Cisco Umbrella: Insights Package

Defend against threats on the internet wherever users go.
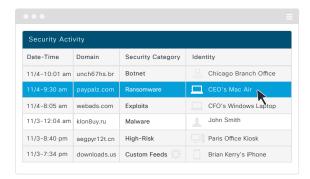
Stop threats before they reach your network or endpoints

First line of defense against threats

Cisco Umbrella is a cloud security platform built into the foundation of the internet. 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.

Visibility and protection everywhere

As a cloud-delivered service, Umbrella provides the visibility needed to protect internet access across all network devices, office locations, and roaming users. All internet activity is logged and categorized by the type of security threat or web content, and the action taken — whether it was blocked or allowed. Logs of all activity can be retained as long as needed and recalled easily for investigation. You can even uncover cloud apps and Internet of Things (IoT) devices in use across your company.

Security Activity

Date-Time	Domain	Security Category	Identity
11/4–10:01 am	unch67hs.br	Botnet	Chicago Branch Office
11/4–9:30 am	paypalz.com	Ransomware	CEO's Mac Air
11/4–8:05 am	webads.com	Exploits	CFO's Windows Laptop
11/3–12:04 am	klon8uy.ru	Malware	John Smith
11/3–8:40 pm	aegpyr12t.cn	High-Risk	Paris Office Kiosk
11/3–7:34 pm	downloads.us	Custom Feeds	Brian Kerry's iPhone

How Umbrella helps

- Reduce malware by 75%[1]

- Reduce remediation time by 50% or more[2]

- Protect on and off-network

How we do it

Intelligence to see attacks before they launch

Our global network infrastructure handles over 180 billion internet requests a day, which gives us a unique view of relationships between domains, IPs, networks, and malware across the internet. Similar to Amazon learning from shopping patterns to suggest the next purchase, we learn from internet activity patterns to automatically identify attacker infrastructure being staged for the next threat, and then block users from going to malicious destinations.

Enterprise-wide deployment in minutes

Umbrella is the fastest and easiest way to protect all of your users in minutes. It's powerful, effective security without the typical operational complexity. By performing everything in the cloud, there is no hardware to install, and no software to manually update.

1. https://www.techvalidate.com/product-research/cisco-umbrella/facts/AF2-8E2-79D 2. https://www.techvalidate.com/product-research/cisco-umbrella/charts/F83-DB9-434

Problems we solve

Gaps in protection

Most mobile and remote workers don't always have their VPN on, and most branch offices don't backhaul all traffic — which means they don't have enough protection. In under 30 minutes, Umbrella can provide worldwide coverage for all on-network devices — including BYOD and IoT — and roaming laptops and supervised iOS 11 devices.

New and targeted attacks

Signature-based tools, reactive threat intelligence, and isolated security enforcement cannot stay ahead of attacks. Umbrella will identify and contain two times more compromised systems than before.

Understaffed teams

We get it — your team is understaffed and you need security that is easy to setup, configure, and use. Not only is Umbrella easy to manage, but it also stops threats earlier and reduces the number of infections and alerts you see from other security products.

Deployment information

On-network: Any network device (e.g. router) can be used to provision Umbrella by pointing external DNS to our IP address. You can also use your existing Cisco footprint — SD-WAN, Integrated Services Router (ISR) 1K and 4K Series, Meraki MR, and Wireless LAN Controllers, to quickly provision protection across hundreds of routers and access points.

Off-network: Available for laptops that use Windows, macOS, Chrome OS, and supervised Apple devices that run iOS 11.3 or higher.

For more details on deployment, configuration, reporting, and our APIs visit docs.umbrella.com.

Try Umbrella today

Visit signup.umbrella.com for a free 14 day trial of Umbrella. If your organization has 1000+ users, you're qualified for the Umbrella Security Report, which provides a detailed post-trial analysis.

Umbrella use cases

- Prevent web and non-web C2 callbacks from compromised systems

- Prevent malware drive-bys or phishing attempts from malicious websites

- Enforce and comply with acceptable use policies across 100 content categories

- Uncover SaaS app shadow IT and block risky apps

- Retain logs forever to improve incident response and policy compliance

- Pinpoint compromised systems using real-time security activity

- Proxy risky domains for deeper inspection of URLS and files using antivirus engines and Cisco Advanced Malware Protection

Does your organization use Cisco SD-WAN?

Deploy Umbrella across your SD-WAN in minutes and instantly gain web and DNS-layer protection against threats wherever users access the internet.

Learn more:
umbrella.cisco.com/sd-wan