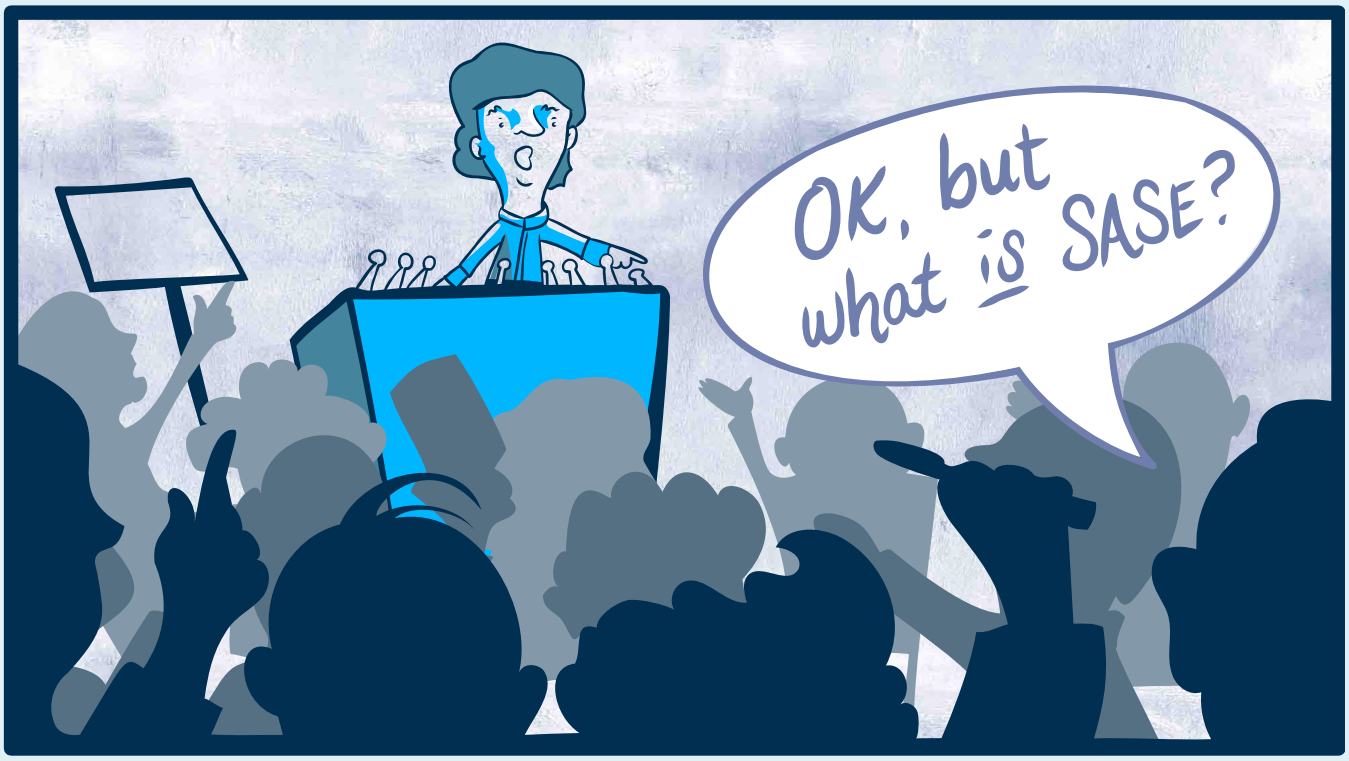
# The Definitive Guide to Secure Access Service Edge (SASE)

SIMPLE SECURITY FOR A COMPLEXIFIED MODERN CLOUD

strongdm

# Table of Contents




## TL;DR

In this article, we'll take a comprehensive look at **Secure Access Service Edge (SASE)** and dive into what it means, how it works, and the benefits of the model. You'll learn how it compares to Software-Defined Wide Area Networking (SD-WAN), the various components of the SASE model, and how to adopt it today. By the end of this article, you'll have a clear understanding of what SASE is and how it fits into the broader context of network security and risk management.

01

# SASE Meaning—More than another buzzword

The rise of digitalization, a hybrid workforce, and cloud-based computing in recent years have accelerated the adoption of Secure Access Service Edge to enable unified cloud-native network and security services.

Originally introduced by Gartner in 2019, the SASE model bridges networking and security solutions to help IT organizations provide holistic, agile service with optimized performance and enhanced security on a global scale.

**BUT WHAT EXACTLY IS IT? HERE'S A QUICK SASE DEFINITION:**

Secure Access Service Edge (more commonly known by the SASE acronym) is a cloud architecture model that combines network and security-as-a-service functions to deliver them as a single cloud-based service. As the enterprise attack surface continues to expand across cloud apps, on-premises resources, and personal devices, a SASE network offers a context-aware solution with a fully integrated security and network stack that can enforce policies wherever the data goes.

This allows organizations to consolidate their network and security tools into one seamless management solution that is cost-efficient and location-independent. In other words, in an era of remote work and with the proliferation of cloud services, Secure Access Service Edge offers organizations a convenient, agile, scalable SaaS solution for networking and security.

02

# How Does SASE Work?

Secure Access Service Edge combines SD-WAN edge capabilities with comprehensive cloud security functions, including:

- Firewall as a service (FWaaS)
- Cloud secure web gateways (SWG)
- Zero-trust network access (ZTNA)
- Cloud access security brokers (CASB)

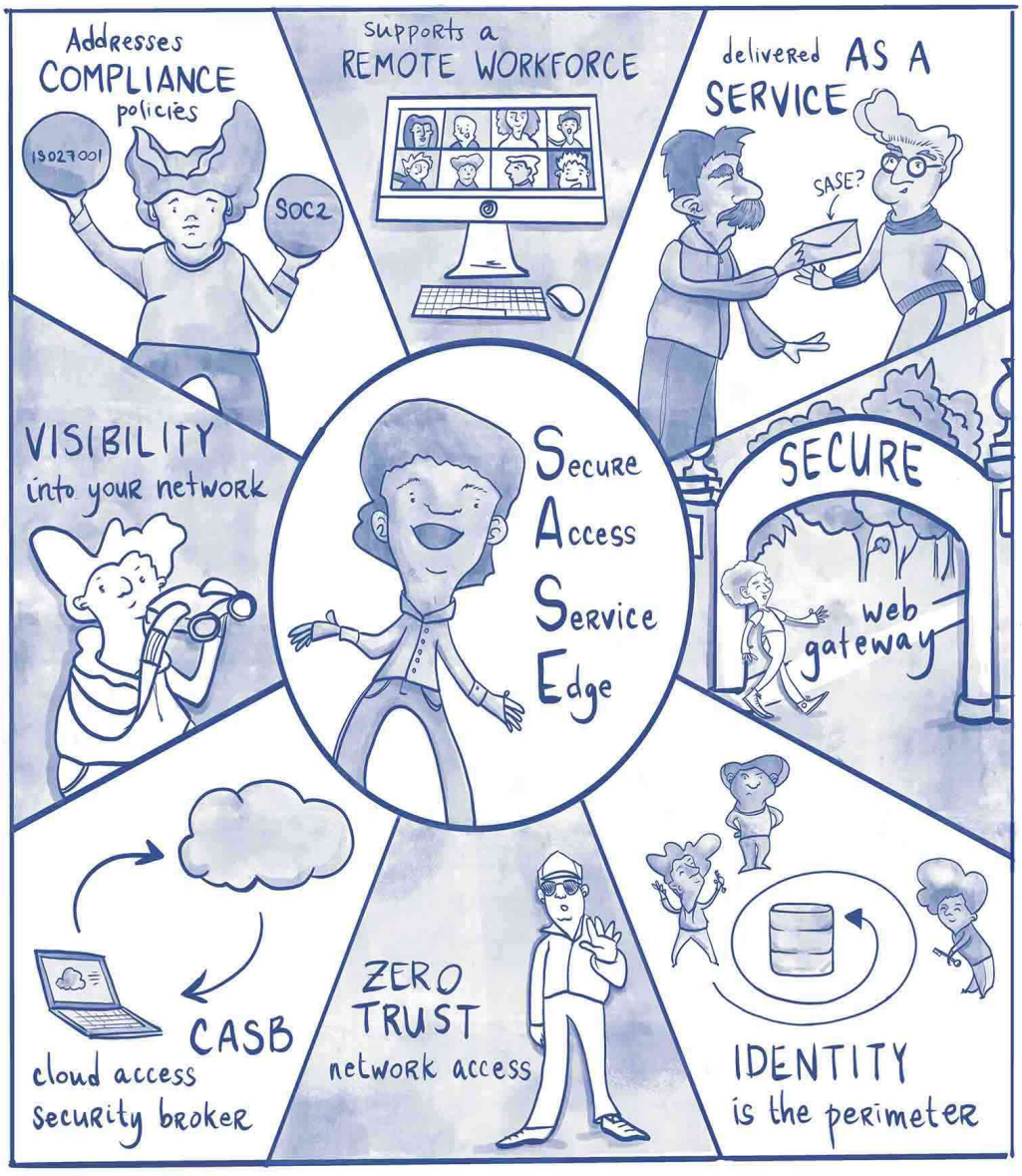
Web Application and API Protection as a Service (WAAPaaS)
Traditionally, application traffic from branch locations traveled through private Multiprotocol Label Switching (MPLS) services to the corporate data center for verification. While this worked well when all applications were hosted in the data center, widespread migration to the cloud means legacy architecture is no longer sufficient.

Today, more and more applications, data, and workloads live in cloud data centers and Infrastructure as a Service (IaaS) platforms rather than in private data centers. This means IT organizations need to rethink how they network and secure their users and resources. Perimeter-based security just isn't equipped to manage remote users accessing applications through the cloud from multiple locations. And routing internet-destined traffic through the data center and corporate firewall first results in diminished performance and user experience.

Secure Access Service Edge aims to address these issues by transforming and unifying both WAN and network security. Traditional network architectures were built around network policy enforcement points and forced-routed traffic—leading to bottlenecks and inefficient aggregation points.

SASE architecture turns this model on its head, instead enforcing security where the traffic is—at user and application endpoints. Security and WAN functions are delivered as a single service at SASE points of presence (PoPs), and users connect to the nearest available PoP in order to access the services.

By integrating advanced SD-WAN and security capabilities, the SASE model reduces operational complexity while ensuring consistent policy enforcement and access control for applications, users, devices, and the Internet of Things (IoT).



03

# Components of the SASE Model

Secure Access Service Edge shifts security focus from traffic-flow-centric to identity-centric, embedding security into the global fabric of the network. In order to successfully integrate security based on user identity and context, an effective solution includes several components:

| Type | Detail |
| --- | --- |
| **strongDM Provides an Audit Trail and Logs.** | SD-WAN provides the foundation for a SASE solution, enabling optimized network routing and enhanced performance. SD-WAN is an agile and reliable alternative to Internet-based VPN and a more affordable alternative to MPLS.<br><br>A few core capabilities include:<br>• Latency optimization<br>• Traffic routing from anywhere<br>• Globally distributed gateways<br>• Secure traffic on-ramp and off-ramp<br>• Inline encryption<br><br>**Zero trust network access (ZTNA)**<br>Zero Trust is a security strategy that operates under the premise that nothing is trusted—not users, data, devices, workloads, or the network itself. It's a framework that ensures all resources can be securely accessed, regardless of location, and applies a least-privileged access strategy.<br><br>ZTNA provides granular-level control to authenticate users to applications, making it a natural fit for SASE. And, because ZTNA is designed to adapt to business changes, it is a reliable and resilient component of a SASE security posture.<br><br>**Cloud access security broker (CASB)**<br>A cloud access security broker (CASB) acts as an intermediary between users and cloud service providers and is designed to protect an organization's cloud-based applications in a complex security environment.<br><br>A CASB consolidates multiple types of security policy enforcement and applies them to everything your business uses in the cloud—no matter what device users are accessing it from, including unmanaged smartphones or personal laptops. This allows organizations to safely use the cloud without compromising their corporate data—a key priority for enterprises that are undergoing digital transformation and operate on both legacy and cloud environments.. |

| Type | Detail |
| --- | --- |
| **Firewall as a service (FWaaS)** | FWaaS is a cloud firewall that delivers advanced next-generation firewall (NGFW) capabilities including:<br>• URL filtering<br>• Advanced threat prevention<br>• Intrusion prevention systems (IPS)<br>• DNS security<br><br>As Gartner explains, NGFWs are "deep-packet inspection firewalls that move beyond port/protocol inspection and blocking to add application-level inspection, intrusion prevention, and bringing intelligence from outside the firewall."<br><br>However, traditional NGFWs weren't made for the cloud. Backhauling traffic to an NGFW at a corporate data center worked when applications were all housed there. But as applications moved into the cloud, and workers began accessing the network from anywhere, this created gaps in perimeter security. FWaaS solves this problem by delivering NGFW capabilities within the cloud environment and allowing organizations to eliminate firewall appliances and simplify their IT infrastructure. |
| **Secure web gateway (SWG)** | An SWG protects web-surfing users and devices from infection and online security threats by enforcing company security policies and filtering malicious traffic in real-time.<br>A robust SWG should provide:<br>• URL filtering<br>• Data loss and leak prevention<br>• Malicious-code detection<br>• Remote browser isolation (RBI)<br>• Application identification and control capabilities<br>This ensures users access applications in compliance with company policies while protecting both users and the organization from security breaches and infection. |
| **Monitoring & audit trail.** | An audit trail is an important part of an organization's security posture. It is a record of every event, activity, or transaction that occurred with your data. An audit trail helps organizations ensure compliance, conduct digital forensics, maintain data integrity, perform business analyses, detect fraud, and protect against data breaches.<br><br>With the sheer size of enterprise data use, the daily volume of audit logs can reach hundreds of thousands. This level of scale and complexity requires automated monitoring and tracking. |

| Type | Detail |
| --- | --- |
| **Threat prevention** | Threat prevention refers to the policies and tools that protect your network. While threat prevention used to focus primarily on perimeter security, as cloud adoption expanded so did the attack surface, and organizations have had to take a multilayered approach to security.<br><br>An advanced threat prevention strategy within a SASE model can include tools for intrusion threat detection and prevention, advanced malware protection, and endpoint security threat prevention. |
| **Scalability** | The ability to scale infrastructures and systems to meet demand is critical for operating a secure network. With the acceleration of cloud computing, users are accessing more applications from more devices and locations than ever before. And more applications mean more data, more traffic, and more threats. SASE relies on dynamic scalability as a core component of network security to adapt to increasingly complex networks with agility. |
| **Data loss prevention (DLP)** | DLP is a set of tools and processes designed to detect and prevent data breaches, exfiltration, or unauthorized destruction of sensitive data. Organizations use DLP to secure their data and ensure compliance.<br><br>DLP is especially important for protecting personally identifiable information (PII) and intellectual property, securing the mobile workforce, enforcing security in bring your own device (BYOD) environments, and securing data on remote cloud systems. DLP is an important part of an integrated security approach under the Secure Access Service Edge model. |
| **Extensibility** | Extensibility is a software design principle that accounts for future growth by allowing the addition of new functions or capabilities. Extensibility goes hand-in-hand with scalability (which typically refers to hardware and systems) to ensure an organization's security strategy and applications can expand to meet growing demand and adapt to emerging threats. |

04

# 11 SASE Benefits


Secure Access Service Edge is an increasingly popular security solution for enterprises today. In fact, Gartner predicts that by 2025, at least 60% of enterprises will have explicit strategies and timelines for SASE adoption encompassing user, branch, and edge access—up from 10% in 2020.

So what makes it so great? Here are 11 key benefits of adopting this model:

### 1. CENTRALIZED AND DYNAMIC RBAC

SASE relies on centralized role-based access control (RBAC), which restricts access based on a user's role within the organization. Roles are assigned by the company and determine the permissions and access each user is granted through the system.

For example, roles might include administrators, specialists, and end-users—each with varying levels of access or permissions. Some employees may have permission to access and modify documents, while others can only view the files.

This allows organizations to secure access in a more targeted and flexible way. With RBAC, employees can only access information that is necessary to do their jobs—limiting the number of people who can access or share sensitive data within the company.

### 2. BIRD'S-EYE-VIEW ACROSS HYBRID ENVIRONMENTS

SASE unifies your network management, giving you a centralized, bird's-eye-view across all your hybrid environments. As organizations increasingly move into the cloud, security environments have become more complex, requiring disparate tools and management solutions to piece them all together. This creates blind spots in data and network management, leaving organizations vulnerable.

SASE solves the problem of siloed data and tools by bridging those technology gaps and bringing network and security management under one seamless umbrella.

### 3. GOVERNANCE OF USERS, APPS, AND DATA USAGE

By unifying the security technology stack, the SASE model improves the overall governance of users, applications, and data usage.

It ensures best practice security solutions (including RBAC, DLP, FWaaP, and SWG) are applied across all environments, eliminating gaps in the security perimeter and enforcing consistent policy and compliance no matter where the user is or how they are accessing data.

### 4. AUDIT TRAIL AND REPORTING

Data monitoring and reporting is an essential component of network security. Relying on machine learning and artificial intelligence, the SASE model builds audit trail and reporting mechanisms into the network architecture to ensure comprehensive visibility and real-time, scalable threat prevention, detection, and analysis at every touchpoint in a hybrid environment.

### 5. SIMPLIFIED SECURITY MODEL

One of the biggest benefits of SASE is that it simplifies the cloud and hybrid security model. Legacy network solutions require additional tools and systems to keep up with the pace of digitalization, the expansion of attack surfaces, and emerging security threats. However, legacy solutions often fall short of the advanced capabilities today's modern IT needs to protect their organizations.

The result: increasingly complex security environments and a growing technology stack that doesn't always work together.

SASE addresses this challenge by applying FWaaS, which embeds security features like URL filtering, anti-malware, and firewalling into its infrastructure. This simplifies security management, enabling organizations to set and enforce uniform policies, identify issues quickly, and secure all edges with consistent protection.

### 6. CONSISTENT EDGE-TO-EDGE SECURITY

SASE combines network and security functions within a single multi-tenant cloud platform that strengthens security and performance. As part of a full network security stack, the solution embeds advanced security functionalities such as SWG, NGFW, and DLP into its architecture, enabling edge-to-edge protection.

### 7. COST REDUCTION

SASE eliminates the need for disjointed physical and virtual appliances from multiple vendors. This reduces costs to adopt and maintain disconnected solutions while simplifying ongoing management from the backend. Reducing complexity further improves cost savings by minimizing the workload for IT, increasing efficiency, and reducing staffing costs—all without sacrificing security.

### 8. LESS ADMINISTRATIVE EFFORT AND TIME

SASE simplifies network security management through one central cloud-based application. Which means the architecture doesn't grow in complexity when the network expands. This reduces the administrative workload and frees up time for IT staff to focus on other high-value priorities.

### 9. REDUCED DEPENDENCIES

The SASE model provides an elegant solution that reduces an organization's dependencies on multiple appliances and vendors. Not only does this minimize costs and resource investments, but it also gives the organization greater control and flexibility over its network infrastructure and edge security.

### 10. FASTER AND MORE RELIABLE SERVICE

SASE replaces traditional VPN appliances with network security based on ZTNA principles. With traditional VPN point solutions, enterprises must deploy additional appliances to fill gaps in functionality (like SD-WAN security and NGFW).

VPN appliances often become bottlenecks that slow down a WAN, negatively impacting performance because they have CPU and resource limitations. The cloud-native SASE solution isn't limited by scale and delivers additional WAN optimization through its underlying infrastructure, enabling faster and more reliable service.

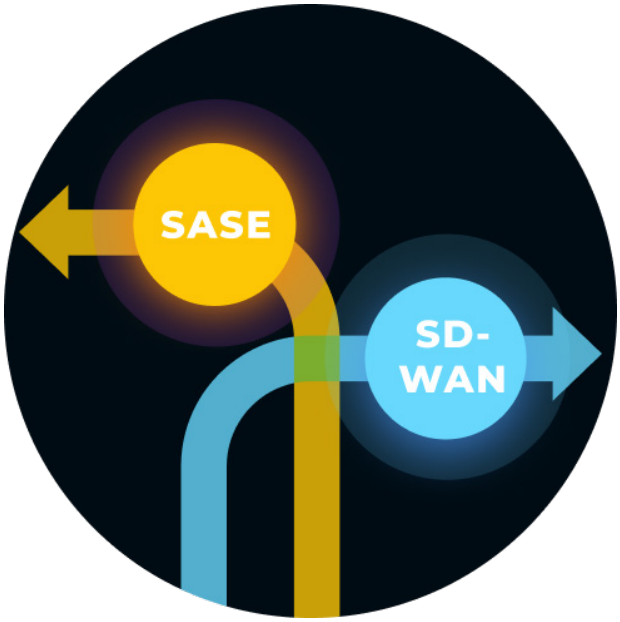
### 11. PERPETUAL DATA PROTECTION

Today, companies collect, process, and distribute massive volumes of data—including sensitive proprietary and personal data. In order to protect data across environments, SASE enables DLP delivery through the cloud, essentially eliminating the need for adopting and maintaining multiple protection tools. This allows organizations to apply consistent security policies at all edges, from mobile devices to the cloud, to on-premise locations.

05

# How Do SASE and SD-WAN Relate?

SASE marries SD-WAN with network security for a holistic network management solution that streamlines access, strengthens security, and boosts performance. To better understand how they relate, it's helpful to understand what SD-WAN is and the problems it sets out to solve.




SD-WAN uses software-defined networking concepts combined with traditional WAN technology to deliver better traffic routing and networking operations. It acts as an overlay network (a network built on top of and supported by another network) on an organization's existing WAN connections to improve network traffic.

### KEY DIFFERENCES BETWEEN SASE AND SD-WAN

Both SASE and SD-WAN are virtualized technologies that cover broad geographic areas and share the same goal: to connect separate branch offices and end users to an enterprise's network resources in a scalable and easily managed way.

However, there are several key differences between these solutions:

| Type | Detail |
|---|---|
| **Deployment and architecture** | SD-WAN can be deployed through physical, software, or cloud connections, depending on the needs of the organization. It primarily connects branch offices to the data center whereas SASE operates solely as a cloud-native solution that focuses on endpoints and end-user devices.<br><br>Enterprises can choose a DIY, managed, or hybrid SD-WAN, where IT either manages the network themselves, outsources management to a third-party vendor, or a combination. SASE platforms deliver combined network and security functionalities from a single as-a-service tool. This typically makes them simpler and more customizable for organizations compared to SD-WAN. |
| **Security** | SD-WAN has some security functionalities but is primarily focused on network management and capabilities. In contrast, SASE has built-in security, adopting many of the benefits of SD-WAN, like scalability and streamlined management, for a more secure, cloud-native solution. |

| Type | Detail |
|---|---|
| **Traffic and connectivity** | SASE and SD-WAN have different architectures, which affects how each handles traffic and connections.<br><br>SD-WAN connects branch offices to the organization's network and data center resources, following configured network policies to determine how to route and backhaul traffic through data centers.<br><br>SASE focuses on cloud environments and connecting endpoints to the service edge. Because it is cloud-based, it doesn't need to backhaul traffic through the data centers, instead routing it through globally distributed PoPs. |
| **Remote access** | Because SASE is cloud-based, it has built-in remote access capabilities—a key benefit for businesses operating in an increasingly remote world. In contrast, SD-WAN relies on expensive third-party services to improve remote access functionality, limiting the scale at which companies may choose to connect remote employees. |

In many ways, SASE is simply an evolution of SD-WAN. It combines SD-WAN capabilities and benefits with advanced network security services for a seamless all-in-one solution.

06

## SASE vs SD-WAN vs SWGs vs UTM / NGFW

Advancing your network and security technology takes time. To ensure you're investing in the right tools and solutions, it's important to understand and compare your options based on your business's unique needs and priorities.

| | Global connectivity | Simplified management | Optimized cloud access | Multilayered protection | MPLS replacement |
|---|---|---|---|---|---|
| SASE | ✔ | ✔ | ✔ | ✔ | ✔ |
| SD-WAN | ✖ | ✖ | ✖ | ✖ | ✔ |
| SWG | ✖ | ✖ | ✖ | ✔ | ✖ |
| UTM/NGFW | ✖ | ✖ | ✖ | ✔ | ✔ |

In a cloud-based, mobile world, point solutions like SD-WAN, SWG, and unified threat management (UTM), or NGFW can't deliver the capabilities businesses need without increasing costs and complexity. SASE overcomes these issues by bridging the gaps of siloed legacy point solutions—resulting in a globally connected, cloud-native platform that provides enhanced access and security.

07

# How Difficult Is It to Actually Adopt SASE?

While adoption is on the rise, making the shift can take time—especially for large enterprises that have already invested resources into existing siloed security and digital transformation initiatives.

Understanding potential challenges to adoption can help you strategically plan your investments and successfully navigate your options.

A few key challenges include:

| Type | Detail |
| --- | --- |
| **SASE maturity** | The markets for Network-as-a-aservice (NaaS) and Security-as-a-service (SECaaS) are immature, which means the vendors building SASE solutions are still evolving. Many approach SASE from different backgrounds and specialties. This means you might have a security vendor that is focusing on building up their cloud and SD-WAN capabilities or a network vendor that is prioritizing their security capabilities.<br><br>Organizations looking to adopt the model should evaluate their priorities to determine which vendor can best address the capabilities they need. |
| **Finding trusted vendors and service providers** | In a similar vein, because SASE technologies are still young, it can take longer to identify a vendor that has the capabilities and support your organization is looking for.<br><br>To overcome this roadblock, stakeholders need to have a clear understanding of which components are top priorities. These are the components you need to build your solution around, so it's important to get those right from the start. From there, you can assess vendors based on your goals and priorities and evaluate the service level they provide. |
| **Moving away from current investments** | Many large enterprises have existing contracts and significant investments in hardware and software solutions that are difficult to leave behind. Often companies have hired and trained employees for the specific skills needed to manage or use a current solution, including entire dedicated teams. Adopting SASE could disrupt those roles and significantly reduce those responsibilities. Organizations that want to shift towards this model will need to consider retraining staff and reassigning roles, which can slow adoption. |

08

# Okay, I get it—so how do we start adopting SASE today?

Transitioning your organization to a SASE model can be a big shift and won't happen overnight. To start making the switch, keep the following tips in mind:

### 1. IDENTIFY YOUR SECURITY AND COMPLIANCE REQUIREMENTS.

SASE isn't a singular tool but rather a framework for integrating and advancing your existing security stack. In order to successfully adopt this model, you'll first need to understand your unique security requirements based on your network environment and user needs.

Additionally, review security policies and standards to ensure your SASE network has built-in compliance measures. By identifying these requirements at the start, you'll be able to design an architecture that meets your needs and ensures the highest standards of security and compliance.

### 2. KNOW YOUR USERS AND APPLICATIONS.

Every organization has a unique user base, and how they operate and interact within your networks should inform the way you configure your architecture. In other words, if you don't understand your IT environment, it will be difficult to properly secure it. And since SASE supports ZTNA, which requires access controls to be defined according to business needs, understanding the structure and use cases for your IT environment is essential for successful adoption.

### 3. GET BUY-IN FROM THE WHOLE TEAM.

As with any major change, migrating to a SASE model will go more smoothly if you have buy-in from your team. Migration requires an overhaul of your IT and security infrastructure, which can disrupt teams, roles, and responsibilities.

Communicate with all stakeholders involved, including internal IT, external partners, contractors, and vendors. Working with these stakeholders from the beginning can help you identify and address concerns, challenges, and potential roadblocks while ensuring a smoother transition for all parties.

### 4. TEST AND PILOT YOUR SASE SOLUTION AGAINST SPECIFIC GOALS.

Once you've adopted a SASE model, how do you know if it's successful? Outline key goals and priorities for your solution, and use those as benchmarks to measure the effectiveness of your migration.

If you're falling short of your goals, identify what gaps may exist in your SASE solution. This approach helps you measure success and gradually implement a more robust and effective solution.

### 5. IMPLEMENT SASE AS PART OF YOUR CLOUD MIGRATION.

Cloud migration and digitalization efforts are on the rise. According to Gartner, 69% of Boards of Directors accelerated their digital business initiatives following COVID-19 disruption.

If your business is joining the great cloud migration, make sure SASE is included as an integral part of your cloud strategy. By making it a key component of your cloud migration, you can more effectively align your cloud initiatives across the organization.

You can also get started with a solution like strongDM. strongDM is a comprehensive infrastructure access platform that helps organizations take the next step in adopting a SASE model by natively supporting any database and networking tool in your environment. Manage and audit access to databases, servers, clusters, and web apps for automated, integrated, role-based security no matter where your users are or what device they're on.


09

# Frequently Asked Questions

***How do you pronounce "SASE"?***
SASE is pronounced “sassy.”

***What is SASE used for?***
SASE is a cloud architecture model that combines networking and security-as-a-service to distribute network and security functions to clients through a single cloud-delivered platform. It is used to improve remote access in an increasingly distributed workforce and bridge the gaps that occur from managing various siloed network and security stacks.

***What are the required characteristics of SASE?***
The main characteristics include:

- Combined SD-WAN and security functions
- Cloud-native architecture that is scalable, agile, and self-healing
- Globally distributed fabric of PoPs to ensure advanced WAN and security capabilities wherever users are located
- Identity-driven services that drive real-time context impacting security policy
- Equal edge-to-edge support

***Is SASE secure?***
Yes. SASE provides end-to-end security. It combines SD-WAN with a full stack of advanced security functionality to deliver a centralized solution that improves data visibility and monitoring, boosts performance, and bridges security gaps at user endpoints rather than the traditional perimeter.

***How is SASE delivered?***
SASE is delivered via the cloud through PoPs or vendor data centers close to the endpoints.

***Is SASE a VPN?***
A VPN is part of the integrated SASE solution. Organizations adopting this model incorporate their existing networking capabilities, such as VPNs, to deliver a seamless cloud solution. For example, VPN services route traffic to the SASE solution, and then to any public or private cloud via software-as-a-service (SaaS).

***Is SASE an SD-WAN?***
SD-WAN is a part of SASE. SASE embeds edge SD-WAN capabilities within its architecture as part of its combined networking and policy-based security functionality.

***Does SASE replace SD-WAN?***
SASE integrates SD-WAN within its network and security framework. In other words, SD-WAN is just the first step in WAN transformation. SASE is the next step towards advanced WAN capabilities that enables the security, cloud, and connectivity functions that SD-WAN lacks.

***Is SASE the future of SD-WAN & security?***
SASE is an evolving framework that addresses the challenges and issues with traditional security and network solutions like SD-WAN. With the rise of hybrid work and cloud adoption, traditional approaches to security and networks are no longer sufficient.

Perimeter-based security isn't built for a distributed workforce and remote world—leaving organizations with disjointed security stacks and gaps in visibility that leave them vulnerable in an ever-expanding attack surface.

SASE offers a streamlined, integrated solution that addresses most network and security requirements at scale within a more efficient, manageable, and cost-effective model.

10

## A Cloud-Based Future for Network Security

Digitalization and remote work are here to stay, which means organizations will need to adopt a network and security posture that can address the needs of remote users and a distributed workforce. SASE offers a vision for the future of network security that is cloud-based, dynamic, and fully integrated.

If you're curious about how strongDM can help, make sure to sign up for our no BS demo.

10

## More Resources

Understanding Data Loss Prevention (DLP)

Understanding Software-defined Wide Area Network (SD-WAN)

Understanding Cloud Access Security Brokers (CASBs)

Zero Trust Explained: The Ultimate Guide to Zero Trust Security

Managing Access to Ephemeral Infrastructure at Scale

strongDM's infrastructure access platform gives every business secure access controls in a way folks love to use. Trusted by the Fortune 500 to fast-growing businesses like Peloton, SoFi, Chime, Yext, and Better, strongDM gives businesses the control and visibility they need at the speed they want with one platform that works for every environment. strongDM is intentionally distributed. Head to **www.strongdm.com** to learn more.