Cisco Umbrella

Ebook

How to streamline cloud security and embrace SASE

Protect remote users and offices with Cisco Umbrella

Cisco Umbrella

Ebook

Work anywhere with confidence

The world has made a massive shift towards a more distributed workforce, and 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 capabilities 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.

Cisco Umbrella

Ebook

Not all cloud security solutions are created equal

With greater security challenges come greater security requirements. As you consider cloud security solutions, you'll want to keep in mind several 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.

Cisco Umbrella

Ebook

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 — 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 grounded in 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 7 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, increasing performance from 23-31% over direct internet access without security protection.

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 C.

Cisco Umbrella peering partnerships

AT&T · BT · Google Fiber · verizon · amazon · DocuSign · DELL Services · HUAWEI · Microsoft · Alibaba.com · salesforce · Google · Adobe · box · Baidu 百度 · Cisco webex

Cisco Umbrella

Ebook

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 information 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. We pull live threat intelligence from global internet activity and analyze 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

Cisco Talos is one of the largest and most trusted providers of cutting-edge security research globally and is backed by over 400 full-time researchers and data scientists. The team uses unrivaled telemetry, statistical analysis, 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, backed by Cisco Talos:

Protects **>24,000** global enterprise customers

Identifies **1.4M+** new malware samples daily

Resolves up to **620 billion** DNS requests daily

Discovers **200+** new vulnerabilities per year

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

Cisco Umbrella

Ebook

See and protect users on any device, anywhere

The need

Today's users access data and apps both on and off network. To truly protect an organization, you need to bring security functions together in the cloud, so you can consistently apply your security policies wherever users work. You also need a solution with visibility that extends from edge to edge, is centrally monitored and managed, and 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 provides 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.

Cisco Umbrella

Ebook

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

AV-TEST, an independent security testing organization, evaluated threat efficacy among leading cloud security vendors. Cisco Umbrella received top marks, with a 96.39% blocking rate from its secure web gateway, the highest in the industry.[1] DNS-layer security also came in as the industry leader. The end result? Umbrella better uncovers and blocks malicious domains, IPs, and URLs before they have a chance to attack your network.

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

[1] source: AV-TEST Evaluates Secure Web Gateway and DNS-Layer Security Efficacy, https://learn-cloudsecurity.cisco.com/umbrella-resources/umbrella/av-test-evaluates-secure-web-gateway-and-dns-layer-security-efficacy

Vendor Number of test cases	Blocking rate (total) 3,572	PE URLs 850	Non-PE URLs 1,756	Phishing URLs 966
Cisco Umbrella	96.39%	93.65%	99.15%	93.79%
Zscaler Internet Access	89.67%	87.29%	93.28%	85.20%
Palo Alto Networks Prisma Access	73.15%	83.88%	57.86%	91.51%
Netskope Secure Web Gateway	61.90%	82.12%	55.52%	55.69%
Akamai Enterprise Threat Protector	58.43%	61.41%	48.35%	74.12%

Cisco Umbrella

Unified management 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 current. You need a solution with the ability to bring these security functions together and 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

Your security staff engages with Umbrella's policy creation, reporting, testing, managing, and more via a single, web-based dashboard. This streamlines security management and helps reduce the resources traditionally required to deploy and maintain security solutions.

Included with Cisco Umbrella is Cisco SecureX, a cloud-native XDR platform that connects the entire Cisco security portfolio with other aspects of your security infrastructure. By integrating security data from across Cisco 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.

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 users aren't 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.

Cisco Umbrella

Ebook

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 provides even more robust protection for your organization. Data from each product and service is shared across others. This means more comprehensive visibility and automated actions, and 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 and Meraki:
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 Secure Endpoint 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 (formerly ThreatGrid):
Examine and sandbox files so they can be safely analyzed, then block any new attempts to download these files if they're malicious.

Cisco Umbrella

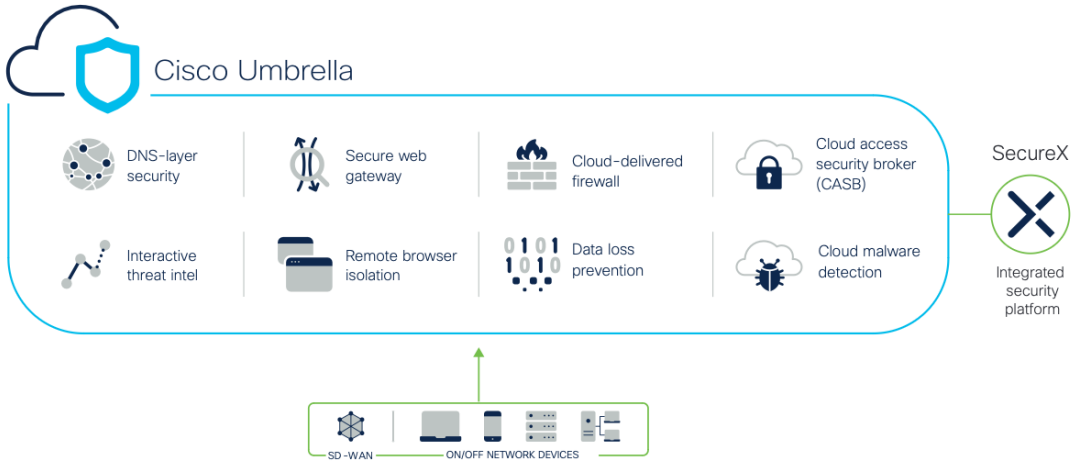
Ebook

Always focused on your security – today and tomorrow

From our start as a leading DNS security provider, Umbrella has grown into a multi-function cloud-native security service. We continually innovate 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 technology advancements.

A full suite of protection

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



Cisco Umbrella

Ebook

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:

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.

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.

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.

Cloud-delivered firewall

Provides visibility and control for 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 application rules (layer 7 application visibility and control). Includes intrusion prevention system (IPS) for an additional layer of signature-based threat detection, fueled by 40,000+ (always growing) signatures from Cisco Talos.

Data loss prevention (DLP)

Discovers and blocks sensitive data from being transmitted to unwanted destinations. Prevents data exfiltration and support compliance mandates. Monitors and enforces in real-time, inspects data in-line with full SSL inspection, and lets users create flexible, easy-to customize policies.

Remote browser isolation (RBI)

Provides a secure browsing experience with protection from zero-day threats and browser-based attacks by isolating web traffic from user devices. Improves productivity, as well as reduces alerts and helpdesk tickets. Deploys rapidly, with three levels of protection to choose from.

Cloud malware detection

Helps keep critical applications safe as they move to the cloud, prevents malware infections from third-party applications, and prevents the spread of cloud malware infections. Umbrella scans cloud file storage repositories, detects cloud malware, and enables administrators to rapidly act, including the ability to delete or quarantine malicious files.

SD-WAN integration, Viptela and Meraki

Easily deploy cloud security protection across your network, branch users, connected devices, and applications. Secures users at the edge from any device while meeting multi-cloud demands. Meraki MX and Viptela devices quickly connect to Cisco Umbrella with automated IPsec tunnels. Extend Meraki's or Viptela's SD-WAN fabric into the Umbrella cloud with a few clicks. Users can leverage intelligent path selection for the fastest, most reliable, and secure connection to private applications.

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.

Cisco Umbrella

Ebook

Cisco Umbrella: synchronize your security

For over 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. As 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 enterprise customers globally.

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

Contact us

Sources:

[1] Cisco Umbrella will soon also offer API-based DLP functionality for out-of-band analysis of data at rest in the cloud.