Solution Endpoint Network Content

Cisco Advanced Malware Protection (AMP)

AT-A-GLANCE

AMP provides an efficient process for solving threats by going beyond detection

The flaw with point-in-time detection alone:

Point-in-time detection alone will never be 100% effective. It only takes one threat to evade detection and compromise your environment. Using targeted, context-aware malware, sophisticated attackers have the resources, expertise and persistence to outsmart point-in-time defenses and compromise any organization at any time. Point-in-time detection is completely blind to the scope and depth of a breach after it happens.

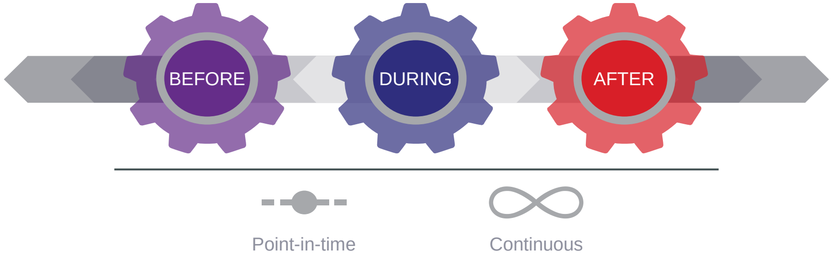
AMP provides retrospective security and point-in-time detection:

AMP offers the only advanced malware protection system that covers the entire attack continuum—before, during and after an attack, with continuous analysis and advanced analytics that enable Cisco's Retrospective Security capabilities.

Retrospective Security lets Security Managers turn back time on threats in their system with tools such as retrospection, attack chain correlation, behavioral indications of compromise (IOCs), trajectory and breach hunting.

AMP simplifies Incident Response:

With these retrospective security tools, you can establish scope, visibility and control in the event of a breach. This enables your security team to quickly and effectively remediate all threats in your environment before it's too late.



Key AMP Benefits

Retrospective Security for Advanced Threats

- Continuous analysis and subsequent retrospective alerting informs users of infected files in the event that the malware determination changes after initial analysis
- AMP captures, analyzes and correlates activity to provide security personnel automated analysis and risk prioritization

Protection Across the Attack Continuum

- Web reputation and zero-day threat intelligence from Cisco Security Intelligence Operations (SIO) stops threats before they enter the network
- File reputation and sandboxing identifies threats during an attack
- Retrospective Security provides retrospection, IOCs, breach detection, tracking, analysis and surgical remediation after an attack where advanced malware has slipped past other defenses

Visibility and Control

- Retrospective alerts inform you of any change in disposition, including who on your network may have been infected and when they were infected
- Dashboards show exactly where the threat has been, what it did and the root causes so you can quickly contain and remediate

Flexibility and Choice

- AMP can be activated on your Cisco Email and Web Security solution with the flip of a switch
- AMP can also be deployed in-line as a dedicated network appliance and at the endpoint as a lightweight connector for greater visibility and control

Cisco Advanced Malware Protection (AMP)

AT-A-GLANCE

Key AMP Features

Point in Time Protection

File Reputation: AMP captures a fingerprint of each file as it traverses the gateway and sends it to AMP's cloud-based intelligence network for a reputation verdict checked against zero-day exploits.

File Sandboxing: When malware is detected, AMP gleans precise details about a file's behavior. AMP then combines that data with detailed human and machine analysis to determine the file's threat level in a sandbox.

Retrospective Security

Continuous Analysis: Continuous analysis combined with advanced analytics enables retrospective capabilities to look back in time to trace processes, file activities and communications in order to understand the full extent of an infection, establish root cause and perform remediation. The need for retrospective security arises when any indication of a compromise occurs, such as an event trigger, a change in disposition of a file or an IOC trigger.

Visibility and Control: AMP solves the problem of malicious files or threats that get through point-in-time detection by continuously analyzing and tracking behavior and activity. AMP delivers dashboards and reports that quickly show's a breach's location and scope and the infection's timeline and root cause.

Collective Security Intelligence

Cisco SIO and Sourcefire's VRT collective security intelligence represent the industry's largest collection of real-time threat intelligence, with the broadest visibility, largest footprint and ability to put it into action across multiple security platforms.

- 1.6 million global sensors
- 100 TB of data received per day
- 600+ engineers, technicians and researchers
- 35% worldwide email traffic
- 24x7x365 operations
- 40+ languages
- 180,000+ File Samples per day
- Advanced Microsoft Disclosures
- FireAMP™ Community
- Snort and ClamAV Open Source Communities
- Sourcefire AEGIS™ Program
- Private and Public Threat Feeds

AMP Platform Features

Features	Content	Network	Endpoint
File Reputation	✓	✓	✓
Sandboxing	✓	✓	✓
Retrospective Detection	✓	✓	✓
Indications of Compromise		✓	✓
File Analysis		✓	✓
File Trajectory		✓	✓
Device Trajectory			✓
Elastic Search			✓
Outbreak Control			✓

Where these solutions protect

Content	Email and web traffic
Network	Network perimeter, datacenters or other critical network appliances
Endpoint	Roaming devices, Macs and PCs

Learn More

Find out more at http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html. Evaluate how Cisco products can work for you with a Cisco sales representative or channel partner.