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. Eighty-five percent of remote users reported that they sometimes go direct to the internet.[2]

"Eighty-five percent of remote users reported that they sometimes go direct to the internet"

ESG Research, Market Dynamics Impacting Remote and Roaming User Security Requirements, Jan 2019

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.

Security challenges

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] These point products are generating thousands of alerts, but many go untouched. In fact, 52% of daily alerts are not investigated.[3]

IT security pain points

Gaps in visibility and coverage

Volume and complexity of security tools

Limited budgets and security resources

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 simplifying the environment, reducing bandwidth costs, and relieving resource constraints.

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 significantly reduces the time, money, and resources previously required for deployment, configuration, and integration tasks. It 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.

Top 3 reasons organizations are looking for a SIG:

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

"76% of respondents prefer a multi-function security platform to solve the remote security challenge"

ESG Research, Market Dynamics Impacting Remote and Roaming User Security Requirements, Jan 2019

Major components of Umbrella

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

DNS-layer security

This is the first line of defense against threats because DNS resolution is the first step in internet access. 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. As a cloud-delivered service, it:

- Provides the visibility needed to protect internet access across all network devices, office locations, and roaming users.
- Logs and categorizes DNS activity by type of security threat or web content and the action taken — whether it was blocked or allowed.
- Retains logs of all activity as long as needed, ready to recall for deeper investigation.
- Can be implemented quickly to cover thousands of locations and users in minutes, 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)

Cisco has enhanced Umbrella to now include a cloud-based full proxy that can log and inspect all of your web traffic for greater transparency, control, and protection. The Umbrella platform now includes:

- The ability to efficiently scan all uploaded and downloaded files for malware and other threats using the Cisco AMP engine and third-party resources
- 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)
- File type blocking (e.g. block download of .exe files)
- Detailed reporting with full URL addresses, network identity, allow or block actions, plus the external IP address
- Content filtering by category or specific URLs to block destinations that violate policies or compliance regulations.

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.

Cloud access security broker (CASB) functionality

Umbrella helps exposes shadow IT by detecting and reporting on the cloud applications in use across your environment. It automatically generates reports on the vendor, category, application name, and volume of activity for each discovered app. The drill down reports include risk information such as web reputation score, financial viability, and relevant compliance certifications.

App Discovery provides:

- Extended visibility into cloud apps in use
- App details and risk information
- Ability to block/allow specific apps

Tenant restrictions enable you to restrict the instance(s) of SaaS applications that all users or specific groups/individuals can access.

This insight can help manage cloud adoption, reduce risk, and block the use of offensive or inappropriate cloud applications in the work environment.

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

Cloud-delivered firewall (CDFW)

With Umbrella's firewall, all activity is logged and unwanted traffic is blocked using IP, port, and protocol rules. To forward traffic, you simply configure an IPsec tunnel from any network device. Management is handled through the Umbrella dashboard, and as new tunnels are created, security policies can automatically be applied for easy setup and consistent enforcement throughout your environment.

Umbrella's cloud-delivered firewall provides:

- Visibility and control for internet traffic across all ports and protocols
- Customizable IP, port, and protocol policies in the Umbrella dashboard
- IPsec tunnel support to securely route traffic to cloud infrastructure
- Automated reporting logs

Correlated threat intelligence for improved incident response

Umbrella analyzes over 200 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

Umbrella and SD-WAN single offer

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). Based on a recent survey with ESG, 80% of organizations use SD-WAN extensively or selectively.[1]

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.

For DNS-layer security, Umbrella can be deployed with a single configuration in the Cisco SD-WAN vManage dashboard. For additional security and more granular controls, Umbrella's secure web gateway and cloud-delivered firewall capabilities can be deployed through a single IPsec tunnel. Our integrated approach can efficiently protect your branch users, connected devices, and application usage from all DIA breakouts.

For more information

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

> **"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

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.
2. ESG Research, Market Dynamics Impacting Remote and Roaming User Security Requirements, Jan 2019
3. Cisco 2020 2020 CISO Benchmark Report, https://www.cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html