

Cisco Umbrella cheat sheet for partners

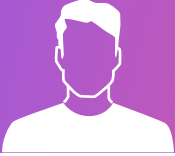


What is Cisco Umbrella?

A cloud security platform that provides the first line of defense against threats on the internet wherever users go – on and off the corporate network.

Elevator pitch

Cisco Umbrella is a cloud security platform that provides the first line of defense against threats on the internet wherever users go. By learning from internet activity patterns, Umbrella automatically uncovers current and emerging threats. And because it's built into the foundation of the internet and delivered from the cloud, Umbrella is the simplest security product to deploy and delivers powerful, effective protection.

Buyers

		
Security admin	CIO/CISO/VP	System/Network admin
<p>Top concerns</p> <ul style="list-style-type: none"> • Implement security policies • Manage security solutions • Interpret alerts and respond to threats <p>Why they'll like Umbrella:</p> <ul style="list-style-type: none"> • Visibility and protection • Integrates with their current security stack • Reduction in malware 	<p>Top concerns</p> <ul style="list-style-type: none"> • Prevent & respond to high-profile data breaches that can damage business • Manage GRC enterprise-wide <p>Why they'll like Umbrella:</p> <ul style="list-style-type: none"> • Simple to deploy & manage • Enterprise-wide protection in minutes 	<p>Top concerns</p> <ul style="list-style-type: none"> • Prevent business disruptions • Increase business benefits • Enforce IT policies <p>Why they'll like Umbrella:</p> <ul style="list-style-type: none"> • 100% uptime & availability • No added latency • Unobtrusive for end users

Customer challenges

Constantly dealing with malware, ransomware, and phishing

Security teams deal with too many malware infections and phishing attacks. They spend a lot of time and effort trying to detect threats and remediate after the fact.

Gap in visibility and coverage.

Organizations have more locations and devices to protect – which means they often lack visibility into all internet activity. Roaming users and branch offices often have minimal protection and are more vulnerable to threats.

Complexity

Existing security products are often difficult to manage, don't scale well, aren't reliable, or won't integrate with other products.

Use cases

- Malware & breach protection
- Off-network coverage
- Extend threat protection
- Protect guest wi-fi
- Content filtering
- Threat intelligence (through Cisco Umbrella Investigate Console or API)

Why Cisco Umbrella?

Best Coverage

- Protect all devices on your network (managed & unmanaged BYOD, IoT, etc.)
- Protect laptops on and off your VPN
- Simplest security to deploy everywhere

Best Protection

- Stop threats across all ports and protocols
- Stop threats before they reach your network or endpoints
- Access intelligence about malware, domains, and IPs across the internet
- Easily integrate with your existing security stack

Best Performance

- No added latency or need to proxy every connection

Key Numbers

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

Qualifying questions

Question	Guidance
How do you protect devices when they are off the corporate network?	Many rely on antivirus or perhaps a more advanced endpoint security product. But, those products are file-based and the threat has to reach the endpoint before they can attempt to block it. Umbrella stops threats earlier.
How do you extend protection across all ports and protocols—especially when devices are off the corporate network?	Many customers only have protection over all ports and protocols with their firewall, which only protects on the perimeter. Umbrella can extend protection and provide a new source of intelligence.
How many malware infections does your team deal with on a weekly basis?	This question can help you quantify a major pain point for the customer.
What are you doing for recursive DNS security & visibility organization-wide?	Umbrella can be an added layer of protection and visibility that customers haven't considered before.
How do you research domains & IPs during incident investigations?	This question will give insight into their current IR process to see if access to Umbrella's threat intelligence (through the Cisco Umbrella Investigate UI or API) would add value.
How much time does your security team spend investigating incidents?	This will help quantify a pain point that Investigate could help address.