Cisco Advanced Malware Protection for Networks

Cisco® Advanced Malware Protection (AMP) offers the only network advanced malware protection system that covers the entire attack continuum – before, during, and after an attack, with continuous analysis and advanced analytics that support Cisco's retrospective security capabilities. Retrospective security lets managers go back in time to investigate threats in their systems with tools such as retrospection, attack-chain correlation, behavioral indications of compromise (IoCs), trajectory, and breach hunting. With these retrospective security tools, you can establish scope, visibility, and control in the event of a breach. This helps your security team to quickly and effectively remediate all the threats in your environment before it's too late.

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.

Cisco AMP for Networks Features

AMP for Networks is based on five key features:

- **File reputation:** Provides advanced analytics and collective intelligence to determine whether a file is clean or malicious. This results in more accurate detection through collective security intelligence.
- **File analysis and sandboxing:** Executes, analyzes, and tests malware behavior in a highly secure environment. This capability allows you to discover previously unknown zero-day threats.
- **Retrospective detection:** Provides alerts when the file disposition changes after extended analysis. You gain awareness of malware that evaded initial defenses.
- **Indications of compromise:** Helps enable the correction and prioritization of file and telemetry events to detect potential active breaches. It provides a prioritized list of high-risk events.
- **File trajectory:** Provides visibility and continuous tracking over time of file propagation in your environment. This feature reduces the time required to scope a malware breach.

These features enable a variety of capabilities, including the following.

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 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 IoC trigger.

Continuous Analysis

AMP for Networks uses cloud-based big data analytics to go beyond point-in-time detection, constantly reevaluating new and historical data gathered over time to detect stealthy attacks.

Drive-By Attack Protection with Client-Side Exploit Prevention

When AMP for Networks is deployed inline, it detects and blocks client-side exploit attempts that can lead to malicious file downloads, known as drive-by attacks.

Indications of Compromise

AMP for Networks automatically correlates multisource security event data, such as intrusion and malware events, to help security teams connect events to larger, coordinated attacks.

Benefits

- **Limits policy-violating files and more:** Tracking data that comes from the web, email, or other attack vectors, the system automatically recognizes files and applications. It then performs broad-based filtering of files using the application and file control policies that you set.
- **Detects and blocks exploit attempts:** Deploying the system inline enables it to detect and block client-side exploit attempts. AMP inline also protects against vulnerability exploit attempts aimed at Adobe Acrobat, Java, Flash, and other commonly targeted client applications.
- **Identifies, blocks, and analyzes malicious files:** The system blocks malicious files from their target system and analyzes files with an unknown disposition locally, and suspect files can optionally be submitted to the collective security intelligence cloud for analysis.

- **Analyzes files and traffic continuously:** Determining that an observed file is malicious triggers retrospective alerts from the AMP for Networks system, even if the file traversed the network hours or days in the past, so that you can take action and mitigate damage.
- **Correlates discrete events into coordinated attacks:** Providing automated and prioritized lists of potentially compromised devices with combined security event data from multiple event sources, AMP for Networks illustrates the risk associated with an ongoing attack.
- **Tracks malware's spread and communications:** Using file trajectory, AMP for Networks enables you to track a file's transmission across the network. Each file in the file trajectory view has an associated trajectory map with a visual display of the file's transfers over time as well as additional information about the file.
- **Contains malware to prevent loss and outbreaks:** Blocking advanced threats and malware communications with a simple policy update is easy with AMP for Networks. With custom detection lists, you are empowered to act whenever you decide, without waiting for a vendor-supplied update to take action.

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 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 over 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?

AMP for Networks provides protection across the attack continuum with a suite of features that work in tandem with the AMP for Endpoint and AMP for Content platforms. By working with your Cisco specialist, you can find the combination that will work best to protect your business.

Next Steps

Evaluate how Cisco products can work for you with a Cisco sales representative or channel partner.

Find out more at http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html.

C45-731875-00 05/14