Cisco Umbrella 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 cloud delivered with no hardware to install or software to maintain. The Umbrella network provides 100% business uptime with 26+ datacenters around the world.

	Wireless LAN (WLAN) best for protecting guest Wi-Fi users	Professional best for small companies	Insights best for mid-sized companies	Platform best for advanced security teams
Licensing	by number of access points	by number of users		
Reduce risk				
Protect any device on the corporate network	✓	✓	✓	✓
Cover Windows and Mac OSX laptops and supervised iOS devices on and off-network		✓	✓	✓
Prevent malware, phishing, and C2 callbacks over any port	✓	✓	✓	✓
Stop acceptable use violations (80+ content categories), plus enforce SafeSearch	✓	✓	✓	✓
Enforce policies				
Network (egress IP) or network device (including VLAN or SSID) granularity[1]	✓	✓	✓	✓
Roaming computer granularity[2]		✓	✓	✓
Active Directory group membership (including specific users or computers) and internal subnet granularity[3]			✓	✓
DNS-layer visibility and control for domain requests and IP responses per security and content settings or customizable destination lists	✓	✓	✓	✓
Proxy risky domains with customizable URL blocking and file inspection using Cisco Advanced Malware Protection (AMP) and anti-virus engine			✓	✓
IP-layer enforcement for C2 callbacks that bypass DNS[2]			✓	✓
Granular customizable block pages and bypass options	✓	✓	✓	✓
Visibility reports				
Real-time, enterprise-wide activity search & scheduled reports	✓	✓	✓	✓
Attribution by external IP	✓	✓	✓	✓
Attribution by roaming computer and/or internal IP[4]		✓	✓	✓
Attribution by Active Directory user or computer[3]			✓	✓
Identify targeted attacks with local vs. global activity report			✓	✓
Cloud & IoT usage report shows risks on over 1800 services			✓	✓

	Wireless LAN (WLAN) best for protecting guest Wi-Fi users	Professional best for small companies	Insights best for mid-sized companies	Platform best for advanced security teams
Integrations				
Deployment: Cisco integrations (Integrated Services Router, AnyConnect, Wireless LAN Controller) and partner integrations (Aruba, Cradlepoint, Aerohive)	✓	✓	✓	✓
Log retention: Amazon Web Services integration using customer-managed or Cisco-managed S3 bucket[5]			✓	✓
Threat enforcement: Partner integrations (Splunk, FireEye, Anomali) and custom integrations (using Umbrella API)				✓
Add-ons				
Support Options – all packages include online & email support	see options for all packages			
Multi-Org Console – centralized management of decentralized organizations			purchased seperately	

Umbrella Investigate

Access our threat intelligence for a complete view of the relationships between domains, IPs, networks, and malware. Enrich your incident response and SIEM data.

Investigate Console – threat intelligence on all domains, IPs, networks, & file hashes. Easily pivot into data for investigation.	purchased seperately	**included**
Investigate API - bring contextual data into SIEM, or incident workflow to quickly surface high-impact security incidents. Tier 1: 3 requests/second Tier 2: 12 requests/second Tier 3: 48 requests/second Investigate API also includes Investigate Console and can run standalone without an Umbrella package.	purchased seperately	

1. Requires network device integration with Cisco Integrated Services Router (ISR) or Cisco Wireless LAN Controller
2. Requires endpoint footprint (Umbrella roaming client or AnyConnect roaming module)
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 (Umbrella virtual appliance or Cisco ISR integration) or endpoint footprint (AnyConnect roaming module or Umbrella roaming client)
5. No Amazon account required when using the Cisco-managed S3 bucket