Cisco Umbrella: Secure Internet Gateway (SIG) Advantage Package

Highest level of protection from a single service

Organizations are facing a difficult dilemma. Given the growing threat landscape alongside an ever-expanding attack surface, they need even higher levels of protection. However, more security vendors result in complex security operations and increases costs. No wonder, according to Gartner, 80% of organizations are interested in vendor consolidation strategy.[1]

1. Gartner Top Security and Risk Trends for 2021

Embrace SASE with SIG Advantage

A rise in remote employees and an increased reliance on SaaS applications create new, wider gaps in security. To put it simply, it's more challenging to protect users at the edge – ensuring seamless connections that optimize productivity without creating performance issues that drag down user satisfaction.

Enter secure access service edge (SASE), an architectural approach that offers an alternative to traditional data center-oriented security. SASE converges networking capabilities with cloud-native security functions to simplify deployment and streamline management in the cloud.

SIG Advantage can help you cut complexity, reduce risk exposure, and improve performance with a single cloud-delivered service that deploys easily and scales with your business.

Highlights include:

- **Deliver secure access anywhere, anytime**
- **Move access control to the edge**
- **Gain efficiencies with an as-a-service model**
- **Make your business more agile**

What if you could reduce complexity and costs and get better security? Since 2006, Cisco Umbrella has delivered reliable, proven protection and has grown to over 24,000 customers. As a pioneer in cloud-delivered security, we got our start with DNS-layer security and now offer a multi-function service that continues to evolve. Now, we've innovated again to deliver the most complete set of advanced security capabilities from a single vendor in a single package with a single subscription for maximum value.

"Nearly half of customers deployed Cisco Umbrella in less than 1 day."

TechValidate survey of 230 users,
May 2021

"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

SIG Advantage: Advanced Security, Simplified

The Umbrella SIG Advantage package significantly simplifies security and reduces the cost, time, and resources previously required for deployment, configuration, and integration. SIG Advantage unifies secure web gateway, cloud access security broker, DNS-layer security, cloud-delivered firewall, data loss prevention, and Cisco Secure Malware Analytics into a single cloud service. Umbrella SIG Advantage represents our highest level of protection with features not available in other packages, including a Layer 7 firewall with intrusion prevention system, data loss prevention and Cisco Secure Malware Analytics for analyzing file behavior.

"74% of Umbrella customers identified "fast and easy deployment" as the top benefit for using Cisco Umbrella."

TechValidate survey of 314 users of Cisco Umbrella, May 2021

DNS-layer security

By enforcing security at the DNS layer, 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

Cloud-delivered firewall (CDFW)

The Umbrella cloud-delivered firewall provides visibility and control for 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 Cisco Talos threat intelligence to detect and block more threats

* General availability targeted for July 2021

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:

- 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 apps
- Tenant restrictions to control the instance(s) of SaaS applications that all users or specific groups/individuals can access

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. By leveraging Cisco Umbrella Investigate, included in the SIG Advantage package, and Cisco Secure Malware Analytics, security analysts can uncover malicious domains, IPs, ASNs and files 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
- Simple APIs to integrate with SecureX and your SIEM for enriching security data
- Ability to predict unknown threats using real-time threat intelligence
- Automated alerts for retrospective events

Remote browser isolation (RBI) Available as an optional add-on

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

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). Eighty percent of organizations extensively or selectively use SD-WAN today.[1]

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.

"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 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 Umbrella SIG Advantage package.

AICPA SOC

SOC 2, Type II
Compliant