Cisco Umbrella

Ebook

How to streamline cloud security and embrace SASE

Protect remote users and offices with Cisco Umbrella

Work anywhere with confidence

The world is making a massive shift towards a more distributed workforce – and, with recent global events, the trend is only accelerating. People now work anywhere and everywhere, from any and every device. But now, with data bypassing centralized security, protecting these users – and your company – from cyber threats is all the more challenging.

Securing today's "work anywhere" organization requires a new, integrated approach – one in which networking and security functions are synchronized in a single, unified service that delivers protection and performance wherever employees access the internet or cloud applications.

Cisco Umbrella – a key component of Cisco's secure access service edge (SASE) architecture – integrates multiple standalone security services and appliances into a single, centrally managed, cloud-native solution. By unifying security functions, Cisco Umbrella helps reduce the resources required for deployment, configuration, and integration. And, by delivering this functionality from the cloud, you can scale to meet the needs of a remote and roaming workforce, shifting network perimeter, and multi-cloud environment – all while simplifying security.

Read on to discover the critical criteria you should consider as you evaluate your cloud security needs – and see what Cisco Umbrella does to protect users wherever they work.

Not all cloud security solutions are created equal

With greater security challenges come greater security requirements. As you begin to consider cloud security solutions, you'll want to keep in mind a number of core requirements. These must-haves will ensure that you can meet the needs of today's remote and roaming, cloud-connected workforce.

Look for a solution with:

Reliable Architecture

Providing consistent speed and performance at any scale, anywhere.

Robust Threat Intelligence

Gathering rich global data to see and stop threats before they become attacks.

Proven Protection

Demonstrably detecting more threats for greater security efficacy.

Unified Management

Monitoring and responding to threats from one centralized dashboard.

Flexible Integration

Working in tandem with both current and future security solutions.

Invest in a solid global cloud architecture

The need

Beyond the obvious need for strong security features and functionality, you're also looking for a cloud security solution that will deliver speed, reliability, and scalability for your organization – all of which are grounded in its underlying cloud architecture. How this architecture is designed, built, and enhanced will directly impact your business.

How Cisco Umbrella delivers

At its core, Cisco Umbrella is backed by containerized, multi-tenant architecture, battle-hardened to provide consistent, scalable performance around the globe. Cisco Umbrella has been running container workloads in production for more than 6 years – longer than any other cloud security vendor. With 30,000 worldwide production containers carrying security traffic at scale, Cisco Umbrella's compute and network can self-heal, using capabilities like a global load balancer and auto scale to transparently resolve issues and devise workarounds. This allows us to continuously and seamlessly provide new capabilities without business downtime.

Rock-solid reliability and lightning-fast performance

1,000+ peering partnerships with top ISPs, CDNs, and SaaS platforms for fastest route

6,000 peering sessions create shortcuts to major ISPs, decreasing latency by 73%

Augmented traffic rerouting automatically protects customers from outages

Carrier-neutral data centers chosen purely on best connections and quality services

Meets common security compliance standards for ISO27001/SOC2 and GDPR

Cisco Umbrella peering partnerships

Alibaba.com · box · facebook · amazon · Google · Microsoft · verizon · salesforce · NETFLIX

See and protect users on any device, anywhere

The need

With today's users accessing data and apps both on and off network, security now needs to be everywhere at once. To truly cover your team, you need to bring security functions together in the cloud, so you can get them to wherever your users work. And you need a solution with visibility that extends from edge to edge, yet is easily centrally monitored and managed, so you can keep up with every user, every app, and every threat.

How Cisco Umbrella delivers

Cisco Umbrella provides multi-function security delivered to all your users in a single cloud service. With Cisco Umbrella, you get the protection and the visibility your business needs to stay on top of your biggest security challenges.

Easily secure Direct Internet Access (DIA)

When your branch and roaming users connect directly to the internet instead of backhauling traffic to headquarters, it can be difficult to get visibility into the threats targeting users, to scale up as more users work off network, and to keep protection updated with appliance-based tools. You need to protect internet access across all devices, locations, and users – even when they're off VPN. Cisco Umbrella lets you introduce robust security across hundreds of DIA devices in minutes, keep tabs on all of your users, and always provide the most up-to-date protection.

Manage and control cloud apps

More and more users rely on cloud-based or SaaS apps to do their work from anywhere. Cisco Umbrella provides visibility into both the sanctioned and unsanctioned cloud services in use across your business, so you can uncover new apps being used, see who is using them, identify potential risk, and easily block specific apps.

Block attacks with the best threat intelligence in the industry

The need

Your security is only as good as the intelligence informing it. But, traditional threat intelligence is reactive, basing security on info gathered only after a successful attack has occurred. With threats increasing in sophistication and speed, you need intelligence that can stay ahead of attacks – learning from internet activity patterns, automatically identifying the attacker infrastructure being staged for the next threat, and blocking those threats before they have the chance to affect your organization.

How Cisco Umbrella delivers

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. Live threat intelligence is pulled from global internet activity and analyzed in real time with a combination of statistical and machine learning models and human intelligence. Cisco Umbrella then uses that intelligence to help you stop threats faster and catch the attacks other security solutions miss.

The brains behind the intelligence

The Cisco Talos Intelligence Group is one of the largest commercial threat intelligence teams in the world, backed by world-class researchers, analysts, and engineers. The team uses unrivaled telemetry and statistical and machine learning models to provide accurate, rapid, and actionable insight for Cisco customers and services. Talos defends users against known and emerging threats, discovers new vulnerabilities in common software, and stops threats in the wild before they can further harm the internet at large.

Every day, Cisco Umbrella:

Protects **>24,000** global daily active users

Blocks **>150 million** DNS queries

Identifies **>60,000** new malicious destinations (domains, IPs, and URLs)

Resolves **>620 billion** DNS requests

Discovers **>3 million** new domains

Enforces and blocks **>7 million** malicious domains and IPs

Cisco Umbrella

"We're stopping a lot of attacks with Cisco Umbrella before they're capable of being weaponized at the application layer. We're blocking tens of thousands of connection attempts on a regular basis – certainly more than we were before."

Mike Mills, Security Engineer, Farm Credit

Choose a solution with proven performance against threats

The need

How a security service provides protection is important — how well that solution protects you matters even more. You need a platform with a proven track record of tried-and-tested threat detection and security efficacy — and if it's backed by third-party validation, all the better.

How Cisco Umbrella delivers

Recently, AV-TEST, an independent security organization, conducted a study of threat efficacy among leading cloud security vendors. Cisco Umbrella received top marks across the board, with a 96.39% total detection rate, the highest in the industry.[1] The end result? Umbrella better uncovers and blocks malicious domains, IPs, and URLs before they have the chance to attack your network.

Cisco Umbrella also demonstrated a significantly lower false positive rate than competitors. With fewer false leads, security analysts can work more efficiently and effectively to protect your employees.

AV-TEST places Cisco Umbrella first in threat detection[1]

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

For every security challenge

The need

Working with an assortment of different security solutions is taxing for security teams – an array of screens to monitor, integrations to build, and workflows to create and keep up with. You need a solution with the ability to not only bring these security functions together, but make them work well together, with shared data, simplified and automated workflows, and a unified interface that's easy to manage.

How Cisco Umbrella delivers

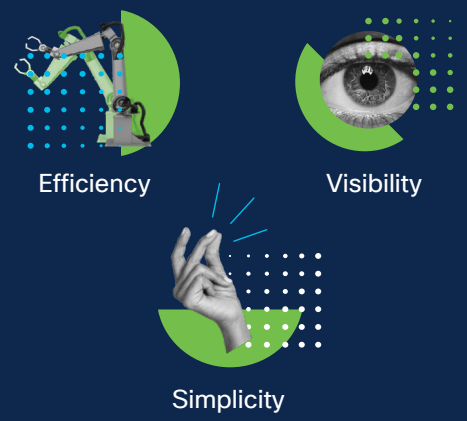
Included with Cisco Umbrella is Cisco SecureX, a cloud-native XDR platform that connects the Cisco security portfolio with your infrastructure to create a simpler, more consistent experience. Compiling security data from across our products and a wide range of third-party security solutions, Cisco SecureX provides context on threats and attacks, accelerates incident investigations, and automates the steps it takes to remediate issues.

By centralizing information in one place, Cisco SecureX gives you greater visibility and improved operational efficiency, radically reducing threat dwell time and the manual tasks it takes to stay compliant and counter attacks.

Cisco Umbrella, meet Cisco SecureX

Cisco Umbrella offers visibility into cloud applications and internet activity across every location, device, and user, on and off network – even when not connected to a VPN. By analyzing and learning from internet activity patterns, Cisco Umbrella can automatically uncover the attack infrastructure for current and emerging threats, and proactively block requests to malicious destinations before a connection is established. This information is then shared with Cisco SecureX to enrich investigations and quickly block the source of attacks.

Together, with unified visibility, faster response times, and a reduction in manual workflows, Cisco SecureX and Cisco Umbrella help reduce the time, money, and resources it takes to investigate and remediate incidents.



Build on existing security investments

The need

Stuck using glitchy integrations? Can't benefit from intelligence trapped in silos? The truth is, the best security comes from a united and 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.

How Cisco Umbrella delivers

Connecting Cisco Umbrella to other solutions in our portfolio, you can provide even more robust protection for your organization. Data from each product is shared across all our other services – this means more comprehensive visibility and even automated actions, where a threat seen by one solution is blocked everywhere else.

Cisco Umbrella uses bidirectional APIs to integrate and amplify your existing investments, extending protection beyond your perimeter. Plus, you can take advantage of pre-built integrations with a variety of security providers (including Splunk, FireEye, and Anomali) as well as up to 10 custom integrations.

Take advantage of the Cisco Security ecosystem:

Cisco Secure Client (formerly AnyConnect):
Simply leverage the mobility client already in place to enable Umbrella protection (no end user action required).

Cisco SD-WAN, powered by Viptela:
Enforce policies at branch offices that use SD-WAN for secure direct internet access.

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

Cisco Secure Endpoint (formerly AMP for Endpoints):
Combine Umbrella threat intelligence with web and file reputation scores from Cisco Talos and Cisco AMP to block malicious content and secure users.

Cisco 4000 and 1000 ISR Series & Cisco Wireless LAN Controllers:
Protect guest and corporate Wi-Fi in minutes.

Cisco SecureX:
Connect the Cisco Secure platform and your security infrastructure in one simplified experience, improving visibility and efficiency.

Cisco Secure Access by Duo:
Secure applications and data at scale with powerful multi-factor authentication (MFA) and advanced endpoint visibility.

Cisco Malware Analytics:
Examine and sandbox files so they can be safely analyzed, then block any new attempts to download these files if they're malicious.

Simplify security with Cisco Umbrella

Cisco Umbrella is a cloud-native security service that unifies a variety of security solutions to help businesses of all sizes secure their network.

Cisco Umbrella includes:

DNS-layer security

Offers the fastest, easiest way to improve your security. Stops threats over any port or protocol before they reach your network or endpoints. Helps improve visibility, detect compromised systems, and protect your users on and off the network.

Secure web gateway (SWG)

Logs and inspects web traffic for complete visibility, URL and application controls, and protection against malware. Lets you use IPsec tunnels, PAC files, or proxy chaining to forward traffic to our cloud-based proxy to enforce acceptable use policies and block advanced threats.

Cloud access security broker (CASB) functionality

Provides application visibility and control (with category blocking, individual app block/allow capabilities, tenant controls, and granular activity controls). Includes App Discovery, which lets you see which cloud apps are in use, view app details and risk information, and enforce specific controls.

Threat intelligence

Provides a unique view of the internet with unprecedented insight into malicious domains, IPs, and URLs. Includes Cisco Umbrella Investigate (available via console and API), which provides real-time context on malware, phishing, botnets, trojans, and other threats, enabling faster incident investigation and response.

SD-WAN integration

Allows you to easily deploy cloud security and protection across your network, branch users, connected devices, and apps.

Cloud-delivered firewall

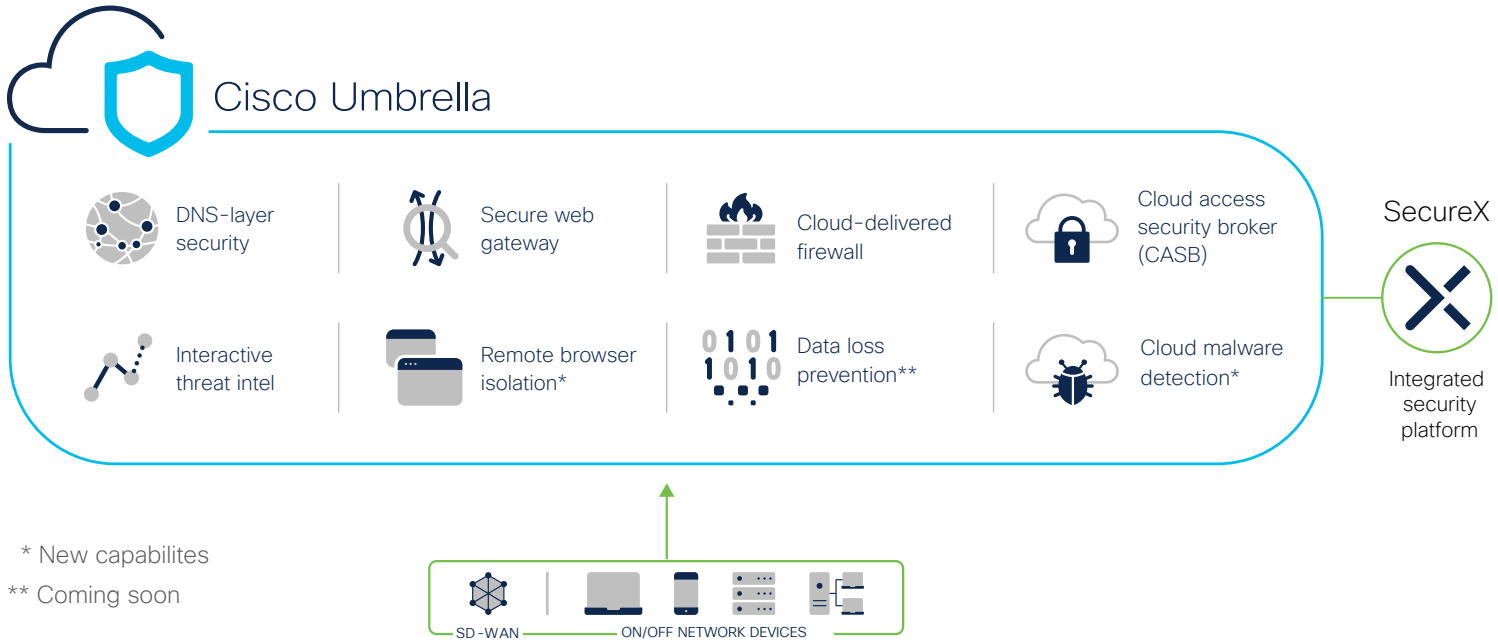
Provides visibility and control for outbound internet traffic across all ports and protocols. Logs all activity and blocks unwanted outbound traffic using IP, port, and protocol rules (layer 3 / 4) and with application visibility and control (layer 7). Allows you to forward traffic by configuring an IPsec tunnel from any network device.

Always focused on your security – today and tomorrow

Since 2006, Cisco Umbrella has delivered reliable, proven protection for over 24,000 customers. From our start as a leading DNS security provider to our growth into a multi-function cloud-native security service, we continue to evolve and innovate. Now, we're innovating again to deliver a simpler, more secure, and more scalable security service for our customers – one that can adapt to meet your changing needs and take advantage of future advancements.

A full suite of protection

Cisco Umbrella supports your SASE journey with an integrated line up of security solutions consolidated in the cloud, delivering flexible security that can scale as your needs evolve.



New and coming soon: Always improving how we protect you

Introducing our newest features and a robust line-up of “coming soon” functionality so your remote workers and offices are even more protected, wherever they are.

New features

Remote browser isolation (RBI) – Get a secure browsing experience with protection from zero-day threats and browser-based attacks by isolating web traffic from user devices. You’ll improve productivity, as well as reduce alerts and helpdesk. Deploy rapidly and choose from three levels of protection.

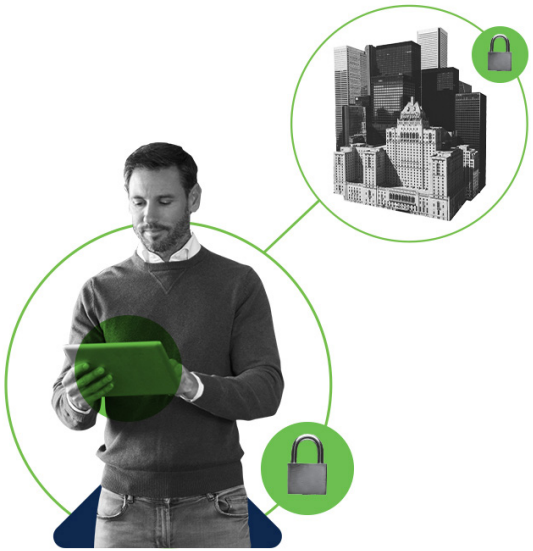
Cloud malware detection – Safely move critical applications to the cloud, prevent malware infections from third-party applications, and prevent the spread of cloud malware infections. Umbrella scans cloud file storage repositories, detects cloud malware, and enables administrators to rapidly act, including to delete or quarantine malicious files.

Coming soon

Data loss prevention (DLP) – Discover and block sensitive data from being transmitted to unwanted destinations. Prevent data exfiltration and support compliance mandates. Plus, you’ll be able to monitor and enforce in real-time, inspect data in-line with full SSL inspection, and create flexible, easy-to-customize policies.

Intrusion prevention system (IPS) – Examine network traffic flows. Prevent vulnerability exploits with an added layer of threat prevention based on Snort 3 technology and signature-based detection. Create firewall policies from a single, unified dashboard. Analyze traffic originating from client users. And take automated actions to catch and drop dangerous packets before they reach their target.

Cisco Umbrella and Meraki MX integration – Achieve higher security efficacy with less effort and resources. Secure users at the edge from any device while meeting multi-cloud demands. Quickly connect Meraki MX devices to Cisco Umbrella with simplified IPsec tunnels. Extend Meraki’s SD-WAN fabric into the Umbrella cloud with the click of a button. Leverage intelligent path selection for the fastest, most reliable, and secure connection to applications.



Umbrella SIG Advantage package – Our most complete set of advanced security capabilities in a single subscription for maximum value. In addition to all features included in SIG Essentials, SIG Advantage will include intrusion prevention system (IPS), data loss prevention (DLP), and cloud malware detection. It also includes Cisco Secure Malware Analytics licenses (formerly known as Threat Grid).

Cisco Umbrella: synchronize your security

For 36 years, Cisco has worked with hundreds of thousands of companies to secure users, devices, applications, and data from a growing number of cyber threats. The world's largest security vendor, we protect 100% of the Fortune 100.

Cisco Umbrella lets the world connect to the internet on any device with confidence, providing the most secure, most reliable, and fastest access to more than 24,000 customers globally.

Contact an expert at Cisco to see how Cisco Umbrella can meet your SASE needs.

Contact us

Sources:

1. DNS-Layer Protection & Secure Web Gateway Security Efficacy Test, AV-TEST, February 2021.