Cisco Advanced Malware Protection for Content

Cisco Advanced Malware Protection (AMP) 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 on Cisco's Email and Web Security Appliances. Retrospective security lets security managers go back in time to investigate threats in their systems. Advanced analytics and collective intelligence determine whether a file is clean or malicious. Alerts are triggered if a file disposition changes after extended analysis. File sandboxing allows you to execute, analyze, and test malware behavior in a highly secure environment. 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 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.

AMP for Content Features

Cisco AMP for Content is based on three key features:

- **File reputation:** AMP captures a fingerprint of each file as it traverses the gateway and sends it to AMP's cloud-based intelligence network for a reputation verdict checked against zero-day exploits.
- **File sandboxing:** When malware is detected, AMP gleans precise details about a file's behavior. AMP then combines that data with detailed human and machine analysis to determine the file's threat level in a sandbox.
- **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.

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

Retrospective security for advanced threats: To deliver effective protection against advanced threats and targeted attacks, AMP doesn't rely on malware signatures, which can take weeks or months to create for each new malware sample. Instead, AMP uses file reputation and file sandboxing to identify and block suspicious files where no known signature exists. Retrospective file analysis gives you the unique ability to go back in time to pinpoint when an outbreak occurred and provides visibility into the scope of the attack.

Protection across the attack continuum: Gain protection across the attack continuum – before, during and after an attack. Spam filters and zero-day threat intelligence from Cisco Security Intelligence Operations (SIO) stop threats before they enter the network, while file reputation and file sandboxing identify threats during an attack. Finally, retrospective analysis provides protection after an attack, when advanced malware has slipped past other layers of defense.

Visibility and control: Data-rich and user-friendly reports provide visibility into the reputation and behavior of files that have attempted to enter the network, and they alert you to any change in disposition, including who on your network may have been infected and when. You can set policies that define the actions to be taken by the security gateway (allow, block, or quarantine) based on data such as file reputation and file behavior.

Flexibility and choice: The integration of AMP with existing Cisco security gateways delivers on the promise of flexibility and choice by giving you another option for deploying AMP in a way that makes the most sense for your environment. By activating AMP as an additionally licensed feature on Cisco Web and Email Security, you can take advantage of the simplest, most cost-effective way to gain advanced malware protection.

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 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 IoC trigger.

Benefits

- Accurately detect malware in files
- Discover previously unknown zero-day threats
- Find and disable malware that has evaded initial defenses

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.

C45-731873-00 05/14