Cisco Advanced Malware Protection

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

BENEFITS

- Gain unmatched global threat intelligence to strengthen front-line defenses
- Get deep visibility into the origin and scope of a compromise
- Rapidly detect, respond to, and remediate malware
- Prevent costly reinfection and remediation scenarios
- Protection everywhere—network, endpoints, mobile devices, email, and web—before, during, and after an attack

Organizations are under attack, and security breaches are constantly making headlines. Today's global community of hackers is creating advanced malware and launching it into organizations through a variety of attack vectors. These multifaceted, targeted attacks can evade even the best prevention tools. These tools inspect traffic and files at the point of entry into the network, block known threats, and let "good" or "unknown" files into the network. Unfortunately, that is where the analysis stops. If a stealthy malicious file manages to evade those defenses, these tools provide little visibility into the activity of threats on your system. This leaves security professionals blind to the scope of a potential compromise and unable to quickly detect malicious behavior, quickly respond, contain, or eliminate malware before it causes significant damage.

Cisco® Advanced Malware Protection (AMP) is a security solution that addresses the full lifecycle of the advanced malware problem. It not only prevents breaches but also gives you the visibility, context, and control to rapidly detect, contain, and remediate threats if they evade front-line defenses, all cost-effectively and without affecting operational efficiency.

Product Overview

AMP is an intelligence-powered, integrated enterprise-class advanced malware analysis and protection solution. You get comprehensive protection for your organization across the attack continuum: before, during, and after an attack.

- **Before** an attack, AMP uses global threat intelligence from Cisco's Talos Security Intelligence and Research Group and Threat Grid's threat intelligence feeds to strengthen defenses and protect against known and emerging threats.
- **During** an attack, AMP uses that intelligence coupled with known file signatures and Cisco Threat Grid's dynamic malware analysis technology to identify and block policy-violating file types and exploit attempts and malicious files trying to infiltrate the network.
- **After** an attack, or after a file is initially inspected, the solution goes beyond point-in-time detection capabilities and continuously monitors and analyzes all file activity and traffic, regardless of disposition, searching for any indications of malicious behavior. If a file with an unknown or previously deemed "good" disposition starts behaving badly, AMP will detect it and instantly alert security teams with an indication of compromise. It then provides visibility into where the malware originated, what systems were affected, and what the malware is doing. It also provides the controls to rapidly respond to the intrusion and remediate it with a few clicks. This gives security teams the level of deep visibility and control they need to quickly detect attacks, scope a compromise, and contain malware before it causes damage.

Global Threat Intelligence and Dynamic Malware Analysis

AMP is built on exceptional security intelligence and dynamic malware analytics. The Cisco Talos Security Intelligence and Research Group, and Threat Grid threat intelligence feeds, represent the industry's leading collection of real-time threat intelligence and big data analytics. This data is pushed from the cloud to the AMP client so that you have the latest threat intelligence to proactively defend against threats. You benefit from:

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

AMP correlates files, behavior, telemetry data, and activity against this robust, context-rich knowledge base to quickly detect malware. Security teams benefit from AMP's automated analysis by saving time searching for breach activity and having the latest threat intelligence at all times to quickly understand, prioritize, and block sophisticated attacks.

The integration of our Threat Grid technology into AMP also provides:

- Highly accurate and context-rich intelligence feeds delivered in standard formats to integrate smoothly with existing security technologies
- Analysis of millions of samples every month, against more than 700 behavioral indicators, resulting in billions of artifacts
- An easy-to-understand threat score to help security teams prioritize threats

AMP uses all of this intelligence and analysis to either inform your security decision making or automatically take action on your behalf. For instance, with constantly updated intelligence, the system can block known malware and policy-violating file types, dynamically blacklist connections that are known to be malicious, and block attempts to download files from websites and domains categorized as malicious.

Continuous Analysis and Retrospective Security

Most network and endpoint-based antimalware systems inspect files only at the point in time when they traverse a control point into your extended network. That's where the analysis stops. But malware is sophisticated and very good at evading initial detection. Sleep techniques, polymorphism, encryption, and the use of unknown protocols are just some of the ways that malware can hide from view. You can't defend against something you can't see, and that is how most major security breaches occur. Security teams don't see the threat at the point of entry and are oblivious to its presence after the fact. They don't have the visibility to quickly detect it or contain it, and before long, the malware has achieved its objectives, and the damage has been done.

Cisco AMP is different. Recognizing that point-in-time, preemptive detection and blocking methods are not 100 percent effective, the AMP system continuously analyzes files and traffic even after initial inspection. AMP monitors, analyzes, and records all file activity and communications on endpoints, mobile devices, and in the network in order to quickly uncover stealthy threats that exhibit suspicious or malicious behavior. At the first sign of trouble, AMP will alert security teams and provide detailed information on the behavior of the threat, so you can answer crucial security questions, such as:

- Where did the malware come from?
- What was the method and point of entry?
- Where has it been and 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?

Using this information, security teams can quickly understand what happened and use AMP's containment and remediation functionality to take action. With a few clicks from AMP's easy-to-use browser-based management console, administrators can contain the malware by blocking the file from ever running on another endpoint again. And since AMP knows everywhere the file has been, it can pull the file out of memory and quarantine it for all other users. In the event of a malware intrusion, security teams no longer need to reimage complete systems to eliminate malware. That takes time, costs money and resources, and disrupts critical business functions. With AMP, malware remediation is surgical, with no associated collateral damage to IT systems or the business.

This is the power of continuous analysis, continuous detection, and retrospective security: the ability to record the activity of every file in the system and, if a supposedly "good" file turns "bad," the ability to detect it and rewind the recorded history to see the origin of the threat and the behavior it exhibited. AMP then provides you with built-in response and remediation capabilities to eliminate the threat. AMP also 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 to further strengthen front-line defenses so this file and files like it will not be able to evade initial detection again.

With AMP, security teams have the level of deep visibility and control necessary to quickly and efficiently detect attacks and discover stealthy malware; understand and scope a compromise; quickly contain and remediate malware (even zero-day attacks) before any damage can be done; and prevent similar attacks from happening.

Main Features

AMP's continuous analysis and retrospective security capabilities are made possible because of these robust features:

- **Comprehensive global threat intelligence:** Cisco Talos Security Intelligence and Research Group, and Threat Grid threat intelligence feeds, represent the industry's largest collection of real-time threat intelligence with the broadest visibility, the largest footprint, and the ability to put it into action across multiple security platforms.
- **Indications of compromise (IoCs):** File and telemetry events are correlated and prioritized as potential active breaches. AMP automatically correlates multisource security event data, such as intrusion and malware events, to help security teams connect events to larger, coordinated attacks and also prioritize high-risk events.
- **File reputation:** Advanced analytics and collective intelligence are gathered to determine whether a file is clean or malicious, allowing for more accurate detection.
- **Antivirus Engine:** Perform offline and system-based detections, including rootkit scanning, to complement Cisco's advanced endpoint protection capabilities such as local IOC scanning, and device and network flow monitoring. The engine can be enabled and used by customers that want to consolidate their antivirus and advanced endpoint protection in one agent.
- **Static and dynamic malware analysis:** A highly secure sandboxing environment helps you run, analyze, and test malware in order to discover previously unknown zero-day threats. Integration of Threat Grid's sandboxing and static and dynamic malware analysis technology into AMP solutions results in a more comprehensive analysis checked against a larger set of behavioral indicators.
- **Retrospective detection:** Alerts are sent when a file disposition changes after extended analysis, giving you awareness of and visibility into malware that evades initial defenses.
- **File trajectory:** Continuously track file propagation over time throughout your environment in order to achieve visibility and reduce the time required to scope a malware breach.
- **Device trajectory:** Continuously track activity and communication on devices and on the system level to quickly understand root causes and the history of events leading up to and after a compromise.
- **Elastic search:** A simple, unbounded search across file, telemetry, and collective security intelligence data helps you quickly understand the context and scope of exposure to an IoC or malicious application.
- **Prevalence:** Display all files that have been run in your organization, ordered by prevalence from lowest to highest, to help you surface previously undetected threats seen by a small number of users. Files run by only a few users may be malicious (such as a targeted advanced persistent threat) or questionable applications you may not want on your extended network.
- **Endpoint IoCs:** Users can submit their own IoCs to catch targeted attacks. These endpoint IoCs let security teams perform deeper levels of investigation on lesser-known advanced threats specific to applications in their environment.
- **Vulnerabilities:** Shows a list of vulnerable software on your system, the hosts containing that software, and the hosts most likely to be compromised. Powered by our threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware, and the potential exploit, providing you with a prioritized list of hosts to patch.

- **Outbreak control:** Achieve control over suspicious files or outbreaks and remediate an infection without waiting for a content update. Within the outbreak control feature:
  - Simple custom detections can quickly block a specific file across all or selected systems
  - Advanced custom signatures can block families of polymorphic malware
  - Application blocking lists can enforce application policies or contain a compromised application being used as a malware gateway and stop the reinfection cycle
  - Custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what
  - Device flow correlation will stop malware call-back communications at the source, especially for remote endpoints outside the corporate network

Deployment Options for Protection Everywhere

Cybercriminals launch their attacks through a variety of entry points into organizations. To be truly effective at catching stealthy attacks, organizations need visibility into as many attack vectors as possible. Therefore, the AMP solution can be deployed at different control points throughout the extended network. Organizations can deploy the solution how and where they want it to meet their specific security needs. Options include those in the following list:

Product Name	Details
Cisco AMP for Endpoints	Protect PCs running Windows, Macs, Linux systems, and Android mobile devices using AMP's lightweight connector, with no performance impact on users. AMP for Endpoints can also be launched from AnyConnect v4.1.
Cisco AMP for Networks	Deploy AMP as a network-based solution integrated into Cisco Firepower NGIPS security appliances.
Cisco AMP on Firewalls and ASA with FirePOWER Services	Deploy AMP capabilities integrated into the Cisco NGFW or ASA Adaptive Security Appliance firewall.
Cisco AMP Private Cloud Virtual Appliance	Deploy AMP as an on-premises, air-gapped solution built specifically for organizations with high-privacy requirements that restrict using a public cloud.
Cisco AMP on ESA, or WSA	For Cisco Email Security Appliance (ESA) or Web Security Appliance (WSA), AMP capabilities can be turned on to provide retrospective capabilities and malware analysis.
Cisco AMP for Meraki MX	Deploy AMP as part of the Meraki MX Security Appliance for cloud-based simplified security management with advanced threat capabilities.
Cisco Threat Grid	Threat Grid is integrated with Cisco AMP for enhanced malware analysis. It can also be deployed as a standalone advanced malware analysis and threat intelligence solution, in the cloud or on an appliance.

Cisco Advanced Malware Protection is truly "everywhere" now. This visibility and control across multiple attack vectors, from network edge to endpoint, is exactly what you need to quickly uncover stealthy malware and eliminate it. But you also need the ability to share information across your security infrastructure for thorough and quick action. The interconnectivity, communication, and integration among all these solutions is important to note here. These are not point products that live in a vacuum. When deployed together, the solutions work together to provide an integrated defense that systematically and rapidly responds to threats. An ecosystem is created whereby the AMP solutions automatically share threat intelligence, indications of compromise, event information, and quarantine information across all the deployments. With AMP "eyes everywhere," organizations can drastically reduce time to detection and time to remediation of malware.

Cisco AMP Leads in Third-Party Test

Cisco is the leader in NSS Labs' Breach Detection Systems Report for the third year in a row, according to the 2016 NSS Labs Breach Detection Systems Comparative Analysis Report. The 2016 NSS Labs comparative product test provides the details on how Cisco AMP achieved:

- 100% Security Effectiveness rating-the highest of all vendors tested
- Only vendor to detect and block 100% of malware, exploits, and evasion techniques during testing
- Fastest time to detection of all vendors tested
- Excellent performance with minimal impact on endpoint or application latency

Why Cisco?

It's no longer a question of if you'll be breached, it's a matter of when. Prevention tools alone will never be 100 percent effective at preemptively detecting and blocking all attacks. Something will get in. Therefore, in the event of a breach, organizations need to be prepared with tools to quickly detect an intrusion, then respond to and remediate it.

Cisco AMP is an intelligence-powered, integrated, enterprise-class advanced malware analysis and protection solution. It provides global threat intelligence to strengthen network defenses, analysis engines to block malicious files in real time, and the ability to continuously monitor and analyze all file behavior and traffic even after initial inspection. These capabilities provide unmatched visibility into potential threat activity and the control to then rapidly detect, contain, and eliminate malware.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps

To learn more about Cisco AMP visit http://www.cisco.com/go/amp. You can also watch this short overview video, see a concise or detailed demonstration of the technology, hear from customers, see how AMP stacks up against the competition, or reach out to your Cisco sales representative to set up a POV with a Cisco AMP specialist.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C22-734228-05 11/16