

Cisco Umbrella: Platform 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.

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	AMP Threat Grid 	CEO's Mac Air
11/4-8:05 am	webads.com	Exploits	CFO's Windows Laptop
11/3-12:04 am	klon8uy.ru	FireEye 	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 80 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.

Integrations to amplify existing investments

Umbrella easily integrates with your existing security stack and local intelligence. Leveraging an open API, you can programmatically extend protection for devices and locations beyond your perimeter, and enrich your incident response data.

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 with 100% uptime, there is no hardware to install, and no software to manually update.

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%
- Decrease remediation time by 20%

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.

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 products.

Use cases



Prevent web and non-web C2 callbacks from compromised systems



Cover your DNS blind spot and retain logs forever to improve incident response and policy compliance



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



Pinpoint compromised systems using real-time security activity, then identify targeted attacks using global context



Enforce and comply with acceptable use policies using 60 content categories and your own lists



Investigate related attacks using a live graph of all internet activity



Gain visibility of cloud service usage (including IoT devices)



Take immediate action on threat intelligence or IOCs detected by your existing security stack

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 for Windows and Mac OSX. 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.
- On-network granularity by internal network or Active Directory identities supports VMware or Hyper-V.
- Passive Active Directory identification supports domain controllers on Windows Server.
- RESTful API supports pre-defined integrations with Cisco AMP Threat Grid, FireEye, Check Point, ZeroFox, ThreatConnect, ThreatQuotient, and others, plus up to 10 custom integrations.

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

Have multiple, decentralized, or partitioned organizations?

- Get the simplest centralized security management ever!
- See how it works at <http://cs.co/umbrellamultiorgbrief>

Common deployment question

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

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