Cisco Advanced Malware Protection for Endpoint

Cisco Advanced Malware Protection (AMP) for Endpoint offers the only advanced malware protection system that covers the entire attack continuum – before, during, and after an attack. It provides the continuous analysis and advanced analytics that support Cisco's retrospective security capabilities. Retrospective security is the ability to look back in time and trace processes, file activities, and communications to understand the full extent of an infection, establish the root cause, and perform remediation. The need for retrospective security arises when any indication of a compromise occurs, such as an event trigger, a change in the disposition of a file, or an indication of compromise (IoC) trigger. Retrospective security lets managers go back in time to investigate threats in their systems. Tools such as retrospection, attack-chain correlation, behavioral IoCs, trajectory, and breach hunting allow security professionals to establish scope, visibility, and control in the event of a breach. This capability helps your security team to quickly and effectively remediate all the threats in your environment before it's too late.

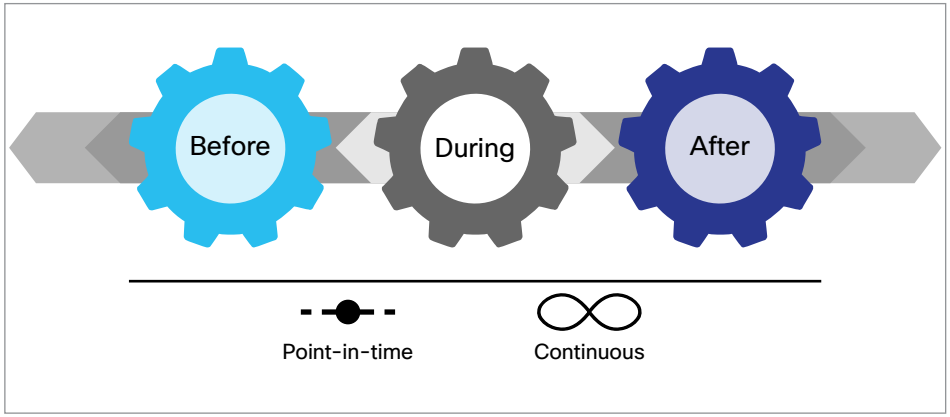
Aside from retrospective security, key features of Cisco AMP for Endpoint include:

- **Continuous analysis:** AMP for Endpoint uses cloud-based big data analytics to go beyond point-in-time detection by constantly reevaluating new and historical data gathered over time to detect stealthy attacks.
- **Outbreak control:** AMP for Endpoint provides the capabilities to detect and control suspicious files across endpoints for both future and past threat occurrences. Outbreak control is one of the key features that help you quickly stop malware from spreading in your environment.
- **IoCs:** AMP for Endpoint automatically correlates multisource security event data, such as intrusion and malware events, to help security teams connect events to larger, coordinated attacks.

The Flaw with Point-in-Time Detection Alone

Point-in-time detection alone will never be 100 percent effective. It takes only one threat to evade detection and 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. Moreover, point-in-time detection is completely blind to the scope and depth of a breach after it happens.

Figure 1. Point-in-Time Versus Continuous Protection



Additional AMP for Endpoint Features

In addition, AMP for Endpoint offers:

- **File reputation:** Employs advanced analytics and collective intelligence to determine whether a file is clean or malicious, improving the accuracy of detection.
- **File analysis and sandboxing:** Uses a highly secure environment to execute, analyze, and test malware behavior, helping you discover previously unknown zero-day threats.
- **File trajectory:** Tracks file propagation in your environment over time, so you can minimize the time required to scope a malware breach.
- **Device trajectory:** Tracks system-level activity and communications over time, allowing you to quickly understand root causes and the history of events leading up to and following a compromise.
- **Elastic Search:** Provides a simple, unbounded search across file, telemetry, and collective security intelligence data, helping you connect the context and scope of an exposure to an IoC or malicious application.

Benefits

With Cisco AMP for Endpoint, you'll get:

- **Protection beyond point-in-time:** AMP for Endpoint applies a retrospective security approach to traditional detection, helping defenses improve on point-in-time capabilities and become more effective, efficient, and pervasive.
- **Attack-chain visibility:** AMP for Endpoint does more than retrospection. It introduces a new level of intelligence, linking, and correlating various forms of retrospection into a lineage of activity available for real-time analysis. It then looks for patterns of malicious behavior on an individual endpoint or across the environment of endpoints.
- **Advanced analysis:** AMP for Endpoint provides automated, advanced behavior-detection capabilities that deliver a prioritized and collated view of top areas of compromise and risk.
- **Investigation that turns the hunted into the hunter:** AMP for Endpoint shifts investigative activities beyond looking for facts and clues to a focused hunt for breaches based on actual events like malware detections and behavioral IoCs.
- **Simplified containment:** AMP for Endpoint provides visibility into a chain of events and context that complements its dashboards and trajectory views. AMP for Endpoint lets you target specific applications, files, malware, and other root causes, making it quick, easy, and simple to break the attack chain.
- **Actionable, contextual dashboards:** Reports are not limited to event enumeration and aggregation. AMP for Endpoint reporting includes actionable dashboards and trending that highlights business relevance and impact from a risk perspective.
- **Tightly integrated platforms:** AMP can be activated on your Cisco Email and Web Security solutions with the flip of a switch. For greater visibility and control, AMP can be deployed inline as a dedicated network appliance and at the endpoint as a lightweight connector.

Collective Security Intelligence

The collective security intelligence of Cisco SIO and Sourcefire's Vulnerability Research Team (VRT) represents a massive collection of real-time threat intelligence. (Sourcefire is now a part of Cisco.) This collection includes 1.6 million sensors distributed around the globe. We receive 100 TB of data and more than 180,000 file samples per day, and we have the ability to monitor 35 percent of worldwide email traffic. More than 600 engineers, technicians, and researchers work around the clock, 365 days a year, in more than 40 languages, to analyze this information as well as public and private threat feeds. And continuous interaction with the FireAMP™, Snort, and ClamAV communities, along with participation in the Sourcefire Awareness, Education, Guidance, and Intelligence Sharing (AEGIS) program, helps us share threat intelligence and remediation best practices. All of this means we're better prepared to defend against tomorrow's attacks.

Why Cisco?

Cisco offers the industry's broadest portfolio of integrated advanced malware protection solutions, providing customers with continuous visibility and control to defeat malware across the extended network and the full attack continuum – before, during, and after an attack. Available as an integrated capability spanning Cisco Email and Web Security, FirePOWER® network security appliances, mobile and virtual systems, and endpoint protection for PCs, AMP offers flexible deployment options and extensive coverage to close ever-expanding attack vectors.

Next Steps

Find out more at the Cisco AMP homepage. In addition, a Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco products will work for you.

C45-731874-02 09/14