Cisco Umbrella

Ebook

A roadmap to Secure Access Service Edge (SASE)

Navigating the challenges of network security beyond the data center

Cisco Umbrella

Ebook

New network, new security challenges

In today’s organizations – with more remote workers, more roaming devices, and more cloud-based apps and services – the edge of the corporate network has expanded far beyond the data center.

In particular, over the past two years, the COVID-19 pandemic has led to exponential growth in user demand for anywhere, anytime network access. Rising cloud adoption has led to organizations considering all-new security investments.

In this ebook, we’ll take a closer look at where the security landscape is heading, highlighting the proactive steps you can take to keep your organization safe and secure, today and tomorrow.

Users and applications are everywhere...

Today's workforce is more dispersed than ever before. The same could be said for their data and applications, which are now stored and accessed in both data centers and the cloud.

Together, this presents organizations with the unique challenge of securing users wherever they work, however they're working.

With hybrid work becoming the new normal for many organizations – for the foreseeable future, at least – network and security teams are tasked with:

providing consistent, secure access to an increasingly distributed, mobile workforce.

reducing complexity.

simplifying and scaling security solutions to keep up with evolving needs.

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

Nearly 50% of IT teams say that keeping up with changing security requirements has gotten more challenging in the past two years.[1]

In response, many teams are trying to meet these new needs by adopting a combination of different, disparate point solutions. But, it can be tough to stay on top of a deluge of alerts and potential threats – all coming from different teams working with different tools.

48% of cybersecurity professionals say that their main challenge is addressing the increasingly sophisticated threat landscape.[1]

76% of IT teams say that remote workers are more difficult to secure.[1]

The future: connect, control, converge

The modern workforce expects seamless access to data and applications wherever they are, on any device. But, securing this modern network has never been a greater challenge. In addition to standard employees, hybrid workforces also include contractors, partners, IoT devices, and more – each requiring secure access to the network and applications.

Rising to this challenge takes time, energy, and resources that overextended organizations don't always have. For instance, 49% of cybersecurity professionals say that their biggest operational challenge is a lack of qualified staff.[2]

To help reduce the strain on security teams, more and more organizations are embracing an entirely new type of security solution – one that converges a variety of individual tools into one connected, cloud-delivered service that makes it easy to set policies, secure behaviors, and meet compliance standards.

The goal is to bring together network and security functions – and bring them closer to users and devices at the edge – in a cloud-based, as-a-service model. Gartner calls this model "Secure Access Service Edge" – or SASE.

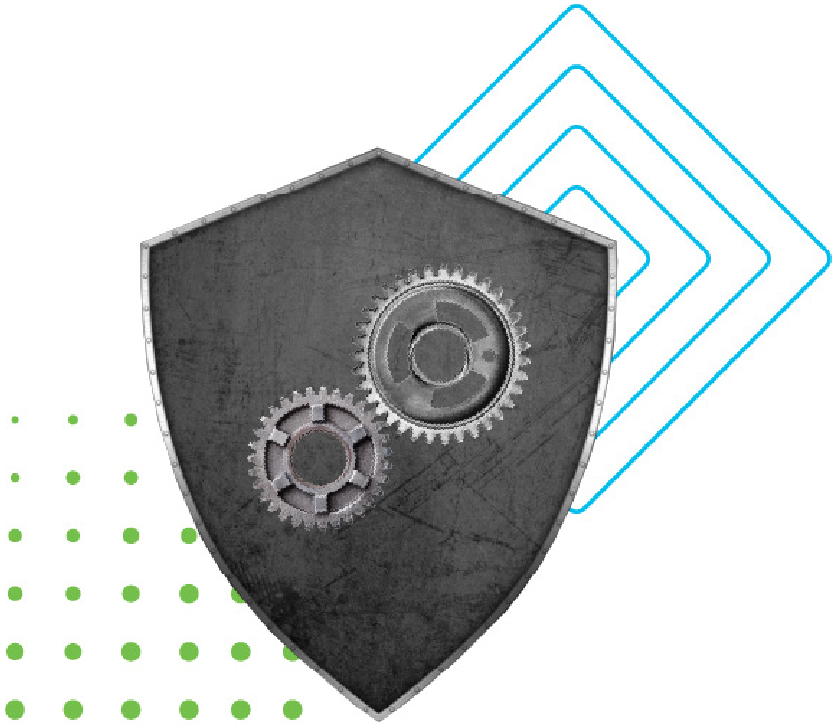
Connect your workforce to applications seamlessly.

Control access through simplified security and policy enforcement.

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

> “Refreshing and maintaining best-of-breed IT and security technologies contributed more to a successful cybersecurity program than any other practice.”

Cisco Security Outcomes Study, Volume 2, December 2021.



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 the SWG, SIGs had the potential to replace some (or all) on-premises security solutions – especially for organizations with distributed networks or standalone SaaS offerings.

2019

Network and cloud security begin to converge to form SASE.

As 2019 came to an end, Gartner defined a new type of security model – an evolution from SIG called Secure Access Service Edge. 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.[3]

2022 and beyond

As security needs evolve, SASE gains traction.

Today, 98% of organizations see "clear and defined benefits" for SASE and are taking the initial steps to adopt the standard.[4] Experts think that, by 2024, 30% of enterprises will adopt cloud-delivered solutions that integrate multiple security solutions. And by 2025, it's predicted that at least 60% of enterprises will have explicit strategies and timelines for SASE adoption – up from 10% in 2020.[5]

Building a SASE architecture

The ideal SASE architecture would include:

Cloud Access Security Broker (CASB)

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

DNS-Layer Security

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

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

Software-based, cloud-deployed network services designed to prevent or mitigate 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.

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.

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, by verifying users' identities and establishing device trust before granting access to authorized applications.

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.

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. SASE can provide better protection and faster performance, while reducing the cost and work it takes to secure the network.

The Cisco SASE vision

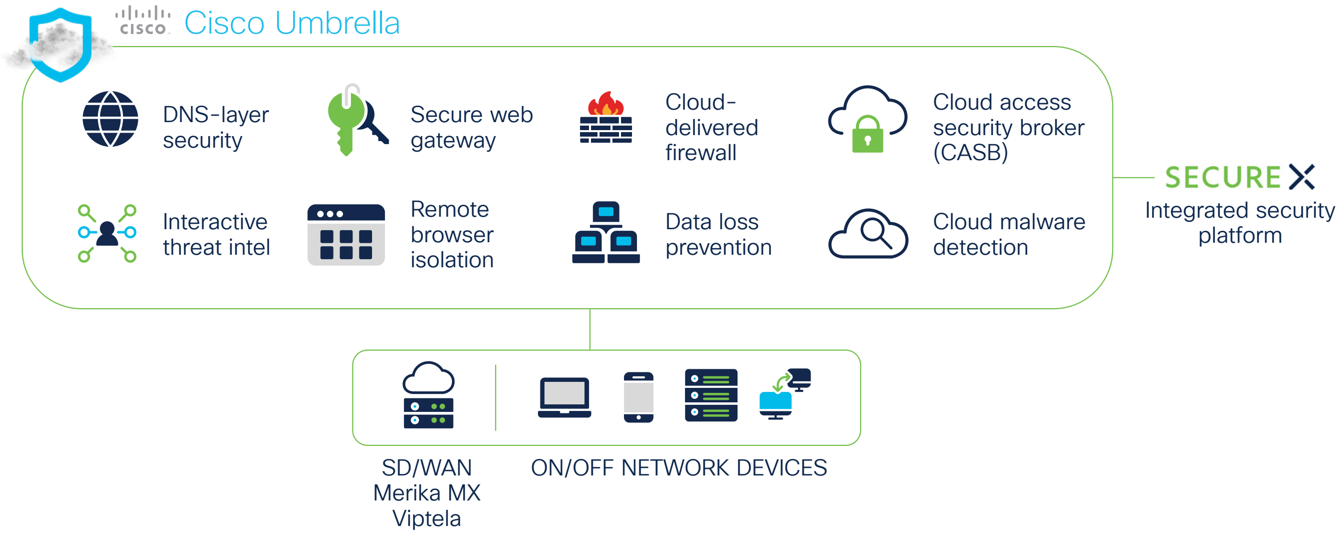
Every organization has its own business goals, architecture, and investments. So, when it comes to improving security posture, there's no one-size-fits-all approach. Moving to a SASE framework is no different. Some will quickly take the leap, while others will need more of a stair-step approach. No matter what your plans are, though, or where you are in your journey, Cisco can be your partner on the path to SASE.

We're committed to building out the strongest and most complete SASE offering in the industry, delivering world-class networking and security capabilities.

At Cisco, we offer simple, flexible deployment and consumption models that can meet your unique situation and scale with your changing needs. We understand the need to secure remote workers, secure the edge, and simplify and streamline your solutions to tighten your security.

So, we've made it 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 heart of the Cisco SASE architecture. Cisco Umbrella offers multiple security functions in a single, cloud-delivered service, creating a simple, scalable, flexible solution.

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

Most secure

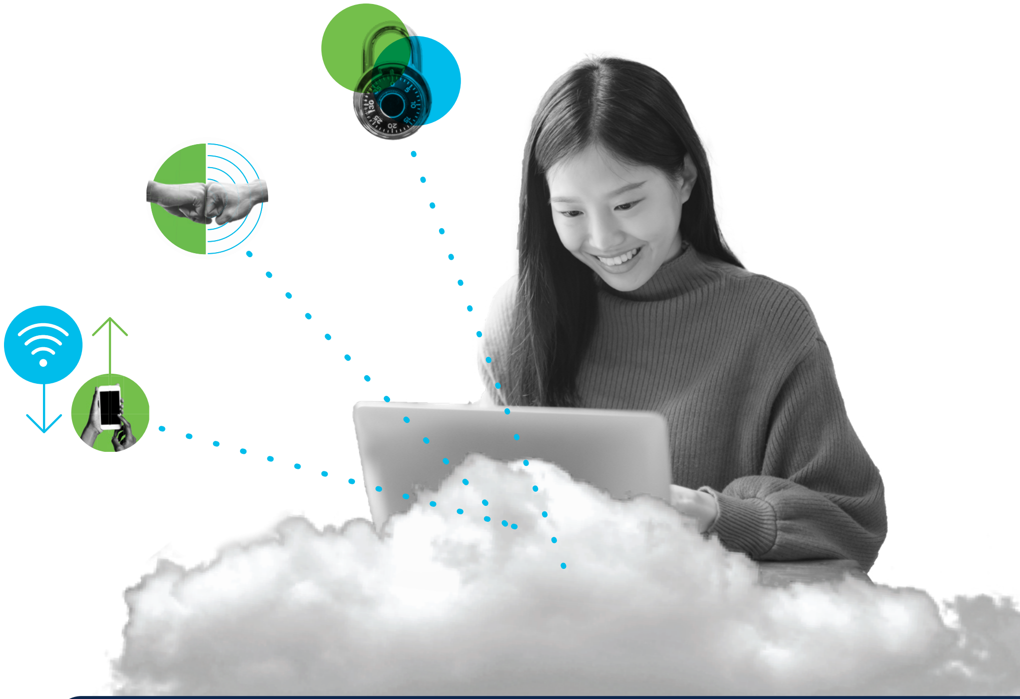
Leveraging insights from Cisco Talos, the world's largest commercial threat intelligence organization, Cisco Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files being used in attacks. Cisco Umbrella also feeds huge volumes of global internet activity into statistical and machine-learning models to identify and block new attacks being staged on the internet, before they can hit their first victim.

Most reliable

Cisco Umbrella delivers extraordinary network reliability and resilience to keep your performance fast and your connections secure. Using Anycast routing, any of our global data centers are available via a single IP address. As a result, your DNS requests are transparently sent to the nearest data center, with automatic failover.

Fastest internet experience

Cisco 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 satisfied users.



> "Organizations with well-integrated functions for identifying assets and risks are nearly 40% stronger at threat detection and response."
>
> *Cisco Security Outcomes Study, Volume 2*, December 2021.

Cisco Umbrella

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

The Cisco Umbrella Advantage

620B daily DNS requests

24K+ enterprise customers

170M+ malicious DNS queries blocked daily

35+ data centers across 5 continents

1,000+ partnerships with top ISPs and CDNs

Sources:

1. Splunk, *The State of Security 2021*, February 2021.
2. Cybersecurity Insiders, *2021 Cloud Security Report*, May 2021.
3. Gartner, *Emerging Technology Analysis: SASE Poised to Cause Evolution of Network Security*, October 2019.
4. Cisco Investments, *2021 CISO Survival Guide to Emerging Trends From the Startup Ecosystem*, July 2021.
5. Gartner, *Checking in on SASE*, March 2021.