Solution brief

Cisco Umbrella

Protect your users and devices with Cisco Umbrella and Cisco AMP for Endpoints

Challenges of protecting endpoints

An estimated 70% of breaches start on endpoints – laptops, workstations, servers, and mobile devices[1]. Why do endpoints continue to be the primary point of entry for attacks?

Gaps in protection

When users and endpoints are off-network, preventative tools like antivirus are often the only protection available. This is not enough when it comes to today's advanced threats.

57% of organizations say that mobile devices are one of the most challenges areas to defend[2]

Gaps in visibility

Organizations are often blind to malware attacks and the scope of a compromise. They have limited visibility into user and endpoint activity, and lack the context to see where malware came from, where it has been, and what it's doing. They can't detect what they can't see.

197 days Industry average detection time for a breach

69 days Industry average time to contain a breach[3]

User error

An attacker sends out a phishing email with a malicious attachment or link. Despite training or countless warnings, it's inevitable, users are going to open or click things that they shouldn't.

56% of organizations say that user behavior is one of the most challenges areas to defend[2]

Needs of an organization

Organizations need deep visibility into where their users are trying to connect on the Internet and the ability to stop malicious behavior across their devices.

Effective protection for endpoints

Cisco Umbrella and Cisco AMP for Endpoints together provide the first and last line of defense to help you prevent, detect and respond to attacks before damage can be done.

Prevent	Detect	Respond
AMP for Endpoints · Blocks attacks at initial inspection monitoring files, memory, and behavior · Uses sandbox (powered by ThreatGrid) to analyze unknown files	**AMP for Endpoints** · Continuously analyzes all file activity to detect malicious behavior and retrospectively alert on net new threats	**AMP for Endpoints** · Shows the full history and context of acompromise · Provides blocking of malware with a single click
Umbrella · Blocks malicious Internet requests (domain, URL, & IP) before connections are ever made	**Umbrella** · Learns where attacks are staged and detects attackers infrastructure in order to proactively block threats	**Umbrella** · Provides rich threat intelligence on domains, IPs, and file hashes so you can triage faster.

AMP for Endpoints

AMP for Endpoints is a cloud-managed endpoint security solution that prevents cyberattacks and rapidly detects, contains, and remediates malicious files on the endpoints.

Overview Video | Demo Video

AMP for Endpoints uses:

- continuous analysis of file behavior
- retrospective detection
- antivirus inspection engine
- static and dynanic file analysis (sandboxing via Threat Grid)
- machine learning
- vulnerability monitoring
- exploit and memory protection

Feature spotlight:

- Proactive Blocking - AMP for Endpoints uses a combination of file reputation, behavioral indicators, sandboxing technology, and global threat intelligence provided by the Talos Security Intelligence Group to analyze unknown files and automatically block malware from trying to run on endpoints.
- Continuous analysis and retrospective security - advanced malware can evade front-linedefenses and infiltrate an endpoint. AMP for Endpoints has you covered. It continuously monitors and records all file activity on endpoints to quickly spot malicious behavior. AMP then shows the complete recorded history of the malware's behavior over time—where themalware came from, where it's been and what it's doing. This enables you to retrospectively detect and remediate threats before damage can be done.

Umbrella

Umbrella is a cloud security platform that provides the first line of defense against threats on the internet for users on or off the corporate network. Umbrella delivers complete visibility into internet activity across all locations and endpoints, and can proactively block malicious requests before a connection is established.

Overview Video | Demo Video

Umbrella helps organizations:

- Stop attacks earlier
- Identify already infected devices faster
- Prevent data exfiltration

Feature spotlight:

- Intelligence - Umbrella is built on a global network that resolves over 175 billion DNS(Domain Name System) requests every day, and derives intelligence directly from that data. Using a combination of machine learning and human intelligence, the datais analyzed to identify patterns, detect anomalies, and create statistical models to automatically uncover current attacks and attacker infrastructure being staged for the next threat.
- Intelligent proxy - The Umbrella intelligent proxy provides customers more granular protection. If Umbrella receives a request for a domain that is neither known good or bad,it is routed to the proxy for deeper inspection. Umbrella uses a combination of Cisco Talos,Cisco web reputation systems, and partner feeds to block millions of malicious URLs. Umbrella provides file inspection using an AV engine and Cisco AMP.

> **"Without Umbrella and AMP for Endpoints, detection and recovery would literally have costs us months of work and frustration."**
>
> **Tony Hynes**
> Director of IT Security
> Axcess Financial

> **"We have much greater confidence in the security of our endpoints with Cisco Umbrella combined with Cisco AMP. We have had zero malware infections since our implementation 3 years ago."**
>
> Engineer, Medium Enterprise
> Financial Services CompanyLearn

Learn more

Cisco AMP for Endpoints

Cisco Umbrella

1. Effective Incident Detection and Investigation Saves Money, IDC, 2016
2. Cisco 2018 Security Capabilities Benchmark Study
3. Ponemon 2018 Cost of a Data Breach Study