What Is Secure Access Service Edge (SASE)?

Secure access service edge (SASE) is a framework for network architecture that brings cloud native security technologies—SWG, CASB, ZTNA, and FWaaS in particular—together with wide area network (WAN) capabilities to securely connect users, systems, and endpoints to applications and services anywhere.

Read the blog: SASE vs. SSE

What it means | How it works | Just a buzzword? | SASE components | 3 benefits | Why it's necessary | Zscaler SASE

What Does SASE Stand For?

SASE (pronounced "sassy"), or **s**ecure **a**ccess **s**ervice **e**dge, first defined by Gartner in the 2019 report "The Future of Network Security is in the Cloud," in a convergence of WAN capabilities with network security functions meant to offer enterprises greater agility, stronger and more reliable network performance, deeper and more granular visibility and control across heterogenous IT environments, and much more.

SASE is distinct from security service edge (SSE), which Gartner defines as a subset of SASE that only focuses on the security services needed from a SASE cloud platform.

How Does SASE Work?

A SASE architecture combines a software-defined wide area network (SD-WAN) or other WAN with multiple security capabilities (e.g., cloud access security brokers, anti-malware), securing your network traffic as the sum of those functions.

Legacy approaches to inspection and verification, such as forwarding traffic through a multiprotocol label switching (MPLS) service to firewalls in your data center, are effective if that's where your users are. Today, though, with so many users working remotely, this "hairpinning"—forwarding remote user traffic to your data center, inspecting it, and then sending it back again—tends to reduce productivity and hurt the end user experience.

SASE stands out from point solutions and other secure networking strategies because it's both secure and direct. Rather than relying on your data center security, traffic from your users' devices is inspected at a nearby point of presence and sent to its destination from there. This means more efficient access to applications and data, making it the far better option for protecting distributed workforces and data in the cloud.

Is SASE Just a Buzzword?

While SASE has garnered a lot of attention from service providers and media focused on networking and security, what's most compelling is the main principle behind the SASE framework—the notion that data center–focused security and network architectures have become ineffective. This notion isn't just a marketing catchphrase; the industry has broadly accepted it.

So, what does a SASE solution offer that makes it so valuable compared to traditional enterprise network security that connects offices via private networks and routes traffic through secure web gateways and firewalls?

As Gartner points out, traditional models in which connectivity and security focus on the data center should focus on the identity of users and devices instead. According to the report, "In a modern cloud-centric digital business, users, devices and the applications they require secure access to are everywhere."

In other words, today's workflows, traffic patterns, and use cases are much different today than when hub-and-spoke networks were conceived. That's because:

- More user traffic is heading to cloud services than data centers
- More work is performed off the network than on it
- More workloads are running in cloud services than data centers
- More SaaS applications are in use than those hosted locally
- More sensitive data is housed in cloud services than inside the enterprise network

> **Instead of the security perimeter being entombed in a box at the data center edge, the perimeter is now everywhere an enterprise needs it to be — a dynamically created, policy-based secure access service edge.**
>
> Gartner, The Future of Network Security Is in the Cloud, 30 August 2019, Lawrence Orans, Joe Skorupa, Neil MacDonald

Components of a SASE Model

SASE can be broken down into six essential elements in terms of its capabilities and technologies:

1. Software-Defined Wide Area Network (SD-WAN)

SD-WAN is an overlay architecture that reduces complexity and optimizes the user experience by selecting the best route for traffic to the internet, cloud apps, and the data center. It also helps you rapidly deploy new apps and services as well as manage policies across a large number of locations.

2. Secure Web Gateway (SWG)

SWGs prevent unsecured internet traffic from entering your internal network. It shields your employees and users from accessing and being infected by malicious web traffic, vulnerable websites, internet-borne viruses, malware, and other cyberthreats.

3. Cloud Access Security Broker (CASB)

CASBs prevent data leaks, malware infection, regulatory noncompliance, and lack of visibility by ensuring safe use of cloud apps and services. They secure cloud apps hosted in public clouds (IaaS), private clouds, or delivered as software-as-a-service (SaaS).

4. Firewall as a Service (FWaaS)

FWaaS helps you replace physical firewall appliances with cloud firewalls that deliver advanced Layer 7/next-generation firewall (NGFW) capabilities, including access controls, such as URL filtering, advanced threat prevention, intrusion prevention systems (IPS), and DNS security.

5. Zero Trust Network Access (ZTNA)

ZTNA solutions give remote users secure access to internal apps. With a zero trust model, trust is never assumed, and least privileged access granted based on granular policies. It gives remote users secure connectivity without placing them on your network or exposing your apps to the internet.

6. Centralized Management

Managing all of the above from a single console lets you eliminate many of the challenges of change control, patch management, coordinating outage windows, and policy management while delivering consistent policies across your organization, wherever users connect from.

3 Benefits of SASE

How can an enterprise enforce access controls and security while facing these common realities? That's where a SASE platform of WAN capabilities (SD-WAN) and comprehensive security services come in. Cloud-based SASE offers significant benefits to organizations that put aside traditional on-premises enterprise network infrastructure and security to take advantage of cloud services, mobility, and other aspects of digital transformation.

1. Reduced IT Costs and Complexity

As they work to enable secure access to cloud services, protect remote users and devices, and close other gaps in their security, organizations have adopted a range of security solutions, adding significant costs and management overhead. Even so, the on-premises network security model is simply not effective in a digital world.

Instead of trying to use a legacy concept to solve a modern problem, SASE flips the security model. Rather than focusing on a secure perimeter, SASE focuses on entities, such as users. Based on the concept of edge computing—processing of information close to the people and systems that need it—SASE services push security and access close to users. Using an organization's security policies, SASE dynamically allows or denies connections to applications and services.

2. Fast, Seamless User Experience

When users were on the network, and IT owned and managed the apps and infrastructure, it was easy to control and predict the user experience. Today, even with distributed multi-cloud environments, many enterprises still use VPNs to connecting users to their networks for security. However, VPNs deliver a poor user experience, and they broaden an organization's attack surface by exposing IP addresses.

Instead of this degradation, SASE provides optimization: It calls for security to be enforced close to what needs securing—instead of sending the user to the security, it sends security to the user. SASE is cloud secure, intelligently managing connections at internet exchanges in real time as well as optimizing connections to cloud applications and services to ensure low latency.

3. Reduced Risk

As a cloud native solution, SASE is designed to address the unique challenges of risk in the new reality of distributed users and applications. By defining security, including threat protection and data loss prevention (DLP), as a core part of the connectivity model, it ensures all connections are inspected and secured, regardless of location, app, or encryption.

A key component of the SASE framework is zero trust network access (ZTNA), which provides mobile users, remote workers, and branch offices with secure application access while eliminating the attack face and the risk of lateral movement on the network.

Why Is SASE Necessary?

Digital business transformation demands greater agility and scalability coupled with reduced complexity and improved security. What's more, modern enterprises need to ensure their users are getting the best experiences from anywhere.

These circumstances have moved SASE from the category of "nice to have" to "necessity." Here are four reasons why:

- **SASE scales with your business:** As your enterprise grows, both your network and your security need to be able to handle the resulting increase in demand. SASE lets your business, network, and security scale together through its cloud-delivered model.
- **SASE makes work-from-anywhere work:** Legacy hub-and-spoke architectures can't tolerate the bandwidth required to give your remote employees the flexibility they need to stay productive. SASE can, and it does so while maintaining enterprise-level security for all users and devices at any location.
- **SASE stands up to cyberthreat evolution:** Security teams are on constant alert, defending from the latest threats. SASE helps them by providing superior security and ease of management, giving these teams the power to handle advanced threats, wherever they come from.
- **SASE gives you a base for IoT adoption:** The internet of things is creating utility for businesses worldwide, but in order to effectively adopt IoT technology and capabilities, you need a strong platform to build an IoT ecosystem on. SASE lets you meet your IoT goals with unprecedented connectivity and security.

All this has driven networking and security vendors to glue together their own versions of a SASE architecture. Many of these vendors claim to engineer a cloud-delivered product, but the truth is a great number of them are just a "cloud platform" built on legacy hardware.

Only one vendor can provide a truly cloud-delivered SASE model. Why? Because we built our platform in the cloud, for the cloud.

> **"By 2024, at least 40% of enterprises will have explicit strategies to adopt SASE, up from less than 1% at year-end 2018."**
>
> Gartner, The Future of Network Security Is in the Cloud

Zscaler SASE

The Zscaler Zero Trust Exchange™ is our SASE solution, offering you a fast, flexible, simple, and secure model for connecting users and devices. Our platform is easy to deploy and manage as an automated, cloud-delivered service, and because it's globally distributed, your users are always just a short hop from their applications.

Here's what makes our SASE unique:

- A native, multitenant cloud architecture that scales dynamically with demand
- Proxy-based architecture for full inspection of encrypted traffic at scale
- Security and policy brought close to users to eliminate unnecessary backhauling
- Zero trust network access (ZTNA) that restricts access to provide native application segmentation
- Zero attack surface, preventing targeted attacks because your source networks and identities aren't exposed to the internet

Through peering with hundreds of partners in major internet exchanges around the world, the Zero Trust Exchange offers optimal performance and reliability for your users.

Want to experience it for yourself? Explore our SASE offering to discover how it can help your business.

FAQs

What Is the Difference Between SD-WAN and SASE?

What Is the Main Goal of SASE?

Learn about:

Your world, secured.

Zero Trust

Security Service Edge (SSE)

Secure Access Service Edge (SASE)

Zero Trust Network Access (ZTNA)

Secure Web Gateway (SWG)

Cloud Access Security Broker (CASB)

Cloud Native Application Protection Platform (CNAPP)

Secure Your Users

Secure Your Workloads

Secure Your IoT and OT

Secure Internet Access (ZIA)

Secure Private Access (ZPA)

Data Protection (CASB/DLP)

Digital Experience (ZDX)

Posture Control

Industry & Market Solutions

Partner Integrations

Zscaler Client Connector

Zero Trust Exchange Platform

Secure Digital Transformation

Application Transformation

Network Transformation

Security Transformation

Resource Library

Security Preview

Security & Risk Assessment

ThreatLabz Analytics & Insights

Upcoming Events

Blog

Zscaler Academy

CXO Revolutionaries

Zpedia

Ransomware Protection ROI Calculator

Pricing & Plans

About Zscaler

Leadership Team

Career Opportunities

Find or Become a Partner

Customer Success Center

Investor Relations

Press Center

News & Announcements

ESG

Compliance

Contact Zscaler

English

Zscaler is universally recognized as the leader in zero trust. Leveraging the largest security cloud on the planet, Zscaler anticipates, secures, and simplifies the experience of doing business for the world's most established companies.

Email Address

Sitemap

Privacy

Legal

Security