Umbrella

IPv4: 208.67.222.222 & 208.67.220.220
IPv6: 2620:119:35::35 & 2620:119:53::53

Cisco Partner
https://cs.co/1page

Cisco **Umbrella** offers flexible, cloud-delivered security when and how you need it. It combines multiple security functions into one solution, so you can extend protection to devices, remote users, and distributed locations anywhere on or off the corporate network.

Benefits:

- Block malware, phishing, CNC callbacks from anywhere.
- Stop threats at the earliest point to reduce triage of alerts.
- Detect and monitor cloud apps in use across your environment.
- Enforce acceptable use policy via granular app controls, content filtering, and URL block/allow lists.
- Keep outbound web traffic secure with inline and out-of-band data loss prevention (DLP).
- ISO27001 certified – details available on the Cisco Trust Portal.

Discovery Questions:

- How do you protect devices when they are off the corporate network?
- How do you extend protection across all ports and protocols – especially when devices are off the corporate network?
- How many malware infections does your team deal with weekly?

FAQs:

Q: Does Umbrella/SIG have entitlement to Secure Client (AnyConnect)?
A: Yes, some packages can request Secure Client (AnyConnect) at no additional cost.

Q: Where do I go to see the SKUs and book the current packages?
A: DNS & SIG packages found in CCW: **UMB-SEC-SUB** or **UMB-EDU-SUB**.

Key SIG Features:

Secure Web Gateway: Cloud-based proxy to log and inspect web traffic.

Cloud-Delivered Firewall: Gain better visibility and control for internet traffic originating from client. Layer 7 application visibility and control, intrusion prevention system (IPS), and layer 3 / 4 firewall.

Cloud Access Security Broker (CASB): Detect and report on the cloud apps in use across your environment.

Remote Browser Isolation (RBI): Protection against browser-based threats.

Data Loss Prevention (DLP): Analyze data in-band and out-of-band and provide visibility and control over sensitive data.

Cloud Malware Scanning: Scan your environment's cloud platforms for malicious files and other risks.

Umbrella Packages:

	DNS Essent	DNS Adv	SIG Essent	SIG Adv	SA[1] Essent	SA[1] Adv
Recursive DNS-Layer Security:						
Block access to domains with malware, phishing, botnets etc.	✓	✓	✓	✓	✓	✓
Application discovery, monitoring, blocking & risk scoring	✓	✓	✓	✓	✓	✓
Filter by domain or category	✓	✓	✓	✓	✓	✓
Application and Network Access / Monitoring:						
Client-based and clientless ZTNA plus VPNaaS					✓	✓
SD-WAN direct internet access (DIA) integration			✓	✓	✓	✓
Experience Insights of endpoint, network & SaaS app performance (ThousandEyes)					✓	✓
Secure Web Gateway (SWG):						
Custom block/allow lists of domains	✓	✓	✓	✓	✓	✓
Custom block/allow lists of URL's			✓	✓	✓	✓
Proxy and inspect web traffic, block malicious files		Partial	✓	✓	✓	✓
Secure Malware Analytics (sandboxing) of malicious files			500/day	✓	500/day	✓
Roaming Security and Client Support						
User protection off corporate network with Secure Client	✓	✓	✓	✓	✓	✓
Windows, MacOS, iOS, ChromeOS and Android support	✓	✓	✓	✓	✓	✓
Cloud Access Security Broker (CASB):						
Advanced discovery, monitoring, control of cloud app usage including AI apps			✓	✓	✓	✓
Scan and remove malware from cloud-based file storage apps			✓	✓	✓	✓
SaaS security posture management (SSPM)					Partial	Partial
Data Loss Prevention (DLP):						
Integrated inline/out-of-band (cloud)inspection and blocking control with Gen AI			Add-on	✓		✓
Firewall as a Service (FWaaS):						
Layer 3 & 4 control of IP's ports and protocols			✓	✓	✓	✓
Layer 7 control with Intrusion Prevention System (IPS)			Add-on	✓		✓
Remote Browser Isolation (RBI):						
Extra browsing protection for designated users			Add-on	Add-on	Risky Sites Only	✓
Threat Intelligence:						
Continuously update threat intelligence from Cisco Talos	✓	✓	✓	✓	✓	✓
Deep Domain, IP and autonomous system number (ASN) for rapid investigations		✓	✓	✓	Coming Soon	Coming Soon
SIEM and XDR Interoperability:						
Integration with multiple tools including Splunk & XDR	✓	✓	✓	✓	via API	via API
Management:						
Single management interface	✓	✓	✓	✓	✓	✓
Customize block page and warn page options	✓	✓	✓	✓	✓	✓
Reporting and Logging:						
Real-time activity search plus API to extract key events	✓	✓	✓	✓	✓	✓
Choose North America or Europe log storage	✓	✓	✓	✓	✓	✓
Cisco-managed S3 buckets or customer AWS S3 buckets	✓	✓	✓	✓	✓	✓
Support:						
24x7 Enhanced Software Support via email and phone (Premium upgrade available)	Add-on	Add-on	Add-on	Add-on	Required	Required

[1] *SA = Secure Access*

Resources:

SalesResources	Umbrella Investigate	SSE Packages	Public Sector
Data Sheets	Virtual Appliances	YouTube channel	Umbrella Packages
Ordering Guide	Partner Learning	Secure Trials Console	Support Packages
Health Check	Umbrella Docs	Umbrella for MSSP's	EDU Packages
	SASE-FedRAMP	MSSP Requirements	Public page

Example SKUs: ***UMB-SEC-SUB*** | ***UMB-EDU-SUB***