EBOOK

The Umbrella Advantage: What Makes Cisco Umbrella Unique

Secure all the places your company reaches – on or off the grid.

cisco

Cisco Umbrella

Freedom to work anywhere.

Mobile 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. Enterprises around the globe are grappling with the transition to the cloud and what that means for network security.

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. Users 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, 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.

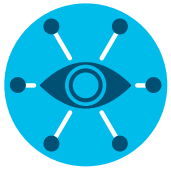
Not all cloud security solutions are created equal.

You'll want to look for a solution that meets the needs of today's mobile, 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

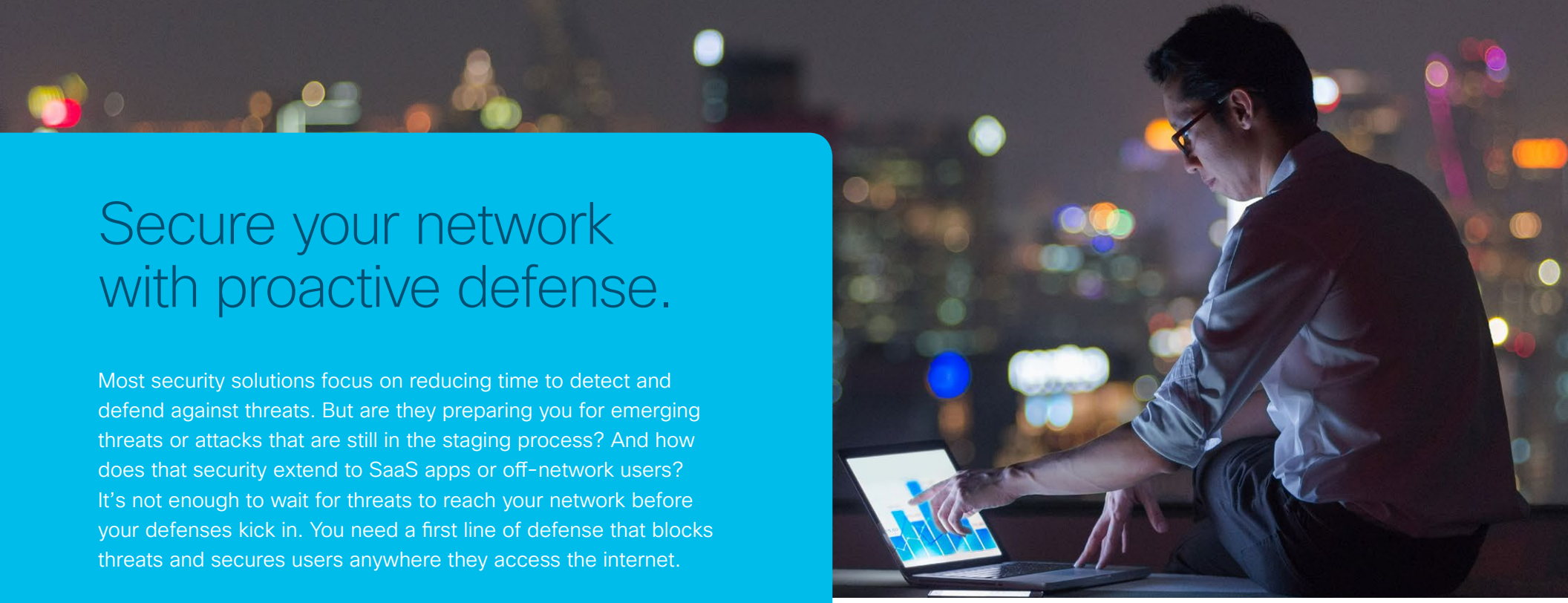
Enterprise-wide deployment in minutes

Get up and running in minutes. With 100% business uptime. No hardware to install. No software to manually update.

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 Company[2]



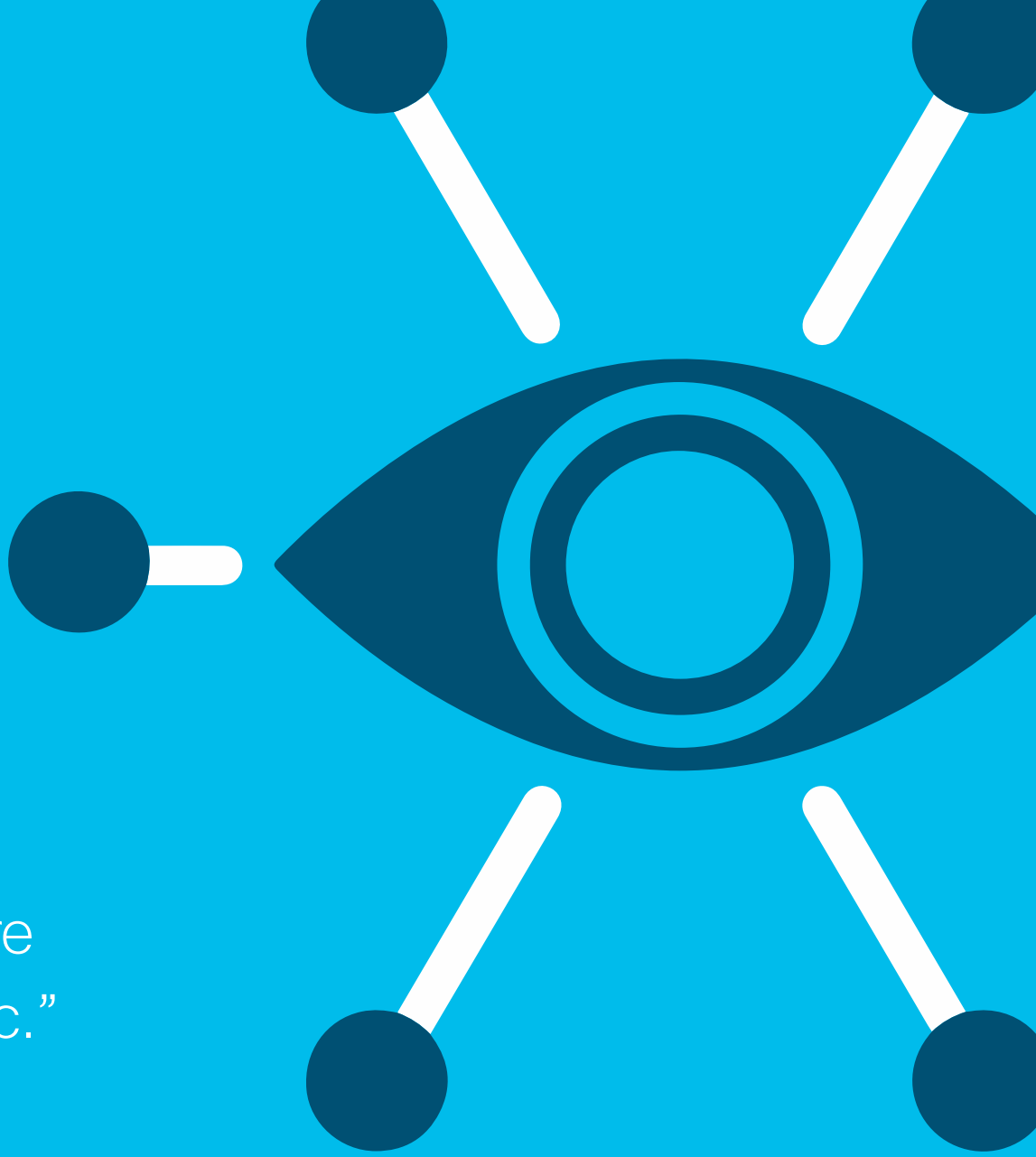
Secure your network with proactive defense.

Most security solutions focus on reducing time to detect and defend against threats. But are they preparing you for emerging threats or attacks that are still in the staging process? And how does that security extend to SaaS apps or off-network users? It's not enough to wait for threats to reach your network before your defenses kick in. You need a first line of defense 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.[1] 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, your network stays secure.

Umbrella enforces more than 7 million malicious destinations at any given time at the DNS layer — without adding any latency.



"Cisco Umbrella added an additional layer of security to our network and gave us more visibility into our internet traffic."

–IT Manager, Healthcare Organization[2]

See and protect anywhere users go.

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.

Gain visibility into cloud apps used across your business.

Uncover new SaaS apps being used, see who's using them, and identify any potential risk. With visibility into sanctioned and unsanctioned cloud services in use across your enterprise, you can finally see what's happening at every level of your organization – and block any app that poses a risk. Take that visibility a step further: Cisco Umbrella also exposes the full extent of shadow IT in your organization. You can easily drill down into app categories and risk levels, and block applications altogether, when necessary. And even when users are off VPN, they're secured with Cisco Umbrella, taking the stress off your security team when users roam.

Breathe easy with the fastest and most reliable cloud infrastructure.

For some solutions, better security means slower internet. But you won't experience broken or slow connections when using Umbrella. Powered by Anycast routing, all our data centers announce the same IP address. This means requests are sent to the fastest available data center – with automated failover – so you aren't waiting for a resolution. And with more than 700 peering partnerships with ISPs and CDNs that provide shortcuts between every network, Umbrella resolves requests even faster. Like most of our customers, that means you'll likely experience a boost in internet speed. Great security should never slow you down.

"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 Company[2]

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.

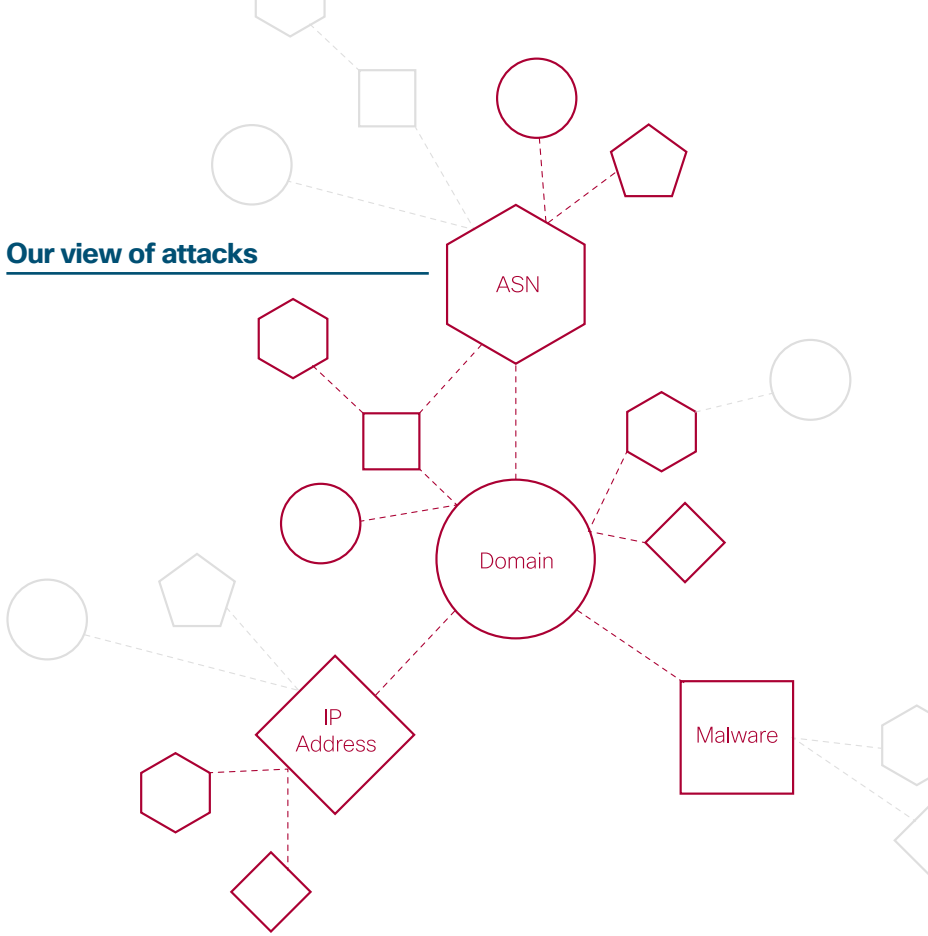
Goodbye, reactive security. Hello, predictive intelligence.

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

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 175 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.

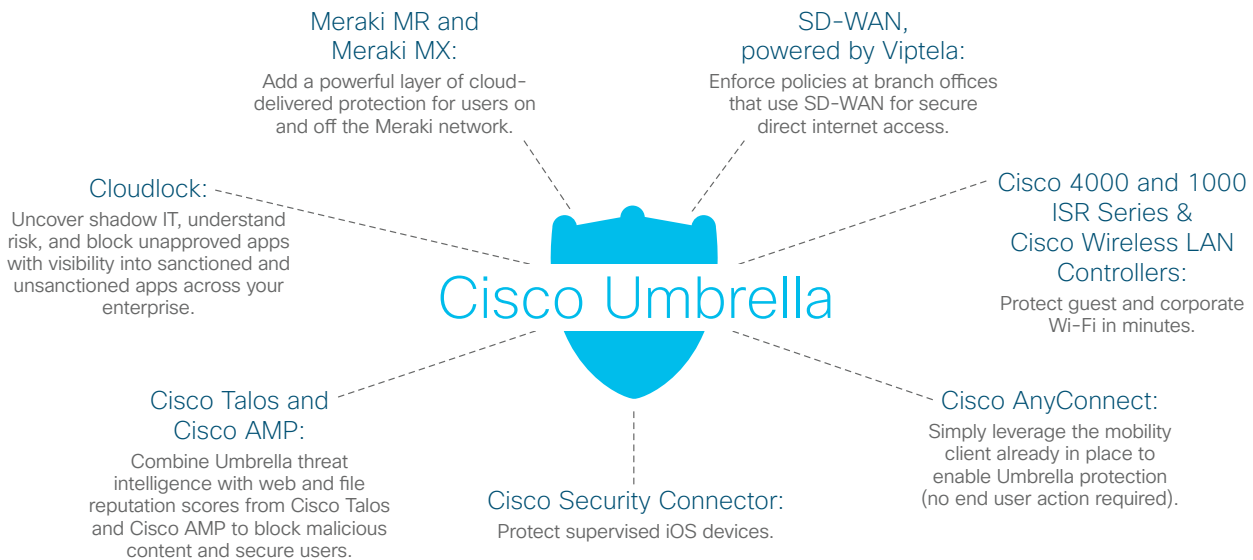
"Cisco Umbrella enhances the other layers we have here. Our email spam tool might let something through, but many times Umbrella catches it anyway."

-Engineer, Large Enterprise Energy & Utilities Company[2]

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.

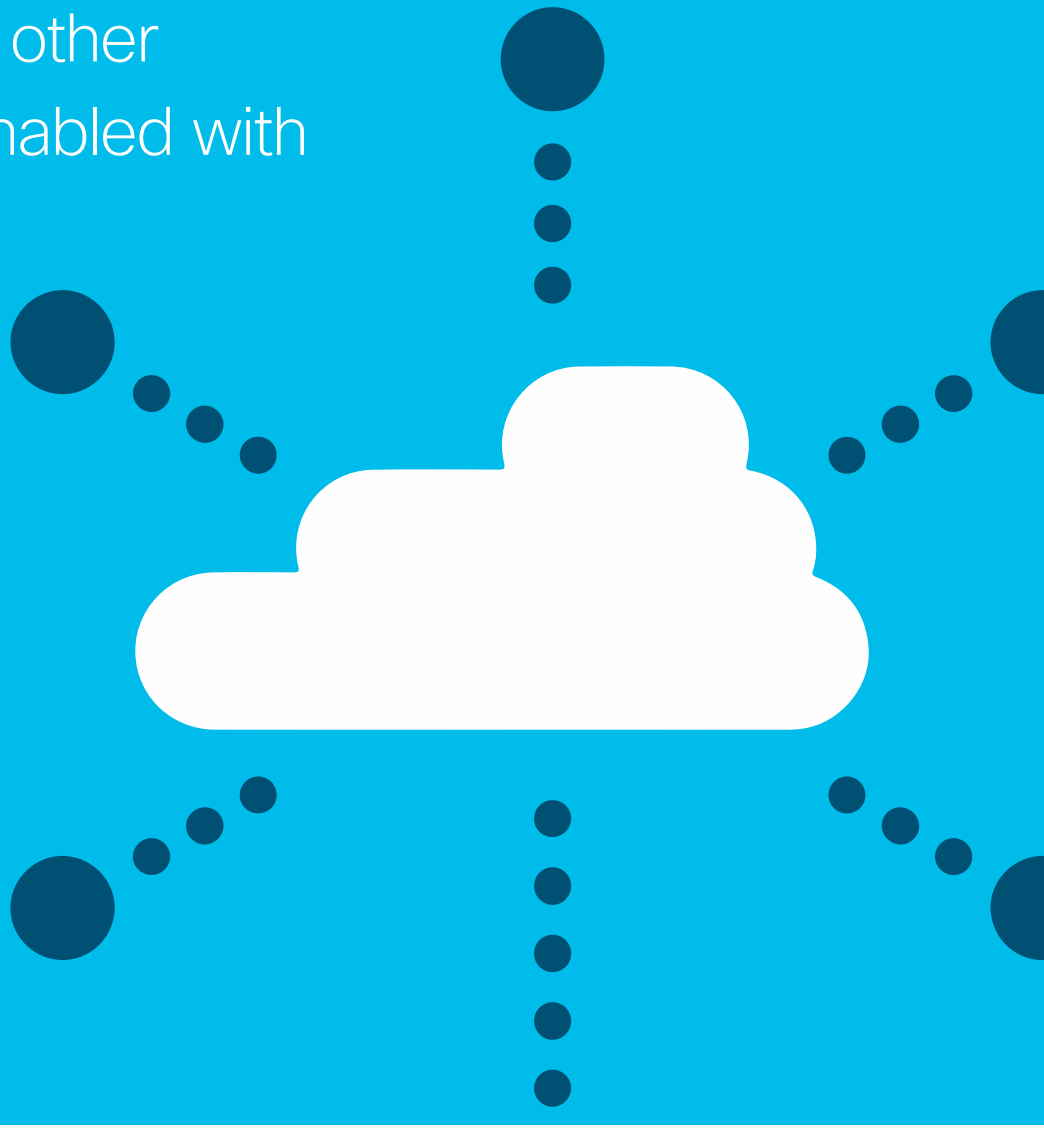


Work with (not against) your security stack.

Cisco Umbrella was built with a bidirectional API to easily integrate with other systems. Dealing with security appliances? Threat intelligence platforms or feeds? Custom, in-house tools? They're all compatible. That means you can extend protection beyond your perimeter and amplify investments you've already made. 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, meaning you'll never be working with a disjointed security stack.

"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 Institution[2]

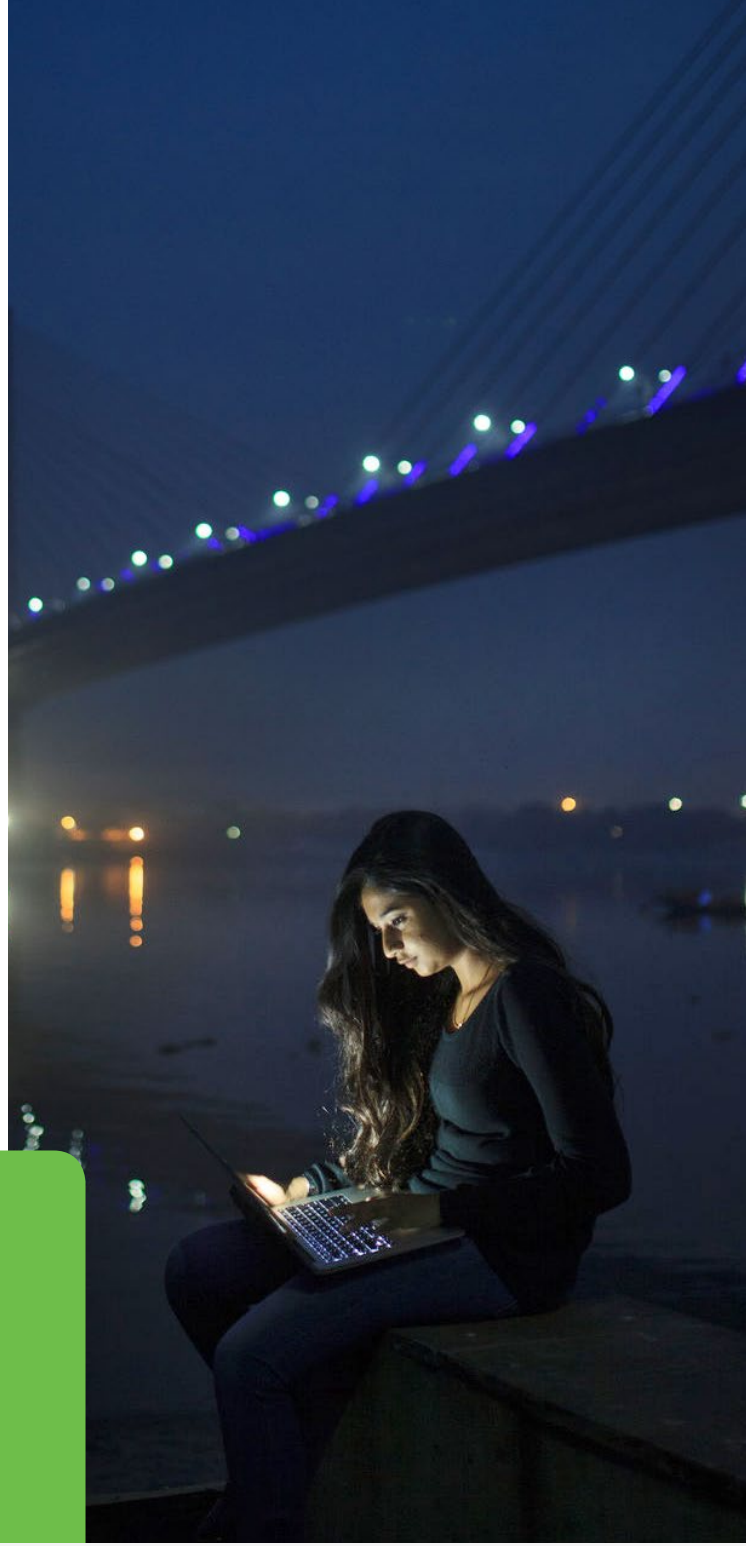


Deploy enterprise-wide in minutes.

Users are working anywhere and everywhere, and they no longer need the VPN to be productive – they just use cloud services. There's cloud security promising quick deployment, but if those solutions take months to get to the edges of your network, you're leaving your enterprise vulnerable in the meantime. 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. Then you can 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.



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.

Cisco Umbrella: Your first line of defense against threats.

Built into the foundation of the internet, Umbrella 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.

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

The Umbrella Advantage

175B
daily DNS requests
(over all ports and protocols)

715
partnerships with
top ISPs and CDNs

90M
global daily active users

3,900
peering sessions

30
data centers across five continents

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

Start free trial

Sources:

1. https://umbrella.cisco.com/blog/2016/01/21/cisco-security-report-more-orgs-should-be-monitoring-dns/
2. https://www.techvalidate.com/product-research/cisco-umbrella