Cisco Umbrella

Cybersecurity eBook
Cisco Public

7 ways to strengthen your security in 2022 and beyond

Discover how to extend protection beyond your network with Cisco Umbrella

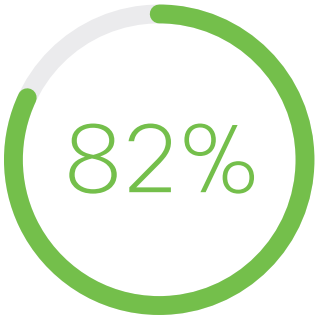
cisco The bridge to possible

Firewalls. Web proxies. SIEM. Appliances. CASB. Third-party intelligence.

A typical company uses, on average, dozens of security vendors (and some use many, many more) to manage their cybersecurity.[1]

Even with all those point products, sometimes you still find your stack lagging behind when it comes to securing users where they access the internet. The definition of "where" continues to expand, as companies move to hybrid work environments and organizations scramble to secure their cloud perimeters, as well as individual users and locations.

Strengthening your security stack doesn't mean a massive overhaul or a loss of customization and control. Here are 7 ways to amplify and extend your stack with cloud security from a single solution — Cisco Umbrella.



of company leaders plan to allow employees to work remotely at least some of the time.[2]

7 ways to extend your protection:

1. Integrate your stack
2. Resolve issues smarter
3. Detect more threats
4. Secure your guests
5. Accelerate network speeds
6. Strengthen your infrastructure
7. Defend from end-to-end

1 Integrate your existing solutions and extend protection

Security appliances. Threat intelligence platforms. Custom in-house tools. You've already made investments in your security stack. It's time to amplify them with the most open cloud security service in the industry.

Built with a bidirectional API, Cisco Umbrella security easily integrates with the other systems in your stack. You can extend protection from on-premises security appliances to devices and sites beyond your perimeter — and amplify investments you've already made.

Convert local threat detection and intelligence from existing systems into global threat prevention to protect branch offices, remote workers, off-network users, and guests. You can also take immediate action on indicators of compromise to reduce the time between detection and prevention from days to seconds.

Open APIs

Umbrella offers pre-built integrations with more than 10 security providers, including Splunk, IBM, FireEye, and Anomali. You can also take advantage of custom integrations to create the end-to-end security solution you've been missing.

2 Resolve issues with better intelligence for better decisions

Your team doesn't need more alarm bells. They need the context behind each alert, to better prioritize, understand, and remediate issues. Cisco Umbrella can help you make faster, more-informed decisions when you need to respond to critical incidents and research potential threats.

Use the Investigate bi-directional API to share data across your systems and pull contextual threat intelligence into your security management or incident response environment. The enriched data about domains, IPs, file hashes, etc. used in attacks speeds investigations, pinpoints attacker infrastructure, and predicts future threats more effectively.

Umbrella gives you the exact context you need

- Malware file analysis
- DNS request patterns
- Related domains
- Attribution
- IP geolocation
- Domain, IP, and ASN relationships
- Passive DNS database
- WHOIS
- Domain and IP reputation

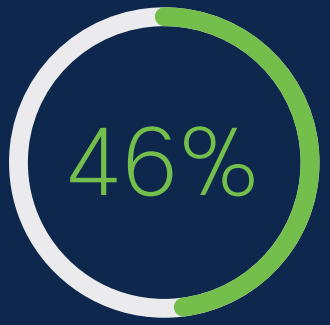
3 Detect more threats to improve threat protection

AV-TEST recently conducted a threat efficacy test of leading cloud security vendors. Cisco Umbrella's secure web gateway (enhanced with DNS security) and DNS-layer protection functionality significantly outperformed competitors with a 96.39% total threat detection rate.[3]

Cisco Umbrella leverages intelligence from Cisco Talos, one of the largest commercial threat intelligence teams in the world, to uncover and block a spectrum of malicious domains, IPs, URLs, and files used in attacks. We also feed volumes of global internet activity into statistical and machine learning models to identify new internet-based attacks more effectively.

AV-TEST places Cisco Umbrella first in threat detection.[3]

Product	Package	Detection rate	False positive rate
Cisco Umbrella	**SIG essentials**	**96.39%**	**0.65%**
Zscaler Internet Access	Transformation	89.67%	0.69%
Palo Alto Networks Prisma Access	Prisma Access for Mobile Users	73.15%	1.29%
Netskope Secure Web Gateway	NG-SWG	61.90%	4.53%
Akamai Enterprise Threat Protector	Advanced Threat	58.43%	1.89%
Number of test cases		3,572	2,165



of organizations had a security incident caused by an unpatched vulnerability. Those with a major breach due to an unpatched vulnerability experienced higher levels of data loss.[4]

"Umbrella provides not only risk reduction but also visibility into the type of threats within our customer's environments, as well as those users that are more active risks. This helps us identify areas to improve user training, lock down additional information, and reduce overall risk to the customer."

Line of Business Manager, Small Business Telecommunications Equipment Company

4 Secure your guests and improve Wi-Fi experiences

Guests on your Wi-Fi want fast Wi-Fi access. Their experience, though, shouldn't allow them to download copyrighted material or view inappropriate content from your network. Or worse, connect to malicious sites and compromise their identities – or your organization's proprietary information.

You need secure, compliant guest Wi-Fi that won't slow down their connections. Cisco Umbrella extends your protection to guests by enforcing network security and content filtering at the DNS layer. Whether you need to secure one, two, or ten thousand hot spots, you can protect them all in minutes by pointing DNS traffic to the global Umbrella network.

With Umbrella, you only need one IP address for your entire enterprise, making it easy to secure guest Wi-Fi in a few steps.

Better protect your guest Wi-Fi access while you:

- Manage policies from a single dashboard
- Gain visibility across all users and endpoints
- Aggregate real-time activity across all Wi-Fi hot spots
- Ensure security and compliance.

Umbrella helps you prevent malware, command and control callbacks, and phishing from compromising guests' devices or stealing guests' identities – over any port, protocol, or app.

Secure and compliant guest Wi-Fi in minutes

"It took less than 10 minutes for us to point our DNS traffic to the Umbrella global network. We could protect our remote offices around the world in less than an hour and a half."

Mark Arnold, Director of Information Security, PTC 6

5 Accelerate network speeds

Security teams are always searching for that perfect balance: implementing stronger cloud security without slowing down performance. Through Anycast routing and our many peering relationships, we deliver high-availability enterprise-grade web filtering and network security without added latency or the need for extra hardware or software.

Anycast Routing

Cisco Umbrella delivers fast, secure internet access across all endpoints using Anycast routing. Every data center announces the same IP address, so requests are transparently routed with automated failover to the fastest server available at the time.

And since every device associated with your organization connects to our IP address, you can protect every endpoint and connection while eliminating latency for users, even when they're off-network.

Peering Relationships

Umbrella peers directly with more than 1,000 organizations to reduce hop count and increase performance. Through more than 6,000 peering sessions with partners, Umbrella creates shortcuts to major internet cloud providers, reducing latency and improving the connection between our customers and their networks.

"Umbrella has given us time-savings due to automation, improvement in operational efficiencies via integrations, breaches averted, threats blocked, faster alerting, and productivity improvements."

Prashanth Anandam, Network Administrator, IKS Health

6 Strengthen your infrastructure and reduce disruptions

Umbrella was built for the cloud, to deliver speed and flexibility, with microservers that use containers for efficiency. We own, actively manage, and tune our own equipment. This focus ensures consistent, unmatched performance, and our optimal usage of hybrid multi-cloud infrastructure minimizes traffic latency.

Plus, Cisco Umbrella Anycast routing infrastructure not only provides speed, it also delivers unparalleled reliability. You get a more resilient system: a global, self-healing network that can handle infrastructure disruptions – natural disasters, equipment failure, or maintenance – without passing on the interruption to your organization.

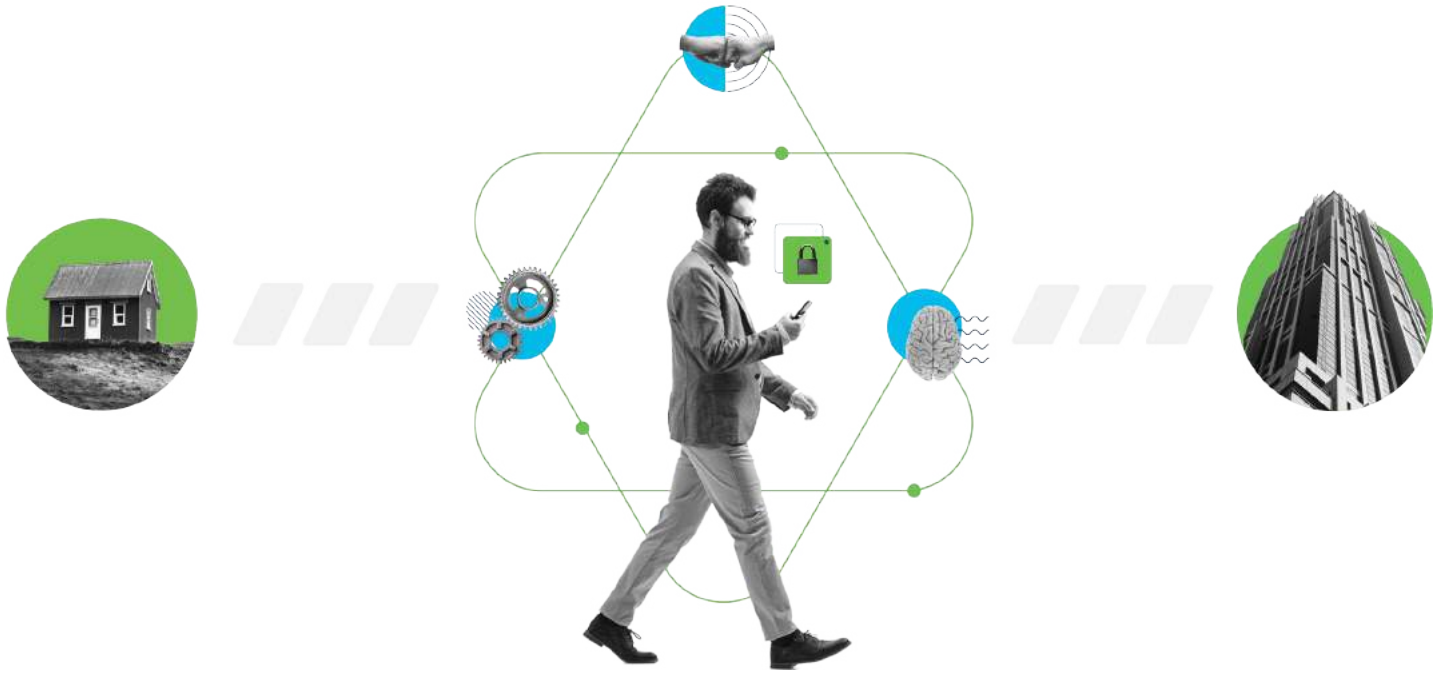
In a performance evaluation by Miercom Labs, Umbrella reduced hop count by up to 33% and improved latency and traffic consistency by up to 73%.[5]

7 Defend from end to end with the power of the entire Cisco security portfolio

Security solutions should work together to help you better defend your organization and respond faster when issues arise.

Our networking and security solutions are built on the principles of integration, intelligence, and automation. Global companies trust our solutions daily to enforce policies, protect and control cloud apps, and keep their networks and endpoints safe from threats.

With Secure X, you can instantly see what's most important across all your control points. In one view you can check on metrics, emerging threats, and products to try, as well as explore the opportunities of our built-in automated workflows.



An ecosystem of security at your fingertips.

Cloudlock

API-based (out-of-band) CASB visibility and protection including user behavior, data, and app security for your most important SaaS apps.

Cisco Talos & Cisco Secure Endpoint

Combine Umbrella threat intelligence with web and file reputation scores from Cisco Talos and Cisco AMP to block malicious content and secure users.

Meraki MR & Meraki MX

Add a powerful layer of cloud-delivered protection for users on and off the Meraki network.

SD-WAN, powered by Viptela

Enforce policies at branch offices that use SD-WAN for secure direct internet access.

Cisco 4000 & 1000 ISR Series & Cisco Wireless LAN Controllers

Protect guest and corporate Wi-Fi in minutes.

Cisco AnyConnect

Leverage the existing mobility client to enable Umbrella protection (no end user action required).

Mobile Protection

Get roaming protection on Chromebooks, iOS, and Android devices.

Secure Access Service Edge (SASE)

Our portfolio crosses networking, security, and observability, and it's uniquely positioned to help you move your hybrid environment to a SASE solution.

Amplify security and extend protection with Cisco Umbrella

Cisco Umbrella offers flexible, cloud-delivered security when and how you need it. Combining multiple security functions into one solution, you can extend protection to devices, remote users, and distributed locations anywhere. It's the easiest way to take your cybersecurity to new levels and effectively protect your users everywhere in minutes.

See for yourself how Cisco Umbrella amplifies your existing security investments.

Try Umbrella for free for 14 days and start blocking the threats others miss.

Start your free trial

The Umbrella Global Network advantage

628B+
daily DNS requests
(over all ports and protocols)

100M+
global daily active users

35+
data centers across
five continents

1,000+
partnerships with top
ISPs and CDNs

6,000+
peering sessions

24k+
customers

Sources:

1. Cisco, *Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020*, February 2020
2. Gartner, *Gartner Survey Reveals 82% of Company Leaders Plan to Allow Employees to Work Remotely Some of the Time*, July 2020
3. Cisco, *DNS-Layer Protection & Secure Web Gateway Security Efficacy Test*, February 2020
4. Cisco, *Securing What's Now and What's Next: 20 Cybersecurity Considerations for 2020*, February 2020
5. Cisco, *Cisco Umbrella Performance Validation by Miercom Labs*, October 2020