Cisco Umbrella At a Glance

Enterprise security and networking are facing a significant transformation as organization embrace SASE, a Secure Access Service Edge. Wide-scale adoption of cloud applications, an increase in remote workers, and expansion of branch offices has rendered the centralized, on-premises security model impractical. The convenience, cost savings, and performance benefits of going direct to the internet is driving a new decentralized approach to networking. Yet with change comes risk and a new set of security challenges. Organizations require a broader set of protection that not only improves security, but simplifies management.

Integrated security from the cloud

Umbrella is the cloud-native, multi-function security service at the core of Cisco's SASE architecture. It unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single cloud service to help businesses of all sizes secure their network. As more organizations embrace direct internet access, Umbrella makes it easy to extend protection to roaming users and branch offices.

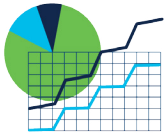
Key SASE benefits

- Broad, reliable security coverage across all ports and protocols
- Security protection on and off network
- Rapid deployment and flexible enforcement levels
- Immediate value and low total cost of ownership
- Single dashboard for efficient management
- Instant scalability across a global network

Security challenges

Gaps in visibility and coverage

Volume and complexity of security tools



Limited budgets and security resources

Better intelligence drives better security

Leveraging insights from Cisco Talos, one of the world's largest commercial threat intelligence teams with more than 400 researchers, Umbrella uncovers and blocks a broad spectrum of malicious domains, IPs, URLs, and files that are being 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.

Block malware easily

Built into the foundation of the internet, Umbrella processes 620 billion internet requests for more than 24,000 businesses every day. By enforcing security at the DNS layer, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established – before they reach your network or endpoints. The secure web gateway logs and inspects all web traffic for greater transparency, control, and protection. The cloud-delivered firewall helps to log and block traffic using IP, port, and protocol rules for consistent enforcement throughout your environment.

Speed up and improve incident response

Umbrella categorizes and retains all internet activity to simplify your investigation process and reduce incident response times. And, by using the Umbrella Investigate console and on-demand enrichment API, you have access to insights (historical and contextual) to prioritize incidents and speed up incident response. With Cisco SecureX (included with all Umbrella subscriptions) you can accelerate threat investigation and remediation by unifying Umbrella's threat intelligence with other Cisco Security products, and your other security infrastructure. Automated response actions simplify security by eliminating manual tasks and stopping attacks earlier in the process.

Packaging options

Our packages were designed to provide the right fit for all organizations. From small businesses without dedicated security professionals to multinational enterprises with complex environments, Umbrella provides more effective security and internet-wide visibility on and off your network. All packages can be integrated with your Cisco SD-WAN implementation to provide a combination of performance, security, and flexibility that delights both your end users and security team.

The Umbrella DNS Security Essentials package includes core DNS-layer security capabilities, to block requests to malicious domains before they reach your network or endpoints. You gain off-network protection and mobile support in this base package, as well as access to Umbrella's APIs (policy, reporting and enforcement), log exporting, the multi-org console, integration with Cisco Threat Response, and identity-based policies (virtual appliance + Active Directory connector). Additionally, this package provides discovery and blocking of shadow IT (by domain) with the App Discovery report.

The Umbrella DNS Security Advantage package includes all the capabilities of DNS Security Essentials plus it enables organizations to proxy risky domains for URL blocking and file inspection using AV engines and Cisco AMP. For organizations looking for deeper context during incident investigations, DNS Security Advantage offers unmatched threat intelligence in the Investigate console and on-demand enrichment API.

The Umbrella SIG Essentials package includes all of the capabilities of the DNS Security Advantage package plus access to a secure web gateway (full proxy), cloud-delivered firewall, sandbox file analysis with Cisco Threat Grid, and cloud access security broker (CASB) functionality. Umbrella combines multiple security services and threat intelligence into a single cloud service to secure your network and remote and roaming users with confidence. Simplify management and get visibility to control and manage apps, anywhere.

Umbrella SIG Advantage package is 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).

The Umbrella advantage

Umbrella has a highly resilient cloud infrastructure that boasts 100% uptime since 2006. Using Anycast routing, any of our 35 plus data centers across the globe are available using the same single IP address. As a result, your requests are transparently sent to the nearest, fastest data center and failover is automatic. Umbrella peers with more than 1000 of the world's top internet service providers (ISPs), content delivery networks (CDNs) and SaaS platforms to deliver the fastest route for any request — resulting in superior speed, effective security and the best user satisfaction.

Get started today

Visit signup.umbrella.com for a free 14 day trial of Umbrella.

AICPA SOC

SOC 2, Type II Compliant

AV-TEST The Independent IT-Security Institute Magdeburg Germany

AVTEST results

Umbrella consistently outperformed the competition in new security efficacy report.

Read the results

TechValidate™

Analyst and customer validation

Read reviews from Cisco Umbrella customers. Access direct research from TechValidate