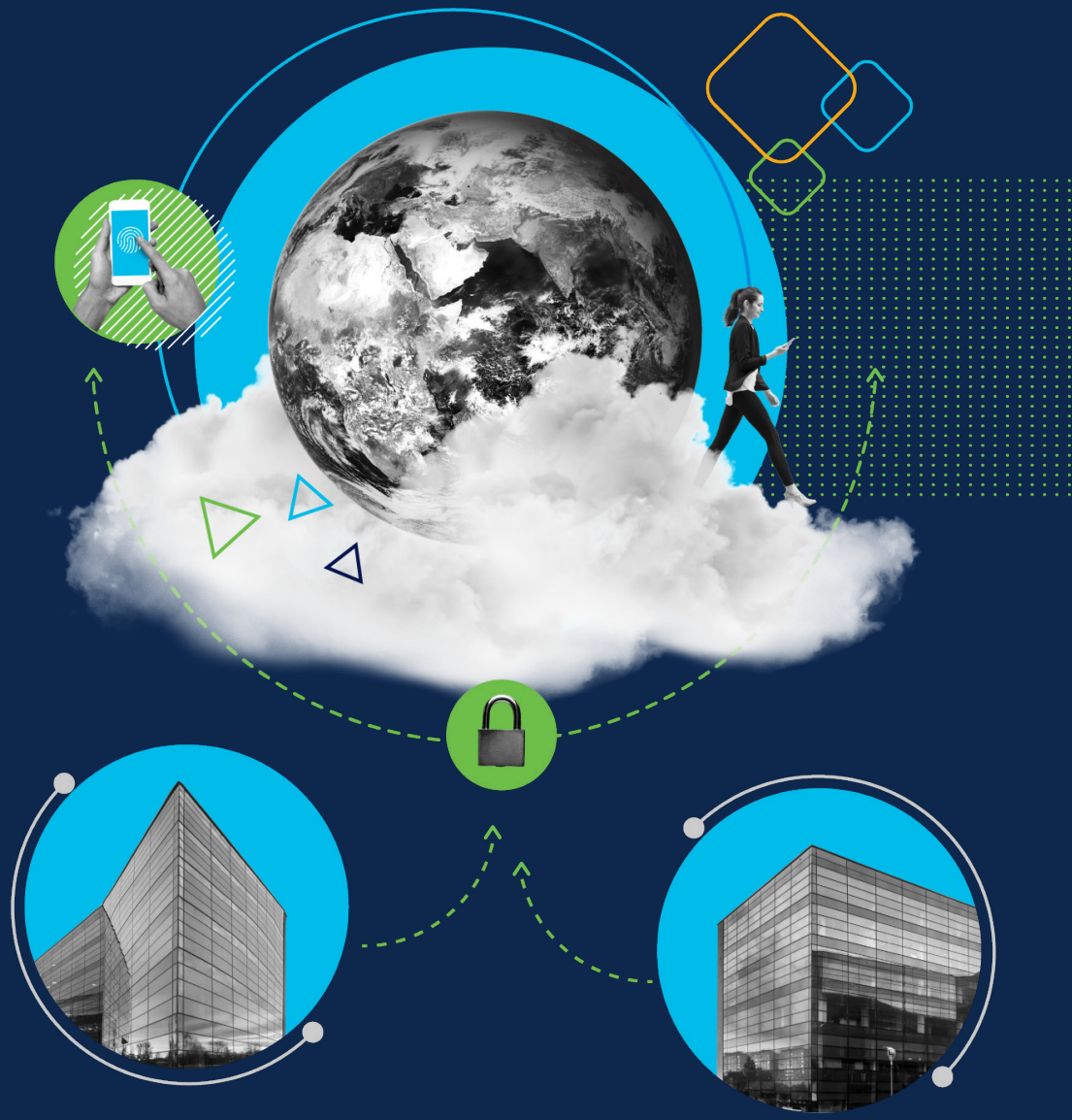
CISCO
SECURE

Ebook
Cisco Public

ATSG

Cloud Security for SD-WAN

Secure your evolving network at the cloud edge.



The next evolution of networking and security

There's no question: your network has left the building, and it continues to evolve. With a growing remote and roaming workforce and the widespread use of cloud-based apps and services, the network edge extends well beyond the data center. As a result, traditional data center-oriented security solutions are no longer providing the protection that users need to stay safe against cyberthreats.

Historically, enterprises used a wide area network (WAN) to connect branches to a data center, backhauling all traffic through a central corporate network. But new business and IT demands are challenging that architecture with the advent of software-defined wide area network (SD-WAN) technology. Now, your security needs to extend to the new network edge, wherever your users are working, to the branch of one.

More than ever, we need a new approach to keep users safe from threats, while delivering consistent network access with low latency to ensure efficiency and productivity. These changes are paving the way to a new convergence of networking and security in the cloud, and a new solution called the Secure Access Service Edge (SASE), which delivers multiple security and network functions from the cloud, including secure web gateway (SWG), cloud access security broker (CASB), and Zero Trust Network Access (ZTNA).

The changing network

Increased cloud adoption

Cloud-native infrastructure and software-as-a-service applications are enabling a shift in the way users work and fundamentally altering the topology of enterprise networks.

More network traffic

Data-intensive applications like streaming video require large amounts of network traffic, which creates demand for more bandwidth that strains existing network infrastructure and centralized security processes.

More network inefficiency

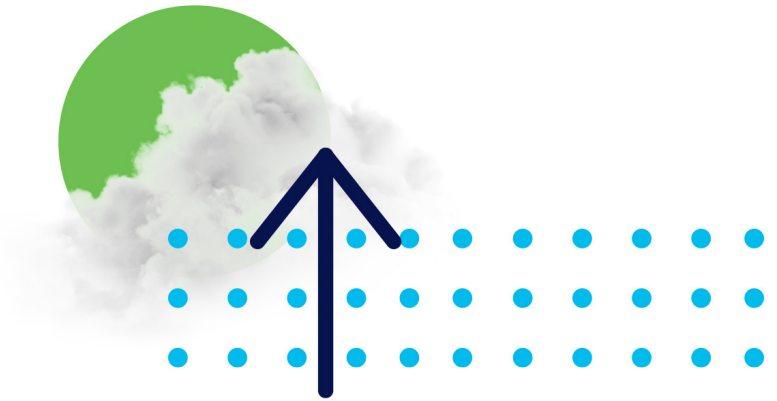
Traditionally, an organization would backhaul network traffic from branch offices and remote workers to apply security policies, often using MPLS links. But as more data and devices join the network, that model leads to bottlenecks.

Higher networking costs

Dedicated MPLS circuits are costly to provision and maintain, and they don't scale or adjust quickly as business needs change. And with the move to cloud services, they simply aren't needed.

New technologies

Software-defined wide area networking (SD-WAN) is growing. It helps improve connectivity, reduce costs, and simplify network and security management across an increasingly complex network architecture.



New security challenges

More remote and roaming workers

Thousands of employees are working from home, either temporarily or indefinitely. When working offline, they need to be protected as well as if they worked in an office, even if their network traffic is going directly to the internet.

Performance issues with SaaS apps

Many businesses today use SaaS apps like Office 365, Salesforce, and Workday to conduct critical business functions. But users can experience latency and lost productivity if that traffic is backhauled to a data center to apply security policies, so many skip the VPN.

New threats taking advantage of security gaps

Today's threats are more sophisticated than ever, and organizations must defend their branches against malware infections, command-and-control callbacks, denial-of-service attacks, and unauthorized access.

Too many security tools

Most organizations find it challenging to orchestrate alerts from different tools, which affects their ability to monitor and correlate information quickly enough to respond to threats before they cause serious damage.

Security talent shortage

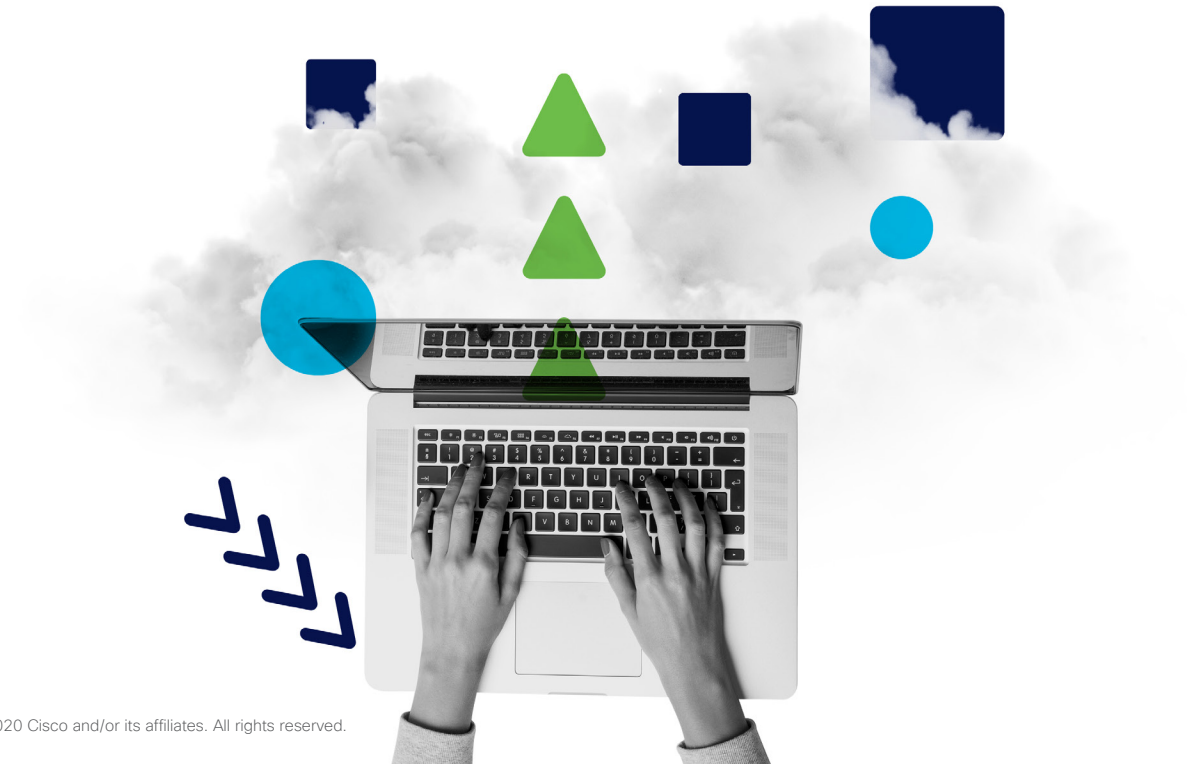
Qualified security professionals are difficult to find, expensive to hire, and tough to retain. The skills shortage leads to security blind spots, especially when networking and security teams are siloed.

Networking and security are converging in the cloud

By 2022, 75% of enterprise-generated data will be created and processed outside the traditional, centralized data center or cloud. As users connect directly to SaaS applications, backhauling traffic to apply security policies adds latency, and is inefficient and expensive.

Organizations are turning to SD-WAN to improve connectivity, reduce costs, and simplify network and security management across an increasingly complex architecture. But security must be top of mind as you transform your network with SD-WAN. Scaling security at every location often means more appliances to ship and manage and more policies to separately maintain, which translates into more money and resources needed. But it doesn't have to be that way.

SD-WAN simplifies your network, and that's the way that your security should be, too.



"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."

Joshua Mudd, Senior Network Engineer, Presidio

Cisco brings security and networking together at the cloud edge

Cisco's integrated networking and security approach protects remote and roaming users, branch offices, and applications. With simplified cloud management and one-touch provisioning, Cisco delivers flexible, optimized SD-WAN network performance along with industry-leading security efficacy from Cisco Umbrella.

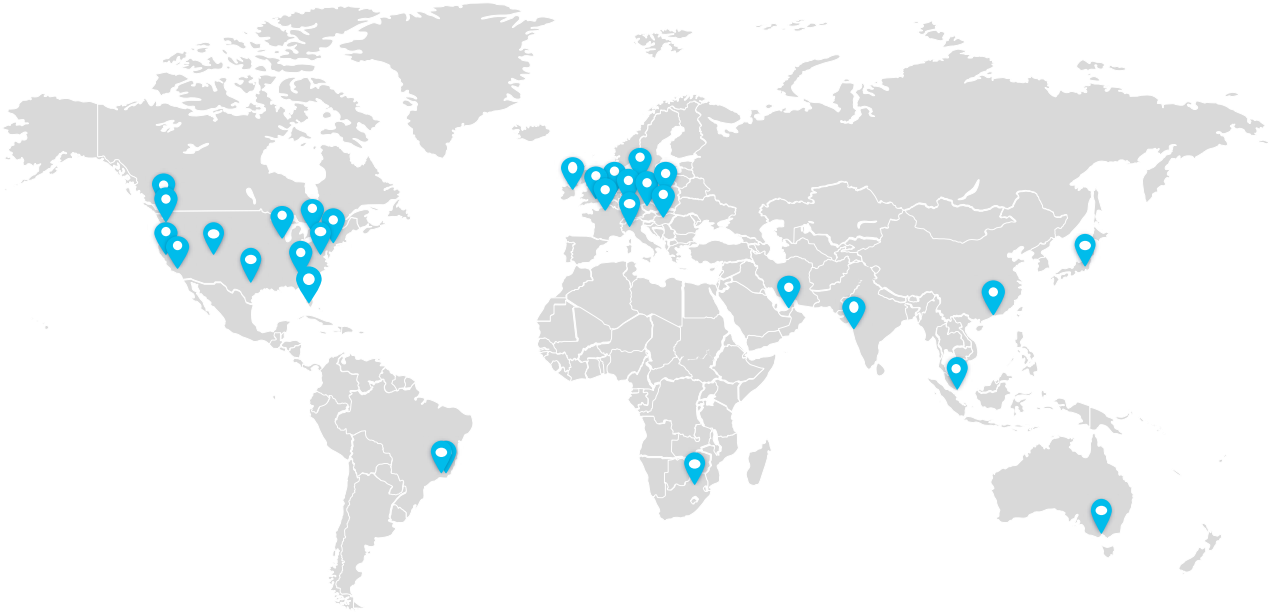
Cisco Umbrella is a cloud-delivered security service at the heart of Cisco's SASE architecture. Umbrella converges multiple functions solutions in the cloud, including DNS-layer security, secure web gateway, cloud-delivered firewall, cloud access security broker, and interactive threat intelligence in a single management panel. Umbrella is the simplest security you'll ever deploy. There is no hardware to install or software to manually update, and the browser-based interface provides quick setup and ongoing management. Distributed organizations need to deploy security quickly and easily – Umbrella customers see immediate value from their investment in minutes, not weeks or months.

By integrating Cisco SD-WAN technology with Cisco Umbrella, organizations can securely access cloud workloads and SaaS applications. The Cisco SD-WAN integration enables customers to easily set-up IPSec tunnels to Umbrella and leverage automation to quickly deploy integrated cloud security across thousands of branches and roaming users. Without automation, customers would need to manually establish a tunnel for each WAN edge device at the branch.

Deploying secure SD-WAN no longer takes months, thanks to the power of the integrated Cisco solution.

Cisco is the largest SD-WAN solution provider in the world, and Cisco SD-WAN Edge devices are automatically registered to Umbrella. A Secure API key is automatically provisioned on the Edge device via HTTPS, eliminating the need to manually enter API keys.

Cisco SD-WAN customers get the advantage of using Cisco DNA Premier licenses for Cisco's SD-WAN management platform, vManage, to define their cloud interconnects. Cisco Umbrella has direct peering with 1,000+ network operators, including leading service providers, SaaS and IaaS providers, and a global footprint of 30+ regional data centers. With direct peering, customers get a secure, high performance and low latency path to applications.



The Cisco Umbrella network has a global footprint of 30+ regional data centers.

Benefits of the Cisco integrated networking and security approach

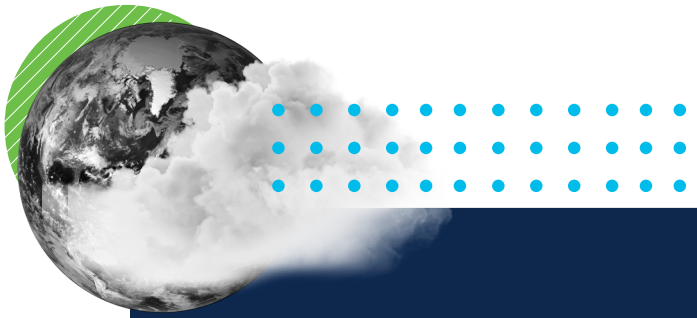
Proven leadership: ranked #1 in cybersecurity market share with $1B in cloud-native investments

Hands-off automation: deploy cloud security across thousands of branches in minutes

Top-notch protection: defend against threats with the #1 ranked solution in security efficacy

Simplified management: single pane of glass across all offices and users

Deeper inspection and controls: SWG and cloud-delivered firewall with IPSec tunnels



Start your cloud security journey with Cisco Umbrella

In October, 2020, AV-TEST performed a review of Cisco Umbrella alongside comparable offerings from Akamai, Infoblox, Palo Alto Networks, Netskope, and Zscaler. Cisco Umbrella security performed significantly better than other vendors in terms of efficacy.

As you transform your network through adoption of SD-WAN technology, Cisco can help you move access control to the edge, make your business more agile, and deliver seamless secure access anytime, anywhere. Cisco Umbrella provides a simple, effective way to deliver the effective security protections your users need without slowing down the pace of business. And with the Cisco SD-WAN and Umbrella integration, you can deploy best-in-class security across your network to all devices and users in minutes.

It only takes minutes to get started on your SASE journey today with Umbrella DNS-layer security. You can add more functionality and SD-WAN integration as your networking and security needs evolve.

“Umbrella is the fastest security ‘win’ you can buy! If I were to come into a new environment, Umbrella would be my first investment.”

Ben Curry, Network Administrator,
The Farmers & Merchants State Bank (TechValidate)

How do you begin your cloud security journey? Start with the DNS layer.

Start your free trial

The Umbrella Advantage

250B+
daily DNS requests
(over all ports and protocols)

30+
data centers across
five continents

100M+
global daily active consumer
and enterprise users

1000+
partnerships with
top ISPs and CDNs