Secure Access Service Edge (SASE)

At a Glance

What is SASE?

In 2019, Gartner coined the term secure access service edge (SASE) to describe a new approach to networking and security. The SASE model consolidates numerous networking and security functions — traditionally delivered in siloed point solutions — in a single, integrated offering.

Gartner describes SASE in terms of five primary functions:

- Software-defined wide area networking (SD-WAN)
- Firewall as a service (FWaaS)
- Secure web gateway (SWG)
- Cloud access security broker (CASB)
- Zero trust network access (ZTNA)

SASE is not a product — it's an architecture. A SASE approach lets organizations:

- Connect users seamlessly to the applications and data they need to access — in any environment, from any location
- Control access and enforce the right security protection anywhere users work
- Converge networking and security functions to deliver secure connectivity as a service

SASE by the numbers

45%

of requests to access protected apps come from outside the business walls[1]

80%

of organizations are either using or evaluating SD-WAN in some capacity[2]

64%

believe network security is more difficult than two years ago[2]

20%

of enterprises will have adopted SWG, CASB, ZTNA, and branch FWaaS capabilities from the same vendor by 2023[3]

40%

of enterprises will have explicit strategies to adopt SASE by 2024[3]

Why SASE?

Digital business transformation and the shift to a more distributed workforce are driving the need for anywhere, anytime access to resources, wherever they may exist. These changes require networking and security to move to the cloud, where they can be delivered as a single converged service with flexible deployment and consumption models.

The shift toward a more distributed workforce is not new, but it has recently accelerated. While the principles of SASE have been forming for years, recent global events brought SASE to the forefront as remote access to applications and "work from anywhere" became a top organizational priority. Organizations rushed to spin up remote access for employees and zero trust network access to help ensure trusted access. Now most people are working anywhere – at home, on the go, at the branch or campus offices – on any device. With this shift, the datacenter is no longer the hub – the user is. To give them secure access to work resources and applications, users must now be treated as a "branch of one."

But the traditional branch isn't gone. Some people may head back to the office soon and worker distribution will inevitably shift again. Throughout these ever-changing times, users still expect a seamless connection to the applications they need.

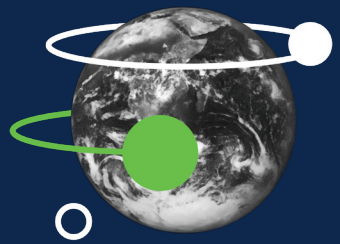
SASE is based on cloud-native capabilities that simplify the IT environment by bringing networking and security teams closer together to drive stronger collaboration and faster response times. For the best results, Gartner recommends that organizations select a single SASE vendor that can provide a broad set of security functions and flexible, high-performance networking that's backed by a reliable track record.

The Cisco SASE approach

Cisco has comprehensive solutions in the core SASE areas of networking, security, and zero trust. The Cisco SASE approach lets organizations:

- Deliver a seamless secure connection experience that users expect to any application, from any device, at any time
- Safely move access control closer to where it's needed – to the user and to the cloud edge
- Make your organization more agile by leveraging the cloud to help remove complexity from your infrastructure and scale
- Converge resources to gain more efficiencies through an as-a-service model for secure networking

The Cisco SASE approach delivers simplicity, visibility, and efficiency. Organizations can build on what they already have by protecting on-premises and cloud investments with the flexibility to evolve the infrastructure in the future. You can scale up or down as worker distribution shifts with a simple, flexible licensing and consumption model. As you transition services from on-premises to the cloud, you can enforce policies consistently across all environments. With open APIs in both networking and security, it's easy to choose what works best by integrating easily to preferred products or our broad and open ecosystem.



Largest SD-WAN solution provider

Cisco is the largest SD-WAN solution provider in the world, with #1 market share and more than 30,000 customers

Cisco SASE components

Networking: Cisco SD-WAN

Cisco SD-WAN is a cloud-delivered overlay WAN architecture connecting branches to headquarters, data centers and multi-cloud environments through a single fabric. The Cisco SD-WAN fabric connects users at the branch to applications in the cloud in a seamless, secure, and reliable fashion. It allows users to deploy applications in minutes on any platform with a consistent user experience. It provides greater agility through simplified deployment and operation of your WAN while still connecting users securely to applications and protecting data from the network edge to the cloud. Cisco SD-WAN helps ensure a predictable user experience for applications, optimizes software-as-a-service (SaaS), infrastructure-as-a-service (IaaS), and platform-as-a-Service (PaaS) connections, and offers integrated security either on-premises or in the cloud. Analytics capabilities deliver the visibility and insights necessary to isolate and resolve issues promptly while providing enhanced network intelligence.

Benefits

- Provide centralized management, analytics, and policy across the global WAN
- Increase user productivity by optimizing cloud and on-premises application performance with real-time analytics, visibility, and control
- Protect users, devices, and applications by deploying cloud-delivered SASE model or on-premises model depending on business requirements and compliance needs
- Centralize cloud management for easy deployment of SD-WAN and security while maintaining policy across thousands of sites
- Establish transport-independent WAN for lower cost and higher diversity
- Meet service-level agreements (SLAs) for business-critical and real-time applications
- Accelerate multi-cloud access with cloud onramp tools for SaaS and public cloud IaaS applications

Pioneer in cloud security

Cisco Umbrella offers complete protection faster, with industry-leading security efficacy and performance

Cisco SASE components

Security: Cisco Umbrella

Cisco Umbrella unifies firewall, SWG, DNS-layer security, CASB, and threat intelligence functions into a single cloud service to help businesses of all sizes secure their users, applications, and data, wherever they work. Umbrella provides global coverage with a broad set of high throughput data centers and peers with 1000+ of the world's top internet service providers (ISPs), content delivery networks (CDNs), and SaaS platforms to deliver the fastest route for any request, resulting in superior speed, effective security, and user satisfaction.

Umbrella DNS-layer security blocks requests to malware, ransomware, phishing, and botnets before a connection is established. The SWG provides logging and deeper inspection for all web traffic for greater transparency, control, and protection. The firewall helps log and block traffic using IP, port, and protocol rules for consistent enforcement throughout your environment. CASB functionality is included to detect and control the use of cloud applications. With Cisco SecureX (included with all Umbrella subscriptions) you can accelerate threat investigation and remediation.

Benefits

- Stop threats earlier before they reach your network or endpoints
- Enforce broad, reliable security coverage across all ports and protocols
- Deliver rapid, scalable security protection on and off network
- Accelerate threat investigation and remediation with contextual intelligence
- Leverage a single security dashboard for efficient management
- Get reliable performance from a global cloud architecture with 100% uptime since 2006

Leader in Zero Trust

Cisco received the highest scores possible in Forrester's 2020 Wave on Zero Trust

Cisco SASE components

Zero Trust Network Access: Cisco Secure Access by Duo

Cisco Secure Access by Duo offers a comprehensive ZTNA solution to secure all access across your applications and environment, from any user, device, and location. ZTNA is a strategic approach to security that centers on the concept of eliminating trust from an organization's network architecture. A ZTNA model considers all resources to be external and continuously verifies trust before granting only the required access.

\With the zero-trust model, you gain better visibility across your users, devices, containers, networks, and applications because you are verifying their security states with every access request. You can reduce your organization's attack surfaces and prevent lateral threat movement by segmenting resources and only granting the absolute minimum access needed. Cisco Secure Access by Duo protects you against compromised credentials and risky devices, as well as unwanted access to your applications and data.

Benefits

- Establish trust in every access request, no matter where it comes from
- Secure access across your applications and network
- Extend trust to support a modern enterprise across the distributed network
- Deploy rapid security protection across on-premises, cloud, remote access, and VPN in a matter of hours and days, not weeks
- Save time and costs by centralizing access security while reducing administrator management and help desk tickets

Why partner with Cisco

Implementing a full SASE architecture is a multi-step cloud journey that will be different for every organization. Cisco has a proven track record in the core SASE areas of cloud-delivered security, SD-WAN, and ZTNA. Cisco provides solutions that include the consolidation, ease of deployment, and management that you need to scale your business and provide effective security for users anywhere they choose to work – without a degradation in speed, performance, or user experience.

Performance you can count on from a networking and security leader

Cisco's commitment to operational excellence and our self-healing integrated architecture enables us to build secure connections in minutes. Cisco customers can take advantage of a global footprint of data centers with direct peering to many service providers, IaaS, and SaaS vendors for unified control and orchestration. Unlike competitors, we're able to deploy enterprise segmentation and application experience optimization with predictable performance and latency controls across our global services.

Extended control beyond the perimeter with a Zero Trust leader

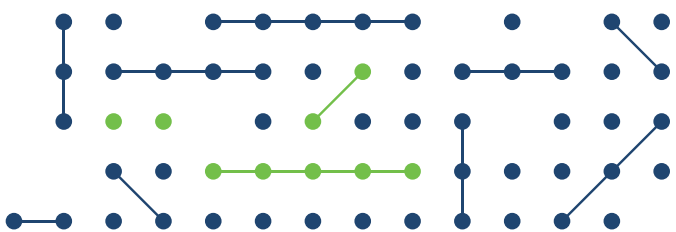
Cisco received the highest scores possible in Forrester's 2020 Wave on Zero Trust. Secure Access by Duo provides controls at the user and device level to verify user identity and device health. Duo establishes user and device trust and provides continuous visibility to extend trust on a per-session basis, both inside and outside the corporate network. By enforcing consistent user and device-based access policies, you can reduce the risk of data breaches and meet compliance requirements.

Simplified purchasing and rapid deployment

Cisco simplifies purchasing with a single Cisco SD-WAN and Umbrella package. With automated deployment options, you can connect hundreds of locations quickly with simplified ongoing management, including policy control from one cloud-based dashboard.

Faster incident response time and improved security efficacy

Leveraging insights from Cisco Talos, one of the world's largest commercial threat intelligence teams with more than 300 researchers, Cisco Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks. We also feed huge volumes of global internet activity into a combination of statistical and machine learning models to identify new attacks being staged on the internet. With Cisco SecureX, you can accelerate threat investigations and reduce remediation times with automated response actions across multiple security products. Simplify your security by eliminating manual tasks and stopping attacks earlier in the process.



Get started today

See why Cisco is trusted with protecting 100% of the Fortune 100 companies. Contact your Cisco sales representative or partner to get started on your SASE journey.

1. Cisco, Duo Trusted Access Report, 2019
2. Enterprise Strategy Group, Transitioning Network Security Controls to the Cloud, May 2020
3. Gartner, The Future of Network Security Is in the Cloud, August 2019