amatis

Internet Security

Your first line of defence

Information & Cyber Security is an increasing concern for UK businesses. Every time that your business users access the internet they risk opening the door to a potential cyber attack. With an increased number of users accessing the internet outside of the corporate network, this risk is growing at an exponential rate.

We help our customers to reduce this risk by creating an effective first line of defence based on Cisco Umbrella. This ensures your users do not visit sites that are suspected of hosting malicious content or are acting as staging points for cyber-attacks.

As a Secure Internet Gateway, Cisco Umbrella provides the first line of defence against threats on the internet wherever users go. Umbrella delivers complete visibility into internet activity across all locations, devices, and users, and blocks threats before they ever reach your network or endpoints. As a cloud-delivered platform, Umbrella integrates easily with your existing security stack and delivers live threat intelligence about current and emerging threats.

Key Benefits:

Everywhere Protection
There are no gaps: whether your users are on the corporate network, at home or utilising a public connection in a coffee shop, they are still protected by Cisco Umbrella. Because Cisco Umbrella is the first line of defence, security teams will have fewer malware infections to remediate and threats will be stopped before they cause damage.

Mitigating Threats Early
By raising your level of defence to the point where you access the internet, you are effectively stopping attacks before they have started and more importantly, before they cause damage.

Increased Visibility
By controlling internet access across your organisation, you gain unprecedented insights into usage and identify any unsanctioned cloud services being used. Cisco Umbrella provides crucial visibility for incident response and also gives you confidence that you're seeing everything.

How Does Cisco Umbrella Work?
Cisco Umbrella utilises the Domain Name System (DNS) which is a mechanism for mapping domain names to IP addresses. Rather than utilising a generic service, when a user clicks on a link or types in a URL the DNS look-up is sent to Cisco Umbrella. It uses intelligence to determine if the request is safe, malicious or risky (meaning it may contain both malicious and legitimate content).

Safe or malicious attacks are routed or blocked accordingly, providing instant protection. Risky requests are effectively sandboxed in a cloud-based proxy where Cisco Talos reputation and other 3rd party feeds are used to determine whether the URL is malicious.

This proxy also inspects files that users have attempted to download from these sites, using both anti-virus engines and Cisco Advanced Malware Protection (AMP). Based on the outcome of this deep inspection, the connection is either allowed or blocked.

- Cloud security at DNS and IP layers providing first-line defence against threats
- Protection on and off the corporate network (Using Any Connect Umbrella integration module)
- Default list of filtering
- Visibility to protect Internet access across all devices, locations & users
- Rapid deployment - no physical hardware to install or manual software updates

amatis

Benefiting From Market Leading Intelligence

Delivered as a cloud service, this solution is able to utilise big data and benefit from intelligent analytics and machine learning to keep pace with the threats we face.

Cisco Umbrella analyses over 150 billion page requests from 90 million users each and every day. It utilises this intelligence, combined with feeds from third party sources to determine whether each web request you make is safe.

A Simple Step, Delivered As-A-Service

Putting in place Internet Security from amatis is probably one of the simplest steps you can take to protect your organisation. As a cloud-based service there is no hardware or software required and no complex configuration.

You simply point your users at the Cisco Umbrella DNS service and immediately gain all of the benefits of DNS protection from the industry leader.

Umbrella integrates with your existing security stack including security appliances, intelligence platforms, and cloud access security broker (CASB) controls.

		Insights
Reduce Risk	Forward external DNS traffic for: Any devices for on-network protection Windows, macOS, iOS & Android for off-network protection	✓
	Reduces malware, phishing and ransomware attacks	✓
	Block domains associated with phishing, malware, botnets, and other high risk categories (cryptomining, newly seen domains, etc).	✓
	SafeSearch for Google, Bing, and YouTube	✓
Enforce Policies	Network or network device (including VLAN or SSID) granularity	✓
	Roaming computer granularity	✓
	SAML/AD group membership and internal subnet granularity	✓
	DNS-layer visibility and control and IP responses per security and content settings	✓
	Enable web filtering	✓
	Create custom block/allow lists	✓
	Proxy risky domains with customisable URL blocking and file inspection	✓
	IP-layer enforcement for C2 callbacks that bypass DNS	✓
	Granular customisable block pages and bypass options	✓
Visibility reports	Real-time, enterprise-wide activity search and scheduled reports	✓
	Attribution by external IP	✓
	Attribution by roaming computer and/or internal IP	✓
	Attribution by user or computer	✓
	Identify targeted attacks with local vs. global activity report	✓
	Cloud & IoT usage report shows risks on over 1800 services	✓
Integrations	Deployment: Cisco - ISR, AnyConnect, WLAN Controller. Partner - Aruba, Cradlepoint, Aerohive, etc.	✓
	Log retention: Customer or Cisco-managed AWS S3 bucket	✓