Cisco Umbrella: DNS Security Advantage Package

Work anywhere, secure everywhere.

Stop threats before they reach your network or endpoints

The leader in DNS-layer security

Cisco Umbrella delivers the most secure, reliable, and fastest internet experience to more than 100 million users. As a leading provider of network security and recursive DNS services, we enable the world to connect to the internet with confidence on any device.

Umbrella resolves your most pressing challenges

Malware and ransomware

Gaps in visibility and coverage

Cloud apps and shadow IT

Difficult to manage security

Block malware without latency

Umbrella is a cloud-native platform built into the foundation of the internet. By enforcing security at the DNS and IP layers, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established – stopping threats over any port or protocol before they reach your network or endpoints. With our selective proxy, it offers deeper inspection of URLs and files for risky domains using antivirus engines and Cisco Advanced Malware Protection (AMP). Umbrella even blocks direct IP connections from command and control callbacks for roaming users.

Improve visibility

Most companies leave their DNS resolution up to their ISP. But as more organizations adopt direct internet connections and users bypass the VPN, this leads to a DNS-blind spot. DNS requests precede the IP connection, which enables DNS resolvers to log requested domains regardless of the connection's protocol or port. Monitoring DNS requests, as well as subsequent IP connections is an easy way to provide better accuracy and detection of compromised systems, improving security visibility and network protection.

Manage and control cloud apps

Umbrella provides visibility into sanctioned and unsanctioned cloud services in use across the enterprise, so you can uncover new services being used, see who is using them, identify potential risk, and block specific applications easily.

Simplify security management

Umbrella is the fastest and easiest way to protect all of your users enterprise-wide in minutes, and reduces the number of infections and alerts you see from other security products by stopping threats at the earliest point. Win no hardware to install and no software to manually update, ongoing management is simple.

[1] https://www.techvalidate.com/product-research/cisco-umbrella/facts/324-36C-800 [2] https://www.techvalidate.com/product-research/cisco-umbrella/facts/AF2-8E2-79D
[3] https://www.techvalidate.com/product-research/cisco-umbrella/charts/F83-DB9-434

Unmatched threat intelligence

Leveraging threat intelligence from Cisco Talos, one of the largest commercial threat intelligence teams in the world with more than 300 researchers, Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being used in attacks. We also feed huge volumes of global internet activity into a combination of statistical and machine learning models to proactively identify new attacks being staged on the internet.

Speed up incident response

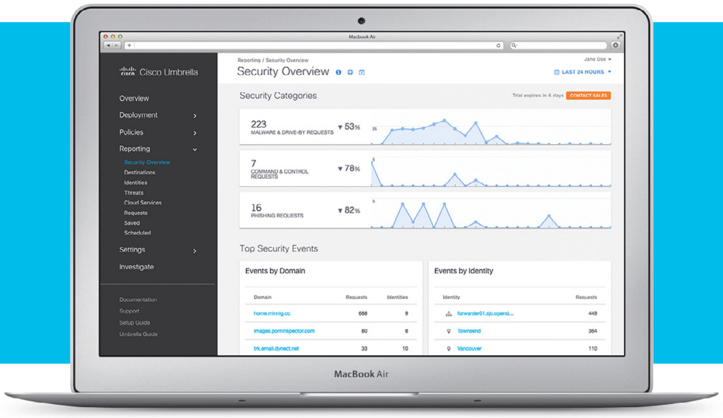
Incident response times lag when security teams don't have access to key information. Umbrella categorizes and retains all internet activity to simplify the investigation process. Using the Umbrella Investigate console and on-demand enrichment API, it provides context to prioritize incidents and speed up incident response. With Umbrella, your SOC can detect and remediate threats faster with Cisco Threat Response. It automates integrations across Cisco security products and aggregates Umbrella intelligence with other intelligence sources to empower you to get quick answers.

Improve performance

Umbrella has a highly resilient network environment that boasts 100% uptime since 2006. Using Anycast routing, any of our 30 plus data centers across the globe are available using the same single IP address, so your requests are transparently sent to the nearest, fastest data center and failover is automatic. Umbrella peers with more than 900 of the world's top internet service providers (ISPs), content delivery networks (CDNs) and SaaS platforms to deliver superior speed and user satisfaction.

Key features:

- Block domains associated with phishing, malware, botnets, and other high risk categories (cryptomining, newly seen domains, etc.)
- Prevent malware or phishing attempts from malicious websites
- Prevent web and non-web callbacks from compromised systems
- Proxy and decrypt risky domains for deeper inspection of URLs and files
- Enable web filtering using 85+ domain content categories
- Pinpoint compromised systems using real-time security activity reports
- Discover and block shadow IT (based on domains) with the App Discovery report
- Use the Investigate web console for interactive threat intel access and the on-demand enrichment API to integrate intelligence into other systems
- Protect mobile and roaming users who are off-network



Reporting / Security Overview

Security Overview

Security Categories

Trial expires in 6 days

223 MALWARE & DRIVE-BY REQUESTS ▼ 53%

7 COMMAND & CONTROL REQUESTS ▼ 78%

16 PHISHING REQUESTS ▼ 82%

Top Security Events

Events by Domain

Domain	Requests	Identities
home.minnig.cc	688	9
images.porninspector.com	80	8
trk.email.dynect.net	33	10

Events by Identity

Identity	Requests
forwarder01.sjc.opend...	449
Townsend	364
Vancouver	110

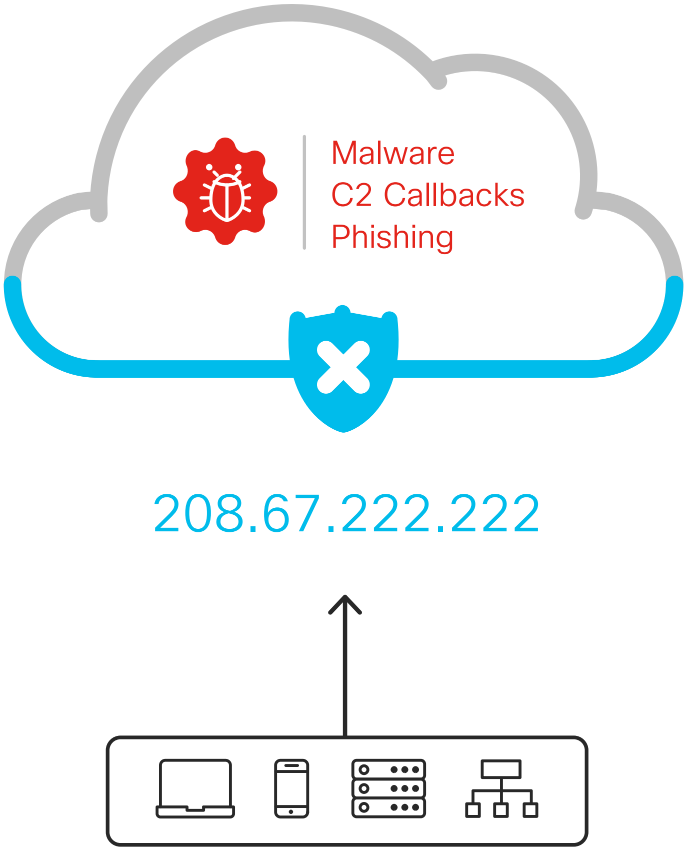
How Umbrella helps:

- Reduce malware by 75%[1]
- Reduce remediation time by 50% or more[2]
- Protect on and off-network

[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

The Cisco DNS Security Advantage

With Umbrella, you can stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration. And because it's delivered from the cloud, Umbrella provides an effective security platform that is open, automated, and simple to use.



Already using Cisco SD-WAN?

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

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

Start a free trial

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, a detailed post-trial analysis.

Deployment information

Umbrella offers APIs for network devices, management, and reporting. With the DNS Security Advantage package, you also have access to our enforcement API which enables other security services to push updates from their block list to Umbrella for extended enforcement everywhere.

On-network: Any network device (e.g. router, DHCP server) can be used to connect to Umbrella. Simply redirect your DNS to Umbrella"s IP address. That's it. You can also leverage your existing Cisco footprint – Cisco AnyConnect, Cisco routers (ISR 1K and 4K series), Cisco Wireless LAN Controllers, and Meraki MR/MX – to provision thousands of network devices and laptops in minutes.

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.