Cisco Umbrella for Managed Security Service Providers (MSSP)

MSSPs lead the charge

The same trends that accelerate business – high SaaS application use, extensive numbers of roaming workers, expanding remote locations – magnify cybersecurity risk. Managed Security Service Providers (MSSPs) are at the forefront of tackling that risk, as end customers turn to them for cybersecurity solutions and expertise.

MSSPs seek security capabilities that serve diverse customer needs, scale to accommodate market and customer base fluctuations, and evolve with continuous enhancements. To minimize operational costs, solutions must fit seamlessly into the MSSP's existing portfolio. And without exception, solutions must provide extraordinary security efficacy.

The leader in DNS-layer security

Cisco Umbrella for MSSPs establishes the first line of defense against threats on the internet. Umbrella is a cloud-delivered service that provides end customers on-and off-network protection from cyberattacks, such as malware, phishing, ransomware, and command and control callbacks.

By analyzing and learning from internet activity patterns, Umbrella uncovers attackers' infrastructures staged attacks, both current and emerging. This enables Umbrella to proactively block requests to malicious destinations before they reach your customers' network or endpoints – without added latency. Stop phishing and malware infections earlier, identify already infected devices faster, and prevent data exfiltration more effectively.

Built for MSSPs

As a cloud-delivered service with no hardware to install or software to manually update, Umbrella reduces MSSP complexity. The MSSP has access to the tools necessary to manage Umbrella including logging and reports, Amazon Simple Storage Service (S3) log management, and a variety of APIs.

With minimal investment and fast time-to-market, Umbrella helps MSSPs to contain overhead cost and improve profit margins while sharpening brand differentiation. It can be deployed in minutes and is simple to manage, enabling the MSSP business to grow without straining security teams.

Subscription licensing via term and pay-as-you-go (Managed Service License Agreement/MSLA) billing models are available.

Use cases

- Prevent malware, ransomware and phishing attempts from malicious websites
- Enforce acceptable use policies using ~100 content categories
- Pinpoint compromised systems using real-time security activity reports
- Manage and control cloud application usage

MSSP benefits

- **Reduce remediation costs and breach damage:** Threats stopped before they cause damage.
- **Shrink the time to detect and contain threats:** Command and control callbacks blocked over any port or protocol.
- **Increase visibility across locations and users:** Deep visibility for incident response. Know that you are seeing everything.
- **Boost operational efficiency:** Centralized settings,multi-tenancy, and centralizedreporting.

Proven security efficacy

Lots of security providers claim they are the best at threat detection and prevention, but can they prove it? Recent third-party research from AV-TEST named Cisco Umbrella the industry leader in security efficacy. Umbrella significantly outperformed top competitors in an evaluation focused on the detection rate of links pointing to PE malware (e.g. EXE files), other forms of malicious files (e.g. HTML, JavaScript), and phishing URLs.

Key numbers

- 200 billion daily internet requests
- 100 million users
- 30+ datacenters worldwide
- 7M+ malicious destinations enforced concurrently at the DNS-layer

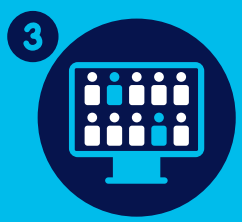
Key differentiators

Deep protection	Broad coverage	MSSP ready
• Protect all devices on customer networks (managed and unmanaged, BYOD, IoT, etc.) • Protect laptops and supervised IOS devices, on-and off-network (VPN on or off) • Stop threats before they reach your customers' networks or endpoints	• Stop threats across all ports and protocols • Leverage deep, real-time threat intelligence • Integrate with existing managed security services	• Multi-tenant architecture • Centralized settings • APIs for enforcement, management, reporting, and threat investigation • No added latency for users

It's never been easier to accelerate your business. It's as simple as 1,2,3.

Deploy in minutes and show customers immediate results

Manage in bulk, using multi tenancy and centralized settings



Monitor multiple customers from a single dashboard

Talk to a Cisco sales representative today

	MSSP with DNS Essentials	MSSP with DNS Advantage	MSSP Insights
Licencing	by # of users	by # of users	by # of users. Monthly, post-paid option available (MSLA)
Customer fit	Good for service providers who deliver high function, pure play security services (MSSP). Typically backed by a Security Operations Center (SOC) and a Security Event and Information Monitoring (SEIM) tool, with 24x7 monitoring and customer support.		Good for service providers who deliver high function, pure play security services (MSSP). Typically backed by a Security Operations Center (SOC) with 24x7 monitoring and customer support.
Positioning/constraints	Training and proficiency exams required prior to provisioning.		
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	
Decrypt and inspect SSL (HTTPS) traffic		With selective proxy	
Enable web filtering	By domain or domain category		
Create custom block/allow lists	Of domains		
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	
Cloud access security broker			
Discover and block shadow IT (based on domains) with Umbrella's App Discovery report	x (end customer only)		
Umbrella Investigate (cell indicates when function is included in package)			
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/day)		●	
Integrate with Cisco Threat Response to aggregate threat activity across Cisco AMP, Threat Grid, Email Security, NGFW, and Umbrella	Reporting and enforcement API only (end customers only)	x (end customer only)	Reporting API only (end customer only)
Deployment & management			
Traffic forwarding			
Forward external DNS traffic for: • On-network protection via Cisco (SD-WAN, Meraki MR, Integrated Services Router, AnyConnect, & Wireless LAN Controller) and third party integrations (Cradlepoint, Aerohive, & others) • Off-network protection via Cisco AnyConnect, Umbrella roaming client, and Cisco Security Connector for iOS	●	●	●
User attribution			
Create policies and view reports by: • Network (egress IP) • Internal subnet [2] • Network device (including VLAN or SSID) [3] • Roaming device • Active Directory group membership (including specific users) [4]	●	●	●
Management			
Customize block pages and bypass options	●	●	●
Use our multi-org console to centrally manage decentralized orgs	MSSP Only		
Use our management API to create, read, update, and delete identities for child orgs	MSSP Only		

	MSSP with DNS Essentials	MSSP with DNS Advantage	MSSP Insights
Deployment & management			
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 [5]	MSSP Only		●
Access domain request logs in our user interface (30 day-detail, 1yr-summary)	●	●	●
Support			
Enhanced - 24 x 7 technical + on-boarding	Required	Required	Basic support included in all - online support, 24 x 5 email
Premium - 24 x 7 technical + on-boarding + Technical Account Manager (TAM)	Optional add-on	Optional add-on	Gold available for purchase - online, 24 x 7 email and phone Platinum avaialble for purchase - online, email, phone and dedicated Technical Account Manager (TAM)

Footnotes
[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