At-a-Glance

Cisco Advanced Malware Protection for Networks

Benefits

- **Detect and block** exploit attempts, malicious files, and policy-violating files
- **Continuously analyze and record** file activity to track malware's spread and scope a compromise
- **Correlate discrete events** into coordinated attacks
- **Gain deep visibility and control** to quickly detect, analyze, and contain breaches
- **Access unmatched global threat intelligence** to strengthen network defenses
- **Reduce event notifications** and get actionable insight into malware to prioritize threats faster

Breach Prevention, Detection, and Response for the Real World

Today's attacks are stealthy and evasive, designed to bypass traditional defenses like firewall, anti-virus and intrusion prevention systems. Having a best of breed perimeter defense is a key part of any security strategy, but these tools will never be 100 percent effective at detecting all threats. Furthermore, they provide little visibility into the activity of threats after they evade first-line defenses. This leaves IT security teams blind to the scope of a potential compromise and unable to quickly detect and contain malware before it causes damage. Organizations need advanced threat capabilities to investigate and analyze attacks that slip by front line defenses.

Cisco Advanced Malware Protection (AMP) for Networks delivers network-based defense that 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 network defenses.
- **During an attack,** AMP uses that intelligence, known file signatures, and dynamic file analysis technology to block malware trying to infiltrate the network.
- **After an attack,** or after a file traverses the network, AMP continuously monitors and analyzes all file activity and traffic. If a file exhibits malicious behavior, AMP will provide deep visibility into the activity of the threat and the control to rapidly respond and contain it.

AMP for Networks not only provides breach prevention capabilities, but in the case of an undetected intrusion, provides rapid breach detection, response, and containment capabilities – all cost-effectively and without impacting operational efficiency.

Threat Intelligence and Malware Analysis

AMP for Networks is built on the largest collection of real-time threat intelligence and malware analytics supplied by Cisco Collective Security Intelligence, the Talos Security Intelligence and Research Group, and AMP 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 250+ engineers, technicians, and researchers
- 24-hour operations

Features

Continuous analysis: Even after a file traverses the network control point, AMP continues to monitor, analyze, and record file activity and behavior to quickly detect malware that evades front-line defenses.

Retrospective security: If a previously deemed "unknown" or "good" file exhibits malicious behavior, AMP sends a retrospective alert and shows you the recorded history of that file's activity so you can scope the compromise and quickly respond.

Cisco Firepower Management Center (FMC): AMP is managed through FMCs easy-to-use web brower-based console. You get visibility into your environment through a single pane of glass with a view into threat activity, hosts, operating systems, applications, users, files, and geolocation information.

Malware analysis and sandboxing: Threat Grid's 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): AMP automatically correlates multisource security event data like file, telemetry, intrusion, and malware events and prioritizes them as potential active breaches. This helps security teams connect events to larger coordinated attacks and prioritize high risk events.

File trajectory: File propagation is continuously tracked over time to provide visibility and reduce the time required to scope a malware breach.

Integration with Cisco AMP for Endpoints: For added visibility into executable activity on endpoints, and to correlate network events with endpoint events, AMP for Networks is compatible with AMP for Endpoints.

The integration of our AMP Threat Grid technology into Cisco AMP for Networks also provides context-rich intelligence feeds. The technology 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 prioritize response.

Continuous Analysis and Retrospective Security

AMP for Networks continuously monitors, analyzes, and records all file activity, regardless of disposition, even after initial inspection at the network control point. If AMP observes suspicious or malicious activity, or if a previously deemed "good" file turns "bad," security teams are sent a retrospective alert and an indication of compromise. AMP also provides visibility into exactly what happened. Security teams can see the complete recorded history of the threat, essentially rolling back time on malware, and quickly get answers to crucial security questions, such as:

- Where did the malware come from?
- What systems were affected?
- What is the threat doing?
- How do we stop it?

Using the File Trajectory feature, security teams can track a file's transmission across the network by viewing a visual display of the file's transfers over time and other information about the file. Then, blocking these malicious files and communications with a simple policy update and a custom detection is easy. You are empowered to act whenever you decide, without the need to wait for a vendor-supplied update.

This is continuous analysis and retrospective security in action, and it equips security teams with the visibility and control to quickly detect, respond to, and contain threats.

Deployment

AMP for Networks is managed through the Cisco Firepower Management Center, an easy-to-use web-based management console. It is deployed as a subscription on a Cisco Firepower next-generation intrusion prevention system (NGIPS) spanning a broad range of network throughput and processing capabilities.

Next Steps

Talk to a Cisco sales representative or channel partner about how AMP for Networks can help you defend your organization against advanced cyberattacks. Learn more at www.cisco.com/go/ampnetwork.

C45-731875-03 02/17