

Cisco Umbrella: Professional 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

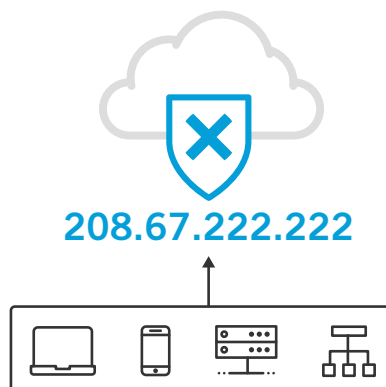
Cisco Umbrella is a cloud security platform built into the foundation of the internet. Enforcing security at the DNS layer, Umbrella blocks requests to malicious and unwanted destinations before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints.

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.

Cisco Umbrella

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 we do it

Intelligence to see attacks before they launch

Our global network infrastructure handles over 120 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. Scheduled reports are automatically sent to your inbox.

How Cisco Umbrella helps

- Reduce malware infections up to 98%
- Cut the number of alerts from your IPS, AV, and SIEM by as much as 50%
- Enforce acceptable use policies with 60+ content categories

What makes Umbrella different

- **Threat Prevention:** not just threat detection
- **Protects On & Off Network:** not limited to devices forwarding traffic through on-premises appliances
- **Always Up to Date:** no need for device to VPN back to on-premises server for updates

Problems we solve

82% of users bypass the VPN¹ and 70% of branch offices go direct-to-net²

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.

70-90% of malware is unique to each organization³

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.

86% of IT managers believe there's a shortage in skilled security professionals⁴

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.

Use cases



Prevent web and non-web C2 callbacks from compromised systems



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



Enforce and comply with acceptable use policies using 80 content categories and your own lists



Pinpoint compromised systems using real-time security activity

Deployment Specifications

- Any network device (e.g. router) can be used to provision Umbrella. Protect all network-connected devices with one IP change in your DHCP server (or scope) or DNS server. Or protect all Wi-Fi-connected devices with a simple checkbox using our Aruba, Cradlepoint, and Aerohive integrations.
- Off-network coverage is available for Windows and macOS, and supervised iOS 11 devices. If you already use the Cisco AnyConnect client for Windows or Mac, no additional agents are required! Simply upgrade to v4.3 or later and enable the roaming security module. Alternatively, deploy the Umbrella roaming client via Windows GPO or Apple Remote Desktop. To protect supervised iOS 11 devices, download and install the Cisco Security Connector application, and enable the Umbrella application extension.

Common deployment question

“How is the Umbrella roaming client more lightweight and transparent compared to other endpoint protections?”

Learn more:
<http://cs.co/lightweight>

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.

Data Sources

1. <http://cs.co/IDG-survey>
2. <http://cs.co/Forrester-BranchOffices>
3. 2015 Verizon Data Breach Report
4. ISACA 2015 Global Cybersecurity Status Report