Cisco Umbrella

CISCO UMBRELLA

Protection outside the firewall

CISCO UMBRELLA:
Protection outside the firewall

In the early days of corporate computing, the employee desktop was hardwired to the network and located safely behind the firewall. But, today, all of that has changed. Now, a growing number of employees access the network—and the internet—from the outside, and they're using laptops, tablets and smartphones to share critical business data wirelessly.

With the rise of cloud-based aps, more and more employees are finding they don't need to log on to the corporate network to get their work done. More and more, associates are working from home or another remote location, like a coffee shop or hotel room, where public Wi-Fi is notoriously unsafe.

With the rise of cloud-based aps, more and more employees are finding they don't need to log on to the corporate network to get their work done.

And these trends aren't slowing down. Gartner predicts that by 2021, 25% of all corporate data traffic will bypass the network perimeter completely.

As alarming as that might be, these statistics are even more concerning:

82% of users bypass the VPN.

70% of branch offices connect directly to the internet.

70–90% of malware is unique to each organization.

So, if most mobile and remote workers don't always have their VPN on, and if most branch offices don't backhaul all traffic, that means the corporate network is more vulnerable to an attack.

HOW TO RESPOND

To provide a first line of defense against internet threats, regardless of where employees may access the network, Cisco created Umbrella.

Umbrella is a cloud-based, secure internet gateway that sits outside the corporate firewall and blocks threats before they ever reach your network or endpoints. It also provides complete visibility into internet activity across all locations, devices and users.

As an open platform, Umbrella easily integrates into an organization's existing security framework and provides live threat intelligence to deter emerging threats.

Umbrella can analyze and learn from patterns of attack and automatically uncover hostile infrastructures and proactively block malicious requests before they can establish any connection—with zero latency for users.

In this way, Cisco Umbrella prevents phishing, malware and ransomware infections and blocks already-infected devices to prevent data exfiltration.

HOW DOES IT WORK?

To access the internet, every computer uses the domain name system (DNS), which maps domain names to IP addresses. Clicking a link or typing a URL address initiates a DNS request and then serves up the website to whatever device is being used. Umbrella uses DNS to enforce security protocols and to connect traffic to the platform.

So, when a remote user is outside of the corporate firewall and attempting to connect to the internet, this connection typically isn't as safe. This means the company laptop may be at risk of being hacked, or of downloading malware that could later infect the corporate infrastructure when the user returns to the office, or when they attempt to log on to the network at a later time.

But, with Cisco Umbrella, users who connect to the internet are protected—even if they're outside the corporate firewalls.

Here's how it works. When Umbrella receives a DNS request, it quickly uses intelligence to determine whether the domain is safe or malicious. Safe domains are routed to the user, and malicious domains are blocked and marked for future reference.

Sometimes the domain is found to contain both safe and malicious code. In those cases, the safe content is routed, and the unsafe content is blocked and shared to the cloud-based proxy for deeper inspection via Cisco Talos—a global cybersecurity network.

Umbrella stats

65 million users

25 data centers worldwide

7+ million malicious destinations enforced concurrently at the DNS layer

98% reduction in malware infections

50% reduction in alerts from IPS, AV and SIEM

20% decrease in remediation times

#1 fastest and most reliable DNS with 65+ million daily active users

80+ billion daily internet requests or connections

80+ million daily malicious requests blocked

3+ million daily new domain names discovered

60,000+ daily malicious destinations identified

GLOBAL INTELLIGENCE NETWORK

Umbrella takes advantage of a vast global network, which resolves billions of internet requests from millions of users around the world every day. This data is analyzed to determine patterns of attack and to help identify attackers' infrastructures.

All of this data is continuously run through statistical and machine-learning models so that Umbrella security researchers can analyze it. By supplementing their findings with threat intelligence provided by Cisco Talos, malicious sites are detected, cataloged and blocked.

QUICK AND EASY INTEGRATION

Umbrella integrates with existing security stacks, appliances, intelligence platforms and cloud access security broker (CASB) controls. Because it's a cloud-based solution, there's no hardware or software to install or manually update. All on-network devices can be provisioned in minutes, including BYOD and IoT. It's also easy to use AnyConnect, Integrated Services Router (ISR) 4K Series, and Wireless LAN Controller 5520 and 8540 to quickly and easily provision thousands of network outlets and roaming laptops.

> Umbrella integrates with existing security stacks, appliances, intelligence platforms and cloud access security broker (CASB) controls.

WANT TO LEARN MORE?

To learn more about Cisco Umbrella and how it can protect users outside the corporate firewall, contact your Ingram Micro Cisco team. ciscosoftware@ingrammicro.com.