

Package comparison

	Professional best for small companies	Insights best for mid-sized companies	Platform best for advanced security teams
Performance			
100% cloud – no hardware to install or software to maintain			
100% uptime – resolves 80B+ requests daily with no added latency			
7M+ unique malicious destinations enforced concurrently across 25 data centers			
Protection			
Add a new layer of predictive security for any device, anywhere			
Prevent malware, phishing, and C2 callbacks over any port			
Enforce acceptable use policies using 60 content categories			
Enforcement			
Block malicious domain requests & IP responses at the DNS-layer			
Block malicious URL paths & direct IP connections at the IP-layer			
Proxy risky domains for URL and file inspection using AV engines and Cisco Advanced Malware Protection (AMP)			
Visibility			
Real-time, enterprise-wide activity search & scheduled reports			
Identify targeted attacks by comparing local vs. global activity			
Identify cloud & IoT usage risks by reporting on 1800+ services			
Management			
Custom block/allow lists, built-in block pages, and bypass options			
Enforcement & visibility per internal network or AD user/group			
Retain logs forever by integrating with your Amazon S3 bucket			
Platform package exclusive			
API-based integrations to enforce & manage 3rd-party block lists			
Investigate Console – threat intelligence on all domains, IPs, & file hashes			
Additional Options			
Support Options – all packages include online & email support	See options for all packages		
Investigate API – enrich local events (SIEM) with global context	Package purchased separately		
Muti-Org Console – centralized management of decentralized orgs		add-on	add-on

Entry-level package options

For organizations looking for protection with more basic functionality, we have three additional Umbrella packages designed for entry-level use cases.

	Roaming best for Cisco NGFW / AnyConnect	Branch best for Cisco ISR 4000 Series	WLAN best for Cisco WLAN or other wireless hotspots
License based on:	number of users	number of Cisco ISR 4k devices	number of access points
Performance			
100% cloud – no hardware to install or software to maintain			
100% uptime – resolves 80B+ requests daily with no added latency			
7M+ unique malicious destinations enforced concurrently across 25 data centers			
Protection			
Add a new layer of predictive security for any device, anywhere	Off-network only	On-network only	On-network only
Prevent malware, phishing, and C2 callbacks over any port			
Enforce acceptable use policies using 60 content categories			
Enforcement			
Block malicious domain requests & IP responses at the DNS-layer			
Block malicious URL paths & direct IP connections at the IP-layer			
Visibility			
Real-time, enterprise-wide activity search & scheduled reports			
Management			
Custom block/allow lists, built-in block pages, and bypass options	Only has allow list and 1 built-in block page		
Enforcement & visibility per internal network or AD user/group		Only per internal network (no Active Directory)	Per SSID, Access Point, AP Group, and User Group (no Active Directory)
Additional Options			
Support Options – all packages include online & email support	See options for all packages		
Investigate Console – access threat intelligence on all domains, IPs, & file hashes through a web-based console	Package purchased separately		
Investigate API – enrich local events (SIEM) with global context	Package purchased separately		