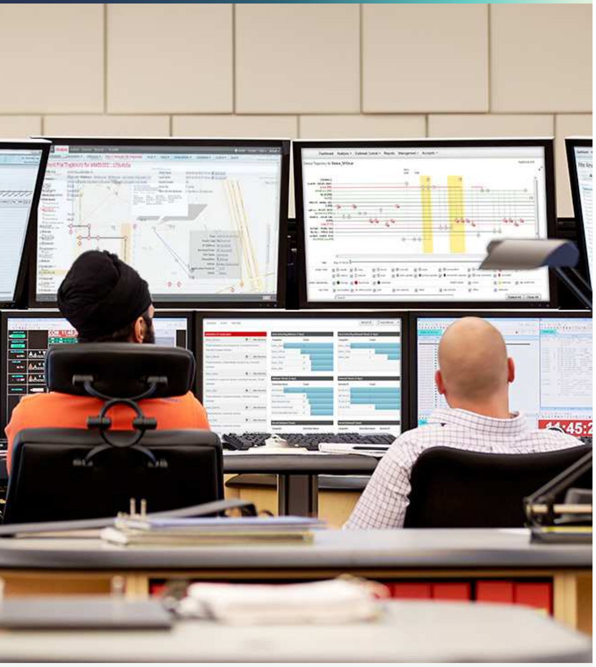
At-a-Glance



Benefits

- **Continuously detect and monitor** malware, immediately and retrospectively
- **Protect Windows operating systems,** Macs, Linux, mobile devices, and virtual environments
- **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 and control** to quickly detect, analyze, and remediate breaches

Cisco Advanced Malware Protection for Endpoints

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

Hackers are creating advanced malware that can evade even the best point-in-time detection tools, like antivirus and intrusion prevention systems. These tools will never be 100 percent effective at detecting all threats. Furthermore, they provide little 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® Advanced Malware Protection (AMP) for Endpoints goes beyond point-in-time capabilities to protect organizations before, during, and after an attack.

- **Before an attack**, AMP uses the best global threat intelligence to strengthen defenses.
- **During an attack**, AMP uses that intelligence, known file signatures, and dynamic file analysis technology to block malware trying to infiltrate your IT environment.
- **After an attack**, AMP monitors all file and executable activity to catch malware that evaded initial detection, and provides the visibility and control to rapidly remediate it.

Cisco AMP for Endpoints not only prevents breaches but also rapidly detects, contains, and remediates threats if they evade front-line defenses, all cost-effectively and without affecting operational efficiency.

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 Cisco Collective Security Intelligence, Talos Security Intelligence and Research Group, and AMP Threat Grid intelligence feeds.

Organizations benefit from:

- 1.1 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: A highly secure environment helps you launch and analyze malware against a large set of behavioral indicators in order to discover previously unknown zero-day threats.

Indications of compromise (IoCs): File and telemetry events are correlated and prioritized as potentially active breaches. AMP automatically correlates multisource security event data, such as intrusion and malware events, to help security teams connect events to coordinated attacks and prioritize high-risk events.

Device trajectory: You can 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 all files that are running across your organization, ordered by prevalence, to help you surface previously undetected threats seen by a small number of users. Files opened by only a few users may be malicious.

Vulnerabilities: AMP shows a list of vulnerable software on your system, the hosts containing that software, and the hosts most likely to be compromised. AMP identifies the vulnerable software being targeted, and the potential exploit, providing you with a prioritized list of hosts to patch.

Application Programming Interface (API): With an API enabled on AMP for Endpoints, users can more easily integrate third-party security tools and access data and events in their AMP for Endpoints account without the need to log into the management console.

Outbreak control: AMP helps you achieve control over suspicious files or outbreaks and remediate without waiting for a content update. It also:

- Quickly blocks a specific file across all or selected systems
- Blocks families of polymorphic malware
- Contains a compromised application being used as a malware gateway and stops the reinfection cycle
- Stop malware call-back communications at the source, even for remote endpoints outside the corporate network
- Helps ensure that mission-critical applications continue to run no matter what

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

The integration of our AMP Threat Grid technology into Cisco AMP for Endpoints also provides context-rich intelligence feeds. The technology analyzes millions of samples every month, against more than 400 behavioral indicators, resulting in billions of artifacts and an easy-to-understand threat score to help security teams prioritize 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 another endpoint. Since Cisco AMP knows every other endpoint where that file has been, it can also pull the file out of memory and quarantine it 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, mobile devices, and virtual systems. 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 cyberattacks. Learn more at www.cisco.com/go/ampendpoint.