Secure Access Service Edge (SASE)

At a Glance

What is SASE?

Secure access service edge (SASE) combines networking and security functions in the cloud to deliver secure access to applications, anywhere users work. The core functions include software-defined wide area network (SD-WAN), firewall as a service, secure web gateway (SWG)s, cloud access security broker (CASB), and zero trust network access (ZTNA). The goal of the SASE model is to consolidate these functions – which were traditionally delivered in siloed point solutions – in a single, integrated cloud service.

SASE helps organizations:

Connect

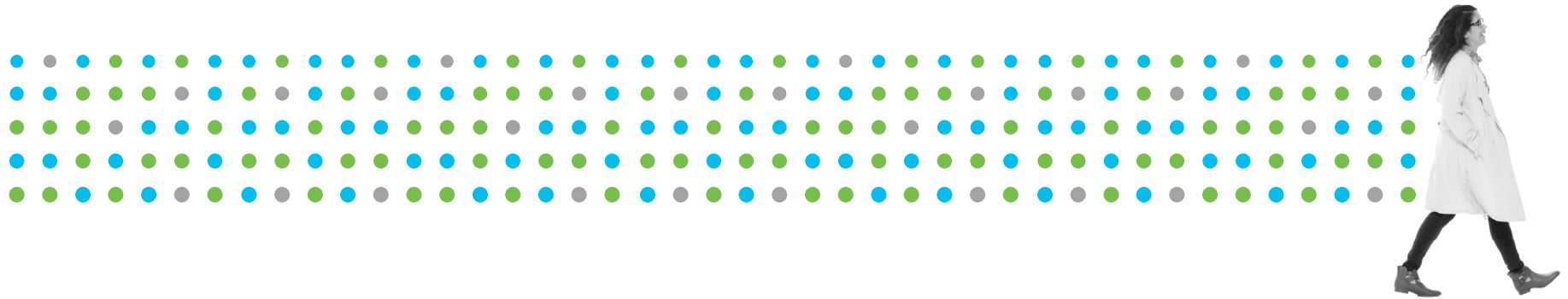
Connect users seamlessly to the applications and data they need to access – in any environment, from any location

Control

Control access and enforce the right security protection anywhere users work

Converge

Converge networking and security functions to deliver secure connectivity as a service



What's driving the move to the secure access service edge?

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, SASE is now in the forefront as remote access to applications and "work from anywhere" became a top organizational priority. 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. Even as employees start returning to the workplace, a recent Gartner survey revealed 82%of respondents intend to permit remote working some of the time.[1] 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.

Our approach

Cisco's SASE architecture combines networking, client connectivity, security, and observability capabilities – all available through a single offer. Our approach helps organizations:

- Connect and secure access to applications, data, and the internet for remote workers, fixed locations, any internet-facing devices, and workloads
- Gain end-to-end observability from the user all the way to applications, over any network or cloud
- Optimize performance by ensuring the fastest, most reliable, and secure path to the cloud
- Adopt zero trust network access by verifying the identity of users and the health of their devices to secure access to applications, on a per-session basis
- Make your business more agile by leveraging the cloud to remove complexity from your infrastructure and provide immediate scalability

Cisco's 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. 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.

SASE by the numbers

40%

of enterprises will have explicit strategies to adopt SASE by 2024[2]

64%

believe network security is more difficult than two years ago[3]

45%

of requests to access protected apps come from outside the business walls[4]

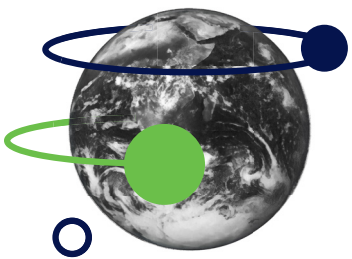
80%

of organizations are either using or evaluating SD-WAN in some capacity[3]

20%

of enterprises will have adopted SWG, CASB, ZTNA, and branch FWaaS capabilities from the same vendor by 2023[2]

Components of Cisco's SASE architecture



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

Connect with SD-WAN: Cisco SD-WAN, powered by Viptela and Meraki

Cisco SD-WAN is a cloud-delivered overlay WAN architecture connecting branches to headquarters, data centers, and multi-cloud environments, while delivering a predictable user application experience. With the flexibility of integrated on-premises or cloud-based security, IT can drive the SASE journey in their own way. Extended integrations with multiple cloud providers using Cloud OnRamp eliminates complexity for a truly zero-touch, more automated experience.

Analytics capabilities deliver the visibility and insights necessary to isolate and resolve issues promptly while providing enhanced network intelligence. All of this can be managed through a centralized dashboard which simplifies IT operations with capabilities like automated provisioning, unified policies, and integrated workflows. With Cisco SD-WAN cloud-first architecture, IT can maintain flexibility to connect any user to any application, across any cloud.

Benefits

- Connect any user to any application with integrated capabilities for multicloud, security, unified communications and application optimization
- Leverage comprehensive on-premises and cloud-based security (with Cisco Umbrella integrations) to help accelerate the transition to a SASE architecture while maintaining compliance
- Deliver enhanced application experience and meet service-level agreements (SLAs) with real-time analytics, visibility, and control business critical applications
- Extend SD-WAN fabric into public clouds with Cloud OnRamp for IaaS, automating access to workloads while driving consistent policy
- Use real-time analytics to steer users over the best path for optimal application performance with Cloud OnRamp for SaaS
- Provide centralized control for intent based policies and security enforcement across the entire network for operational simplicity

Components of Cisco's SASE architecture

Connect with Remote Access: AnyConnect

Cisco AnyConnect is a security endpoint agent that empowers remote workers with frictionless, highly secure access to the internet or the enterprise network from any device, at any time, in any location while protecting the organization. It also provides the visibility and the control you need to identify who and which devices are accessing the extended enterprise. Cisco AnyConnect's wide range of security services include functions such remote access, posture enforcement, web security features, and roaming protection. Cisco AnyConnect gives your IT department all the security features necessary to provide a robust, user-friendly, and highly secure remote user experience.

Benefits

- Streamline user access to the internet, and internal resources or applications
- Gain deeper visibility into users accessing the network on or off premises
- Ensure policy enforcement and device posture for all users
- Provide flexibility with support for multiple devices and platforms
- Simplify infrastructure with one client enabling cloud security, endpoint security, and access functions

Components of Cisco's SASE architecture

Leader in Zero Trust

Cisco has been named a leader in Forrester's Wave on Zero Trust two years running

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 Duo, you can implement zero trust for the workforce by verifying the identity of users and health of devices across each access attempt, with custom security policies that protect every application. This helps prevent any unauthorized lateral movement through an environment and protects you against compromised credentials and risky devices, as well as unwanted access to your applications and data. Duo offers capabilities such as simple and effective multi-factor authentication (MFA), complete device visibility, adaptive policies, remote access with or without VPN, and single sign-on (SSO) for any and every application.

Benefits

- Establish user and device 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

Components of Cisco's SASE architecture

Pioneer in cloud security

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

Control with cloud security: Cisco Umbrella

Cisco Umbrella is the cloud-native, multi-function security service at the core of Cisco's SASE architecture. It unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single cloud service to help businesses of all sizes secure their users, applications, and data. As more organizations embrace direct internet access, Umbrella makes it easy to extend protection to roaming users and branch offices. Umbrella provides global coverage with a broad set of high throughput data centers and peers with more than 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 utilizes DNS layer security to block requests to malware, ransomware, phishing, and botnets before a connection is established. The secure web gateway provides logging and deeper inspection for all web traffic for greater transparency, control, and protection. The cloud-delivered firewall helps to 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

Components of Cisco's SASE architecture

Observability: ThousandEyes

With the increased reliance on the internet and cloud services, more networks are outside your ownership or direct control. Organizations need to ensure the performance and integrity of the underlying transport, even when you don't own the infrastructure or control how service providers route traffic.

ThousandEyes not only gives you complete visibility from the user to the application over any network, but also provides actionable insight into any performance issues so you can resolve incidents quickly to maintain reliable connectivity and optimal application experience.

Benefits

- Reduce mean time to identify and resolve (MTTI/MTTR) by immediately pinpointing the source of issues across internal network, ISPs, and cloud and application providers
- Gain successful escalations with service providers based on data that can be easily shared across internal and external stakeholders
- Eliminate wasteful finger pointing and effectively manage OLAs/SLAs across internal teams and external providers

Why partner with Cisco

Implementing a full SASE architecture is a multi-step journey that will be different for every organization. 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, security, and observability leader

Cisco's commitment to operational excellence and our 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 thousands of 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.

Simplified purchasing and rapid deployment

Cisco simplifies purchasing with a single SASE offer that allows you to purchase all of the core components – cloud security, zero trust network access, SD-WAN, and observability – and will enable an easy transition to a single subscription service in the future. Whether you want to purchase all components at once or over time, Cisco makes it easy to build a SASE architecture your way. With automated deployment options and many product integrations, you can connect hundreds of locations quickly with simplified ongoing management.

Extended control beyond the perimeter with a Zero Trust leader

Cisco received the highest scores possible in Forrester's 2020 Wave on Zero Trust in multiple criteria including market approach, advocacy, vision and strategy, device security, and the future state of zero-trust infrastructure. 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.

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. https://www.gartner.com/en/newsroom/press-releases/2020-07-14-gartner-survey-reveals-82 percent-of-company-leaders-plan-to-allow-employees-to-work-remotely-some-of-the-time
2. Gartner, The Future of Network Security Is in the Cloud, August 2019
3. Enterprise Strategy Group, Transitioning Network Security Controls to the Cloud, May 2020
4. Cisco, Duo Trusted Access Report, 2019