

EBOOK

The Cisco Umbrella Advantage

The freedom to work securely – anywhere and everywhere.

 Cisco Umbrella



Get the freedom to work anywhere.

Remote workers. Branch offices. An ever-expanding perimeter. You're likely dealing with these challenges while you fight to contain cyber threats and protect your users – and your company. But you're not alone.

In the past, most – if not all – of the apps and infrastructure we used at work sat behind a firewall. Employees came into a physical office and logged into the network to start working. Today, “the office” can be anywhere: A coffee shop. Public transit. A remote destination. And what's happening to your perimeter? It's expanding and blurring. Remote workers are bypassing the VPN. Data is bypassing perimeter security and flowing directly from mobile devices and apps to the cloud. Traditional security just can't keep up.

That's where Cisco Umbrella comes in. We've built a reputation on easy deployment and powerful protection anywhere users go, on or off network. Why? So you can build your security on a solution you can trust. Simply point your DNS to the global Umbrella network, and your entire organization is covered in minutes. Powered by predictive intelligence, Umbrella acts as your first line of defense against threats. With Umbrella DNS-layer security, you can see threats before they're coming, and block them before they become attacks. Read on to learn how this unique advantage can make a difference for your organization.

Not all cloud security solutions are created equal.

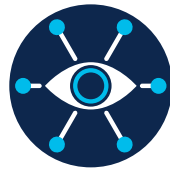
You'll want to look for a solution that meets the needs of today's remote, cloud-connected workforce, and is easy to manage on a day-to-day basis.



Complete threat protection

Block requests to malicious destinations before a connection is even established. You need to protect proactively – without adding any latency.

[Learn more >](#)



Visibility anywhere and everywhere

Get the visibility you need to protect internet access across devices, office locations, and roaming users – even off VPN.

[Learn more >](#)



Intelligence to see attacks before they happen

Automatically identify where attacker infrastructure is being staged by using the power of security research, Cisco Talos intelligence, and statistical models to learn from internet activity patterns.

[Learn more >](#)



Integrations to amplify your existing investments

Extend protection for devices and locations beyond your perimeter, reduce security alerts, and enrich your incident response data to remediate threats faster, before damage occurs.

[Learn more >](#)



The most effective security, deployed in minutes

Get up and running in minutes. No hardware to install. No software to manually update. 100% business uptime. And the most effective security available.

[Learn more >](#)

“Cisco Umbrella has reduced [our] overall infection rate... On average, we were seeing 20,000 blocked malicious alerts a day, and using Umbrella, we have been able to target those infected hosts and trim that number down to less than 100.”

-IT Architect, S&P 500 Electronics Company¹



Secure your network with DNS-layer security.

Most security solutions focus on reducing the time it takes to detect and defend against threats. But are they preparing you for emerging threats or attacks that are still in the staging process? You need fast, effective security that blocks threats and secures users anywhere they access the internet.

Use the internet to your security advantage.

More than 91% of malware uses DNS to gain command and control, exfiltrate data, or redirect web traffic.² Cisco Umbrella uses the internet's infrastructure to stop threats over all ports and protocols, effectively stopping malware before it reaches your endpoints or network. Using statistical and machine-learning models to uncover both known and emerging threats, Umbrella proactively blocks connections to malicious destinations at the DNS and IP layers. And because DNS is a protocol used by all devices that connect to the internet, you simply point your DNS to the Umbrella global network, and any device that joins your network is protected. So when your users roam or access SaaS apps, your network stays secure.

Proactive DNS-layer security, as easy as 1, 2, 3:



1

Block dangerous connections between your users and malicious domains



2

Stop command-and-control (C2) callbacks and data exfiltrations – easily



3

Reduce security incidents and alerts by neutralizing them before they occur



“Cisco Umbrella gives us more confidence in our ability to proactively protect our customers and employees, and more efficiency in our incident response process.”

-Vivek Raman, Head of Security, Yelp

See and protect anywhere users go.

Easily secure Direct Internet Access (DIA).

If you're like most companies, your branch offices connect directly to the internet instead of backhauling traffic to headquarters – which can be a nightmare for the security team. It's a resourcing hassle to keep appliance-based tools updated. They can't scale up as more users work off network. And you're left with limited or zero visibility into the threats targeting those users. You need to protect internet access across all devices, office locations, and roaming users – even when they're off VPN.

Manage and control cloud apps.

Umbrella provides visibility into sanctioned and unsanctioned cloud services in use across your business, so you can uncover new applications being used, see who is using them, identify potential risk, and easily block specific applications. Even when users are off VPN, they're secured with Cisco Umbrella, taking the stress off your security team.

Secure remote workers with the fastest, most reliable cloud infrastructure.

Boasting 100% uptime since 2006, Umbrella uses Anycast routing to ensure all of our 30-plus data centers around the globe are available under the same single IP address. 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, effective security, and user satisfaction.





“Cisco Umbrella is truly a first line of defense; it gets rid of most of the bad things out there at the DNS layer and for any port/protocol. I like the fact we can secure branches and distributed locations that don’t have the same security stack as our HQ.”

-System Integrator, Medium Enterprise Computer Software Company²

Block attacks before they happen.

Your security is only as good as the intelligence informing it. But traditional threat intelligence is reactive, basing security on information gathered only after an attack is successfully carried out. With threats increasing in sophistication and speed, you need intelligence that can learn from internet activity patterns, automatically identify attacker infrastructure being staged for the next threat, and block those threats before they have the chance to attack your organization.

Goodbye, reactive security. Hello, predictive intelligence.

With Cisco Umbrella, you can take a proactive approach to blocking threats. We gather data on attackers' techniques and infrastructure, so you can better detect and understand attacks. Take advantage of live threat intelligence that we pull from global internet activity and analyze in real time with a combination of statistical and machine learning models and human intelligence.

Turn intel into action.

Powerful threat intelligence could become information overload without the infrastructure to act on it. Umbrella has that horsepower, actively processing and enforcing more than 7 million unique malicious domains and IPs concurrently at the DNS layer. Every day, Umbrella analyzes 200 billion internet requests, and 60,000+ new destinations are added to our block list. Simply put, with Umbrella, you're going to see – and block – what other security solutions miss.

Our view of attacks



The secret behind the statistics.

Our models do more than reputation scoring. Umbrella analyzes both historic and live data to categorize the “guilt” of domains and IPs into three main approaches: guilt by inference, guilt by association, and patterns of guilt. And with models automatically scoring and classifying data, you can detect anomalies and uncover both known and emerging threats, faster than ever before.



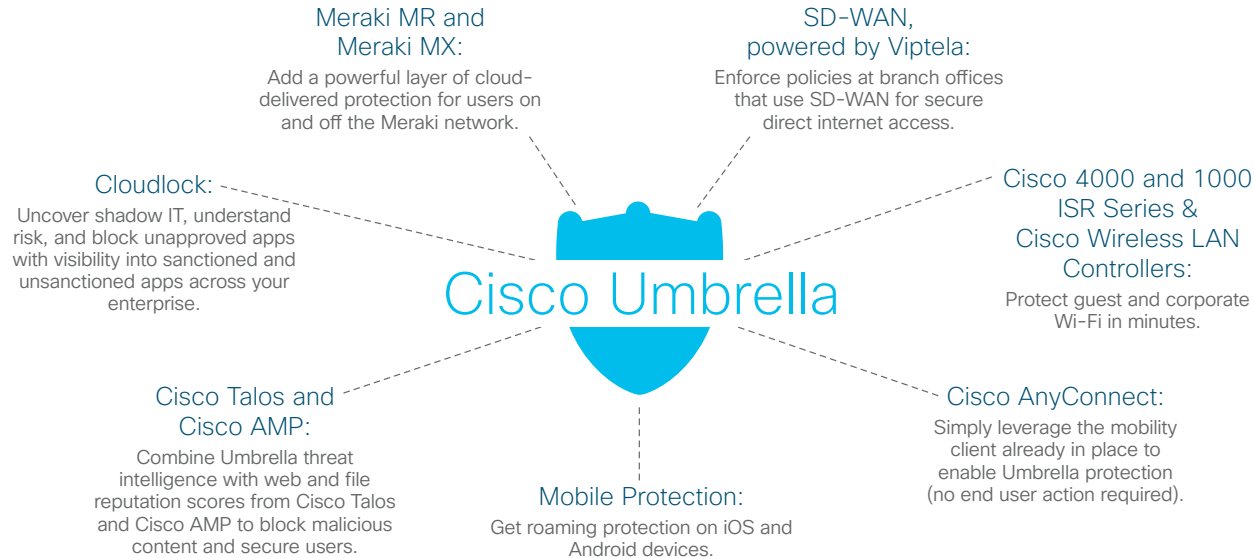
“Cisco Umbrella enhances the other layers we have here. Our email spam tool might let something through, but many times Umbrella catches it anyway.”

-Engineer, Large Enterprise Energy & Utilities Company²

Amplify your existing investments.

Glitchy integrations. Hundreds of hours of professional services help. Siloed intelligence data. If you're using traditional security tools, you're probably having trouble getting your systems to talk to each other. The truth is, the best security comes from an integrated defense. You need a solution that works with your existing stack and local intelligence, so you can enrich incident response data and easily extend protection to devices and locations beyond your perimeter.

Take advantage of the Cisco Security ecosystem.

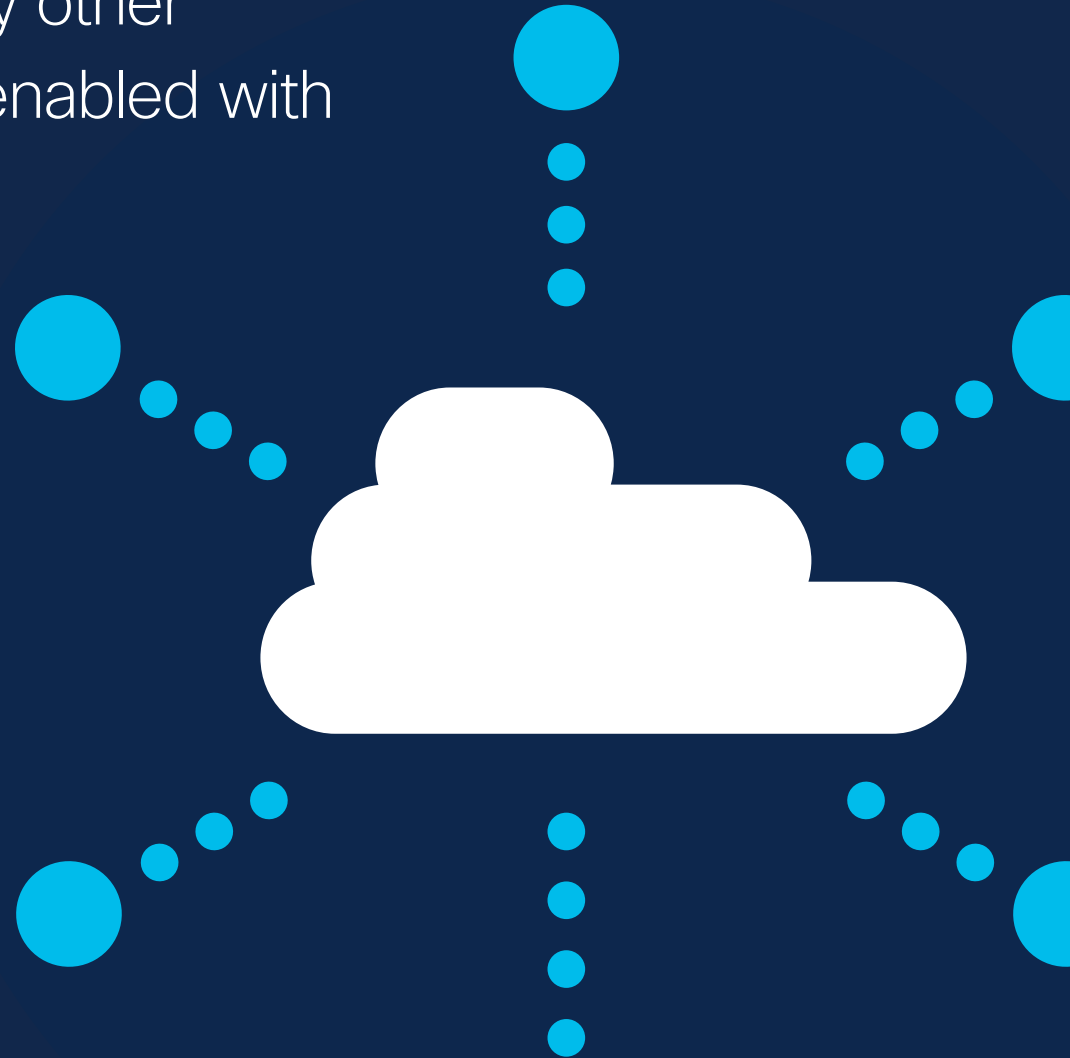


Work with
(not against)
your security stack.

Dealing with security appliances? Threat intelligence platforms or feeds? Custom, in-house tools? Cisco Umbrella uses bidirectional APIs to integrate and amplify your existing security investments, extending protection beyond your perimeter. Plus, you can tap into pre-built integrations with more than 10 security providers (including Splunk, FireEye, and Anomali) and manage up to 10 custom integrations.

“By far Cisco Umbrella is the biggest bang for the buck, including how easy it is to implement. There aren’t many other products out there that can be enabled with about an hour’s worth of work.”

-CIO, Educational Institution²



Deploy enterprise-wide in minutes.

Users are working anywhere and everywhere, and they no longer need the VPN to be productive – they just use cloud services. You need a fast, easy way to protect users anywhere they access the internet. And you need it now. Not in three months.

Deploy in minutes. Never miss a threat again.

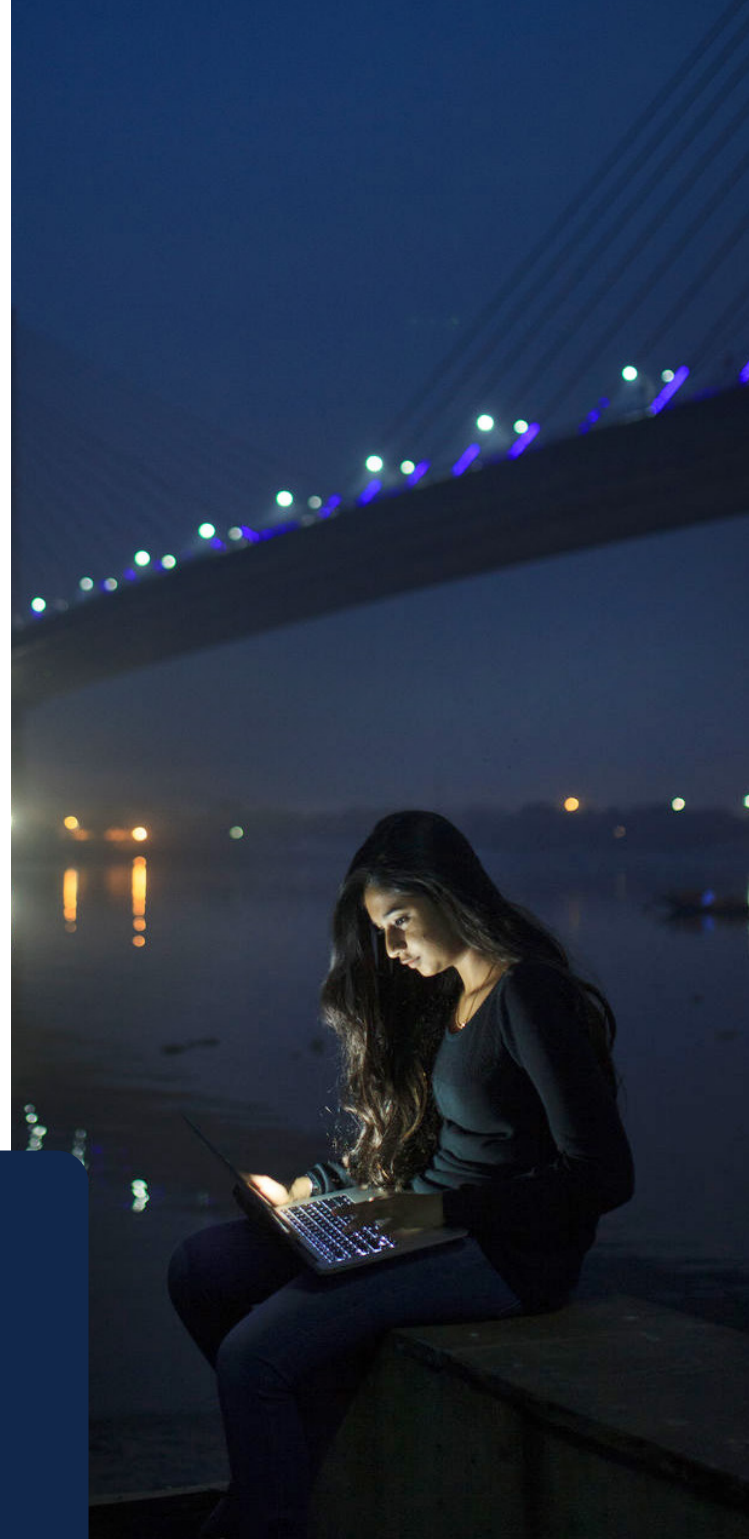
Security can't wait, so we've made it our mission to get you up and running in minutes, with 100% business uptime. When your security is delivered via the cloud, there's no hardware to install or software to manually update, making it easier on your security team to deploy and manage. We use DNS as the main mechanism to get traffic to our platform for inspection. And because DNS is a protocol used by all devices that connect to the internet, you don't have to introduce any new processes or break existing ones. You simply redirect your DNS to Umbrella. That's it.

Quick deployment for powerful security.²

79% of respondents realized value from Cisco Umbrella in less than one week.

72% of customers reduced investigation time by 50% or more.

#1 outcome achieved with Cisco Umbrella was improvement in security efficacy.



Block threats others miss.

Recently, the independent security organization, AV-TEST, conducted a study of threat efficacy among leading cloud security vendors. Cisco Umbrella significantly outperformed the competition with a 51% detection rate for DNS-layer protection. And Cisco Umbrella takes threat protection even further, increasing the blocking rate to 72% with selective proxy.

Unmatched threat intelligence.

Cisco Umbrella leverages 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 often used in attacks. We also feed huge volumes of global internet activity into a combination of statistical and machine learning models to identify new attacks being staged on the internet.

The result? Umbrella uncovers and blocks malicious domains, IPs, and URLs before they have the opportunity to attack your network.

AV-TEST places Cisco Umbrella first in threat detection.⁴

Vendor	Detection Rate Number of test cases 3,668
Cisco Umbrella (DNS-layer with selective proxy)	72.6%
Cisco Umbrella (DNS-layer)	51.8%
Infoblox BloxOne	35.3%
Akamai Enterprise Threat Protector	26.5%
Palo Alto Networks Next-Generation Firewall	13.7%

The economic value of DNS security.

Research conducted by Global Cyber Alliance estimates \$100B - \$200B global losses could have been prevented by DNS-layer security.³

Cisco Umbrella: Your first line of defense against threats.

Built into the foundation of the internet, Umbrella is a cloud service that delivers complete visibility into internet activity across all locations, devices, and users. We help you see and block threats before they ever reach your network or endpoints.

By analyzing and learning from internet activity patterns, Umbrella automatically uncovers attacker infrastructure staged for current and emerging threats, and proactively blocks requests to malicious destinations before a connection is established.

The Umbrella Global Network Advantage

200B+

daily DNS requests
(over all ports and protocols)

5,000+

peering sessions

100M+

global daily active users

20K+

customers

30+

data centers across five continents

190

countries worldwide

900+

partnerships with top ISPs and CDNs

Cisco Umbrella delivers the most secure, most reliable, and fastest internet experience to more than 20,000 customers. As a leading provider of network security and recursive DNS services, we enable the world to connect to the internet on any device with confidence.

Get worldwide threat protection in minutes. Try it out for 14 days.

[Start free trial](#)

Sources:

- <https://www.techvalidate.com/product-research/cisco-umbrella>
- <https://umbrella.cisco.com/blog/2016/01/21/cisco-security-report-more-orgs-should-be-monitoring-dns/>
- <https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf>
- <https://learn-umbrella.cisco.com/analyst-reports/av-test-dns-layer-protection-and-secure-web-gateway-security-efficacy-test-results>