STONE SOLUTIONS

Cloud Enterprise Network Security

Cisco Umbrella at a glance

stone
A CONVERGE COMPANY

CONVERGE
TECHNOLOGY SOLUTIONS

cisco Meraki

cisco Meraki

stone
A CONVERGE COMPANY

Cloud Enterprise Network Security

cisco Cisco Umbrella

cisco
Premier
Partner

Cisco Umbrella at a glance

Integrated Security from the Cloud

Cisco Umbrella is a cloud-native platform that delivers the most secure, reliable, and fastest internet experience to more than 100 million users daily. Umbrella unifies firewall, secure web gateway, DNS-layer security, cloud access security broker (CASB), and threat intelligence solutions into a single platform to help businesses of all sizes secure their network. As more organisations embrace direct internet access, Umbrella makes it easy to extend protection to roaming users and branch offices.

Better Intelligence Drives Better Security

Leveraging insights from Cisco Talos, one of the world's largest commercial threat intelligence teams with more than 300 researchers, Umbrella uncoversand blocks a broad spectrum of malicious domains, IPs, URLs, and files thatare 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.

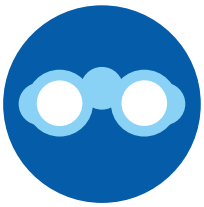
Block Malware Easily

Built into the foundation of the internet, Umbrella processes 180 billion internet requests for more than 18,500 businesses every day. By enforcing security at the DNS and IP layers, Umbrella blocks requests to malware, ransomware, phishing, and botnets before a connection is even established — before they reach your network or endpoints. The cloud-delivered 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 categorises 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 prioritise incidents and speed up incident response. Plus, it easily integrates with other intelligence sources and security orchestration tools for better management.

Security Challenges



Gaps in visibility and coverage

Volume and complexity of security tools

Limited budgets and security resources

Key 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

Cisco Meraki

Cloud Enterprise Network Security

Cisco Umbrella

Packaging options

Our packages were designed to provide the right fit for all organisations. 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 SASE / SSE solution 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 organisations to proxy risky domains for URL blocking and file inspection using AV engines and Cisco AMP. For organisations 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 Secure Malware Analytics, and cloud access security broker (CASB) functionality. With a single, cloud platform, you can combine multiple security services and threat intelligence to secure your network and remote and roaming users with confidence. Simplify management and get visibility to control and manage apps, anywhere.

Analyst and Customer Validation

See why Umbrella was named best secure web gateways software of 2019. Read the reviews and access direct research from TechValidate from customers.

Take the Next Step

Request a demo or speak with a Stone Sales Representative about how Cisco Umbrella can help you defend against threats on the internet

CLICK HERE for a free 14 day trial of Umbrella

The Umbrella Advantage

Umbrella has a highly resilient cloud infrastructure that boasts 100% uptime since 2006. Using Anycast routing, any of our 30 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 900 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.

cisco Meraki

stone
A CONVERGE COMPANY

Packaging Comparison

cisco Cisco Umbrella

Cisco Umbrella secures internet access and controls cloud app usage from your network, branch offices, and roaming users. Unlike disparate security tools, Umbrella unifies secure web gateway, cloud access security broker, DNS-layer security, cloud-delivered firewall, data loss prevention, malware protection with sandboxing, and remote browser isolation functionality into a single cloud service. Umbrella acts as a secure on-ramp to the internet and delivers deep inspection and control to support compliance and provide effective threat protection. Backed by Cisco Talos, one of the largest threat intelligence teams in the world, Umbrella exposes threats for better investigation and response. By delivering all this from the cloud, Umbrella offers visibility and enforcement to protect users anywhere.

cisco SECURE

	DNS Essentials	DNS Advantage	SIG Essentials
	Block threats at the DNS layer across your enterprise in minutes without added latency	Get DNS protection plus additional web security and threat insights to speed up investigations	Deploy advanced security functions and simplify management with the most effective security in the industry
Security & Controls			
DNS-layer Security			
Block direct-to-IP traffic for C2 callbacks that bypass DNS[1]		●	●
Block domains for malware, phishing, botnet, and other high risk	●	●	●
Block domains from SIEM and XDR integrations and custom lists using the Umbrella API	●	●	●
Secure web-gateway (SWG)			
Proxy web traffic for inspection		Traffic associated with risky domains via selective proxy	All web traffic
Decrypt and inspect SSL (HTTPS) traffic		With selective proxy	●
Enable web filtering	By domain or domain category	By domain or domain category	By domain or URL category
Create custom block/allow lists	Of domains	Of domains	Of URLs
Block URLs based on Cisco Talos and other third party feeds, and block files based on AV engine and Cisco Advanced Malware Protection (AMP) data		With selective proxy	●
Use retrospective security to identify previouslybenign files that became malicious			●
Remote browser isolation (RBI)			
Provide safe access to risky sites			Isolate Risky optional add-on
Provide safe access to web apps			Isolate Web Apps optional add-on
Provide safe access to any web destination			Isolate Any optional add-on
Cloud-delivered firewall			
Create layer 3/layer 4 policies to block specific IPs, ports, and protocols			●
Deepen protection for outbound traffic using application layer 7 policies with intrusion prevention system (IPS)			Optional add-on
Use IPSec tunnel termination			●
Cloud data loss prevention (DLP)			
Scan outbound web traffic inline in real time or out of band at rest in the cloud to block sensitive data from leaving your organisation			Optional add-on
Cloud access security broker (CASB)			
Discover and block shadow IT with App Discovery report	By domain	By domain	By URL
Create policies with advanced app controls at the activity level (uploads, attachments, and posts) or tenant controls (corporate vs. personal)			●
Support			
Enhanced - 24 x 7 technical + on-boarding	Required		
Premium - 24 x 7 technical + on-boarding + Technical Account Manager (TAM)	Optional upgrade		

[1]Requires endpoint footprint (Umbrella roaming client, Chromebook client, or AnyConnect roaming module).