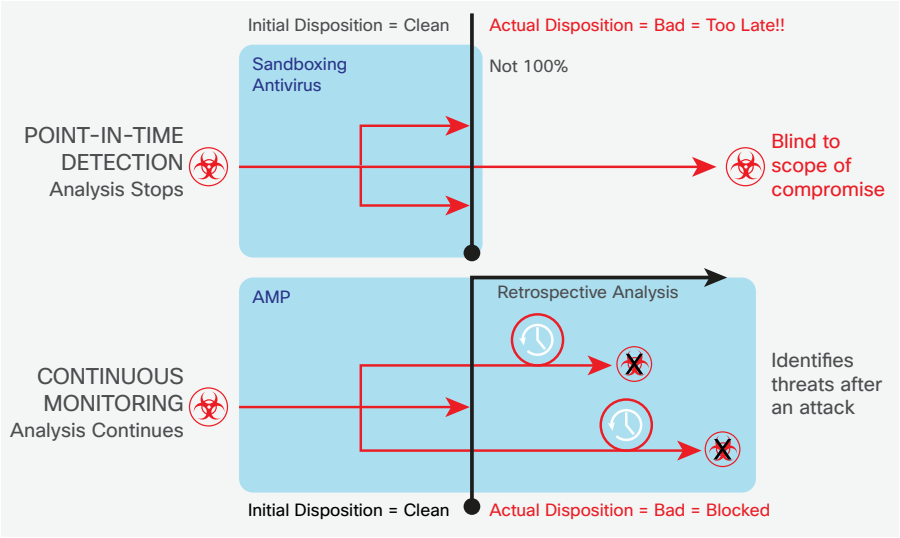
Advanced Malware Protection on Cisco Email Security

Advanced Malware Protection (AMP) is a comprehensive solution that enables malware detection and blocking, continuous analysis, and retrospective alerting. It uses the vast cloud security intelligence networks of both Cisco and Sourcefire (now part of Cisco).

Take advantage of AMP with a simple add-on license to your Cisco® Email Security solution. Gain superior protection across the attack continuum — before, during, and after an attack — with the most cost-effective, easily deployed approach to advanced malware protection.

Figure 1. Retrospective Analysis with AMP



Increasingly Sophisticated Email Threats

While email remains one of the top methods for distributing malware, email-based exploits have become more sophisticated over time. The exponential growth in new malware samples and modes of attack has made it impossible for traditional anti-malware solutions and security measures to keep up. Even the most advanced security techniques can be defeated by targeted, context-aware malware that can modify its behavior to evade detection and infiltrate the extended network where it is difficult to locate, let alone eradicate.

To deal with these threats, you need a security solution that goes beyond traditional measures. You need one that provides continuous monitoring and analysis across the extended network and throughout the full attack continuum: before, during, and after an attack.

Key Features of AMP on Cisco Email Security

AMP uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats across the attack continuum. Features include:

- **File Reputation** captures a fingerprint of each file as it traverses the Cisco Email Security gateway and sends it to AMP's cloud-based intelligence network for a reputation verdict. Given these results, you can automatically block malicious files and apply administrator-defined policies. The Cisco Email Security user interface is the same and the policy-reporting frameworks are similar to the ones you already know.
- **File Sandboxing** provides you with the ability to analyze unknown files that are traversing the Cisco Email Security gateway. A highly secure sandbox environment enables AMP to glean precise details about a file's behavior and to combine that data with detailed human and machine analysis to determine the file's threat level. This disposition is then fed into AMP's cloud-based intelligence network and used to dynamically update and expand the AMP cloud data set for enhanced protection.
- **File Retrospection** solves the problem of malicious files that pass through perimeter defenses but are subsequently deemed a threat. In doing so, it addresses the inherent weakness of most perimeter defenses: They are effective only at a single point in time. Even the most advanced techniques may fail to identify malware at the perimeter because polymorphism, obfuscation, sleep timers, and other tactics are highly skilled at enabling malware to avoid detection as it crosses the wire. Malicious files simply wait until they are inside the network to do their dirty work.

  That's where File Retrospection comes in. File Retrospection provides a continuous analysis of files that have traversed the security gateway, using real-time updates from AMP's cloud intelligence network to stay abreast of changing threat levels. Once a file is identified as a threat, administrators are alerted by AMP and given visibility into who on the network may have been infected and when. As a result, AMP helps you to identify and address an attack quickly, before it has a chance to spread.

Benefits

- **Advanced 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, 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 Email Security, you can take advantage of the simplest, most cost-effective way to gain advanced malware protection.

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.

To Learn More

Find out more at www.cisco.com/go/esa.

A Cisco sales representative, channel partner, or systems engineer can help you evaluate how Cisco products will work for you.

C45-730848-00 02/14