Cisco Umbrella: Platform Package

Defend against threats on the internet wherever users go

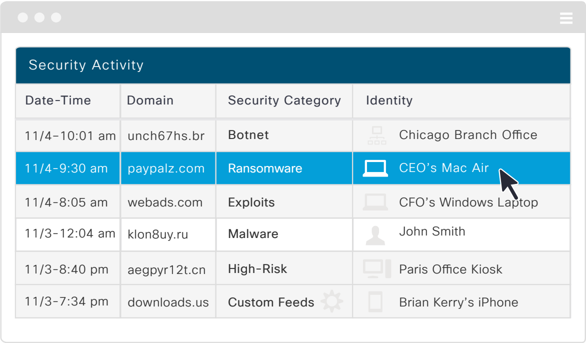
Stop threats before they reach your network or endpoints

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.



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 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%
- Protection on and off the corporate network

Challenges we help to address

Gaps in protection

Many remote and roaming workers by bypass their VPN, and many 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 and off-network devices.

82% of users bypass the VPN[1] and 70% of branch offices have direct internet access[2]

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.

70-90% of malware is unique to each organization3

Understaffed team

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.

86% of IT managers believe shortage in skilled security professionals4

How we do it

Intelligence to see attacks before they launch

Our global network infrastructure handles over 175 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. Additionally, as part of the Platform package, you get access to our threat intelligence via the Cisco Umbrella Investigate web console.

Integrations to amplify existing investments

Umbrella has a number of Application Programming Interfaces (APIs) these include the network device API, management API, and reporting API. With the Platform package, you also have access to our enforcement API which enables you to easily integrate with your existing security stack and local intelligence.You can programmatically extend protection for devices and locations beyond your perimeter, and enrich your incident response data.

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.

Use cases

- Prevent web and non-web C2 callbacks from compromised systems
- Prevent malware or phishing attempts from malicious websites
- Enforce and comply with acceptable use policies using over 80 content categories
- Uncover SaaS app shadow IT and block everywhere
- Proxy risky domains for deeper inspection of URLS and files
- Retain logs forever to improve incident response and policy compliance
- Pinpoint compromised systems using real-time security activity reports
- Investigate related attacks using a live graph of all internet activity
- Automate blocking based on threat intelligence from your existing security stack

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

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