CISCO
SECURE

eBook
Cisco Public

How Modern Security Teams Fight Today's Cyber Threats

The scope of security protection has broadened

In the past, when all devices used at a company sat safely guarded within a corporate network, security meant bolstering the network perimeter with up-to-date firewalls and deploying antivirus software to stop malware that had managed to penetrate the network.

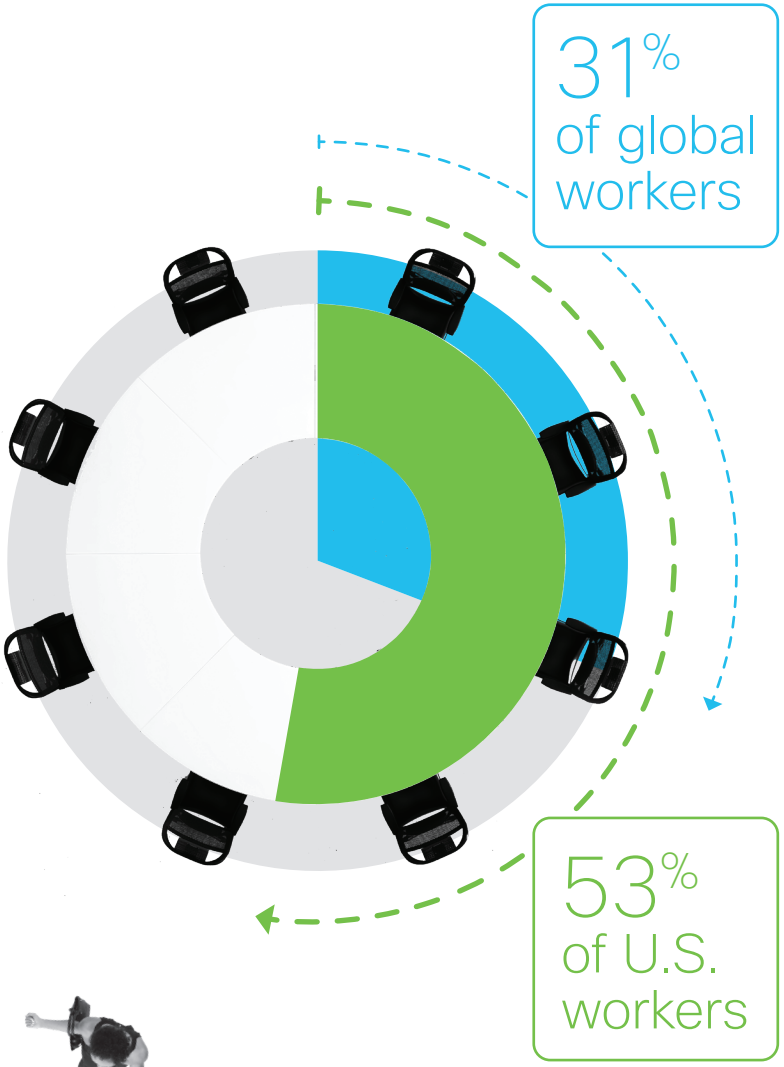
Web proxies, email gateways, and sandboxes have provided additional security support for years. As long as devices remained in network, these services stood at the frontlines, reactively repelling and ousting attacks.

But times have changed.

Users have left the building

According to Gartner, 53% of the U.S. workforce and 31% of global workers will be remote in 2022, a trend that the COVID-19 pandemic only accelerated. More off-network users increased vulnerability to threats.

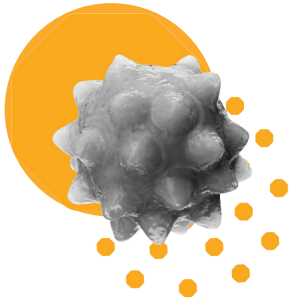
The increased adoption of hybrid work models means security teams are continually challenged to keep users connected and networks secure. Securing devices is a growing problem for organizations now unable to rely on connecting endpoints to campus networks for visibility and pushing updates. At the same time, employees are connecting to corporate resources with more personal, unmanaged devices, which creates blind spots for security teams.



Attackers continue to advance

Globally, companies have experienced a jump in cybersecurity threats or alerts during the pandemic. With users accessing the corporate network and cloud applications remotely, malicious actors tried to take advantage of potential security gaps. Thanks to this, 61% of organizations experienced a jump of 25% or more in cyberthreats or alerts since the start of COVID-19.

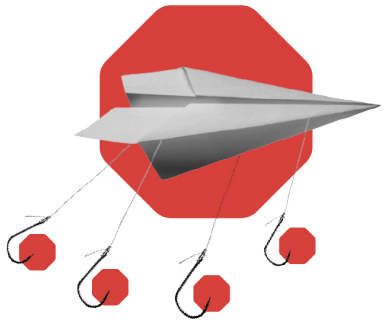
Cybersecurity threat trends data from 2021 showed that:



48% of organizations found information–stealing malware activity

50% of organizations encountered ransomware-related activity

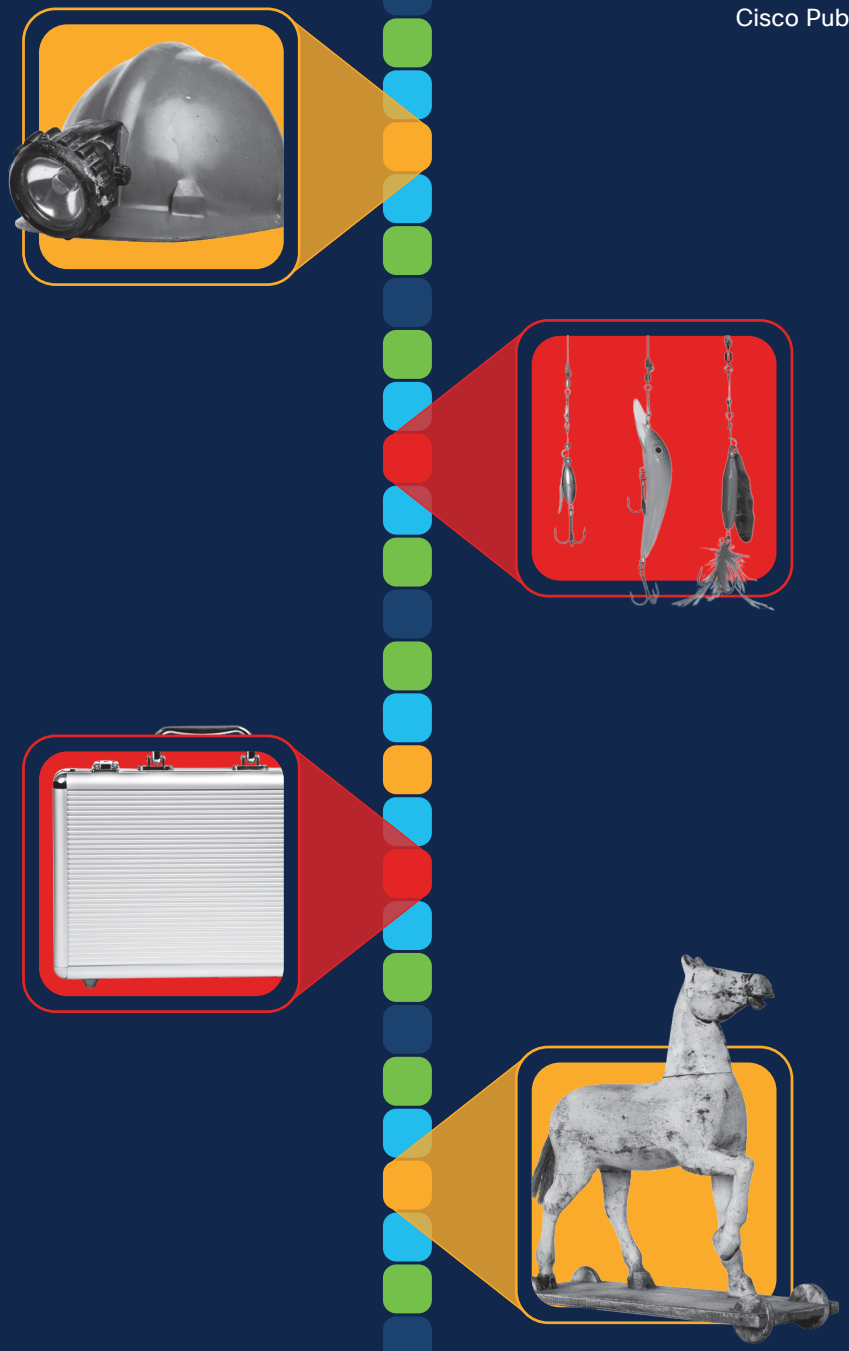
69% of organizations experienced some level of unsolicited cryptomining



86% of organizations had at least one user try to connect to a phishing site

In short, attackers continue to develop in sophistication just as workforce mobility creates new challenges for security teams.

Cryptomining, phishing, ransomware, and trojans averaged 10x the internet activity of all other threat types

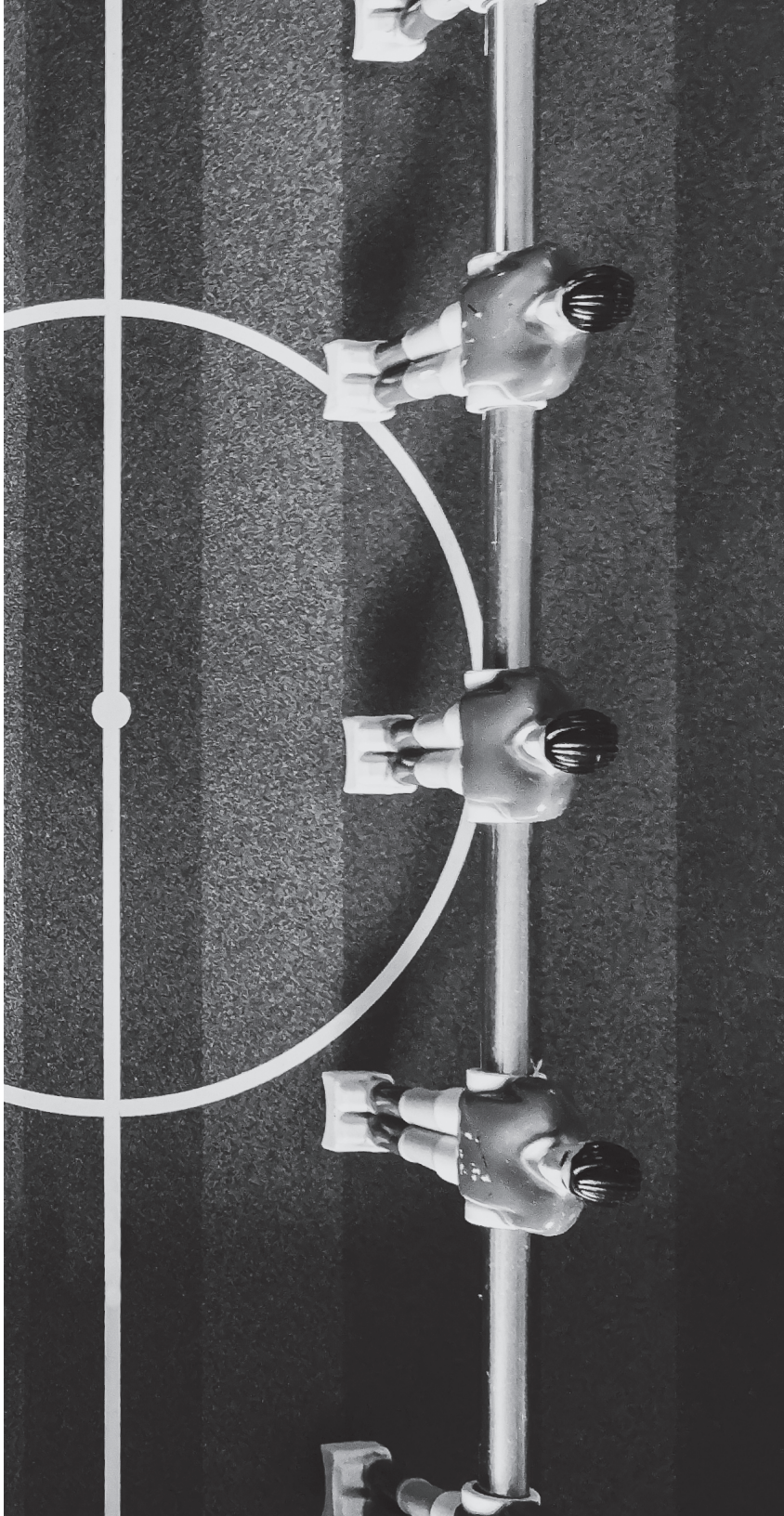


cisco SECURE

DNS-layer security is the first line of defense

DNS is a foundational component of how the internet works and is used by every device on the network – and can also be a highly effective way to enforce security. Long before a malware file is downloaded and before an IP connection over any port or any protocol is even established, there's a DNS request.

This crucial first layer blocks domains associated with malicious behavior before they get into your network. Implementing DNS-layer security tools is critical for halting attacks earlier, long before they infiltrate the perimeter.



Simpler and more effective cybersecurity builds business resilience

DNS-layer security has the added advantage of ubiquity.

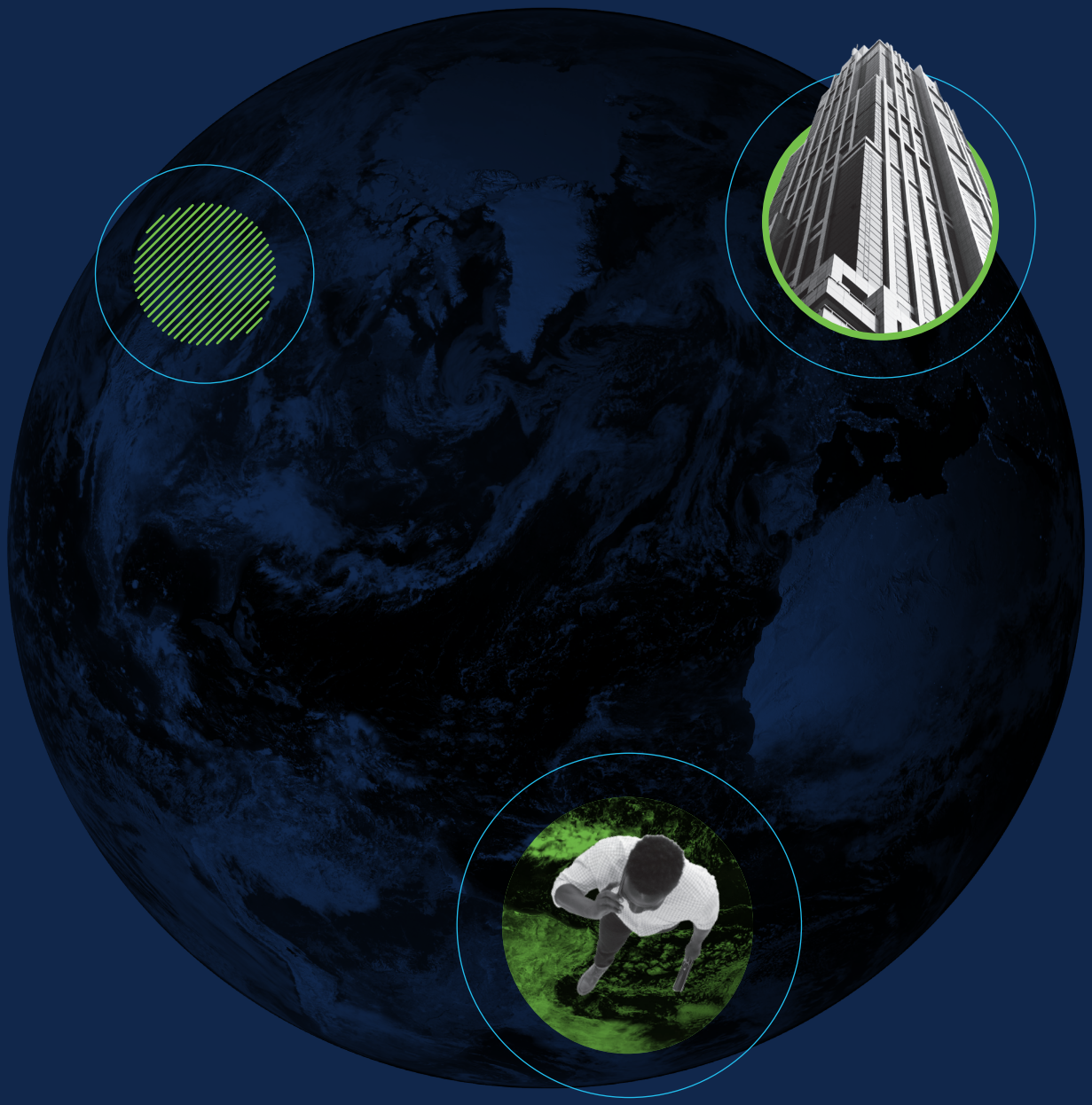
By pointing all of the organization's DNS requests – whether they come from network, endpoint, or mobile devices – at the same DNS provider, security teams can ensure that users get the same protection whether they are working on or off the corporate network.

Plus, because DNS-layer security stops attacks before they reach the network's perimeter, the number of security alerts generated by a firewall or other elements of the security stack is reduced.

> "DNS presents security and risk management leaders with some excellent opportunities to anticipate, prevent, detect and respond to prevailing threats."
>
> Craig Lawson, John Watts, Gartner 2021

Protect users anywhere and everywhere

Security teams need a way to enforce policies and protect users anywhere they work, on any device.

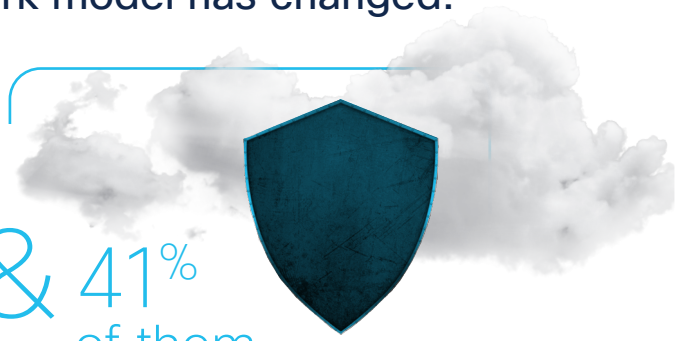


While many organizations use a VPN, users often do not turn on the VPN – either due to performance issues or because they don't need it to get their work done – and therefore aren't protected. Security teams need an easier way to enforce security everywhere.

DNS-layer protection gives security teams a cloud security solution that provides flexible security protection on and off network, consistent policies across remote locations, and better performance everywhere. This is crucial, both for teams who need to scale up their security in hybrid environments, and for security professionals who might be overwhelmed with disparate security solutions or multiple alerts across platforms.

Due to COVID, the work model has changed:

88% organizations plan to increase cybersecurity spending in 2021

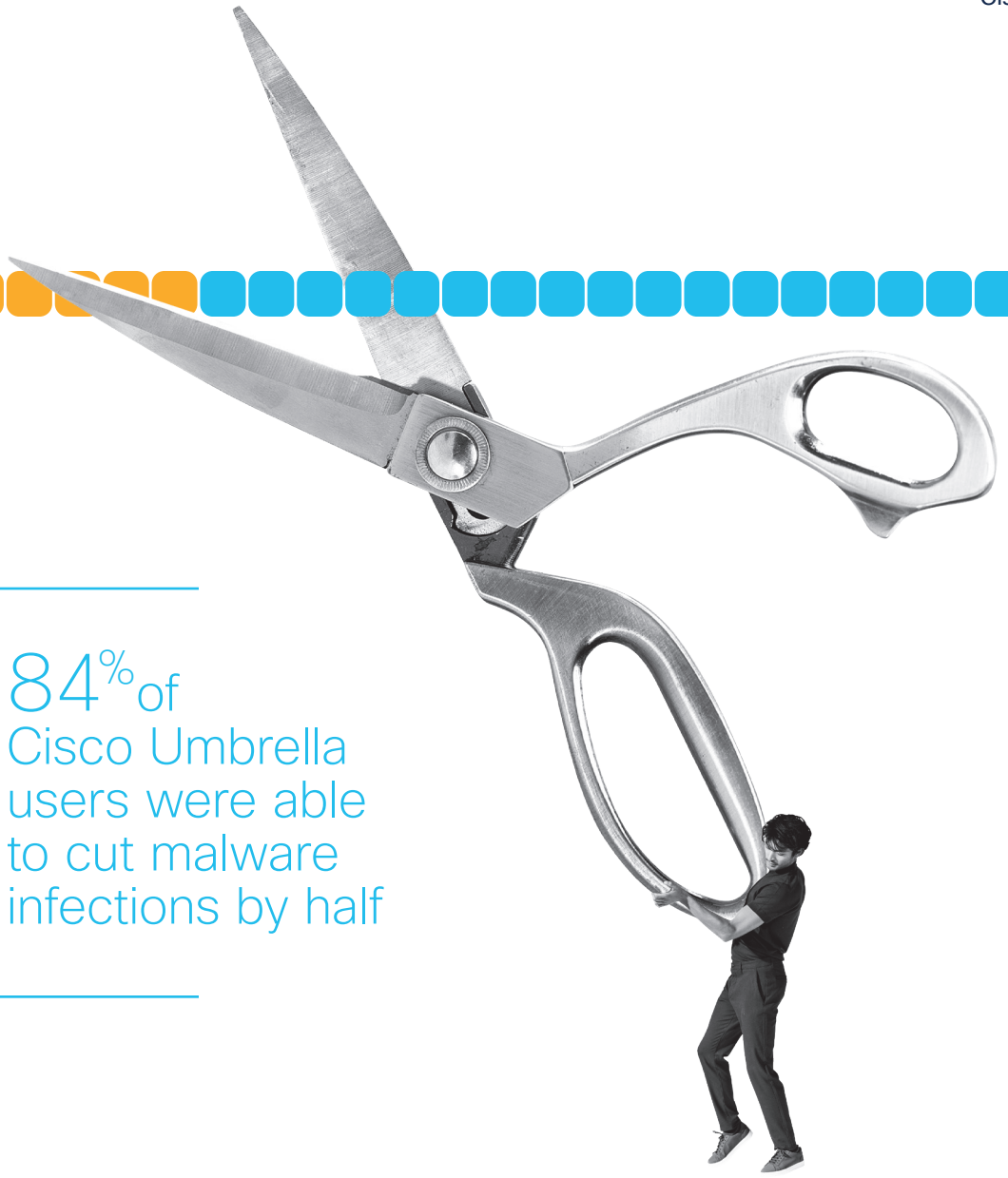


& 41% of them are prioritizing cloud security

The State of Security Report, 2021

Securing users with Cisco Umbrella

Every day, Cisco Umbrella's 35+ data centers process more than 620 billion internet requests from over 190 countries. This real-time DNS data is further enriched with data from private feeds and a handful of public ones.



Cisco Umbrella blocks more than 170 million malicious DNS queries every day and discovers more than 200 new vulnerabilities each year. These nodes of attack infrastructure are opportunities for identifying and neutralizing threat architecture before it can be used for new attacks.

With a malware detection rate of over 70% (well-beyond other DNS-layer protection solutions), Cisco Umbrella provides the global visibility, predictive intelligence, and DNS-layer protection that is indispensable to organizations and security teams today.

84% of Cisco Umbrella users were able to cut malware infections by half

cisco SECURE

Use expert intelligence to your advantage

At Cisco, we believe it's better to predict and prevent cyberattacks than to respond and remediate after they strike. To do this, security teams need tools that provide internet-wide visibility beyond corporate networks – into where attackers stage infrastructure for current and future attacks.

They also need reliable, up-to-date intelligence to fight the growing number of sophisticated threats. Most threat intelligence today is static, outdated, or incomplete, and is hardly useful ammunition in the fight against constantly evolving attackers.

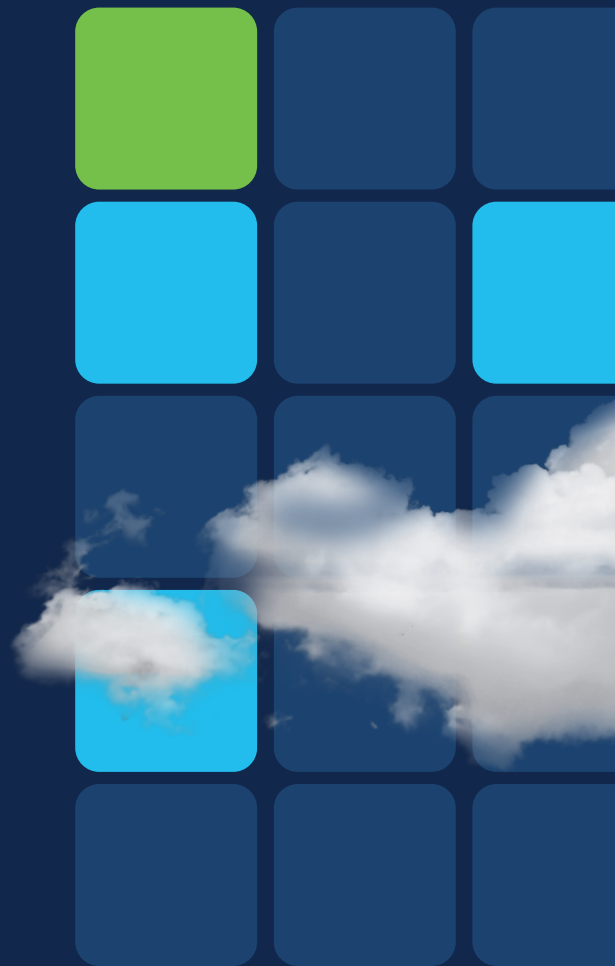
Now imagine a team of hundreds of security researchers. With Cisco Talos threat intelligence, Umbrella conducts statistical and machine learning models to uncover new attacks staged on the internet. Plus, the Umbrella Investigate console and API provides real-time context on malware, phishing, botnets, and other threats, enabling faster incident investigation and response.

Cisco Umbrella is the solution to modern security challenges

As a trusted partner of over 24,000 companies, Cisco Umbrella provides the quickest, most effective way to improve your security stack. Gain a new layer of breach protection in minutes, with internet-wide visibility on and off your network, no matter your company size.

Umbrella:

- Provides cloud-delivered security at the DNS layer, allowing security teams to protect any device on your network.
- Can prevent initial infections, contain command-and-control callbacks, and stop data exfiltration from already infected devices.
- No hardware to install or software to maintain.
- Logs all Internet activity and offers API-based integrations with your current security stack to extend protection everywhere.



Try it out for 14 days.

Start a free trial