Cisco Umbrella: DNS Security Package Comparison

Umbrella provides the first line of defense against threats on the internet by blocking requests to malicious destinations (domains, IPs, URLs) before a connection is established. All packages are 100% cloud-delivered with no hardware to install or software to maintain. The Umbrella global network includes 30 datacenters around the world with 100% business uptime. Security intelligence is gathered from 180 billion daily DNS requests from more than 90 million users.

	Professional	NEW DNS Essentials	Insights	NEW DNS Advantage	Platform
Reduce Risk					
Protect any device on the corporate network	●	●	●	●	●
Cover laptops (Windows, Mac OS, and Chromebook) and supervised iOS devices off-network	●	●	●	●	●
Prevent malware, phishing, a=nd C2 callbacks over any port	●	●	●	●	●
Block high risk other security categories (cryptomining, newly seen domains, etc.)	●	●	●	●	●
Stop acceptable use violations (up to 100 content categories), plus enforce SafeSearch	●	●	●	●	●
Enforce policies					
DNS-layer control by security setting, content filtering, and customized block/allow list (domains)	●	●	●	●	●
Proxy risky domains with customizable URL blocking and file inspection using Cisco Advanced Malware Protection (AMP) and anti-virus engine			●	●	●
IP-layer blocking for C2 callbacks that bypass DNS [1]			●	●	●
Customizable block pages and bypass options	●	●	●	●	●
Network (egress IP) or network device (including VLAN or SSID) granularity [2]	●	●	●	●	●
Roaming computer granularity [1]	●	●	●	●	●
Active Directory group membership (including specific users or computers) and internal subnet granularity [3]		●	●	●	●
View activity (reporting)					
Real-time, enterprise-wide activity search & scheduled reports	●	●	●	●	●
Identify targeted attacks with local vs. global activity report		●	●	●	●
Application Discovery and blocking to combat shadow IT		●	●	●	●
Attribution by external IP and internal IP [4]	●	●	●	●	●
Attribution by roaming computer [5]	●	●	●	●	●
Attribution by Active Directory user [3]	●	●	●	●	●
Manage					
Log storage location options in Europe or US	●	●	●	●	●
Log retention by customer or Cisco-managed AWS S3 bucket [6]	●	●	●	●	●
Reporting API - simply extract key events from Umbrella [http://cs.co/umbrellareportingapi]	●	●	●	●	●
Multi-org console - centrally manage decentralized orgs	●	●	●	●	●
Management API - create, read, update, or delete identities for child orgs [http://cs.co/umbrellamanagementapi]	w/Multi-Org only	●	w/Multi-Org only	●	w/Multi-Org only

Cisco Umbrella: DNS Security Package Comparison

	Professional	NEW DNS Essentials	Insights	NEW DNS Advantage	Platform
Threat Intelligence					
Cisco Threat Response		●	●	●	●
Investigate console: threat intelligence on all domains, IPs, networks, & file hashes	Add-on		Add-on	●	●
Investigate On-demand Enrichment API	Add-on		Add-on	●	
Integrations					
Deployment: Cisco integrations (SD-WAN, Meraki MR, Integrated Services Router, AnyConnect, & Wireless LAN Controller) and partner integrations (Cradlepoint, Aerohive, & others)	●	●	●	●	●
Enforcement API: for custom and partner integrations (Splunk, FireEye, Anomali, & others)		●		●	●
Support for legacy packages					
Basic – online support, 24 x 5 email	●		●		●
Gold – online, 24 x 7 email and phone	Add-on		Add-on		Add-on
Platinum – online, email, phone and dedicated Technical Account Manager (TAM)	Add-on		Add-on		Add-on
Support for new packages					
Cisco Software Support- Enhanced		●		●	
Cisco Software Support- Premium		Add-on		Add-on	

Footnotes:

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

[2] Requires network device integration with Cisco Integrated Services Router (ISR) or Cisco Wireless LAN Controller

[3] Active Directory (AD) policies and attribution requires Umbrella AD connector with network footprint (Umbrella virtual appliance) or endpoint footprint (Umbrella roaming client or AnyConnect roaming module)

[4] Internal IP attribution requires network footprint (Virtual Appliance (which is only included in Insights and Platform) or Meraki MR integration Cisco ISR integration, or Cisco ASA integration)

[5] Roaming computer attribution requires endpoint footprint (AnyConnect roaming module or Umbrella roaming client)

[6] No Amazon account required when using the Cisco-managed S3 bucket