Cisco Umbrella: Secure Internet Gateway (SIG) Essentials Package

The new normal – decentralized networks

Exploding SaaS usage. Proliferating remote locations. Swelling ranks of roaming workers. It's the new normal, and it's driving a transformation in enterprise security and networking.

The wide-scale use of cloud applications has become fundamental to business operations. New research from ESG notes that 86% of organizations today are extensively or moderately using public cloud computing services (Saas or IaaS).[1]

Traditionally, organizations routed internet traffic from branch offices back to a central location to apply security. Yet in today's branch offices with high cloud application use, this centralized security approach has become impractical due to the high cost and performance issues of backhauling traffic. Many remote offices find ways to go direct to the internet for convenience and performance benefits.

For these reasons, many organizations are adopting decentralized networking approaches guided by SD-WAN to optimize remote location performance. Eighty percent of organizations extensively or selectively use SD-WAN today.[1] This enables more efficient direct-internet-access (DIA), but also opens new security challenges.

Internal Data Corp estimates that the SD-WAN market will see a compound annual growth rate of 30.8 percent from 2018 to 2023.

International Data Corporation (IDC)
SD-WAN Infrastructure Forecast

1. ESG Research, Transitioning Network Security Controls to the Cloud, May 2020, https://learn-umbrella.cisco.com/ebook-library/transitioning-network-security-controls-to-the-cloud.

Security challenges drive SASE convergence

With these shifts, centralized security policy enforcement diminishes, and the risk of successful attacks or compliance violations increases. Security teams struggle to keep up. Many organizations have lots of separate point solutions that are difficult to integrate and manage. Sixty-four percent of organizations reported that network security at the edge has become more difficult than it was 2 years ago. And, 26% said that the number of disparate network security tools was a major contributor to that increased difficulty.[1]

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

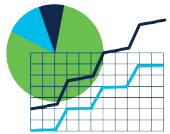
SIG Essentials delivers a simple, secure, and scalable approach to SASE. SIG Essentials can help you cut complexity, reduce risk exposure, and improve performance with a single cloud-delivered service.

IT security pain points

Network decentralization and the accompanying security challenges underlie the top IT security pain points with which organization of all sizes, in all industries grapple. To lessen the pain (and create new value) security leaders are moving toward consolidated, cloud-delivered solutions that provide broad protection for users while also significantly simplifying security and reducing the cost, time, and resources previously required for deployment, configuration, and integration.

Gaps in visibility and coverage

Volume and complexity of security tools



Limited budgets and security resources

Top 3 reasons organizations are looking for a SIG:

- Improved security coverage
- Centralized/consistent policies across remote locations
- Better performance and user satisfaction

Key benefits:

- Broad security coverage across all ports and protocols
- 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
- Unmatched speed and reliability with hybrid Anycast

Solution: Cisco Umbrella – SIG Essentials package

The Umbrella Secure Internet Gateway (SIG) Essentials package offers a broad set of security functions that until now required separate firewall, web gateway, threat intelligence, and cloud access security broker (CASB) solutions. By enabling all of this from a single, cloud-delivered service and dashboard, Umbrella provides higher security efficacy with less effort and less resources. In a recent security efficacy test performed by AV-TEST, Cisco Umbrella received the highest threat detection rate in the industry at 96.39%.[2] SIG Essentials can be integrated with your SD-WAN implementation to provide a unique combination of performance, security, and flexibility that delights both your end users and security team.

> “80% of organizations are interested in vendor consolidation strategy.”
>
> Gartner
> Top Security and Risk Trends for 2021

2. AV-TEST Evaluates Secure Web Gateway and DNS-Layer Security Efficacy, October 30, 2020. https://umbrella.cisco.com/info/av-test-evaluates-secure-web-gateway-and-dns-layer-security-efficacy

Major components of Umbrella

The following components are integrated seamlessly in a single, cloud-delivered service:

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 (500 samples/day)
- 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

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
- Detection and blocking of vulnerability exploitation
- Scalable cloud compute resources eliminates appliance capacity concerns Cisco Talos threat intelligence to detect and block more threats

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 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.

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). Internal Data Corp estimates that the SD-WAN market will see a compound annual growth rate of 30.8 percent from 2018 to 2023.

Umbrella and SD-WAN are core elements of Cisco's secure access service edge (SASE) architecture that consolidates 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. platforms deliver lightning-fast performance.

Correlated threat intelligence for improved incident response

Umbrella analyzes over 620 billion DNS requests daily. We ingest this massive amount of internet activity data from our global network and continuously run statistical and machine learning models against it. Our unique view of the internet enables us to uncover malicious domains, IPs, and URLs before they're used in attacks. Umbrella security researchers constantly analyze this information, and supplement it with intelligence from Cisco Talos to discover and block an extensive range of threats.

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
- Better prioritize incident investigations
- Speed incident investigations and response
- Predict future attack origins by pinpointing and mapping out attackers' infrastructures
- Easily integrate Investigate data other security orchestration tools.

"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

For more information

Contact your Cisco sales representative for more information on the Umbrella SIG Essentials package.

SOC 2, Type II
Compliant