EBOOK

A Roadmap to SASE

Navigating the challenges of network security beyond the data center.

Cisco Umbrella

New network, new network 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 – DNS, SIG, SWG, CASB, FWaaS, SASE – 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 ultimately secure your network.

In this ebook, we'll take a look at where the security landscape is heading, identify the gaps in today's security stack, and highlight the steps you can take to keep your organization safe and secure, today and tomorrow.

In this ebook:

The network is changing like never before…

A growing remote and roaming workforce, the increasing adoption of direct internet access at branch offices, and the widespread use of cloud-based apps and services have expanded the edges of the network well beyond the data center. As a result, traditional data center–oriented security solutions are no longer providing the protection users need.

60%

of orgs expect majority of apps to be SaaS by 2021[1]

50%

of workforce will be roaming by 2021[1]

79%

of orgs shifting to some or all direct internet access (DIA)[1]

…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.

77%

of orgs use over 25 disparate tools[1]

79%

say it's challenging to orchestrate alerts[2]

69%

say 2 or 3 people are involved in an incident[3]

The future of security: consolidation, cloud, and convergence

Securing the modern network is a considerable 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 *consolidates* and *converges* a variety of individual components into one unified, *cloud-delivered* service.

By bringing previously disparate point solutions together, a service like this can deliver robust, flexible security from one simple, easy-to-manage source. And, by delivering this security from the cloud, this solution is easy to deploy and can provide protection anywhere, on or off network.

63%

of orgs use less than 10 security vendors, suggesting that consolidation is a priority.[4]

93%

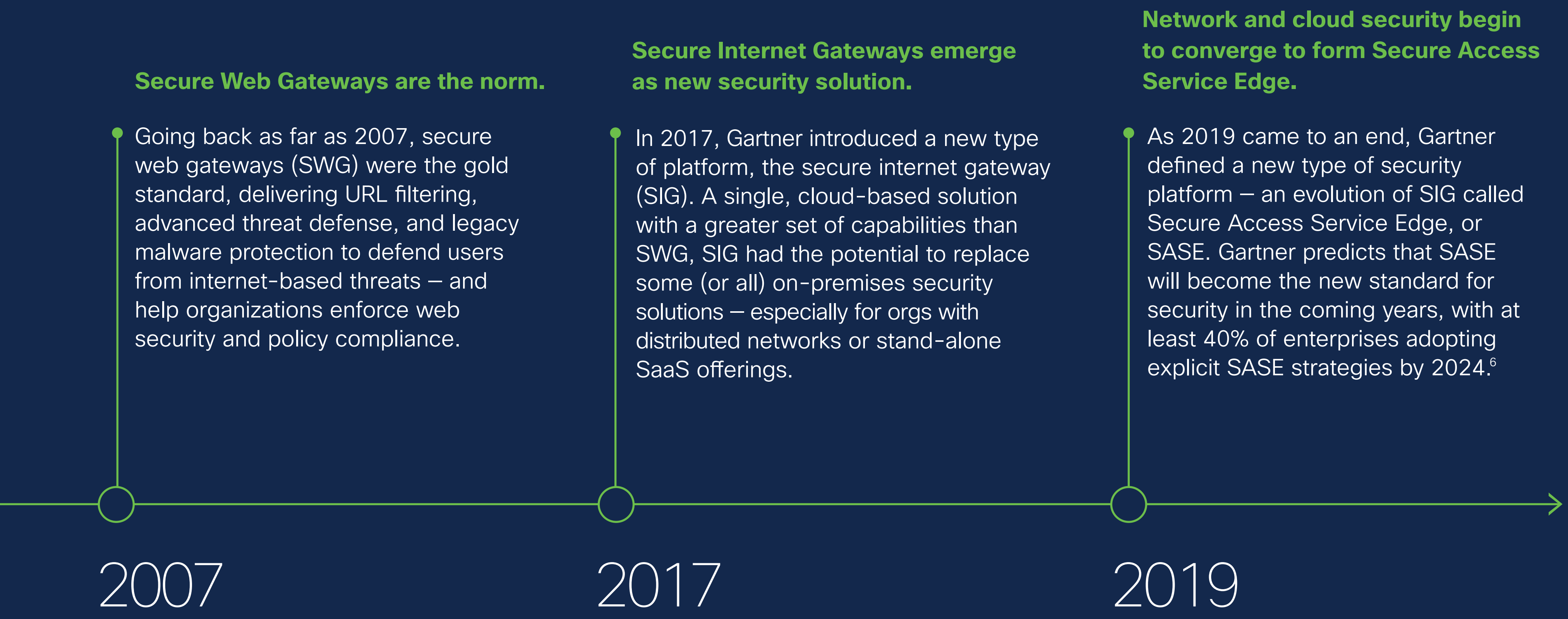
of orgs agree that moving security to the cloud has increased efficiency, allowing security to focus on other areas.[4]

76%

of orgs are looking for multifunction cloud security services.[5]

A timeline of changing security standards

As security converges 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.



Secure Web Gateways are the norm.

Going back as far as 2007, secure web gateways (SWG) were the gold 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.

2007

Secure Internet Gateways emerge as new security solution.

In 2017, Gartner introduced a new type of platform, 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.

2017

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

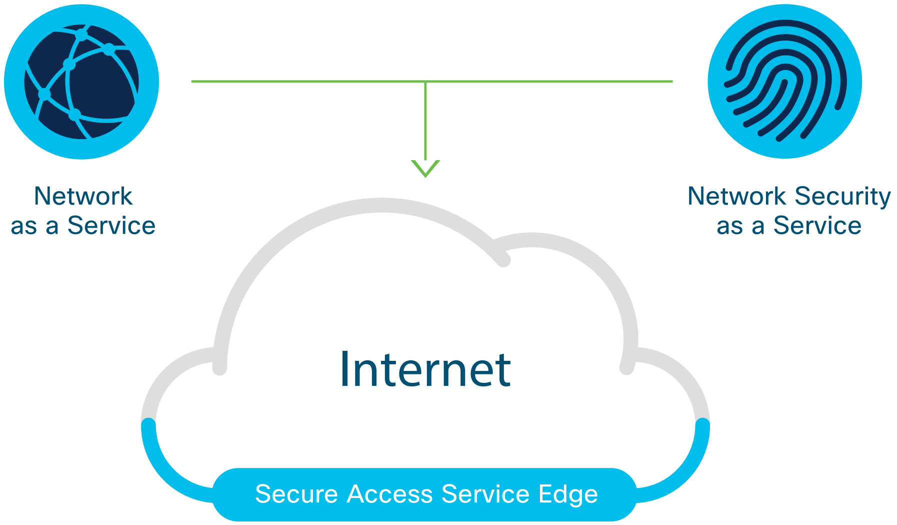
As 2019 came to an end, Gartner defined a new type of security platform – an evolution of SIG called Secure Access Service Edge, or SASE. Gartner predicts that SASE will become the new standard for security in the coming years, with at least 40% of enterprises adopting explicit SASE strategies by 2024.[6]

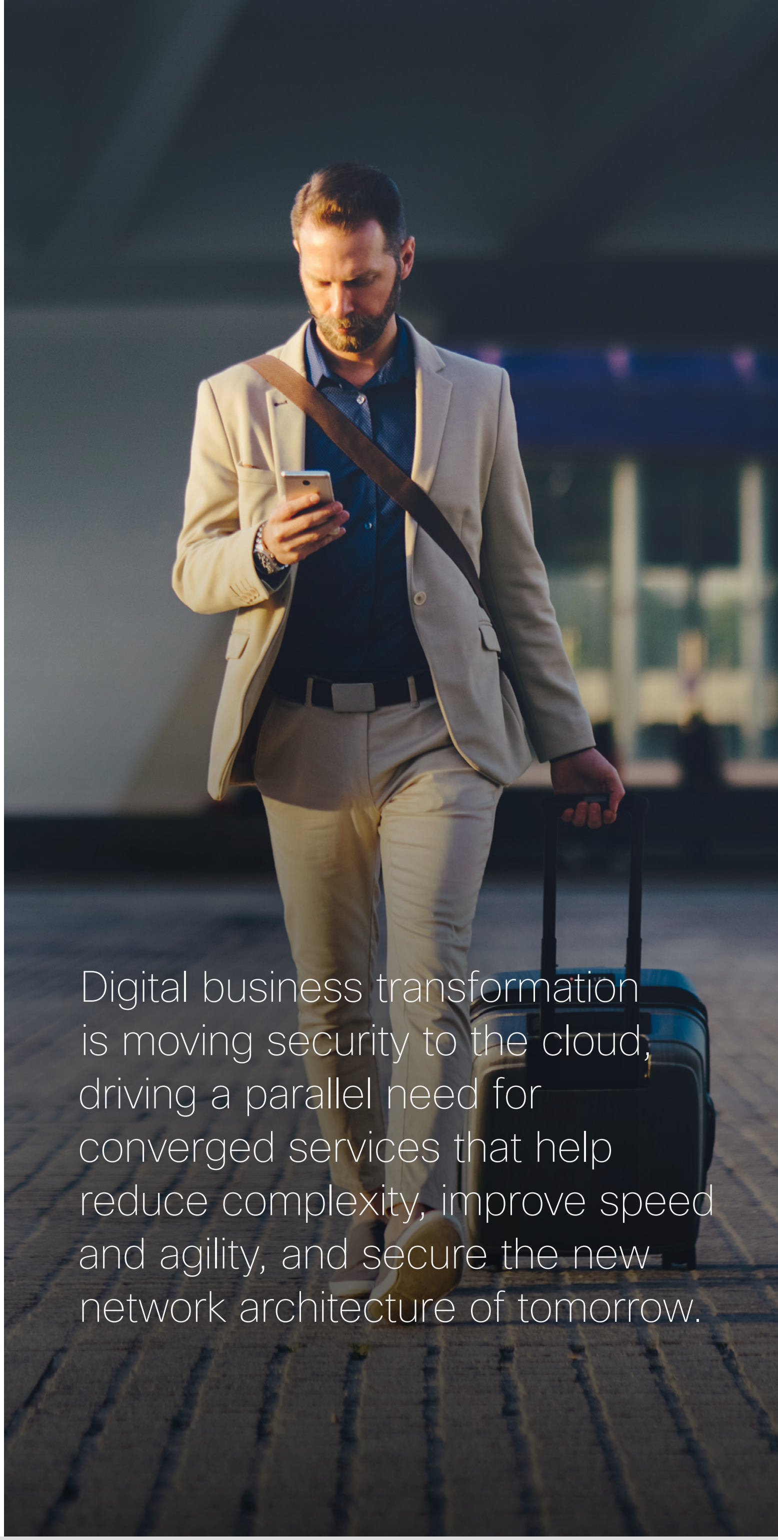
2019

So what exactly is SASE?

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

By consolidating a variety of powerful point solutions 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.

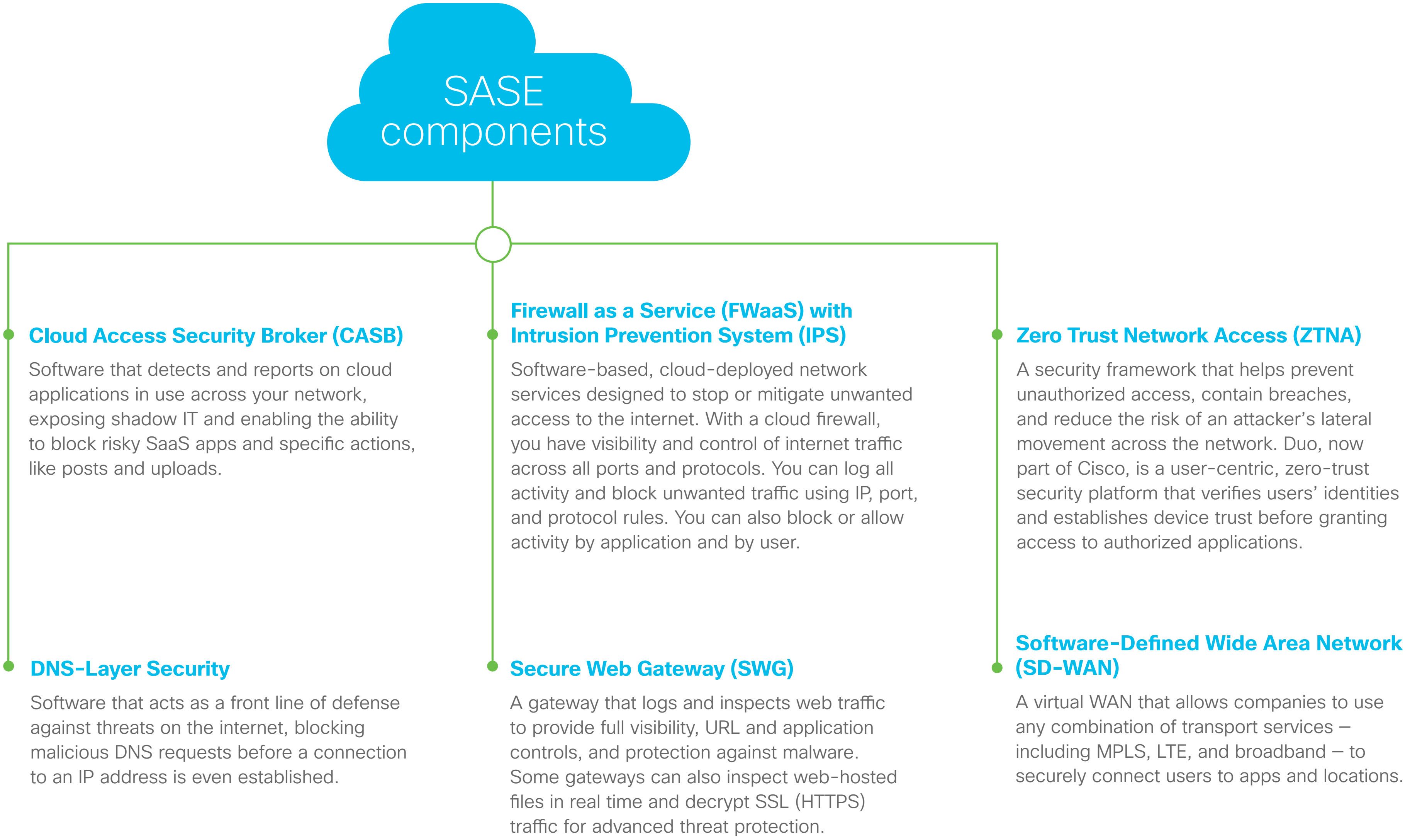




Digital business transformation is moving security to the cloud, driving a parallel need for converged services that help reduce complexity, improve speed and agility, and secure the new network architecture of tomorrow.

The next evolution in cloud convergence

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



SASE components

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.

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.

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.

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. 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.

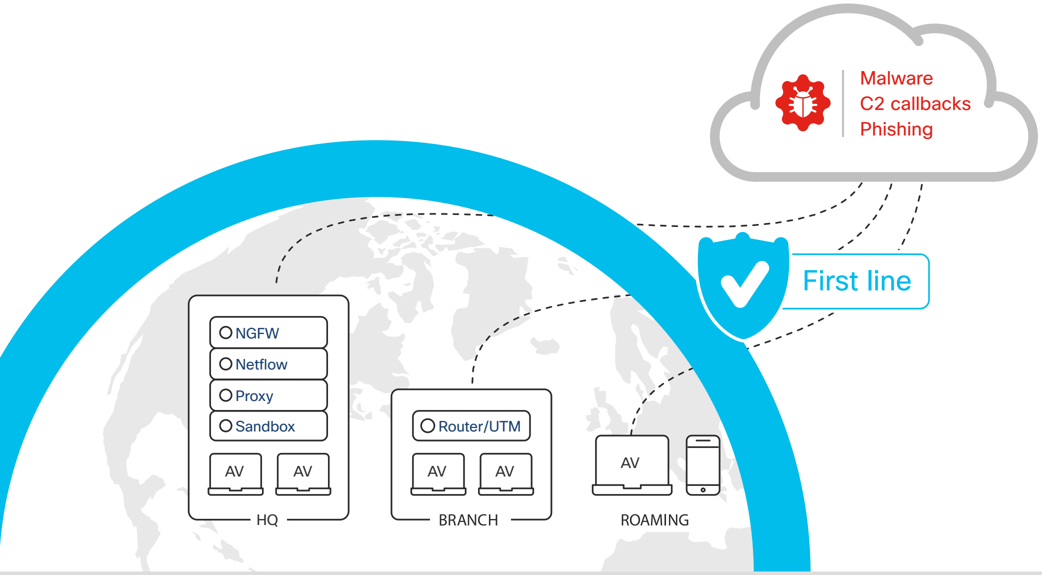
Software-Defined Wide Area Network (SD-WAN)

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 first step to a more secure network

Stronger network security doesn’t happen overnight, but getting started on your journey doesn’t have to be complicated: Start simple by enforcing security at the DNS layer.

Because DNS requests precede IP connection, DNS resolvers can stop threats before they reach your network or endpoints, blocking requests to malicious or unwanted destinations over any port or protocol. A critical component to keeping users safe on the internet, DNS security provides a single view of all internet activity across every location, while helping you prevent threats at the earliest point of contact.



DNS-layer security can:

Reduce malware by[7]

75%

Reduce remediation time by[8]

>50%

Protect users on and off network

100%

Meet Cisco Umbrella.

Cisco 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 highly 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 requests are transparently sent to the nearest, fastest data center and failover is automatic.

Fastest internet experience

Umbrella peers with more than 900 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.

200B+

daily DNS requests
(over all ports and protocols)

30+

data centers across
five continents

100M+

global daily active users

900+

partnerships with
top ISPs and CDNs

Simplify network security with a single cloud security service.

Cisco is paving the way to delivering multiple security functions in the cloud, creating a simple, scalable, flexible platform that can meet the unique needs of your business.

Interactive Threat Intelligence for Improved Incident Response

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-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.

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).

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.

Cisco SD-WAN Integration

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

Cisco Umbrella

The Cisco Umbrella advantage

The security landscape will only continue to evolve. As we continue to move toward the vision of SASE, Cisco Umbrella is a major step in the right direction, offering strong security functionality in a single, cloud-delivered solution.

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

Sources:

1. ESG Research Survey, Cisco Secure Internet Gateway Survey, January 2019
2. 2019 Cisco Benchmark Study
3. IDC Research, Investigation or Exasperation? The State of Security Operations
4. 2019 CISO Benchmark Study Cisco Cybersecurity Series
5. Cisco commissioned ESG Research Insights Report
6. Gartner, The Future of Network Security Is in the Cloud; 30 August 2019; Lawrence Orans, Joe Skorupa, Neil MacDonald
7. TechValidate survey of 180 users of Cisco Umbrella
8. TechValidate survey of 155 users of Cisco Umbrella