Cisco Advanced Malware Protection

Visibility and Control for Breach Prevention, Detection, and Remediation

Organizations are under attack, and security breaches are happening every day. Hackers are creating advanced malware that can evade even the best point-in-time detection tools, like antivirus and intrusion prevention systems. These tools inspect traffic at the point of entry into your extended network, but they will never detect 100 percent of all the threats trying to infiltrate the organization. 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.

Cisco® Advanced Malware Protection (AMP) goes beyond point-in-time capabilities and is built to protect organizations before, during, and after an attack.

Benefits

- Protection before, during, and after an attack
- Rapid detection of, response to, and remediation of stealthy malware
- Unmatched global threat intelligence and malware analysis
- Deep visibility into the origin and scope of a compromise
- Better-informed security decisions and faster investigations
- Protection everywhere: network, endpoints, servers and data centers, mobile devices, virtual environments, and email and web gateways

Continuous Analysis and Retrospective Security

- Even after a file is initially inspected, Cisco AMP continues to monitor, analyze, and record all file activity and behavior, regardless of disposition.
- If a previously deemed "unknown" or "good" file exhibits malicious behavior, AMP automatically sends an alert and shows you the history of that file's activity and behavior so you can scope the compromise and quickly remediate.

Visibility and Control

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

Flexibility and Choice

- Cisco AMP can be deployed on multiple platforms: endpoints, networks, mobile devices, virtual environments, servers, and more. Organizations can deploy the solution how and where they want it.

- **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 continuously monitors and analyzes all file activity, processes, and communications. If a file exhibits malicious behavior, AMP will detect it and provide retrospective alerts, indications of compromise, tracking, and analysis, so security teams can surgically remediate it.

AMP 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 Malware Analysis

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:

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

The integration of our AMP Threat Grid technology into Cisco AMP also provides context-rich intelligence feeds. The technology analyzes millions of samples every month, against more than 560 behavioral indicators, resulting in billions of artifacts and an easy-to-understand threat score to help security teams prioritize responses.

Cisco AMP automatically correlates files, behavior, telemetry data, and activity against this robust, context-rich knowledge base to block attacks, provide greater insight into threats, and allow for faster and easier response.

Continuous Analysis and Retrospective Security

Cisco AMP continuously monitors, analyzes, and records all file activity, regardless of disposition, even after initial inspection. If AMP observes suspicious or malicious activity, security teams will be sent an alert and an indication of compromise. AMP will also provide visibility into exactly what happened. Security teams can see the complete history of the threat 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 this information, security teams can use AMP's easy-to-use browser-based management console to quickly take action.

Next Steps

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

Flexible Deployment Options

The Cisco AMP solution is deployable on multiple platforms (see Table 1).

Table 1. Cisco AMP Deployment Options

Product Name	Details
Cisco AMP for Endpoints	Protect PCs running Windows, Macs, Linux systems, Android mobile devices, and virtual environments 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™ network security appliances.
Cisco AMP for ASA with FirePOWER Services	Deploy AMP capabilities integrated into the Cisco 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 for CWS, ESA, or WSA	For Cisco Cloud Web Security (CWS), 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 AMP Threat Grid	AMP 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.

C45-731876-04 05/18