Ebook

Investing in a long-term security strategy

The 3 keys to achieving SASE

Cisco Umbrella

Table of contents

In this ebook:

Changing access needs, cloud migration, and SASE

A solid framework for SASE

The fundamentals of cloud security migration

- Simplicity
- Security
- Scalability

Cisco Umbrella: an investment in cloud security

What makes Cisco Umbrella unique?

Make your move to the cloud

Changing access needs, cloud migration, and SASE

There has been massive disruption in the way we work. The workforce has grown increasingly distributed, with apps and data dispersed across locations. Users now work anywhere and everywhere, and through it all expect fast, seamless, secure access.

How can networking and security ensure consistent high-performance, high-security access? And how can they continue to meet these needs in the face of continued disruption and evolution?

Organizations seeking the answers to these questions have increasingly looked to the cloud; the migration to cloud-based security and networking solutions has significantly accelerated. But, there hasn't always been a clear pathway toward to the cloud. Until now.

As organizations work to migrate to the cloud – and work moves away from the data center towards the edges of the network – exposure to threats continues to rise. To protect against these growing risks – while optimizing performance at every connection – networking and security can no longer work in silos. Instead, they must work together in tandem to connect and protect users at the edge, securely and efficiently.

This is where SASE enters the picture. Recently introduced by Gartner, SASE – or Secure Access Secure Edge – is a forward-thinking framework in which networking and security functions converge into a single integrated service that works at the cloud edge to deliver protection and performance in one simplified approach.

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

Gartner 2020 Secure Access Service Edge Forecast, Joe Skorupa and Nat Smith

Properly executed, SASE can offer organizations a number of unique benefits:

1. Move access control closer to where it's needed – the user and the cloud edge
2. Reduce complexity and consolidate security functions in an efficient as-a-service model
3. Make your business more agile in a constantly changing world
4. Simplify deployment, management, and policy enforcement across all environments
5. Deliver seamless, scalable, secure internet and cloud access anytime, anywhere

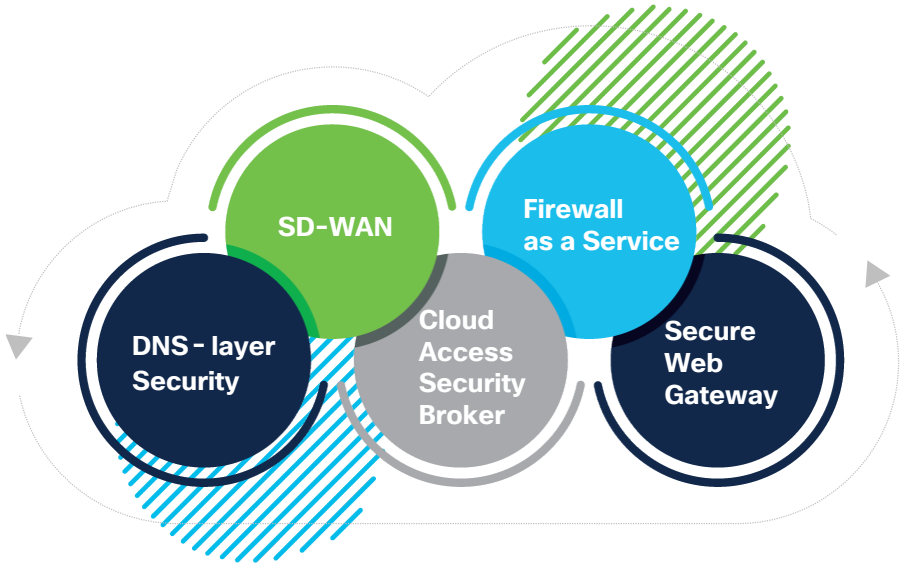
A solid framework for SASE

At the moment, Gartner notes, no vendor offers a complete, comprehensive SASE product. However, they believe there are already SD-WAN and cloud-based security providers well-positioned to realize a full SASE portfolio over the next few years. It's this commitment to the SASE vision, they say, that your organization should be looking for in your current security solution – a solid foundation for the future to come.

Tomorrow's SASE platform will not only need to deliver a number of core consolidated services – including secure web gateway (SWG), cloud access security broker (CASB), Zero Trust network access (ZTNA), firewall-as-a-service (FWaaS), and SD-WAN capabilities – it will also require a checklist of other elements critical to long-term SASE success. These include:

- Services integrated from one vendor
- A flexible consumption model
- Microservices-based architecture
- Effective security and threat prevention
- Global presence and peering relationships
- Support for all devices and agencies

SASE converges security and networking functions



Gartner believes that, by 2023, 20% of enterprises will have adopted SWG, CASB, ZTNA, and branch FWaaS capabilities from the same vendor – brought together, these core service functions are a major step in the direction of SASE.[1]

Gartner Hype Cycle for Network Security, 2020

SASE can help you streamline networking and security in the cloud, delivering:

1. Simplicity

Consolidate services.

2. Security

Control and protect, anywhere and everywhere.

3. Scalability

Evolve to meet changing network and security needs.

In the coming pages we'll take a closer look at each of these fundamentals and why they matter to the future of your networking and security.

The fundamentals of cloud security migration

Simplicity

The first key to SASE success lies in your ability to simplify how you connect and secure traffic. By consolidating services into a single platform that extends across users, devices, clouds, campuses, and branches, you can streamline virtually every aspect of your networking and security processes – including deployment, configuration, integration, policy management, investigation, response, and reporting.

Consolidation also ensures you're ready for the future: You may only have an SD-WAN or zero trust solution today, but it's likely you'll need to extend to other services in time, and a consolidated platform will make that transition – and your evolution to full SASE – that much easier.

With a consolidated solution, you can:

Instantly protect against threats by deploying cloud security across your SD-WAN fabric to thousands of branches in minutes

Centrally manage all policies and configurations, even across multi-cloud environments, with zero-touch provisioning

Provide secure access wherever users and apps reside – SaaS, IaaS, or your data center

Offer secure access to your choice of applications in any cloud environment

Protect roaming users – while making security invisible – with zero trust network access architecture

Maximize efficiency for networking and security teams by simplifying integration and orchestration

Simplify maintenance and management with aggregated data and alert response from a single dashboard

Security

Next, you need the means to secure this new normal – to streamline policy enforcement, increase threat protection, and extend security services from the data center to any cloud. To do so, you need the flexibility to deploy the security that's needed by location and by user – and the ability to easily scale and centrally manage that protection across your network or SD-WAN.

Here again, convergence is key – by combining multiple security functions into a single, cloud-native service, you gain greater capability with less complexity. You also need a solution that allows you to integrate multiple security services together, so you can manage them all from one location – and the flexibility to scale security to meet your business needs.

Let's say you start with DNS-layer security – a first line of defense against threats before they can reach your network or endpoints. From there, you might expand to add a secure web gateway for deeper inspection or a cloud-delivered firewall to secure web and non-web traffic. Then, you might layer on a cloud access security broker to ensure protected access to cloud-based apps.

With this level of flexible integration, each component takes you one step closer to SASE – and to more robust and more powerful protection.

"The one-click integration of Cisco Umbrella with SD-WAN has been great. It makes deployment and configuration much easier in a distributed environment. This is a big step forward in simplifying the distribution and management of edge security."

Presidio, Joshua Mudd, Senior Network Engineer

Scalability

As cloud adoption accelerates, your internet traffic quickly multiplies. You need the ability to scale to meet that traffic, maintaining maximum performance and high-throughput security every step of the way.

How do you get there? There are a number of critical components that lead to a scalable security solution: Microservices-based architecture gives you the flexibility to optimize performance anywhere. Direct peering with ISPs, CDNs, and SaaS platforms provides the fastest route to any request. And a high-performance, high volume network allows for superior speed, reliability, and latency.

In particular, for a SASE solution, you should be looking for flexible architecture that easily integrates with other services. This architecture should allow you to:

Build on what you already have
so you can get the most from existing on-premises and cloud investments

Scale up or down
with flexible consumption models

Simplify policy enforcement
across environments as you transition from on-prem to the cloud

Expand and extend capabilities
with open APIs and a broad ecosystem, letting you choose the solutions that work best for your business

In this way, you can meet the high demands of SASE – and have the adaptability to respond to any other needs, changes, or disruptions that may come your way.

Cisco Umbrella: an investment in cloud security

SASE demands the very best of your security and networking solutions. But the very definition of "best-of-breed" has evolved: the best products are only truly useful when integrated with and supported by the very best platform and network. Cisco's Umbrella product is at the heart of Cisco SASE architecture – the platform best suited to fulfill the true vision of SASE. And the Umbrella global network is the backbone underneath it all, featuring a modern, container-based approach with micro-service components and multi-tenant architecture that deliver service flexibility and automated scalability.

Built with simplicity, security, and scalability in mind, Cisco Umbrella is a cloud-native security service that unifies a variety of leading networking and security solutions in one platform, with open APIs and an ecosystem designed for maximum product extensibility.

What makes Cisco Umbrella unique?

Simple

- Streamlined procurement – single offer, single license that combines Cisco Umbrella and SD-WAN
- Rapid return on investment – quick deployment at scale across environments
- Easy integration with existing security tools to simplify administration
- Increased operational efficiency – simplified deployment, management, and policy enforcements across environments
- Reduction in time, money, and resources needed to investigate and remediate incidents

Secure

- Partnerships with 40+ leading IT companies – to integrate threat intel and security enforcement and trigger appropriate actions
- 96% efficacy[2]
- 72% reduction in dwell time with Cisco SecureX – saving hundreds of hours of analyst time with orchestration and automation[3]
- 72% elimination of manual investigation with Cisco SecureX[3]

Scalable

- Direct peering with 1,000+ partners (2x competitors) – enabling the fastest route to and from SaaS apps
- Ability to meet multi-cloud demand at scale – with seed and low latency
- Up to 73% reduction in latency compared to ISPs[4]
- 33% reduction in hop count – for improved experience with SaaS apps[4]

"There are lots of benefits with Cisco SD-WAN – my network team is so happy with it. Now, they focus on critical tasks rather than being burdened with maintenance and updates. And the performance improvements have dropped service ticket queues to nearly zero."

Joel Marquez, IT Director, Tamimi Markets

Cisco Umbrella

Make your move to the cloud

Much like digital transformation, combining networking and security in the cloud is a multi-step journey that will be different for every organization. Cisco built the network; we're in the best position to secure it moving forward. Working together, we can help you do your journey, your way, as you integrate tools, move to the cloud, and move towards SASE.

Contact a Cisco representative to learn what Cisco Umbrella can do for your business.

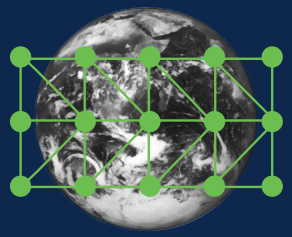
Get in touch

1. *Gartner Hype Cycle for Network Security,* Pete Shoard, 2020
2. *DNS-Layer Protection & Secure Web Gateway Security Efficacy Test,* AV-TEST, February 2020
3. https://www.cisco.com/c/en/us/products/security/securex/index.html
4. Miercom Independent Testing Labs

SASE is about more than products. At Cisco, we're building the most comprehensive SASE approach, backed by the full breadth of everything that makes Cisco a leader:

Industry leader

- 100% of the Fortune 100 use Cisco
- $1B in cloud-native investments
- The pioneer in DNS-layer security
- The leader in zero trust



Global presence

- Largest SD-WAN provider
- Largest partner ecosystem (Partner ecosystem 3x > competitors)
- Largest private threat intelligence team
- Direct peering with 1,000+ top ISPs, CDNs, and SaaS platforms

Top-level performance

- 96% threat detection rate — the highest in the industry[2]
- Up to 73% latency reduction[4]
- 100% business uptime for DNS security services