forfusion

Cisco Partner
Advanced Security Architecture Specialized

White Paper

Secure Access Service Edge (SASE) At a Glance

Your journey to SASE

Secure Workplace

Your journey to SASE

The demand for anywhere, anytime access has grown as the workforce has become more distributed and cloud traffic continues to soar. How can IT leverage a simpler, more scalable method to securely connect users to the applications they need? By bringing network and security functions closer to users and devices, at the edge—and moving to a cloud-based, as-a-service model called Secure Access Service Edge (SASE).

Remote work accelerated in 2020 and with it, SASE adoption

Gartner gave a name to an architecture that's been in motion for years, heightened by a sudden shift to remote work. While the principles of SASE were in place well before 2020, the pandemic brought SASE to the forefront as remote access to applications and 'work from anywhere' became a top organisational priority.

SASE marks a shift from the data centre as the centre of the universe to a more cloud-centric model. Organisations now need the ability to instantly change to enable secure connectivity for in-office, work from home, or anywhere in between.

Simply put, SASE is another way to describe your journey to the cloud.

"SASE enables companies to operate during times of disruption and provides highly secure, high-performance access to any application, regardless of user location."

Gartner's Initial Secure Access Service Edge Forecast
Joe Skoruapa, Nat Smith 2020
- Gartner

SASE is a journey many had already begun, one that Cisco has been on for years

The first thing to know about SASE is that it's not a product, it's an architecture. And because everyone starts from a different place, transitioning your network to the cloud is a journey. Some move fast while others take more of a stair-step approach.

SASE is a relatively new name but not new for Cisco. They had already built the foundation for SASE with their cloud-based, scalable architecture. Cisco has the most complete, end-to-end SASE solution today.

Did you know?

Gartner defines SASE through five primary services, each of which Cisco delivers today.

- SD-WAN
- Cloud access security broker
- Secure web gateway
- Cloud-delivered firewall
- Zero Trust network access

Accelerate your journey to the cloud

3 Cs for SASE

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

Integrate networking and security in minutes

SD-WAN and cloud-native security deliver complete protection in one unified offer. Integrate SD-WAN with built-in, cloud-native security in one click and provide secure access wherever users and applications reside. Cisco integrates Umbrella with every WAN edge device, making it easy for you to securely connect users at the home or branch office. Cisco Secure Access by Duo ensures users are who they say they are, and devices are healthy before establishing the connection.

Cisco SASE architecture

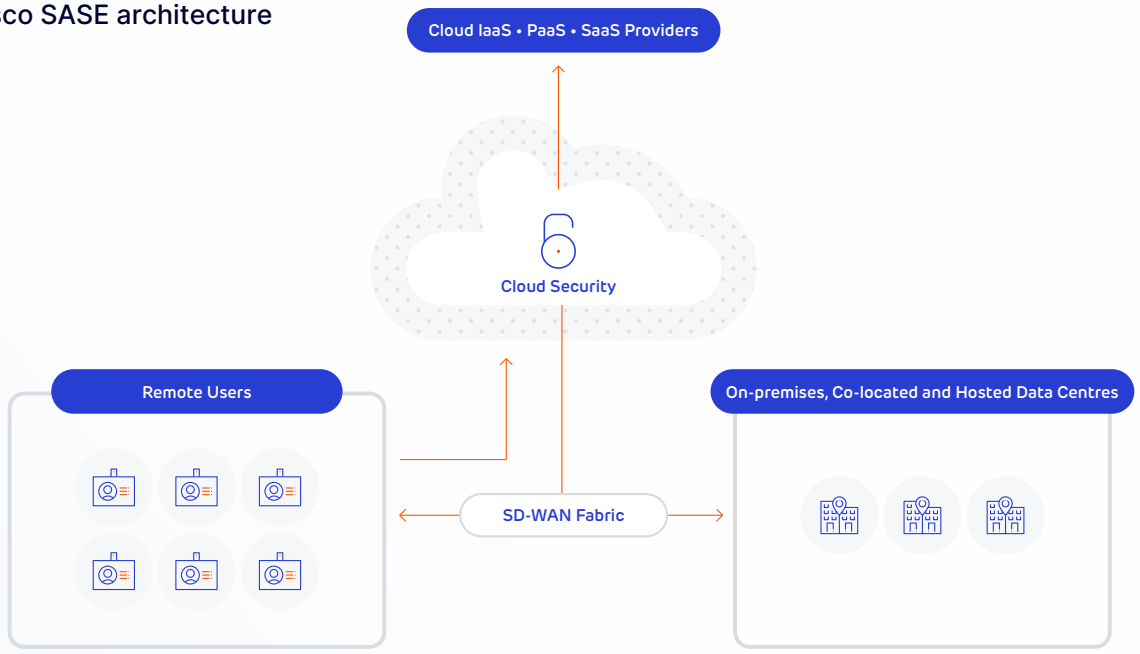


Figure 1: Cisco SASE architecture.
IaaS – infrastructure as a service • PaaS – platform as a service • SaaS – software as a service

Components of Cisco's SASE architecture

Connect with SD-WAN

Cisco SD-WAN is a cloud-delivered overlay WAN architecture connecting branches to headquarters, data centres, 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.

With flexibility to connect any user to any application, across any cloud.

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

Benefits

- Connect any user to any application with integrated capabilities for multicloud, security, unified communications and application optimisation
- 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 centralised control for intent based policies and security enforcement across the entire network for operational simplicity

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 organisation.

Security services include functions such as 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

Zero Trust Network Access: Cisco Secure Access by Duo (ZTNA)

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 centres on the concept of eliminating trust from an organisation'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 unauthorised 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 centralising access security while reducing administrator management and help desk tickets

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 organisations 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 centres 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.

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

Observability: ThousandEyes

With the increased reliance on the internet and cloud services, more networks are outside your ownership or direct control. Organisations 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

SASE use cases

Realise the benefits of SASE across any workforce environment with the best onboarding experience for users and IT. Whatever your use case, you can quickly onboard in a variety of ways through simple, automated solutions removing time, cost and complexity from your deployment.

Give remote workers secure access to applications

Unleash your workforce by delivering a seamless connection to applications in any environment from any location. Easily connect users to everything they need from your corporate environment and provide secure remote access to the cloud, data center, SaaS, IaaS and colocated facilities. Connect remote users with a single, unified policy—and keep them connected and protected when they're roaming. Umbrella provides secure connectivity in a single push with a single policy, all part of the most comprehensive cybersecurity platform in the industry.

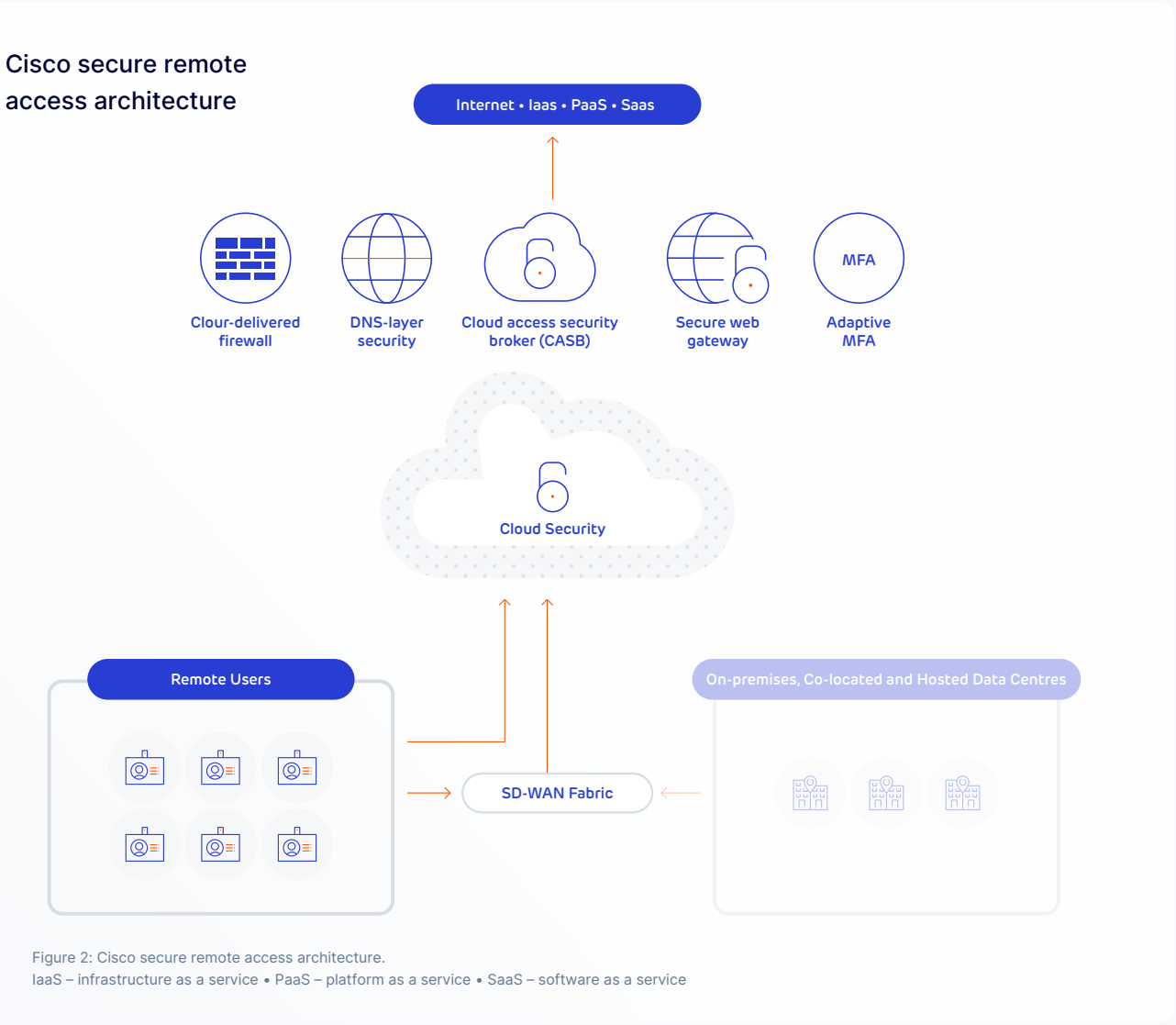


Figure 2: Cisco secure remote access architecture.
IaaS – infrastructure as a service • PaaS – platform as a service • SaaS – software as a service

Extend control beyond the perimeter with Zero Trust.

Cisco 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. Duo enables customers to deploy zero-trust security measures both inside and outside the corporate network. Enforce consistent user and device-based access policy to reduce the risk of data breaches and meet compliance requirements.

Enable connectivity to branch offices with cloud-scale SD-WAN

Automate deployment of cloud security across your SD-WAN fabric to thousands of branches and instantly begin protecting against threats. Secure and connect users over any transport to any cloud with a simple and intuitive onboarding to SASE. Cisco SD-WAN delivers automated tunneling through one-click, full-mesh VPN between all branch locations so you can scale up or down with ease. End-to-end security segmentation honors enterprise intent and provides branches with secure connectivity to everything they need: from on-premises and colocated facilities to integrated cloud services ranging from AWS to Azure, and more.

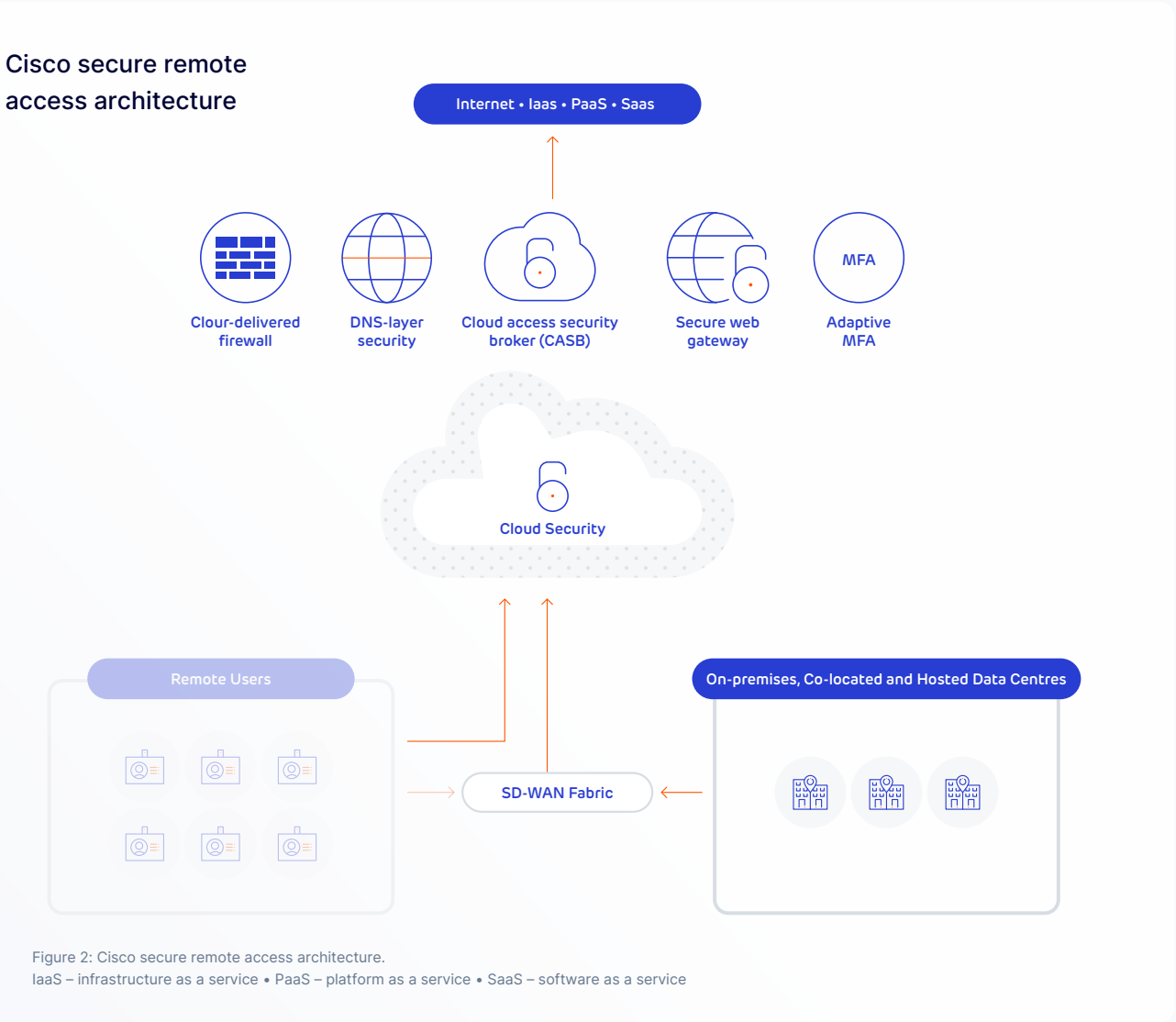


Figure 2: Cisco secure remote access architecture.
IaaS – infrastructure as a service • PaaS – platform as a service • SaaS – software as a service

SASE your way with Cisco

To simplify management and interoperability between SASE components, Gartner recommends a consolidated, single vendor approach for networking and security. Cisco has broken new ground with a convergence of these two functions, as networking and security are core competencies. With automated capabilities you can quickly create an end-to-end SASE infrastructure in minutes, all from one vendor.

Cisco has you covered for what's now and what's next

Because your cloud journey is unique, you need the flexibility to get there your way. Cisco deliver secure connectivity for remote workers and branch offices in minutes. With the depth and breadth of their unique portfolio, helping you realise SASE a number of ways. Build on what you already have and protect your investments by using an existing Cisco footprint. Scale up or down with personalised, flexible licensing and consumption models. And expand capabilities as you grow with an integrated platform approach and open APIs.

Deliver immediate business outcomes with SASE

- 73% Reduction in application latency[1]
- 40% Faster performance on Microsoft 365
- 65% Lower cost of connectivity
- 59% Faster onboarding of new services
- 60% Lower TCO for Zero Trust

Proven networking and security leader

- Protects 100% of the Fortune 100
- #1 in cybersecurity market share
- #1 in SD-WAN market share
- 3x larger partner ecosystem than competitors

[1] Miercom Labs report

About Forfusion

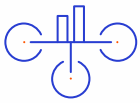
Forfusion specialises in supporting and delivering Cisco solutions into mid-market and enterprise. As an Advanced Security Architecture Specialized Partner we can help you navigate your SASE journey.

We consistently deliver robust, dependable solutions into extremely secure and challenging environments, we can be relied on to innovate, and de-risk significant business investments for our clients. Challengers and problem-solvers, we uncover our customers' requirements and work with them in a long-term partnership.

Our straight-talking nature and painstaking attention to detail ensure that we deliver expert services without compromise. And because we are committed to conducting business with strong moral principles, our clients can count on us to do what is right for them every step of the way.

Empowering companies to mitigate risk, and plan for the future through innovation and adoption, as well as optimising business performance through digital transformation.

Our Advanced Specializations are:



Advanced Enterprise Networks Architecture

Advanced Collaboration Architecture

Advanced Security Architecture.

Our engineering and support teams hold between them the following Cisco certifications:

61x CCNA

7 x CCNP

4 x CCIE

forfusion

cisco Partner
Advanced Security Architecture Specialized

Learn more about how Forfusion and Cisco can help your SASE journey.

Find out more →

Sign up for free webinar →

Free Cisco Umbrella trial →

Transforming business, together.
forfusion.com