

# 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 onramp 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 Essentials	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 with Cisco SD-WAN, and large companies with advanced security and web policy needs
<b>Licencing</b>	by the number of users		
<b>Security &amp; Controls</b>			
<b>DNS-layer security</b>			
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 <sup>1</sup>		•	•
<b>Secure web gateway</b>			
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			•
<b>Cloud-delivered firewall</b>			
Create layer 3/layer 4 policies to block specific IPs, ports, and protocols			•
Use IPSec tunnel termination			•
<b>Cloud access security broker</b>			
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			•
<b>Umbrella Investigate</b>			
Access Investigate's web console for interactive threat intelligence (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 per day)		•	•
Integrate with Cisco Threat Response to aggregate threat activity across Cisco AMP, Threat Grid, Email Security, NGFW, and Umbrella	With enforcement API only	•	•

	DNS Security Essentials	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 with Cisco SD-WAN, and large companies with advanced security and web policy needs
<b>Licencing</b>	by the number of users		
<b>Deployment &amp; management</b>			
<b>Traffic forwarding</b>			
Forward external DNS traffic for:			
<ul style="list-style-type: none"> <li>On-network protection via Cisco (SD-WAN, Meraki MR, Integrated Services Router, &amp; Wireless LAN Controller) and third party integrations (Cradlepoint, Aerohive, &amp; others)</li> <li>Off-network protection via AnyConnect, Umbrella roaming client, and Cisco Security Connector for iOS</li> </ul>	•	•	•
Send outbound network traffic via IPSec tunnel, proxy chaining, or PAC files!			•
<b>User attribution</b>			
Create policies and view reports by:			
<ul style="list-style-type: none"> <li>Network (egress IP)</li> <li>Internal subnet<sup>2</sup></li> <li>Network device (including VLAN or SSID)<sup>3</sup></li> <li>Roaming device</li> <li>Active Directory group membership (including specific users)<sup>4</sup></li> </ul>	•	•	•
Create policies and view reports using SAML			•
<b>Management</b>			
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 using own internal tools	•	•	•
<b>Reporting and logs</b>			
Leverage real-time activity search and our reporting API to easily extract key events	•	•	•
Choose North America or Europe for log storage	•	•	•
Use customer or Cisco-managed AWS S3 bucket to export and retain logs as long as needed <sup>5</sup>	•	•	•
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)			•
<b>Support</b>			
Enhanced - 24 x 7 technical + on-boarding	Required		
Premium - 24 x 7 technical + on-boarding + Technical Account Manager (TAM)	Optional upgrade		

Footnotes:

- Requires endpoint footprint (Umbrella roaming client, Chromebook client, or AnyConnect roaming module)
- Internal IP attribution requires network footprint (our virtual appliance), Meraki MR integration, Cisco ISR integration, or Cisco ASA integration, or Cisco SD-WAN integration. Select third-party integrations available too
- Requires network device integration with Cisco Integrated Services Router (ISR) or Cisco Wireless LAN Controller or Meraki MR
- 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)
- No Amazon account required when using the Cisco-managed S3 bucket