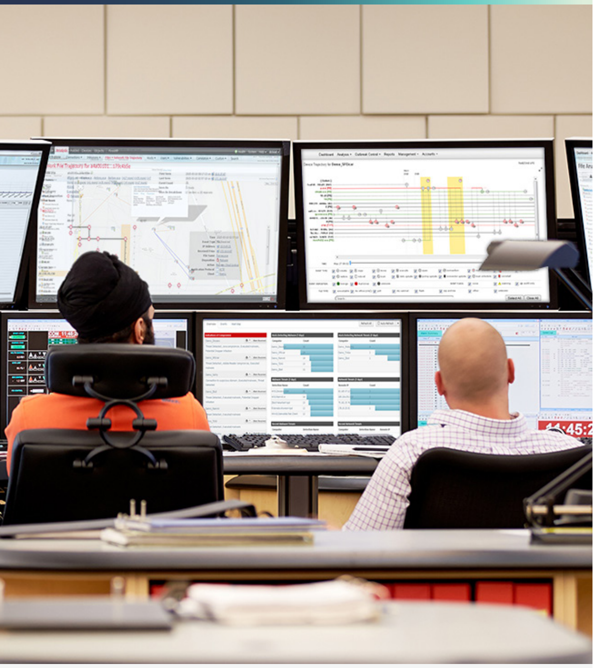
At-a-Glance



Cisco Advanced Malware Protection for Endpoints

Benefits

- **Continuously detect and monitor** malware, immediately and retrospectively
- **Protect Windows operating systems,** Macs, Linux, and mobile devices
- **Record file activity** over time to track malware's spread and scope a compromise
- **Correlate discrete events** into coordinated attacks
- **Access global threat intelligence** to strengthen network defenses
- **Gain deep visibility, context, and control** to quickly detect, analyze, and remediate breaches
- **Get agentless detection** to catch malware before it compromises the OS level

Breach Prevention, Detection, Response, and Remediation for the Real World

Hackers are creating advanced malware that can evade even the best prevention tools, like antivirus and intrusion prevention systems. These tools will never be 100 percent effective at preventing all threats. Furthermore, they provide no visibility into threats that evade initial detection. This leaves IT security teams blind to the scope of a potential compromise and unable to quickly detect and remediate malware before it causes damage.

Cisco AMP for Endpoints is a cloud-managed endpoint security solution that provides the visibility, context, and control to not only prevent breaches, but also rapidly detect, contain, and remediate threats if they evade front-line defenses and get inside, all cost-effectively and without affecting operational efficiency.

- **Prevent:** Strengthen defenses using the best global threat intelligence and block malware in real time.
- **Monitor and detect:** Continuously monitor and record all file activity to quickly detect stealthy malware.
- **Respond:** Accelerate investigations and automatically remediate malware across PCs, Macs, Linux, and mobile devices.

Threat Intelligence and Dynamic Malware Analysis

Cisco AMP is built on an extensive collection of real-time threat intelligence and dynamic malware analytics supplied by the Talos Security Intelligence and Research Group, and Threat Grid intelligence feeds.

Organizations benefit from:

- 1.5 million incoming malware samples per day
- 1.6 million global sensors
- 100 terabytes of data per day
- 13 billion web requests
- Team of engineers, technicians, and researchers
- 24-hour operations

Features

Continuous analysis and retrospective security: AMP continues to monitor, analyze, and record file activity to quickly detect malware that evades front-line defenses and help you scope a compromise and quickly respond.

Dynamic malware analysis and sandboxing: Analyze malware against a large set of behavioral indicators in order to discover previously unknown zero-day threats.

Indications of compromise (IoCs): File, telemetry, and intrusion events are correlated and prioritized as potentially active breaches, helping security teams to rapidly identify malware incidents and connect them to coordinated attacks.

Device trajectory: Continuously track executable activity and communications on devices and on the system level to quickly understand root causes and the history of events leading up to and after a compromise.

Prevalence: AMP displays low prevalence files that are running across your organization to help you surface previously undetected threats seen by a small number of users.

Vulnerabilities: Identify vulnerable software and close attack pathways. AMP identifies the vulnerable software being targeted, the potential exploit, and shows a prioritized list of hosts to patch.

Integration with Cognitive Threat Analytics (CTA): See an average 30% more infections, uncover file-less or memory-only malware, catch malware before it compromises the OS-level, and get visibility into devices with no AMP for Endpoints connector installed.

Antivirus Engine: Perform offline and system-based detections, including rootkit scanning, to complement other AMP capabilities such as local IOC scanning, and device and network flow monitoring. The engine can be enabled by customers that want to consolidate their antivirus and advanced endpoint protection in one agent.

Outbreak control: Achieve control over outbreaks and remediate without waiting for a content update.

- Quickly block a specific file across all or selected systems
- Block families of polymorphic malware
- Contain a compromised application being used as a malware gateway and stop the reinfection cycle
- Stop malware call-back communications at the source, even for remote endpoints outside the corporate network

For more features, see the AMP for Endpoints Data Sheet.

AMP for Endpoints' built-in sandboxing technology, powered by Threat Grid, analyzes millions of samples every month, against more than 700 behavioral indicators, resulting in billions of artifacts and an easy-to-understand threat score to help security teams uncover stealthy malware and prioritize their response.

Continuous Analysis and Retrospective Security

Cisco AMP for Endpoints continuously monitors, analyzes, and records all file and executable activity, regardless of disposition, even after initial inspection. If AMP observes suspicious activity, security teams will be sent an alert and can see the complete history of the threat to quickly get answers to these questions:

- Where did the malware come from?
- What was the method and point of entry?
- Where has it been? What systems were affected?
- What did the threat do and what is it doing now?
- How do we stop the threat and eliminate the root cause?

With a few clicks from AMP's browser-based management console, the file can be blocked from executing on all endpoints. Since Cisco AMP knows every other endpoint where that file has been, it can also quarantine the file for all users. Security teams no longer need to reimage complete systems to eliminate malware. That takes time, money, and resources. With AMP, malware remediation is surgical, with no associated collateral damage to IT systems or the business.

Also, AMP remembers what it sees, from the threat's signature to the behavior of the file, and logs the data in AMP's threat intelligence database. This further strengthens front-line defenses so this file, and files like it, will not be able to evade initial detection again.

Deployment

Cisco AMP for Endpoints is managed through an easy-to-use, web-based console. It is deployed through AMP's lightweight endpoint connector, with no performance impact on users. Analysis is done in the cloud, not on the endpoint. The solution is offered as a subscription on endpoints, including coverage for Windows, Macs, Linux, and mobile devices. AMP for Endpoints can also be launched from AnyConnect v4.1.

Next Steps

Talk to a Cisco sales representative or channel partner about how Cisco AMP for Endpoints can help you defend your organization from advanced cyber attacks. Learn more at www.cisco.com/go/ampendpoint.