HUGHES®

An EchoStar Company

Understanding SASE: A Strategic Guide for IT Leaders

Chapter 1:
Core Components of SASE

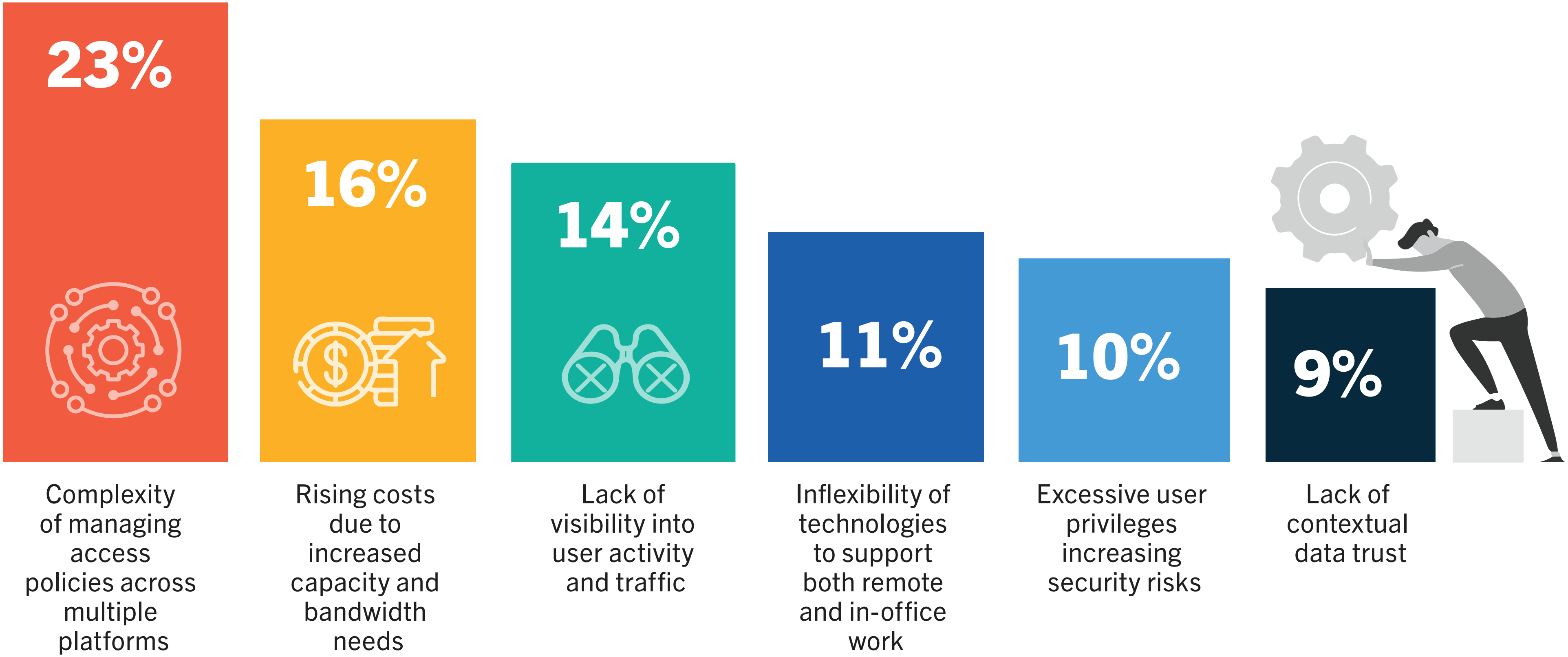
What is SASE?

Secure Access Service Edge (SASE) is a cutting-edge network architecture that unifies networking and security functions into a single, cloud-native service model. First conceptualized by Gartner® in 2019, SASE has since been rapidly adopted by many modern enterprises.It represents a fundamental shift in how organizations connect and secure their digital resources. By integrating networking and security functionalities into a single service, SASE offers a more flexible, scalable, and efficient way to protect and connect today's distributed workforce and resources. According to the 2025 State of Secure Network Access Report—a survey from 400+ IT leaders and cybersecurity professionals—32% are currently implementing SASE solutions, with an additional 31% evaluating its potential.

At its core, SASE combines essential network and security services, such as Software-Defined Wide Area Networking (SD-WAN), Secure Web Gateways (SWG), Cloud Access Security Brokers (CASB), Zero Trust Network Access (ZTNA), and Firewall as a Service (FWaaS), into a cohesive solution that is delivered from the cloud. This convergence simplifies network architecture, reduces latency, and enables seamless and secure access to applications and data across locations, including branch offices, remote workspaces, and cloud environments.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally. All rights reserved.

What is the greatest challenge your organization faces with its current secure access solutions?



HUGHES
An EchoStar Company

The Evolution of SASE

The journey to SASE reflects broader trends in IT. In traditional setups, organizations have relied heavily on data centers with robust firewalls and Virtual Private Networks (VPNs) to manage and secure their networks. However, as applications and data began to migrate to the cloud, the limitations of a centralized security model became clear. With more employees working remotely, accessing cloud apps, and bringing personal devices, security became harder to enforce through traditional perimeter-based models.

Enter SASE, which moves away from static, perimeter-based security toward a flexible, cloud-native approach that secures users and devices, no matter where they connect. In a SASE model, security policies are applied based on the user's identity, the application being accessed, and the context of the connection. This framework ensures that the same security posture extends from on-premises to cloud environments, adapting dynamically to the users and applications needs.

Why is SASE Important?

There is a strong demand for a secure, reliable, and user-friendly network experience that meets modern security standards. Many cybersecurity implementations have negative consequences in the form of increased latency and slower network speeds.

- **Performance:** With cloud-based delivery, data does not have to be routed back to a central data center. This reduces latency and enables faster access to cloud applications. Traditional security solutions like VPNs are notorious for hairpinning traffic that requires data to be re-routed, sometimes over long distances.

- **Security:** SASE includes security measures like Zero Trust principles, threat detection, and data protection that is integrated into a unified solution that is easier to manage.

- **Scalability:** SASE's cloud-native design makes it easy to grow and adaptable with businesses of all sizes. SASE can benefit small and large businesses alike. The most common use case for SASE is secure access from anywhere, meaning distributed businesses with multiple locations or a need to connect remotely.

- **Efficiency:** By merging multiple tools into a single solution, SASE can reduce both the complexity and cost associated with managing separate networking and security technologies. There are many tools that can be updated or replaced by SASE for the same or better business outcomes.

Identifying Core Components of SASE

SASE's architecture is built on several foundational components. To meet the definition of SASE outlined by Gartner and other tech analyst firms, the components must have the following:

1. SD-WAN

SD-WAN is the networking foundation of SASE, designed to optimize and simplify the management of Wide Area Networks (WANs). Unlike traditional WAN architectures, SD-WAN provides a software-defined approach that allows traffic to be intelligently routed based on conditions such as application type, bandwidth needs, and connection quality. The most important, mission critical traffic gets prioritized, while other traffic that will not impact user experience is loaded in the background.

By leveraging multiple types of connections (such as broadband, LTE, and MPLS), SD-WAN enables high-performance access to applications without compromising security. With SD-WAN, companies can route traffic directly to the internet or to the cloud, bypassing traditional data centers. This reduces latency and enhances the user experience, especially for cloud-based applications.

2. SWG

A SWG is a security measure that inspects internet-bound traffic and enforces security policies to protect users from web-based threats. SWGs block malicious sites, control access to content, and scan for threats, protecting users from harmful web-based content and attacks. Hughes Managed SASE utilizes Next Gen SWG that allows for granular cloud app controls and the ability to selectively enable apps to third-parties, exceeding compliance regulations. It also takes advantage of modern Machine Learning (ML) to detect data in motion for cloud and web traffic.

In the context of SASE, SWGs are crucial for securing users as they browse the web regardless of whether they are working on-premises or remotely. This continuous monitoring provides the first layer of defense against malware, phishing, and other online threats.

3. CASB

CASB acts as an intermediary between cloud users and cloud service providers. The CASB scans the network to identify all cloud applications that are being used by employees, both sanctioned and unsanctioned. It also tracks user behavior and has visibility into who is accessing what and if those patterns fall outside of pre-established norms.

In a SASE solution, the CASB component offers visibility and control over the use of cloud applications, enabling organizations to enforce data security policies as users access Software as a Service (SaaS) apps, whether on managed or unmanaged devices. This is part of what allows SASE to function whether employees are in the office or working remotely.

4. ZTNA

ZTNA, often described as “the new VPN,” is a security approach that is based on the principle of Zero Trust: never trust, always verify. Unlike traditional VPNs, which assumes that users who have network access are trusted, ZTNA verifies users’ identities and context continuously before granting access to applications and resources.

ZTNA restricts access on a per-user and per-application basis, ensuring users only connect to the applications that they are authorized to access. ZTNA asks who is accessing, what they are accessing, how they are accessing, where they are accessing from, if this is part of their regular user behavior and more, all in a fraction of a second.

5. FWaaS

FWaaS extends the traditional firewall capabilities to the cloud. FWaaS inspects and filters traffic to and from users, devices, and applications, applying security rules that block threats and ensure safe connectivity. Unlike traditional firewalls that are deployed at specific locations, FWaaS is a cloud-delivered service that applies protection to all traffic across an organization’s network, no matter where the users are connecting from.

In the SASE architecture, FWaaS provides the crucial perimeter security that safeguards users and data from external threats. It is the primary prevention tool that keeps most threats from getting anywhere near your network.

6. Bonus Components of SASE

Though not considered core components, some additional related components of SASE that are often packaged with the core components include Data Loss Prevention (DLP) and Remote Browser Isolation (RBI). Hughes Managed SASE comes with both DLP and RBI. Hughes DLP is built from the ground up, works with more SaaS applications, and has more integrations than any other DLP on the market today. Our RBI solution stops employees from harming their device or your network, even if they click on a phishing link or a risky website.

What do you consider the most valuable benefits of implementing SASE?

54%
Enhanced security posture

50%
Enhanced productivity and secure access for remote workforce

47%
Scalability and flexibility to adapt to business needs

Consolidation of SD-WAN and security into a unified platform
45%

52%
Simplified management of security and networking functions

49%
Improved application performance and bandwidth optimization

46% Cost reduction through consolidation of tools and services

43% Consistent security policy enforcement across the network

HUGHES®
An EchoStar Company

Chapter 2: Benefits of SASE for Modern Enterprises

Most modern enterprises are becoming increasingly distributed. The rise in demand for remote and hybrid work, coupled with the need to expand and open more physical locations, means businesses are quickly realizing the need for a new solution to their network and security needs. Some of the benefits that SASE provides that appeal to these distributed enterprises include:

1. Enhanced Security Through a Unified Approach

In traditional models, security is often scattered across multiple tools and platforms, creating gaps that attackers can exploit. SASE consolidates various security functions—such as SWG, CASB, ZTNA, and FWaaS—into a unified platform that simplifies management and reduces the likelihood of misconfigurations. By centralizing policy enforcement, SASE ensures consistent security coverage across all devices, users, and locations. This unified approach also facilitates real-time threat detection and faster responses to emerging security incidents.

2. Improved Network Performance and User Experience

One of the critical advantages of SASE is its ability to optimize network performance. Traditional networks often route traffic through central data centers, resulting in latency and degraded user experience, especially for cloud-based applications. With SASE, traffic is directed to the nearest edge node and then securely routed to its destination. This reduces the number of hops and provides direct, low-latency connections to cloud applications, significantly improving user experience, particularly for remote and mobile employees. Hughes Managed SASE utilizes hundreds of nodes across the globe, meaning your data never has to travel far, drastically reducing latency when compared to other SASE solutions.

3. Cost Savings and Simplified Management

Managing multiple security and networking solutions can be costly and complex, especially for organizations with limited IT resources. SASE helps streamline operations by consolidating these tools into a single platform, reducing the total cost of ownership. Additionally, SASE's cloud-native architecture removes the need for on-premises hardware and ongoing maintenance costs. Simplified management also reduces the operational burden on IT teams, allowing them to focus on strategic initiatives rather than routine maintenance.

4. Enabling Secure Remote Work and Hybrid Environments

The COVID-19 pandemic accelerated the shift to remote work, creating new security and networking challenges. Traditional VPN solutions, often used for remote access, can be difficult to scale and may introduce latency issues. By integrating ZTNA, SASE offers a more scalable and secure alternative for remote access. ZTNA provides a seamless and secure way for employees to access applications from anywhere without compromising security. This makes SASE ideal for hybrid and fully remote work environments where employees need secure and reliable access to corporate resources regardless of location.

Chapter 3:
Managed vs. Unmanaged SASE

As organizations embrace SASE to meet their network security needs, one key decision is whether to manage the SASE deployment in-house (unmanaged SASE) or partner with a managed SASE provider. Each approach has its advantages, but managed SASE offers distinct benefits that can streamline deployment, reduce operational burdens, and improve overall security outcomes.

Understanding Managed vs. Unmanaged SASE

Before diving into the benefits of managed SASE, let us clarify what each approach entails:

- **Unmanaged SASE (DIY):** In an unmanaged (DIY) SASE model, the organization's IT or security team is responsible for deploying, configuring, and maintaining all SASE components. This requires in-depth knowledge of SASE technology, vendor management, and ongoing updates and monitoring. While unmanaged SASE provides maximum control, it can place significant demands on in-house teams.

- **Managed SASE:** In a managed SASE model, an external service provider takes on the responsibility for configuring, managing, and optimizing SASE components. Managed SASE providers offer end-to-end services, including security monitoring, performance tuning, and incident response, as well as 24/7 support. Organizations that choose managed SASE can benefit from the provider's expertise and resources, freeing up the internal teams so they can focus on strategic initiatives.

Benefits of Managed SASE

- **In-Depth Expertise:** Managed SASE providers employ teams of experts with extensive experience in SASE technologies, cloud security, and networking. By leveraging this expertise, organizations can ensure that their SASE deployment is designed and optimized according to best practices.

- **24/7 Monitoring and Support:** Managed SASE providers offer around-the-clock monitoring and support, ensuring that the network remains secure and performance remains optimized even outside of regular business hours.

- **Automated Updates and Patches:** With managed SASE, providers take care of routine updates, patches, and system maintenance, reducing the risk of vulnerabilities and ensuring that the solution is always up to date.

- **Accelerated Deployment Process:** Managed providers have established deployment processes and expertise, enabling them to deploy SASE solutions more quickly and efficiently than in-house teams.

- **Support for New Locations and Users:** As organizations expand, managed SASE providers can quickly onboard new users and locations without placing additional demands on in-house teams.

- **Rapid Incident Response:** With a dedicated team monitoring for threats, managed providers can respond to incidents quickly, often mitigating risks before they impact the organization. This proactive approach reduces the likelihood of data breaches and other security incidents.

- **Lower Total Cost of Ownership (TCO):** Managed SASE solutions reduce TCO by consolidating network and security services under one provider, eliminating the need for separate investments in security appliances, firewalls, VPNs, and other hardware.
- **Built-in Compliance Tools:** Managed SASE providers offer compliance controls, such as data encryption, access control, and activity monitoring, aligned with common regulatory frameworks.
- **Reduced Risk of Compliance Violations:** By enforcing consistent security policies and implementing best practices, managed SASE solutions minimize the likelihood of compliance breaches and associated penalties.

Use Cases: When Managed SASE is Ideal

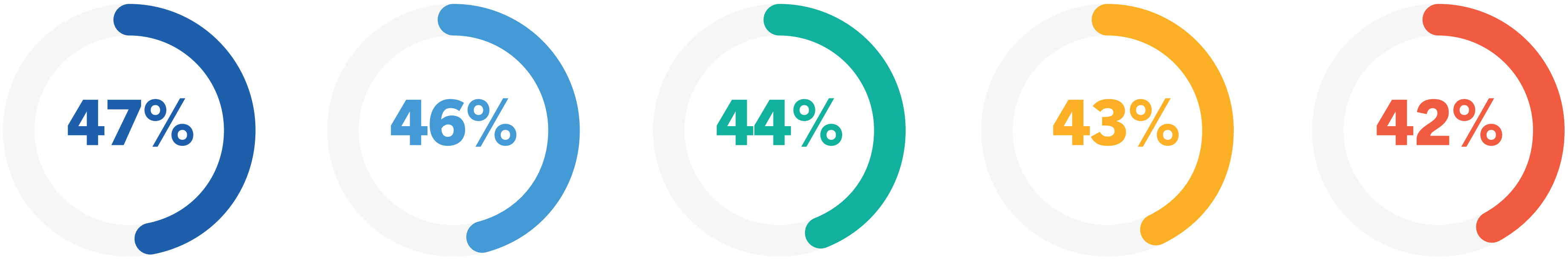
1. **Small to Medium-Sized Businesses (SMBs):** SMBs with limited IT resources can benefit from managed SASE's end-to-end services, gaining access to enterprise-grade security without the need to build an extensive in-house team.
2. **Organizations Lacking SASE Expertise:** Organizations new to SASE or cloud-based security can benefit from the knowledge and support of a managed provider, ensuring their deployment is optimized from the start.
3. **Companies with Dynamic Workforces:** Managed SASE is ideal for organizations with distributed or remote workforces as it .allows them to easily scale security and provide secure access for employees working from different locations.
4. **Industries with High Compliance Requirements:** Regulated industries, such as healthcare and finance, can use managed SASE to ensure continuous compliance with industry standards, thanks to the provider's built-in compliance controls and reporting capabilities.

Managed SASE as a Strategic Advantage

Choosing managed SASE allows organizations to offload the complexity of SASE management and take advantage of the provider's expertise, tools, and support. For many organizations, managed SASE not only simplifies deployment and operations, but also enhances security, optimizes performance, and provides a predictable cost structure.

Managed SASE offers a strategic advantage for those looking to streamline security management, reduce operational burdens, and focus on their core business. As SASE becomes an essential part of the modern network security landscape, managed SASE will play a critical role in helping organizations achieve secure, scalable, and resilient networks. Hughes offers a managed SASE solution that provides businesses with ease of use, peace of mind, and the highest levels of satisfaction and support.

What are your organization’s primary reasons for using or considering MSPs and/or MSSPs?



Lack of in-house expertise

Access to specialized skills or expertise

Enhanced incident response capabilities

Proactive threat detection and response

24/7 monitoring and support

40%
Scalability and flexibility

39%
Accelerated deployment of security solutions

37%
Improved compliance with regulations

35%
Cost savings

34%
Global coverage and support

HUGHES®
An EchoStar Company

Conclusion and Key Takeaways

SASE has emerged as a proven solution that is here to stay and is likely to see rapid adoption in the coming years. SASE addresses the challenges of modern enterprise connectivity and security with a cloud-native, all-in-one approach. By integrating essential services like SD-WAN, SWG, CASB, ZTNA, and FWaaS, SASE delivers unmatched flexibility, efficiency, and security for businesses that are trying to balance their network and security needs.

SASE not only simplifies network architecture, but also empowers organizations to enforce strong security policies without compromising performance. Whether enabling secure remote access, optimizing cloud connectivity, or consolidating IT infrastructure, SASE represents a paradigm shift in how enterprises think about and implement secure networking.

For enterprises evaluating their next steps in network and security evolution, SASE offers a clear path forward. The choice between managed and unmanaged SASE solutions will depend on the unique needs and resources of each organization. However, with its ability to streamline operations, reduce costs, and enhance user experiences, SASE is poised to become the gold standard for secure network access in the coming years.

Adopting SASE is more than a technical decision—it is a strategic move that aligns IT infrastructure with the demands of a cloud-driven, remote-enabled world. By embracing SASE, organizations can future-proof their operations, ensure seamless connectivity, and maintain a strong security posture, no matter where their users or data reside.

If you are looking for a security partner to help implement parts of or all of a modern SASE infrastructure, learn more about Hughes Managed SASE at www.hughes.com/what-we-offer/managed-cybersecurity/managed-sase.

To access the full 2025 State of Secure Network Access Report: www.hughes.com/resources/2025-state-securenetwork-access-report

HUGHES®
An EchoStar Company

11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com