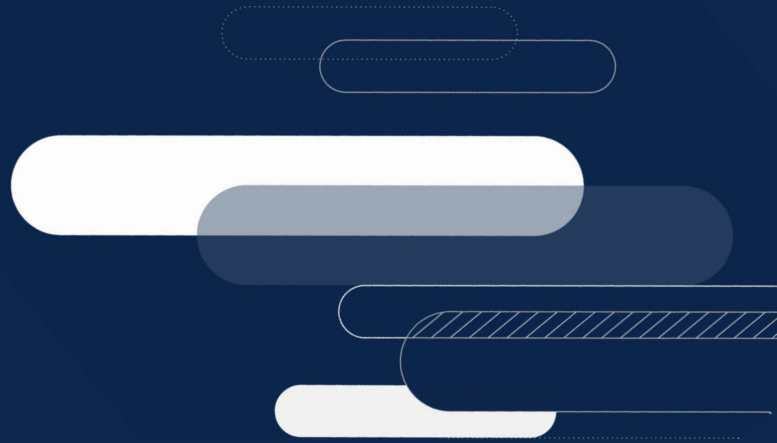


Cisco Umbrella Secure Internet Gateway

Hybrid work is the new normal

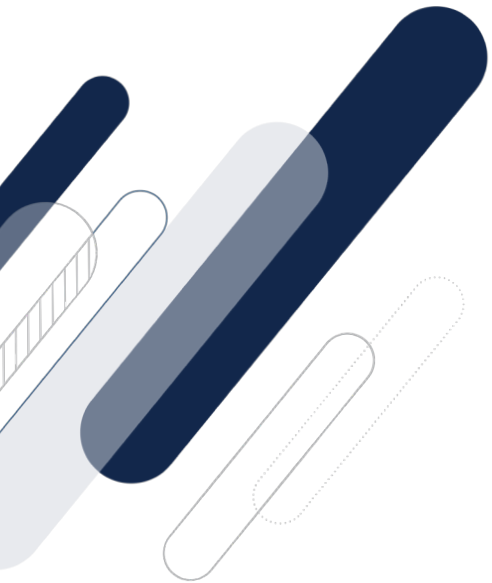
Exploding SaaS usage. Proliferating remote locations. Swelling ranks of roaming workers. In today's hybrid work environment, employees have the autonomy to work when, where, and how they are most productive. Not only are users highly distributed, but also applications are spread across data centers, public clouds, and private clouds. It's the new normal, and it's driving a transformation in enterprise security and networking.

Eighty-six percent (86%) of CIOs say it's important to empower a distributed workforce with seamless access to applications and consider high-quality collaborative experiences top of mind.[1]

Traditionally, organizations routed internet traffic from branch offices and roaming users back to a central location to apply security. Today, centralized security approaches are impractical. Backhauling traffic is expensive and can create performance bottlenecks, so roaming users often bypass their VPN to go direct to the internet for convenience and performance benefits.

As a result, many organizations are turning to software defined wide area networks (SD-WAN) for remote location optimization. This enables more efficient direct internet access (DIA) but also opens new security challenges.

1. Source: Accelerating Digital Agility Research (CIO Data), Cisco, 2021, https://ebooks.cisco.com/story/accelerating-digital-agility-2021/page/1]



Overarching needs and persistent pains

As centralized security policy enforcement diminishes, the risk of successful attacks or compliance violations increases. Security teams struggle to keep up with the increase in point solutions, which are difficult to integrate and manage. In a July 2021 survey of over 3,600 IT and security professionals, 37% of the respondents reported that they have too many security solutions and technologies to achieve cyber resiliency.[2]

Organizations strive to address these overarching needs:

- Enable highly distributed users to access applications and data seamlessly and securely across data centers and multiple cloud providers
- Protect against pervasive cyberthreats with consistent security policies, enforced across different locations and devices
- Deliver a high-quality user experience across a hybrid work environment with excellent performance
- Provide an excellent user experience for security professionals, including end-to-end visibility, rapid threat identification, and streamlined remediation

While attending to these needs, organizations want to relieve these persistent cybersecurity pain points.

- Gaps in visibility and coverage
- Volume and complexity of security tools
- Limited budgets and security resources

2. Source: The sixth annual Cyber Resilient Organization Study from IBM Security™, July 2021, https://www.ibm.com/resources/guides/cyber-resilient-organization-study/

SASE starts with converged security in the cloud

To satisfy the needs and reduce the pain, organizations are beginning to adopt an architectural approach known as the secure access service edge (SASE).

This approach converges networking capabilities with cloud-native security functions to simplify deployment and streamline management in the cloud. Its promise is to reduce challenges and create new value via consolidated, cloud-delivered solutions that protect users while simplifying cybersecurity implementation and management.

No one moves to a SASE architecture all at once. Organizations evolve toward the new approach with iterative steps. Many customers begin by converging into one unified security service a set of capabilities that previously were separate appliances or single-function cloud solutions. Gartner says that by 2025, 80% of organizations will have adopted a strategy to converge security capabilities for accessing web, cloud services, and private apps. Up from 20% in 2022.

Source: "Critical Capabilities for Security Service Edge," Gartner, 16 February 2022

"Cisco Umbrella combines the functionality of many point products into a single cloud-native solution that can scale to meet the security needs of any organization. Now with the Cisco SD-WAN integration, Umbrella security services can be brought to the branch in a matter of minutes."

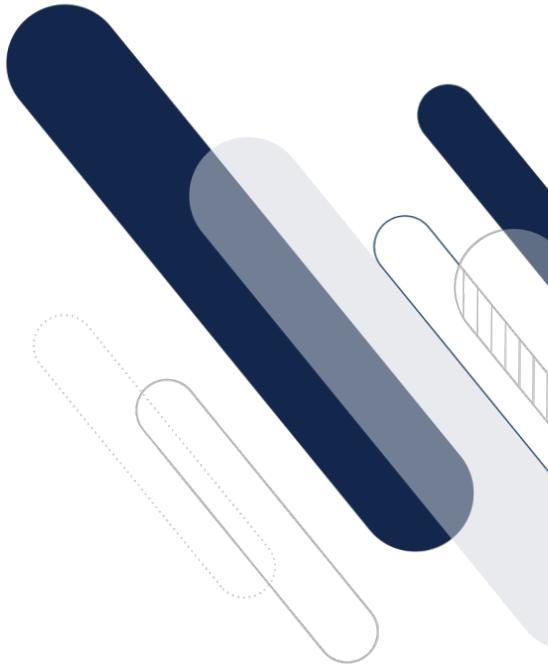
Mike Pfeiffer, Technical Solutions Architect, WWT

Cisco Umbrella: The ideal place to start

Cisco Umbrella is a cloud-delivered security service that secures internet access and controls cloud application usage across networks, branch offices, and roaming users. It unifies multiple functions in a single solution that traditionally required on-premises security appliances (firewalls, proxies, gateways) or single-function cloud-based security solutions. Umbrella combines secure web gateway (SWG), cloud-delivered firewall, DNS-layer security, cloud access security broker (CASB), remote browser isolation (RBI), data loss prevention (DLP), interactive threat intelligence, and more. By enabling all of this from a single, cloud-delivered service and dashboard, Umbrella provides the industry's highest security efficacy with less effort and fewer resources.

In a security efficacy test performed in the summer of 2022 by AV-TEST, an independent testing firm in Europe, Cisco Umbrella achieved the highest threat detection rate. Umbrella's 90.41% detection rate was 13% to 41% higher than its top competitors.[3]

[3]Source: AV-TEST Evaluates Secure Web Gateway & DNS-Layer Security Efficacy, DNS Tunneling Protection, https://umbrella.cisco.com/info/av-test-analyst-report-2022



Highlights

- Security protection on and off network
- Rapid deployment and flexible enforcement levels
- Immediate value and low total cost of ownership
- Single dashboard for efficient management
- Flexible, broad collection of open APIs with highly customizable API keys
- Unmatched speed and reliability with hybrid Anycast

Benefits

- Broader security coverage across all ports and protocols
- Increased visibility into internet activity across all locations and users
- Better visibility into cloud applications used across the business
- Lowered remediation costs and breach damage
- Reduction in time to detect and contain threats

DNS-layer security

By enforcing security at the DNS and IP layers, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established — stopping threats over any port or protocol before they reach your network or endpoints.

Highlights include:

- The visibility needed to protect internet access across all network devices, office locations, and roaming users
- Detailed reporting for DNS activity by type of security threat or web content and the action taken
- Ability to retain logs of all activity as long as needed
- Fast rollout to thousands of locations and users to provide immediate return on investment

This level of protection is enough for some locations and users, yet others need additional visibility and control to meet compliance regulations and further reduce risk.

Secure web gateway (full proxy)

Umbrella includes a cloud-based full proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. IPsec tunnels, PAC files and proxy chaining can be used to forward traffic for full visibility, URL and application-level controls, and advanced threat protection.

Highlights include:

- Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations
- The ability to efficiently scan all uploaded and downloaded files for malware and other threats using the Cisco Secure Endpoint (formerly Cisco AMP) engine and third-party resources
- Cisco Secure Malware Analytics (formerly Threat Grid) rapidly analyzes suspicious files (unlimited samples)
- File type blocking (e.g., block download of .exe files)
- Full or selective SSL decryption to further protect your organization from hidden attacks and time-consuming infections
- Granular app controls to block specific user activities in select apps (e.g., file uploads to Dropbox, attachments to Gmail, post/shares on Facebook)
- Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address

Data Loss Prevention (DLP)*

Cisco Umbrella data loss prevention analyzes sensitive data in-line** to provide visibility and control over sensitive data leaving your organization.

Highlights include:

- Easy enablement as part of Umbrella secure web gateway
- 80+ built-in content classifiers including PII, PCI, and PHI
- Customizable built-in content classifiers with threshold and proximity to tune and reduce false positives
- User-defined dictionaries with custom phrases (such as project code names)
- Detection and reporting on sensitive data usage and drill-down reports to help identify misuse
- Inspection of cloud app and web traffic content and enforcement of data policies

* Included in the SIG Advantage package. Available as an optional add-on in the SIG Essentials package.

** Cisco Umbrella will soon also offer API-based DLP functionality for out-of-band analysis of data at rest in the cloud. The combined multimode DLP capabilities will include unified policies and reporting.

Cloud access security broker (CASB)

Umbrella helps expose shadow IT by detecting and reporting on cloud applications in use across your environment. Insights can help manage cloud adoption, reduce risk and block the use of offensive or inappropriate cloud applications.

Highlights include:

- Data loss prevention (DLP) to prevent sensitive data from leaving the organization and in the cloud (see separate DLP section
- Reports on vendor category, application name, and volume of activity for each discovered app
- App details and risk information such as web reputation score, financial viability, and relevant compliance certifications
- Cloud malware detection to detect and remove malware from cloud-based file storage applications and ensure that applications remain malware-free.
- Ability to block/allow specific cloud applications
- Tenant restrictions to control the instance(s) of SaaS applications that all users or specific groups/individuals can access

Cloud-delivered firewall (CDFW)

The Umbrella cloud-delivered firewall provides visibility and control for non-web traffic that originated from requests going to the internet, across all ports and protocols.

Highlights include:

- Deployment, management and reporting through the Umbrella single, unified dashboard
- Customizable policies (IP, port, protocol, application and IPS policies)
- Layer 3 / 4 firewall to log all activity and block unwanted traffic using IP, port, and protocol rules
- Layer 7 application visibility and control to identify thousands of applications and block/allow them**
- Intrusion prevention system (IPS)* to examine network traffic flows and prevent vulnerability exploits with an added layer of threat prevention using SNORT 3 technology and signature-based detection.
- Detection and blocking of vulnerability exploitation
- Scalable cloud compute resources eliminates appliance capacity concerns

** Included in the SIG Advantage package. Available as an optional add-on in the SIG Essentials package.

Cisco Secure Malware Analytics

Cisco Secure Malware Analytics (formerly known as Threat Grid) combines advanced sandboxing with threat intelligence into one unified solution to protect organizations from malware. Additionally with SIG Advantage, security analysts gain access to the full Secure Malware Analytics console, enabling them to execute malicious files in a glovebox, track file execution actions, and capture network activity generated by the file. When combined with Investigate, security analysts may go further and uncover malicious domains, IPs, ASNs mapped to a file's actions to get the most complete view of an attackers' infrastructure, tactics, and techniques.

Highlights include:

- Ability to detect hidden attack methods and report on malicious files
- Single, correlated source of intelligence to speed threat hunting and incident response
- Secure Malware Analytics APIs to integrate with SecureX and your SIEM for enriching security data (SIG Advantage)
- Retrospective notification if file disposition changes (originally good / later deemed malicious)

Remote browser isolation (RBI)*

By isolating web traffic from the user device and the threat, Umbrella remote browser isolation (RBI) delivers an extra layer of protection to the Umbrella secure web gateway so that users can safely access risky websites.

Highlights include:

- Isolation of web traffic between user device and browser-based threats
- No performance impact on end users
- Protection from zero-day threats
- Granular controls for different risk profiles
- Rapid deployment without changing existing browser configuration
- On-demand scale to easily protect additional users on all devices, browsers, and operating systems

*Available as an add-on to SIG Essentials or SIG Advantage

Correlated threat intelligence for improved incident response

Umbrella analyzes over 620 billion DNS requests daily. We ingest this massive amount of internet activity data and continuously run statistical and machine learning models against it. Fueling this with the threat intelligence from Cisco Talos, one of the largest and most trusted providers of cutting-edge security research globally, means that we can uncover malicious domains, IPs, and URLs before they're used in attacks.

This threat intelligence powers not only Cisco Umbrella, but also your ability to respond to incidents. Your analysts can leverage Umbrella Investigate for rich intelligence about domains, IPs, and malware across the internet, enabling them to:

- Gain deeper visibility into threats with the most complete view of the internet
- Prioritize incident investigations
- Speed incident investigations and response
- Predict future attack origins by pinpointing and mapping out attackers' infrastructures
- Integrate Investigate data other security orchestration tools.

"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

Umbrella and SD-WAN Integration

Backhauling internet bound traffic from remote sites is expensive and adds latency. Many organizations are upgrading their network infrastructure by adopting SD-WAN and enabling direct internet access (DIA).

Umbrella and SD-WAN are core elements of Cisco's secure access service edge (SASE) architecture that consolidate networking and security functions. With the Umbrella and Cisco SD-WAN integration, you can simply and rapidly deploy Umbrella across your network and gain powerful cloud-delivered security to protect against threats on the internet and secure cloud access. This market-leading automation makes it easy to deploy and manage the security environment over tens, hundreds or even thousands or remote sites. Umbrella offers flexibility to create security policies based on the level of protection and visibility you need – all in the Umbrella dashboard.

Packages

Umbrella SIG Essentials

Deploy advanced security functions and simplify management with the most effective security in the industry.

Umbrella SIG Advantage

Includes all the functionality in Umbrella SIG Essentials, plus advanced security functions like layer 7 firewall with intrusion prevention system (IPS), data loss prevention (DLP), and more.

Reserved IP

Optional add-on that provides a unique IP address deployed to an Umbrella data center that is mapped to a customer's web traffic and not shared with other customers. This allows the customer to use SaaS applications that require "allow listing," a list of pre-designated/known IPs.

Cisco SecureX extends simplicity, visibility, and efficiency

Cisco SecureX (included with Umbrella subscriptions) accelerates your threat investigation and remediation by unifying Umbrella's threat intelligence with data from additional Cisco Security products and your other security infrastructure. It unifies your entire security ecosystem in one location for greater simplicity and visibility. It automates workflows to increase operational efficiency. Cisco SecureX helps reduce complexity with a built-in platform experience.

Global cloud architecture enables reliable security with great performance

Umbrella's battle-hardened global cloud architecture delivers network resiliency and reliability to keep your performance fast and your connections secure. Over 1000 peering partnerships with top IXPs, CDNs and SaaS platforms deliver lightning-fast performance. The architecture automates routing for top-notch availability and reliability. The containerized, multi-tenant architecture is flexible and scalable.

For more information

Contact your Cisco sales representative for more information on the Cisco Umbrella Secure Internet Gateway (SIG).