Cisco Advanced Malware Protection for Endpoints

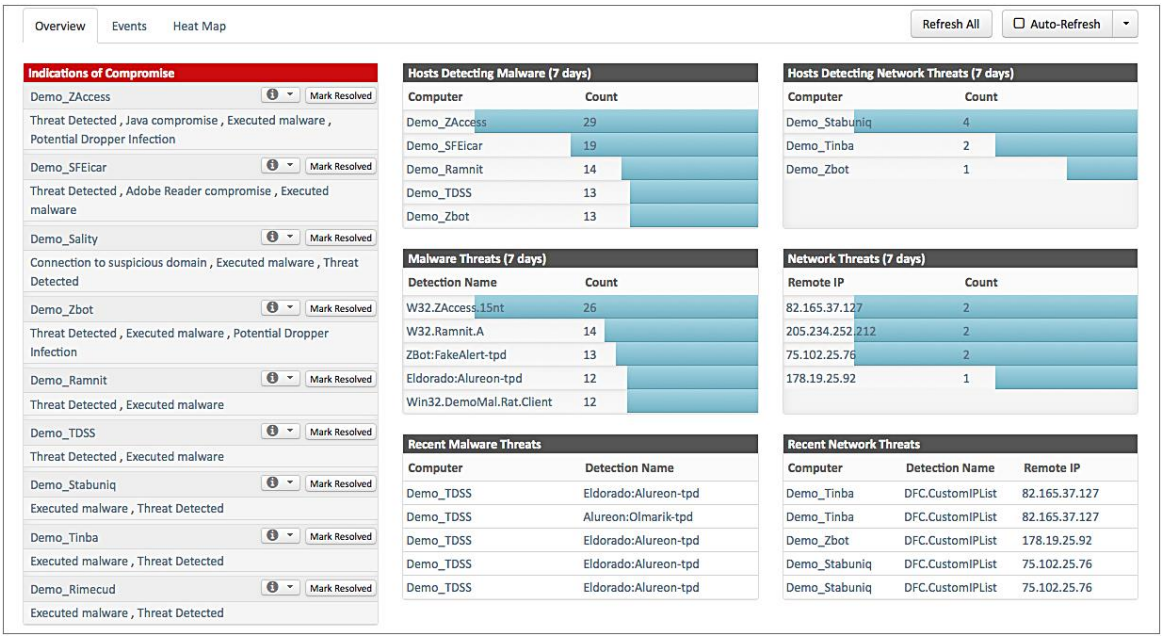
Product Overview

With today's sophisticated malware, you have to protect endpoints before, during, and after attacks. Cisco® Advanced Malware Protection (AMP) for Endpoints goes beyond point-in-time detection to provide the level of visibility and control you need to stop advanced threats missed by other security layers. You get comprehensive protection for your organization across the attack continuum - before, during, and after an attack. Cisco AMP for Endpoints is an intelligent, enterprise-class advanced malware analysis and protection solution that uses a telemetry model that uses big data, continuous analysis, and advanced analytics to detect, track, analyze, control, and block advanced malware outbreaks across all endpoints: Windows PCs, Macs, Linux, mobile devices, and virtual systems.

Benefits include:

- **Protection that moves beyond point-in-time:** Cisco AMP for Endpoints goes beyond point-in-time detection to analyze files and traffic continuously. This capability helps enable retrospective security. You can look back in time and trace processes, file activities, and communications to understand the full extent of an infection, establish root causes, and perform remediation. The result: more effective, efficient, and pervasive protection for your organization.
- **Monitoring that enables unmatched visibility:** Cisco AMP for Endpoints offers more than retrospection. It introduces a new level of intelligence, linking and correlating various forms of retrospection into a lineage of activity available for analysis in real time. It can then look for patterns of malicious behavior from an individual endpoint or across the environment of endpoints.
- **Advanced analysis that looks at behaviors over time:** Cisco AMP for Endpoints provides automation through advanced behavioral detection capabilities that deliver a prioritized and collated view of top areas of compromise and risk.
- **Investigation that turns the hunted into the hunter:** Cisco AMP for Endpoints shifts activity from looking for facts and clues as part of an investigation to a focused hunt for breaches based on actual events like malware detections and behavioral indications of compromise (IoCs).
- **Containment that is truly simple:** Cisco AMP for Endpoints provides visibility into the chain of events and context that complements its dashboards and trajectory views. AMP provides the ability to target specific applications, files, malware, and other root causes. Breaking the attack chain is not only quick but also easy.
- **Dashboards that are actionable and contextual:** Reports are not limited to event enumeration and aggregation. Cisco AMP for Endpoints reporting includes actionable dashboards and trending (see Figure 1) that highlights business relevance and impact from a risk perspective.
- **Integrated platforms that work better together:** Cisco AMP for Endpoints can be fully integrated with the Cisco AMP for Networks solution to further increase visibility and control across your organization.

Figure 1. Actionable and Contextual Dashboards



Increase Visibility and Control for Effective Security

Organizations struggle to find a solution that can effectively address the full lifecycle of the advanced malware problem: providing protection, incident response, and remediation against the latest threats without overburdening the budget or sacrificing operational efficiency. Part of the challenge comes from a lack of continuity and intelligence between detection and blocking technologies and incident response and remediation technologies.

Often, this lack of intelligence can leave an organization unaware of the full extent and depth of an outbreak, which cause incident response and remediation efforts to begin well after an outbreak. In addition, lack of continuity can cause infected systems and root causes to be missed during these efforts, leading to an endless cycle of reinfection.

As a result, security professionals often lack visibility into the scope of advanced malware in their network, struggle to contain and remediate it after an outbreak, and cannot address fundamental questions, including:

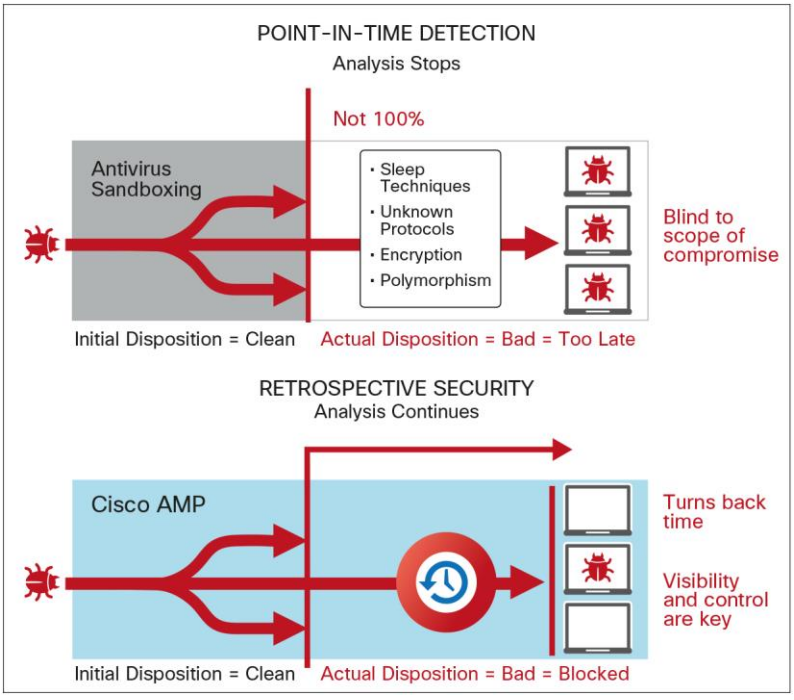
- What was the method and point of entry?
- What systems were affected?
- What did the threat do?
- Can we stop the threat and eliminate the root cause?
- How do we recover from the attack?
- How do we prevent it from happening again?

Cisco AMP for Endpoints Discovers, Analyzes, Blocks, and Remediates Advanced Malware

Point-in-time detection alone will never be 100 percent effective. It takes only one threat that evades detection to compromise your environment. Using targeted context-aware malware, sophisticated attackers have the resources, expertise, and persistence to outsmart point-in-time defenses and compromise any organization at any time. Furthermore, point-in-time detection is completely blind to the scope and depth of a breach after it happens, rendering organizations incapable of stopping an outbreak from spreading or preventing a similar attack from happening again.

Cisco AMP for Endpoints goes beyond point-in-time detection, delivering a lattice of detection capabilities combined with big data analytics, to continuously analyze files and traffic on endpoints to determine if advanced malware is present (Figure 2). Sophisticated machine-learning techniques evaluate more than 400 characteristics associated with each file to analyze and block advanced malware. The combination provides protection that goes beyond traditional point-in-time detection. Retrospective security, the ability to roll back time on attacks, can detect and alert you to files that become malicious after the initial point of entry.

Figure 2. Point-in-Time Detection Compared with Continuous Analysis and Retrospective Security



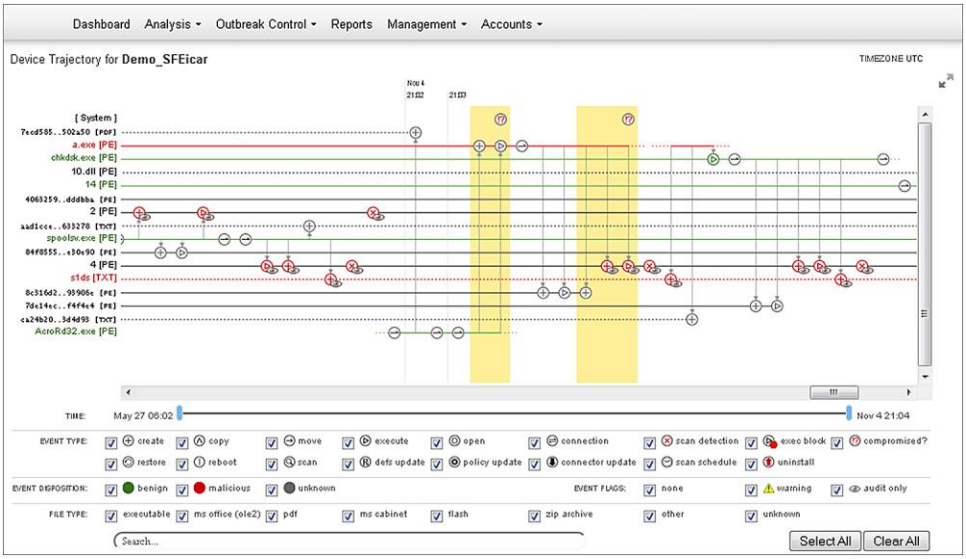
See More than Ever Before and Control Advanced Malware

Today's malware is more sophisticated than ever. Evolving quickly, it can evade discovery after it has compromised a system while providing a launching pad for a persistent attacker to move throughout an organization. Sleep techniques, polymorphism, encryption, and use of unknown protocols are just some of the ways that malware can hide from view. The continuous analysis and retrospective security features of Cisco AMP for Endpoints let you uncover elusive malware and help you answer the following key questions in the battle against advanced threats.

- **What was the method and point of entry? What systems were affected?**

  Powerful innovations like file trajectory and device trajectory (Figure 3) use AMP's big data analytics and continuous analysis capabilities to show you the systems affected by malware, including patient zero and the root causes associated with a potential compromise. These capabilities help you quickly understand the scope of the problem by identifying malware gateways and the path that attackers are using to gain a foothold into other systems.

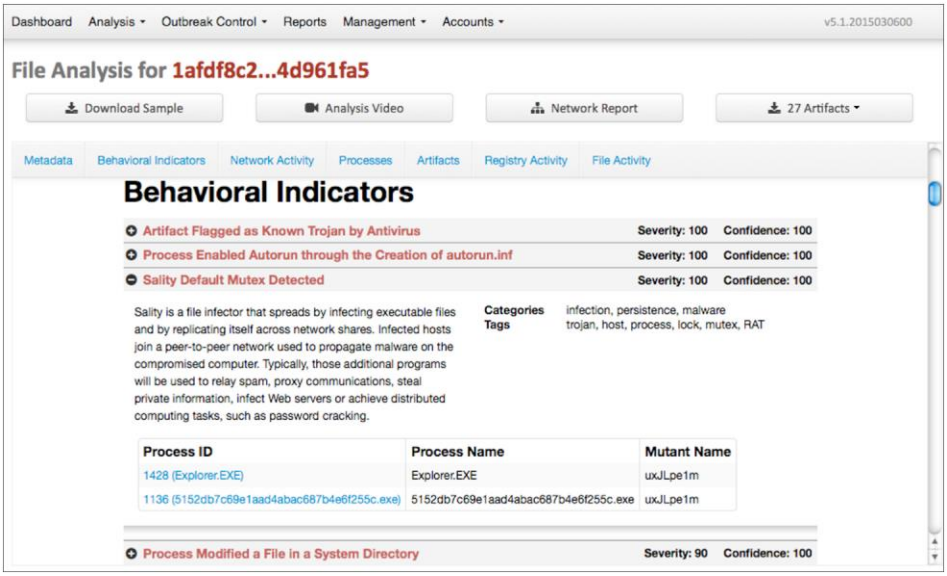
Figure 3. Deep Analysis with Device Trajectory



- **What did the threat do?**

  Cisco AMP for Endpoints File Analysis (Figure 4), backed by the Talos Security Intelligence and Research Group and powered by AMP Threat Grid's sandboxing technology, provides a safe, highly secure sandbox environment for you to analyze the behavior of malware and suspect files. File analysis produces detailed information on file behavior, including the severity of behaviors, the original filename, screenshots of the malware executing, and sample packet captures. Armed with this information, you'll have a better understanding of what is necessary to contain the outbreak and block future attacks.

Figure 4. File Analysis



Device trajectory further aids a quick analysis of threat activity on a computer by tracking file and network activity at the endpoint in chronological order. You gain complete visibility into the events that occurred leading up to and following a compromise, including parent processes, connections to remote hosts, and unknown files that may have been downloaded by malware.

Indications of compromise (IoCs) are often subtle and require immediate investigation before they are erased or an attacker moves on. With the Cisco AMP for Endpoints Elastic Search, security teams can quickly hunt down the scope of exposure to an attack with simple but flexible search capabilities that immediately present results without the need to scan and pull data from endpoints.

- **Can we stop the threat and root causes? Can we prevent it from happening again?**

  Cisco AMP for Endpoints Outbreak Control gives you a suite of capabilities to effectively stop the spread of malware and malware-related activities, like call-back communications or dropped file execution, without waiting for updates from your security vendor. This gives you the power to move directly from investigation to control with a few mouse clicks, significantly reducing the time a threat has to spread or do more damage and the time it normally takes to put controls in place.

  Furthermore, AMP can automatically remediate systems without a full scan. The technology continuously cross-references files analyzed in the past against the latest threat intelligence and quarantines any files previously deemed clean or unknown that are now known to be a threat.

Protect Endpoints, Mobile Devices, Virtual Systems, and the Network

Cisco AMP for Endpoints protects you against advanced malware and increases security intelligence across all endpoints - PCs, Macs, Linux, mobile devices, and virtual systems. Its lightweight connector architecture uses big data analytics, which simplifies defense-in-depth requirements to address advanced malware.

Furthermore, Cisco AMP for Endpoints integrates with Cisco AMP for Networks to deliver comprehensive protection through a single pane of glass and across extended networks and endpoints. Now, using continuous analysis, retrospective security, and multisource indications of compromise, you can identify stealthy attacks that manage to traverse from the endpoint to inline at the network level, correlate those events for faster response, and achieve greater visibility and control.

Scale Up Protection for the Enterprise

AMP is optimized for the enterprise. In terms of privacy, all Cisco AMP for Endpoints connectors use metadata for analysis. Actual files are not needed and not sent to the cloud for analysis. For organizations with high privacy requirements, a private cloud option is also available. This single on-premises solution delivers comprehensive advanced malware protection using big data analytics, continuous analysis, and security intelligence stored locally on premises.

As for manageability, the Cisco AMP for Endpoints console interface provides complete management, deployment, policy configuration, and reporting for Windows systems, Mac systems, Linux systems, mobile devices, and virtual systems.

As for performance, Cisco AMP for Endpoints deployed on PCs, Macs, Linux, mobile devices, and virtual environments use lightweight connector architectures, requiring less storage, computation, and memory than other security solutions, speeding protection against attacks.

Gain Truly Comprehensive Security Intelligence

Cisco AMP for Endpoints is built on big data and unmatched security intelligence. Cisco Security Intelligence Operations, Talos Security Intelligence and Research Group, and AMP Threat Grid threat intelligence feeds represent the industry's largest collection of real-time threat intelligence with the broadest visibility, largest footprint, and ability to put it into action across multiple security platforms. This data is then pushed from the cloud to the AMP client so that you have the latest threat intelligence at all times.

The integration of our AMP Threat Grid technology into AMP for Endpoints also provides over 350 unique behavioral indicators that evaluate the actions of a file submission, not just its structure, providing insight to unknown malware including associated HTTP and DNS traffic, TCP/IP streams, processes it's affecting, and registry activity. AMP Threat Grid also provides users with context-rich, actionable content everyday - more than 8 million samples are analyzed each month resulting in billions of artifacts. And finally, AMP Threat Grid's highly accurate content feeds, delivered in standard formats to seamlessly integrate with existing security technologies, enable organizations to generate context-rich intelligence specific to their organization.

Cisco AMP Leads in Third-Party Test

Cisco is the leader in NSS Labs' Breach Detection Systems Report for the second year in a row, according to the 2015 NSS Labs Breach Detection Systems Comparative Analysis Report. The 2015 NSS Labs comparative product test provides the details on how Cisco AMP achieved:

- 99.2% Security Effectiveness rating-the highest of all vendors tested
- Only vendor to block 100% of all evasion techniques during testing
- Excellent performance with minimal impact on endpoint or application latency

Table 1 highlights the best-in-class capabilities of Cisco AMP for Endpoints. Table 2 lists the software requirements.

Table 1. Features and Benefits of Cisco AMP for Endpoints

Feature	Benefits
Continuous analysis	Cisco AMP for Endpoints uses cloud-based big data analytics to go beyond point-in-time detection, constantly re-evaluating data gathered over time to detect stealthy attacks.
Retrospective security	Retrospective security is the ability to look back in time and trace processes, file activities, and communications in order to understand the full extent of an infection, establish root causes, and perform remediation. The need for retrospective security arises when any IoC occurs, such as an event trigger, a change in the disposition of a file, or an IoC trigger.
Dashboards	Gain visibility into your environment through a single pane of glass - with a view into hosts, devices, applications, users, files, and geolocation information, as well as advanced persistent threats (APTs), threat root causes, and other vulnerabilities - to provide a comprehensive contextual view so that you can make informed security decisions.
Collective security intelligence	Cisco Security Intelligence Operations, Talos Security Intelligence and Research Group, and AMP 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 are file and telemetry events correlated and prioritized as potential active breaches. Cisco AMP for Endpoints 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.
File analysis and sandboxing	A highly secure environment helps you execute, analyze, and test malware behavior in order to discover previously unknown zero-day threats. Integration of AMP Threat Grid's sandboxing technology into AMP for Endpoints results in more dynamic 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 and visibility to malware that evaded 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 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.
Low prevalence executables	Display all files that have been executed across your organization, ordered by prevalence from lowest to highest, to help you surface previously undetected threats seen by a small number of users. Files executed 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 IoC's let security teams perform deeper levels of investigation on lesser known advanced threats specific to applications in their environment.
Vulnerabilities	This feature shows a list of hosts that contain vulnerable software, a list of the vulnerable software on each host, and the hosts most likely to be compromised. Powered by our threat intelligence and security analytics, AMP identifies vulnerable software being targeted by malware, shows you the potential exploit, and provides you with a prioritized list of hosts to patch.
Outbreak control	Achieve control over suspicious files or outbreaks, and quickly and surgically control 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 re-infection cycle; custom whitelists will help ensure that safe, custom, or mission-critical applications continue to run no matter what; and device flow correlation will stop malware call-back communications at the source, especially for remote endpoints outside the corporate network.
Integration with AMP Threat Grid	The integration of AMP Threat Grid's sandboxing technology and advanced malware analysis capabilities into AMP for Endpoints provides over 350 unique behavioral indicators analyzing the actions of a file, easy to understand threat scores, and billions of malware artifacts at your disposal for unmatched scale and coverage from global threats.
AMP Private Cloud Virtual Appliance	AMP for Endpoints can be deployed as an on-premises, air-gapped solution built specifically for organizations with high-privacy requirements that restrict using a public cloud.
Launch from AnyConnect v4.1	With a Cisco AnyConnect v4.1 remote access VPN client installed, users can elect to launch the AMP for Endpoints connector on that remote endpoint. This allows for a rapid expansion of endpoint threat protection to VPN-enabled endpoints and further minimizes the potential of an attack from a remote host. Gain more insight into remote endpoints, and accelerate remediation efforts during or after an attack.

Table 2. Software Requirements

Cisco AMP for Endpoints	• Microsoft Windows XP with Service Pack 3 or later • Microsoft Windows Vista with Service Pack 2 or later • Microsoft Windows 7 • Microsoft Windows 8 and 8.1 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Mac OS X 10.7 and later • Linux Red Hat 6.5 and 6.6 • Linux CentOS 6.4, 6.5, and 6.6
Cisco AMP for Endpoints on Android mobile devices	• Android version 2.1 and later

Platform Support and Compatibility

Cisco AMP for Endpoints includes Cisco AMP for Endpoints licenses and subscriptions (1, 3, and 5 year options) and the lightweight connector. Cisco AMP for Endpoints is compatible with Cisco AMP for Networks. Cisco AMP for Endpoints can also be launched from Cisco AnyConnect v4.1 on remote endpoints.

Warranty Information

Find warranty information on the Cisco.com Product Warranties page.

Ordering Information

To place an order, visit the Cisco Ordering Home Page, contact your Cisco sales representative, or call us at 800 553-6387.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx, accelerate your growth, and 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.

For More Information

For more information, please visit the following link:

- Cisco AMP for Endpoints

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 C78-733181-04 10/15