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-delivered firewall, DNS-layer security, and cloud access security broker (CASB) functionality into a single platform. 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 with 100% uptime, Umbrella offers visibility and enforcement to protect users anywhere.

	DNS Security Essential	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
	Good for small companies or as first line of defense for any size company	Good for mid-sized companies or as first line of defense for any size company	Ideal for companies who use Cisco SD-WAN for direct internet access at branch and satelitte offices, and large companies with advanced needs for functionality to address security and enforce acceptable use policies
Licencing	By # of users	By # of users	By # of users
Security & Controls			
DNS-layer security			
Block domains associated with phishing, malware, botnets, and other high risk categories (cryptomining, newly seen domains, etc.)	●	●	●
Block domains based on partner integrations (Splunk, Anomali, & others) and custom lists using our enforcement API	●	●	●
Block direct-to-IP traffic for C2 callbacks that bypass DNS[1]		●	●
Secure web gateway			
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, URL, or category
Create custom block/allow lists	Of domains	Of domains	Of URLs
Block URLs based on Cisco Talos and third party feeds, and block files based on AV engine and Cisco Advanced Malware Protection (AMP) data		With selective proxy	●
Use Cisco Threat Grid cloud sandbox environment to analyze suspicious files (200 files/day)			●
Use retrospective security to identify previously-benign files that became malicious			●

	DNS Security Essential	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
Security & Controls			
Cloud-delivered firewall			
Create layer 3/layer 4 policies to block specific IPs, ports, and protocols			●
Layer 7 Cloud Firewall			optional add-on
Use IPSec tunnel termination			●
Cloud access security broker			
Discover and block shadow IT (based on domains) with our App Discovery report	●	●	
Discover and block shadow IT (based on URLs) with App Discovery report			●
Create policies with granular controls (block uploads, attachments, and posts) for select apps			●
Umbrella Investigate			
Access Investigate's web console for interactive threat intelligence (5 logins)[2]		●	●
Use the Investigate on-demand enrichment API to enrich other tools/systems with domain, URL, IP, and file threat intelligence (2,000 requests per day)[2]		●	●
Integrate with Cisco SecureX to aggregate threat activity across Cisco AMP, Threat Grid, Email Security, NGFW, and Umbrella	Reporting and enforcement API only	●	●
Traffic forwarding			
Forward external DNS traffic for: • On-network protection via Cisco (SD-WAN, Meraki MR, Integrated Services Router, & Wireless LAN Controller) and third party integrations (Cradlepoint, Aerohive, & others) • Off-network protection via AnyConnect, Umbrella roaming client, and Cisco Security Connector for iOS	●	●	●
Send outbound network traffic via IPSec tunnel, proxy chaining, or PAC files			●

	DNS Security Essential	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
Security & Controls			
User attribution			
Create policies and view reports by: • Network (egress IP) • Internal subnet[3] • Network device (including VLAN or SSID)[4] • Roaming device • Active Directory group membership (including specific users)[5]	●	●	●
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 and logs			
Leverage real-time activity search and our reporting API to easily extract key events	●	●	●
Choose North America or Europe for 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[6]	●	●	●
Access domain request logs in our user interface (30 day: detail, 1yr: summary)	●	●	●
Access full URL logs in our user interface (30 days: detail)			●
Access firewall (IP, port, and protocol) logs in our user interface (30 days: detail)			●

	DNS Security Essential	DNS Security Advantage	Secure Internet Gateway (SIG) Essentials
Support			
Enhanced – 24 x 7 technical + onboarding	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)
2. 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)
3. 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
4. Requires network device integration with Cisco Integrated Services Router (ISR) or Cisco Wireless LAN Controller
5. 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)
6. No Amazon account required when using the Cisco-managed S3 bucket