Cisco Umbrella

Ebook
Cisco Public

A roadmap to SASE

Navigating the challenges of network security beyond the data center

New network, new security challenges

Network security is no longer confined to the data center. As security shifts to the cloud, the tried-and-true perimeter-based model just can't keep up. Today's cybersecurity professionals are contending with an entirely new type of network and an entirely new set of security needs – now more than ever, they need a new way to keep users, data, and devices safe from threats.

With all the different security solutions (and acronyms) out there, it can be tough to sort out which approach is best, as well as which technologies you need to reduce complexity, improve speed and agility, and deliver secure network access for your users. In this ebook, we'll look at where the security landscape is heading and highlight the steps you can take to keep your organization safe and secure, today and tomorrow.

In this ebook:

Users and applications are everywhere

The future: connect, control, converge

SASE: network and security convergence

The Cisco SASE vision

Meet Cisco Umbrella

Users and applications are everywhere

With more remote workers than ever before, more roaming devices to protect, and the widespread use of cloud-based apps and services, the edges of the network have expanded well beyond the data center.

For the past decade, the demand for anywhere, anytime access has grown as the workforce has become more distributed and IT teams have adapted to connect and protect users in new ways.

Users are accessing applications from multiple locations – and the applications they're accessing are just as distributed. As the world continues to move in this direction, organizations are faced with a growing challenge: how can network and security teams provide consistent, secure access to an increasingly distributed, mobile workforce without taking on more complexity?

believe network security is more difficult than two years ago

...and security teams and tools are falling behind.

Security operations and IT teams are trying to keep up with changing security needs by using a combination of different point solutions, but this fragmented approach to security only adds complexity. It can be tough to stay on top of a deluge of alerts and potential threats coming from a variety of tools.

16%

of companies saw over 100,000 alerts per day

(Cisco CISO Benchmark Study, 2020)

93%

agree moving security to the cloud has increased efficiency, allowing security to focus on other areas

(Cisco 2019 Benchmark study, 2019)

The future: connect, control, converge

Today's workforce expects seamless access to applications wherever they are, on any device. The need for cloud-delivered security service expands daily as contractors, partners, IoT devices and more each require network access. IT must protect users and devices as if they were located at a corporate office or branch. Each requires secure access to applications and must now be treated as a "branch of one."

Securing the modern network is a challenge, requiring a great deal of time, energy, and resources that overextended organizations don't always have. To fill in the gaps, today's teams are increasingly seeking an entirely new type of security solution — one that converges a variety of individual components into one connected, cloud-delivered service that makes it easy to control policies and behaviors.

In this new paradigm, IT requires a simple and reliable approach to protect and connect with agility. This is forcing a convergence of network and security functions closer to users and devices, at the edge — and is best delivered as a cloud-based, as-a-service model called secure access service edge (SASE).

Connect your workforce to applications seamlessly

Control access through simplified security and policy enforcement

Converge networking and security functions to meet multi-cloud demands at scale

The evolution of SASE

As networking and security converge in the cloud, we get closer to achieving one simple goal: giving teams the ability to control and secure users, apps, devices, and data – anywhere and everywhere.

2007

Secure Web Gateways are the norm.

Going back as far as 2007, secure web gateways (SWG) were standard, delivering URL filtering, advanced threat defense, and legacy malware protection to defend users from internet-based threats – and help organizations enforce web security and policy compliance.

2017

Secure Internet Gateways emerge as a new security solution.

In 2017, Gartner introduced a new product category, the secure internet gateway (SIG). A single, cloud-based solution with a greater set of capabilities than SWG, SIG had the potential to replace some (or all) on-premises security solutions – especially for orgs with distributed networks or stand-alone SaaS offerings.

2019

Network and cloud security begin to converge to form Secure Access Service Edge.

As 2019 came to an end, Gartner defined a new type of security model – an evolution from SIG called Secure Access Service Edge, or SASE. Gartner predicts that SASE will become the new standard for security in the coming years, with at least 40% of enterprises adopting explicit SASE strategies by 2024.

What is SASE?

SASE (pronounced “sassy”) offers an alternative to traditional data center–oriented security, with a new type of cloud-based architecture that brings together networking and security services in one unified solution. This converged network and security solution is designed to deliver strong secure access from edge to edge – including the data center, remote offices, roaming users, and beyond.

By consolidating a variety of network and security functions in one service that can be deployed anywhere from the cloud, SASE can provide better protection and faster performance, while reducing the cost and work it takes to secure the network.

Digital business transformation is moving security to the cloud, driving a parallel need for converged services that help reduce complexity, improve speed and agility, and secure the new network architecture of tomorrow.

The next evolution in cloud convergence

SASE combines networking and security point solutions into one unified, cloud-delivered service.

Cloud Access Security Broker (CASB)

Software that detects and reports on cloud applications in use across your network, exposing shadow IT and enabling the ability to block risky SaaS apps and specific actions, like posts and uploads.

Firewall as a Service (FWaaS) with Intrusion Prevention System (IPS)

Software-based, cloud-deployed network services designed to stop or mitigate unwanted access to the internet. With a cloud firewall, you have visibility and control of internet traffic across all ports and protocols. You can log all activity and block unwanted traffic using IP, port, and protocol rules. You can also block or allow activity by application and by user.

Zero Trust Network Access (ZTNA)

A security framework that helps prevent unauthorized access, contain breaches, and reduce the risk of an attacker's lateral movement across the network. Duo, now part of Cisco, is a user-centric, zero-trust security platform that verifies users' identities and establishes device trust before granting access to authorized applications.

DNS-Layer Security

Software that acts as a front line of defense against threats on the internet, blocking malicious DNS requests before a connection to an IP address is even established.

Secure Web Gateway (SWG)

A gateway that logs and inspects web traffic to provide full visibility, URL and application controls, and protection against malware. Some gateways can also inspect web-hosted files in real time and decrypt SSL (HTTPS) traffic for advanced threat protection.

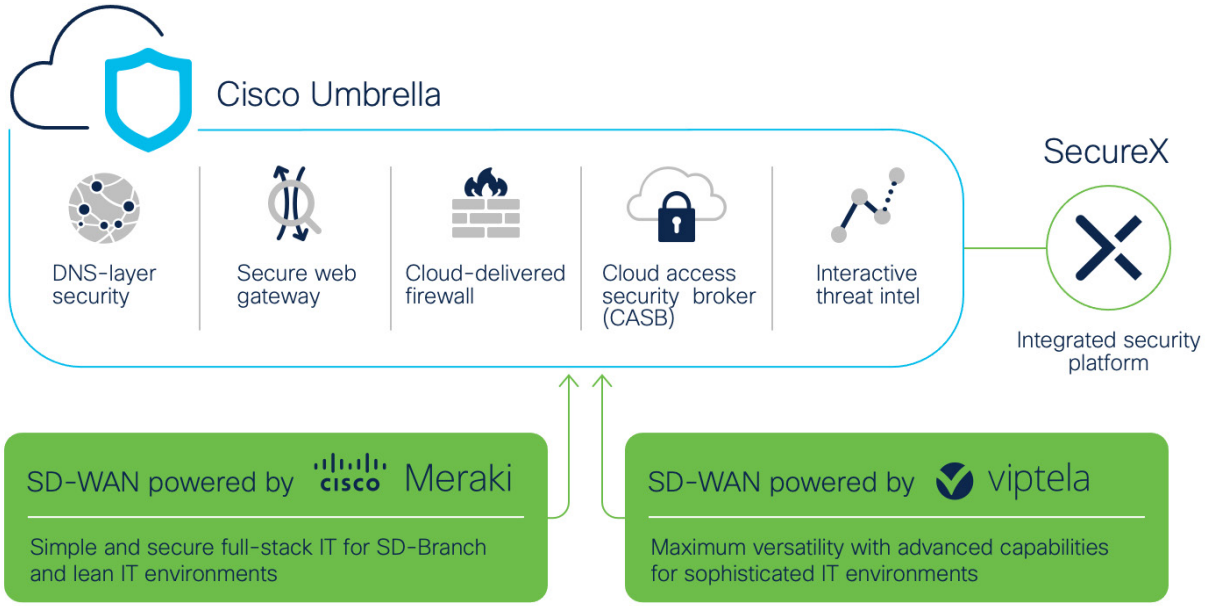
Software-Defined Wide Area Network (SD-WAN)

A virtual WAN that allows companies to use any combination of transport services – including MPLS, LTE, and broadband – to securely connect users to apps and locations.

The Cisco SASE vision

Every organization has different architectures, business goals and investments. When it comes to transformation, there's no one-size-fits-all approach. And moving to a SASE framework is no different. Some will move quickly, while others need to take more of a stair-step approach – and we at Cisco understand that. We can bridge your journey to SASE from wherever you are.

Whether you're looking to onramp to a cloud architecture, securely connect users who can't come to the office, or move security from on prem to the cloud, Cisco can help. We are committed to building out the strongest SASE offering in the industry as we deliver our networking and security capabilities natively through a unified, global cloud infrastructure.



We offer simple, flexible deployment and consumption models that meet your unique situation and scale with your needs. Our highly available, global cloud infrastructure provides secure access wherever users and applications reside. We've already built the prerequisite foundation for SASE with our microservices-based, scalable architecture. Our unified cloud platform approach supports the primary SASE use cases (SD-WAN, FWaaS, SWG, CASB, and ZTNA) so you can start streamlining security and networking today. It's now possible to:

1. **Connect all users and devices to applications with reduced latency.**
2. **Monitor and secure enterprise traffic from a single, cloud-native platform.**
3. **Protect and defend any roaming user.**
4. **Provide visibility and control over all SaaS applications, sanctioned or otherwise.**
5. **Capture deep insights from the endpoint all the way to cloud services.**

Meet Cisco Umbrella

Cisco is leading the way to SASE, and Cisco Umbrella is at the center of the Cisco SASE approach. Umbrella delivers multiple security functions in a single, cloud-delivered service, creating a simple, scalable, flexible solution that can meet the unique needs of your business.

Umbrella delivers the most secure, most reliable, and fastest internet experience to more than 100 million users daily. By unifying multiple security solutions into a single service, Umbrella helps businesses embrace direct internet access, secure cloud applications, and extend protection to roaming users and branch offices.

Most secure

Leveraging insights from Cisco Talos, one of the world's largest commercial threat intelligence teams, Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks. Umbrella also feeds huge volumes of global internet activity into statistical and machine-learning models to identify new attacks being staged on the internet.

Most reliable

Umbrella has a resilient cloud infrastructure that boasts 100% uptime since 2006. Using Anycast routing, any of our 30+ data centers across the globe are available using the same single IP address. As a result, your DNS requests are transparently sent to the nearest, fastest data center with automatic failover.

Fastest internet experience

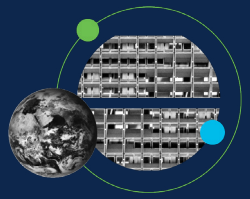
Umbrella peers with more than 1,000 of the world's top internet service providers (ISPs), content delivery networks (CDNs), and SaaS (software as a service) platforms to deliver the fastest route for any request – resulting in superior speed, effective security, and user satisfaction for your business.

The Umbrella Advantage

250B
billion daily DNS requests

30+
data centers across five continents

100M
global daily active users



1000+
partnerships with top ISPs and CDNs

Simplify security with Cisco Umbrella

SD-WAN Integration

Easily deploy Umbrella across your network of Cisco SD-WAN devices in minutes, and gain powerful, cloud-delivered security to protect branch users, connected devices, and application usage from threats across all direct internet access breakouts.

Cloud-Delivered Firewall

Log all activity and block unwanted traffic using IP, port, protocol, and app rules. As new tunnels are created, security policies can be applied automatically for easy setup and consistent enforcement throughout your environment.

DNS-Layer Security

Block requests to malicious and unwanted domains and IPs before a connection is even established – stopping threats before they reach your network or endpoints.

Secure Web Gateway

Log and inspect all web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files, and proxy chaining can be used to forward traffic to Umbrella for full visibility, URL- and application-level controls, and advanced threat protection.

Interactive Threat Intelligence

Uncover malicious domains, IPs, and URLs before they are used in attacks, and accelerate incident investigations. Use the Umbrella web console or APIs to get real-time access to Umbrella's robust threat intelligence.

Cloud Access Security Broker (CASB)

Detect and analyze cloud applications in use across your environment. Automatically generate reports on the app name, vendor, category, risk, and volume of activity for each discovered app. Better manage cloud adoption, reduce risk, and block specific behaviors in applications (like uploading and posting).

Start your SASE journey

Your roadmap to SASE starts with Cisco Umbrella.

- Broad, reliable security coverage across all ports and protocols
- Protection on and off network
- Rapid deployment and flexible enforcement levels
- Immediate value and low total cost of ownership
- Single dashboard for efficient management

See for yourself. Attend an upcoming Cisco Umbrella live demo.

Register now