SOLUTION BRIEF

Protect your endpoints with Cisco AMP for Endpoints and Cisco Umbrella

Challenges of protecting endpoints

An estimated 70% of breaches start on endpoints - laptops, workstations, servers, and mobile devices. 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.

65%

of organizations say attacks evaded existing preventative tools[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.

55%

of organizations are unable to determine cause of breach[3]

100 DAYS

average time to detection[4]

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.

48%

of attackers bypass endpoint defenses because of user error[5]

Needs of an organization

Organizations need deep visibility into what files and users are doing on the endpoint itself, and where that endpoint is trying to connect to on the internet—plus the control to stop malicious behavior.

Effective protection for endpoints

Cisco AMP for Endpoints and Cisco Umbrella are two security solutions that work in harmony to provide the visibility, context, and control needed to prevent, detect and respond to attacks targeting endpoints, before damage can be done.

PREVENT

AMP for Endpoints

- Blocks known malware at initial inspection
- Uses sandbox (powered by Threat Grid) to analyze unknown files

Umbrella

- Blocks malicious internet requests (domain, URL, & IP) requests, regardless of delivery mechanism (email, web drive-by, etc.)

DETECT

AMP for Endpoints

- Continuously analyzes all file activity on endpoints to quickly detect malicious behavior and retrospectively alert security teams

Umbrella

- Prevents command and control (C2) callbacks to attacker's servers to stop data exfiltration and execution of ransomware encryption

RESPOND

AMP for Endpoints

- Shows the full history and context of a compromise
- Can stop attacks via outbreak control capabilities and quarantining files

Umbrella Investigate

- Provides up-to-the-minute threat data and historical context about domains, IPs, and file hashes for faster investigation

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 dynamic 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-line defenses 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 the malware 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 100 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 data is 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.

" Cisco Advanced Malware Protection, in combination with Cisco Umbrella, has decreased the number of ransomware outbreaks to zero during the last 8 months."

Freek Bosscha,
IT Architect, NHL University

" 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 Company Learn

Want to learn more?

Contact a Port 53 rep:
510-353-3903

Or visit Port53Tech.com