Cisco Umbrella Package Comparison

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.

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
	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	Unlock the highest levels of protection and control with advanced security functions like layer 7 firewall with IPS, DLP, and more
Licensing	By # of covered users	By # of covered users	By # of covered users	By # of covered users
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 Cisco SecureX, direct integrations (Splunk, Anomali, & others) and custom lists using enforcement API	●	●	●	●
Secure web gateway (SWG)				
Proxy web traffic for inspection		Traffic associated with risky domains via selective proxy	All web traffic	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, URL, or category	By domain, URL, or category
Create custom block/allow lists	Of domains	Of domains	Of URLs	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 previously-benign files that became malicious			●	●

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
Security & Controls				
Remote browser isolation (RBI)				
Provide safe access to risky sites			Isolate Risky optional add-on	Isolate Risky optional add-on
Provide safe access to web apps			Isolate Web Apps optional add-on	Isolate Web Apps optional add-on
Provide safe access to any web destination			Isolate Any optional add-on	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			●	●
Data loss prevention (DLP)				
Enable inline inspection of web and cloud app traffic for sensitive data			Optional add-on	●
Cloud access security broker (CASB)				
Discover and block shadow IT with App Discovery report	By domain	By domain	By URL	By URL
Create policies with advanced app controls at the activity level (uploads, attachments, and posts) or tenant controls (corporate vs. personal)			●	●
Cloud malware detection				
Scan and remove malware from cloud-based file storage apps			2 applications	All supported applications

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
Security & Controls				
Umbrella Investigate				
Access Investigate's web console for interactive threat intel[6]		5 logins	5 logins	5 logins
Use the Investigate On-demand Enrichment API to enrich other tools/systems with domain, URL, IP, and file threat intelligence (2,000 requests/day)[6]		●	●	●
Integrate with SecureX to aggregate activity across Cisco and 3rd party products	Reporting & enforcement APIs	All APIs	All APIs	All APIs
Uncover malicious domains, IPs, ASNs and files to get the most complete view of an attackers' infrastructure, tactics, and techniques		●	●	●
Secure Malware Analytics				
Use Cisco Secure Malware Analytics Cloud (formerly Threat Grid) sandbox on suspicious files			500 samples/day; simple verdict	Unlimited samples; detailed inspection
Secure Malware Analytics console access				3 users
Interact with malware samples in glovebox				●
Advanced search (samples, artifacts, registry, URLs, etc.)				●
Traffic forwarding				
Forward external DNS for: · On-network protection via Cisco (SD-WAN, Meraki, ISR, & AnyConnect WLAN Controller) and third-party integrations (Cradlepoint, Aerohive, & others) · Off-network AnyConnect via Umbrella roaming client or Cisco Security Connector iOS app	●	●	●	●
Cisco AnyConnect client (license included) to deploy Umbrella module to forward traffic	●	●	●	●
Send outbound network traffic via IPsec tunnel, proxy chaining, or PAC files			●	●

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
Security & Controls				
User attribution				
Create policies and view reports by network (egress IP), internal subnet[2], network device (including VLAN & SSID)[3], roaming device, and Active Directory group (including specific users)[4]	●	●	●	●
Create policies and view reports using SAML			●	●
Management				
Customize block pages and bypass options	●	●	●	●
Use our multi-org console to centrally manage decentralized orgs	●	●	●	●
Use our management API to create, read, update, and delete identities for child orgs	●	●	●	●
Reporting & logs				
Leverage real-time activity search and our reporting API to easily extract key events	●	●	●	●
Choose North America or Europe log storage	●	●	●	●
Use customer AWS S3 bucket to export and retain logs as long as needed, or a Cisco-managed S3 bucket to export and retain logs for 30 days[5]	●	●	●	●
Access domain request logs in our user interface (30 day-detail, 1yr-summary)	●	●	●	●
Access full URL logging and firewall logging in our user interface (30 days-detail)			●	●

	DNS Essentials	DNS Advantage	SIG Essentials	SIG Advantage
Security & Controls				
SecureX				
Optional no-charge product ID that initiates email notification regarding SecureX access and customer experience onboarding help[7]	●	●	●	●
Cisco Talos Incident Response (CTIR)				
Global incident response capability and proactive services: Service Level Objective of up to 4 hours by phone, 40 hours per year (Small)	Optional add-on	Optional add-on	Optional add-on	Optional add-on
Global incident response capability and proactive services: Service Level Objective of up to 4 hours by phone, 80 hours per year (Medium)	Optional add-on	Optional add-on	Optional add-on	Optional add-on
Global incident response capability and proactive services: Service Level Objective of up to 4 hours by phone, 120 hours per year (Large)	Optional add-on	Optional add-on	Optional add-on	Optional add-on
Support				
Enhanced – 24x7 technical + on-boarding	Required	Required	Required	Required
Premium – 24x7 technical, on-boarding, +Technical Account Manager (TAM)	Optional add-on	Optional add-on	Optional add-on	Optional add-on

1. Requires endpoint footprint (Umbrella roaming client, Chromebook client, or AnyConnect roaming module)
2. Internal IP attribution requires network footprint (our virtual appliance, not available in Professional package) or Meraki MR integration Cisco ISR integration, or Cisco ASA integration
3. Requires network device integration with Cisco Integrated Services Router (ISR) or Cisco Wireless LAN Controller
4. 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)
5. No Amazon account required when using the Cisco-managed S3 bucket
6. MSSPs can purchase (and use):
    - Investigate Console (licensed per analyst)
    - Investigate Integration API (licensed per analyst)
    - MSSPs cannot purchase the Investigate API Tier 1, 2, or 3

   End customers can purchase
    - Investigate Console (licensed per analyst)
    - Investigate Integration API (licensed per analyst)
    - Investigate API (Tier 1, 2, 3) (licensed per site)
7. SecureX is available with all Umbrella packages

919338632 06/22