At-a-Glance

Cisco Advanced Malware Protection for Web Security

Sophisticated Web Security for Sophisticated Threats

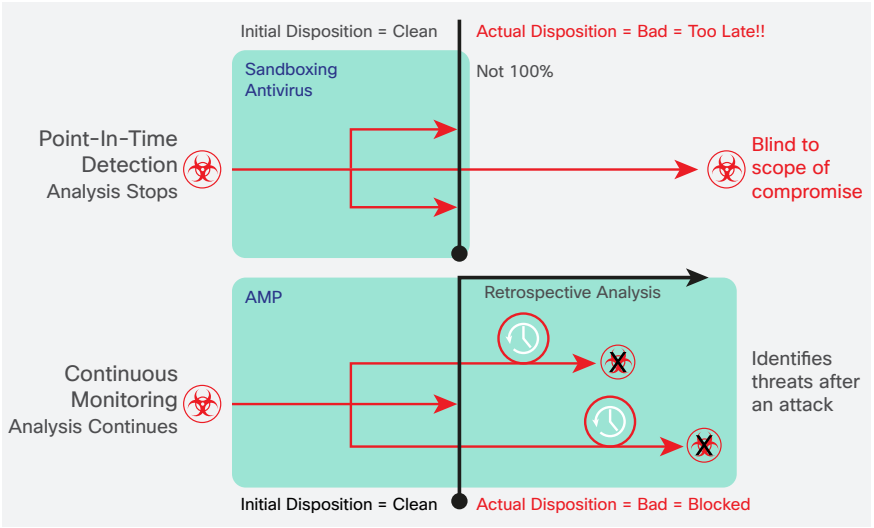
Effective web security today requires a lot more than blocking navigation to bad websites. You can download viruses or malware through legitimate websites as well. And there are new vulnerabilities with mobile access, social media, and interactive applications. As web threats continue to rise, it is critical to have a solution that goes beyond the basics in threat detection, URL filtering, and application control.

You need a web security solution that provides continuous monitoring and analysis to help your security team catch even the stealthiest threats. You need the Cisco® Advanced Malware Protection (AMP) for Web Security with Cognitive Threat Analytics (CTA) for WSA.

Why AMP Is So Important

Traditional web security measures are not enough to stop today's advanced threats. Integrating AMP with Cisco's web security solutions gives you advanced threat capabilities alongside traditional web security features, to protect against the most advanced attacks.

Figure 1. Retrospective Analysis with AMP



AMP adds malware detection, blocking, continuous analysis, and retrospective alerting (Figure 1) to your Cisco Web Security Appliance license. Features include:

- **Flexibility and choice:** The integration of AMP with existing Cisco security gateways gives you another option for deploying AMP in a way that makes the most sense for your environment.

Benefits

- **Advanced threat detection:** AMP for Web Security gives you comprehensive protection against all web-related threats for protection before, during, and after an attack.
- **Continuous analysis and retrospective security:** After a file crosses the web gateway, AMP continues to watch, analyze, and record its activity, regardless of the file's initial disposition. If malicious behavior is spotted later on, AMP sends a retrospective alert so that you can contain and remediate the malware.
- **Strengthened network defenses:** AMP for Web Security is built on big data and exceptional security intelligence. Our Cisco Talos group analyzes millions of malware samples and terabytes of data per day and pushes that intelligence to AMP. AMP then correlates files, telemetry data, and file behavior against this context-rich knowledge base to proactively defend against known and emerging threats.

- **Advanced sandboxing:** Get data-rich, detailed analytics on the behavior, reputation, and threat level of files that have attempted to enter the network. You gain visibility and control over your environment.
- **Reduced time to discovery of threats operating inside the network:** Turn your web proxy into a security sensor and automatically investigate suspicious web traffic.

Next Steps

Find out more about Cisco AMP for Web Security at http://www.cisco.com/go/ampforweb

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

- **File reputation:** AMP captures a fingerprint of each file as it traverses the Cisco web security gateway and sends it to Cisco's cloud-based intelligence network for a reputation verdict. With these results, you can automatically block malicious files and apply administrator-defined policies.
- **File analysis:** Powered by AMP Threat Grid technology, you get static and dynamic analysis (sandboxing) of unknown files that traverse the web gateway. Threat Grid analyzes samples in a highly secure environment using more than 700 behavioral indicators along with global threat intelligence to glean precise details about a file's behavior and threat level.
- **File retrospection:** AMP solves the problem of malicious files that evade your perimeter defenses. It continuously analyzes files that have traversed the security gateway, regardless of their initial disposition. When a file is identified as a threat, AMP sends a retrospective alert that gives you visibility into who on the network may have been infected and when. Security teams can then identify and address an attack quickly, before it has a chance to spread.

Cognitive Threat Analytics Complements AMP to Further Increase Visibility

Cisco's cloud-based Cognitive Threat Analytics solution is included as part of the AMP add-on license to the Web Security Appliance. With Cognitive Threat Analytics you can detect and respond to sophisticated, clandestine attacks that are already under way or are attempting to establish a presence within your environment.

The integration of Cognitive Threat Analytics with AMP for Web Security allows you to:

- Automatically identify and investigate suspicious or malicious web-based traffic.
- Analyze information generated by your existing web security solutions without the need for additional hardware or software.
- Zero in on malicious activity that has bypassed security controls and is using web-based communications, including standard, encrypted, and anonymous channels that can be used to attack your organization.
- Create a baseline of normal activity and identify anomalous traffic occurring within your network.
- Analyze device behavior and web traffic to pinpoint command-and-control communications and data exfiltration.

For more detailed information on Cisco Cognitive Threat Analytics, go to www.cisco.com/go/cognitive.

C45-730851-03 10/16