial, providing the support needed to ensure SASE is adopted gradually, with step-by-step component integration. This phased approach simplifies the process and reduces complexity.



back

next

3. SASE replaces SD-WAN

The Myth

A prevalent myth is that SASE intends to completely replace SD-WAN, rendering existing investments in SD-WAN obsolete.

The Facts

SASE does not replace SD-WAN. In practice, SASE builds upon the foundation provided by SD-WAN. Rather than replacing it, SASE enhances SD-WAN by incorporating advanced security features. SD-WAN remains a vital component, responsible for intelligent traffic routing and providing the connectivity backbone that SASE leverages to deliver a unified network and security solution. The synergy between SD-WAN and the security functions integrated into SASE forms the basis for a robust and agile network environment.

back

next

4. SASE is fully automated

The Myth

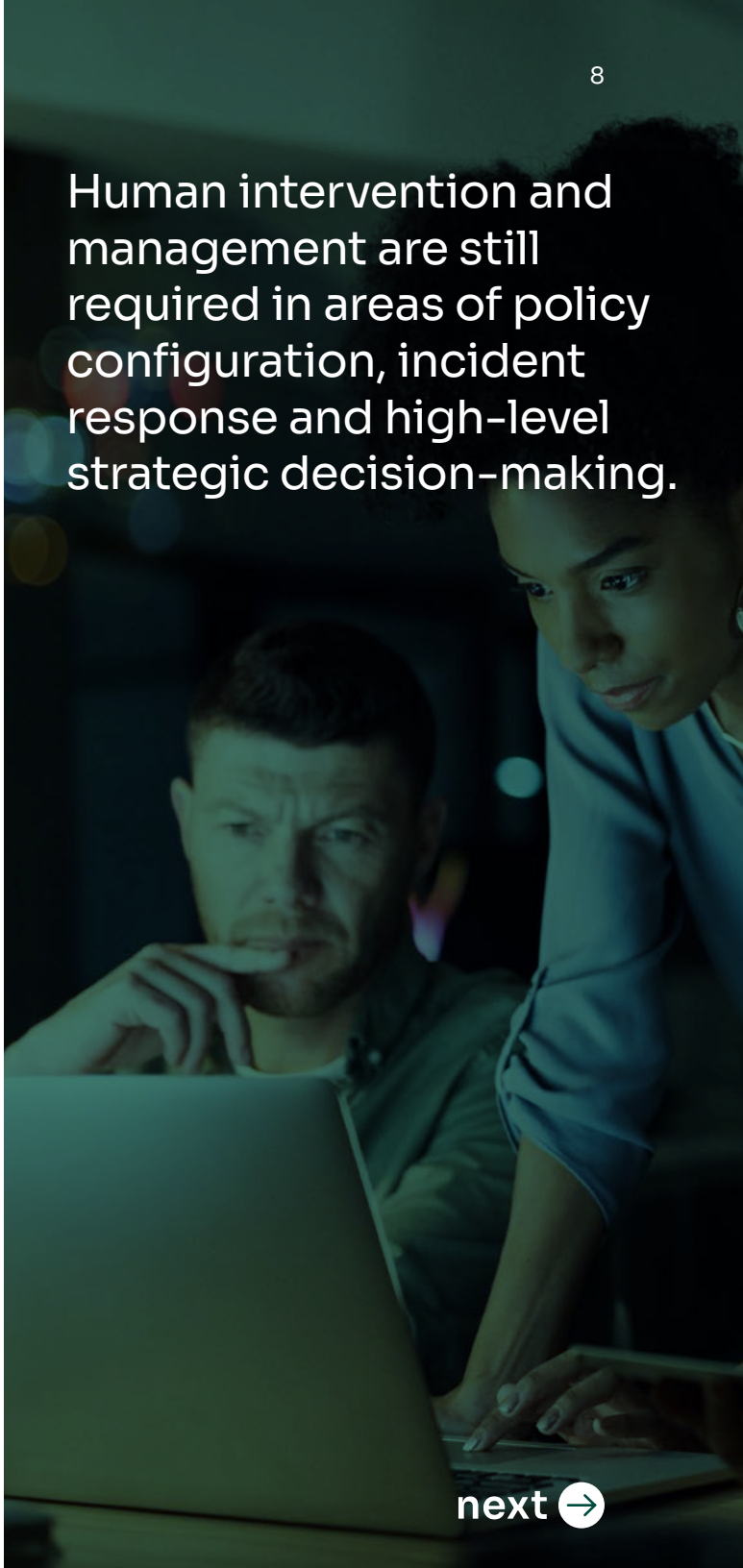
Some believe that because SASE operates in a cloud environment and leverages automation, it eliminates the need for human oversight.

The Facts

SASE is a network architecture integrating networking and security services delivered through a unified cloud platform. There is some automation, but it is not entirely automated and requires some human oversight to adjust network configuration and security protocols.

There are aspects of SASE that leverage automation and AI (e.g., to enhance security measures or to monitor and respond to threats). Some automation is also used to integrate security functions, scale and improve efficiency. However, human intervention and management are still required in areas of policy configuration, incident response and high-level strategic decision-making.

Automation works best as a force multiplier, enhancing the capabilities of your team rather than replacing them. The combination of automation and human intervention makes SASE robust and optimizes network performance. Having a team that is well-versed in SASE and SD-WAN and can integrate the solutions irrespective of which technology provider is involved is crucial to getting the best out of your SASE investment. A dedicated team that understands the balance of automation and human management will ensure that your business meets its core goals.



back

next

Conclusion

While skepticism about SASE's complexity persists, over 30% of organizations have already embraced it.[4] Industry forecasts predict that over 60% of enterprises will have explicit strategies and timelines for SASE adoption by 2025, underscoring its role as a cornerstone of modern network and security architectures.6 This evolution isn't merely a tech upgrade; it's a strategic response to the demands of hybrid work, cloud-first initiatives and relentless cyber threats.

For global leaders, SASE serves as a call to break down silos and unite network and security teams, turning initial challenges into opportunities for growth. Whether you decide to build an in-house team or partner with a trusted advisor, the choice you make today will pave the way for a future defined by greater agility and resilience.

If you're already exploring SASE or standing at the starting line, the NCR Atleos Telecom and Technology team is ready to support you with a complimentary consultation to help chart your course. Click to contact us today or e-mail ncratleos.telecomandtechnology@ncratleos.com and one of our network experts will be happy to help you.

References

1. Network World. "Network connectivity issues are leading cause of IT service outages."
2. NCR Atleos internal research.
3. SDxCentral. "6 SASE and SD-WAN trends to watch."
4. Cybersecurity Insiders and Hughes. "2025 state of secure network access."
5. SDxCentral. "Why successful SASE implementations rely on consultants and professional services."

Contact us to find out more.
U.S. 800.225.5627 ▪ Outside the U.S. 937.445.1936 ▪ ncratleos.com