Cisco Umbrella at a glance.

In the past, desktops, business apps, and critical infrastructure were all located behind the firewall. Today, more and more is happening off-network. More roaming users. More corporate-owned laptops accessing the internet from other networks. More cloud apps, mean that users don't need to be on the corporate network to get work done. And more branch offices connecting directly to the internet.

By 2021, Gartner predicts the average company will have 25% of its corporate data traffic bypassing the network perimeter. When a user is off-network, they are more vulnerable and the organization lacks visibility and protection. If you rely on perimeter security alone, you're not fully protected. These gaps open the door for malware, ransomware, and other attacks.

The first line of defense

As a Secure Internet Gateway, Cisco Umbrella provides the first line of defense against threats on the internet wherever users go. Umbrella delivers complete visibility into internet activity across all locations, devices, and users, and blocks threats before they ever reach your network or endpoints. As a cloud-delivered, open platform, Umbrella integrates easily with your existing security stack and delivers live threat intelligence about current and emerging threats.

By analyzing and learning from internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for attacks, and proactively blocks requests to malicious destinations before a connection is even established — without adding any latency for users.

With Umbrella, you can stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration.

Enforcement built into the foundation of the internet

The Domain Name System (DNS) is a foundational component of the internet — mapping domain names to IP addresses. When you click a link or type a URL, a DNS request initiates the process of connecting any device to the internet. Umbrella uses DNS as one of the main mechanisms to get traffic to our cloud platform, and then uses it to enforce security, too.

When Umbrella receives a DNS request, it uses intelligence to determine if the request is safe, malicious or risky — meaning the domain contains both malicious and legitimate content. Safe and malicious requests are routed as usual or blocked, respectively. Risky requests are routed to our cloud-based proxy for deeper inspection. The Umbrella proxy uses Cisco Talos web reputation and other third-party feeds to determine if a URL is malicious. Our proxy also inspects files attempted to be downloaded from those risky sites using anti-virus (AV) engines and Cisco Advanced Malware Protection (AMP). And, based on the outcome of this inspection, the connection is allowed or blocked.

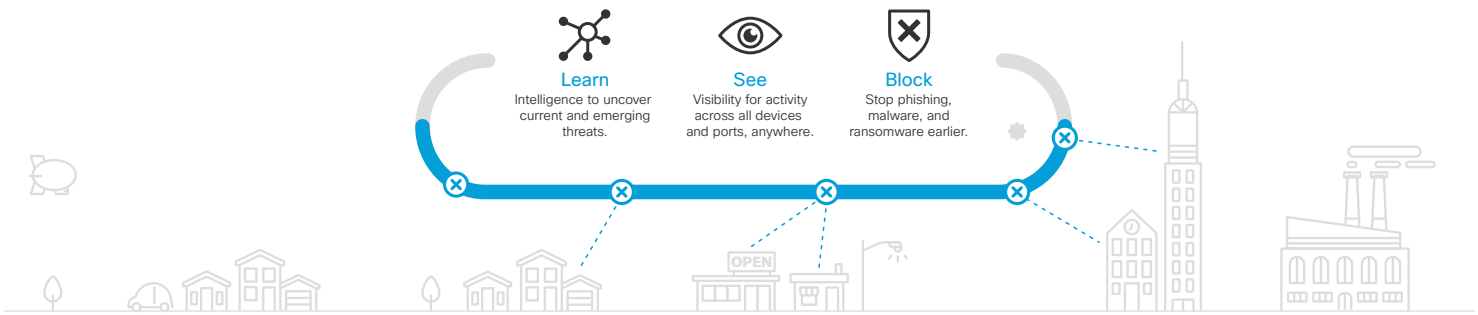
Benefits

Mitigate remediation costs and breach damage: Because Cisco Umbrella is the first line of defense, security teams will have fewer malware infections to remediate and threats will be stopped before they cause damage.

Reduce the time to detect and contain threats: Cisco Umbrella contains command & control callbacks over any port or protocol and provides real-time reports on that activity.

Increase visibility into internet activity across all locations and users: Cisco Umbrella provides crucial visibility for incident response and also gives you confidence that you're seeing everything.

Identify cloud apps used across the business: Cisco 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, and identify potential risk.



Intelligence to stop attacks before they launch

The Umbrella global network, which is the network that our recursive DNS service is built on, resolves billions of internet requests from millions of users around the world every day. We analyze this massive amount of data to detect patterns and uncover attacker infrastructure.

We ingest all of that internet activity data from our global network in real-time into our massive graph database, and then continuously run statistical and machine learning models against it. This information is also constantly analyzed by the Umbrella security researchers and supplemented with intelligence from Cisco Talos. Using this combination of human intelligence and machine learning we identify malicious sites — whether it's domains, IPs, or URLs — all across the Internet.

Plays nice with others

Umbrella integrates with your existing security stack including security appliances, intelligence platforms, and cloud access security broker (CASB) controls. Umbrella can push log data about internet activity to your SIEM or log management systems, and using our enforcement API, you can programmatically send malicious domains to Umbrella for blocking. This allows you to amplify existing investments, and easily extend protection everywhere.

Enterprise-wide deployment in minutes

Umbrella is the fastest and easiest way to protect all of your users in minutes. Because it is delivered from the cloud, there is no hardware to install or software to manually update. You can provision all on-network devices — including BYOD and IoT — in minutes and use your existing Cisco footprint — AnyConnect, Integrated Services Router (ISR) 4K Series, and Wireless LAN Controller 5520 and 8540 — to quickly provision thousands of network egresses and roaming laptops.

Next steps

Talk to a Cisco sales representative or partner about how Cisco Umbrella can help to protect your mobile, cloud-connected organization from advanced threats. Visit our page at umbrella.cisco.com to learn more.

Key Features

- Visibility and protection everywhere
- Intelligence to uncover attacks earlier
- Simple deployment and management
- Open platform for integration
- Fast and reliable cloud infrastructure

Key Numbers

- 100 billion daily internet requests
- 65 million users
- 25 datacenters worldwide
- 7M+ malicious destinations enforced concurrently at the DNS-layer

Cisco Umbrella