SOLUTION BRIEF

Detect and Stop Advanced Email Threats

Cisco Email Security and McAfee® Advanced Threat Defense

Email continues to be the most highly exploited attack vector, with ransomware and business email compromises capturing cybersecurity professionals' attention, resources, and time. Safeguarding this vital communication channel continues to be a major challenge for organizations of all sizes. The interoperability between Cisco's Email Security Appliance and McAfee® Advanced Threat Defense provides an automated, closed-loop solution that detects sophisticated attacks and enables action before malicious email attachments reach users.

McAfee Compatible Solution

- Cisco Email Security Appliance
- McAfee Advanced Threat Defense 4.x

The Business Problem

Email attachments continue to be a primary attack vector for organizations large and small. The *Verizon Data Breach Investigations Report 2017* notes that 66% of malware was installed via malicious email attachments.[1] And while the volume of security threats is increasing exponentially, security professional headcounts cannot be increased proportionally.

Isolated silos of security solutions add complexity and hinder the ability to assess the threat landscape throughout the environment. High-value threat indicators of compromise are lost in the deluge of overflowing alerts and log files.

Companies need to enhance detection, automate protection, and streamline workflows to increase staff efficiency and effectiveness if they are going to keep up.

McAfee Advanced Threat Defense and Cisco Email Security Solution

Cisco Email Security Appliance interoperates with McAfee Advanced Threat Defense to identify and forward unknown email attachments to McAfee Advanced Threat Defense for in-depth analysis and identification of potential zero-day threats. With inline deployment of McAfee Advanced Threat Defense, the Cisco Email Security Appliance can then take policy-based remediation, such as deleting or quarantining the attachment, and prevent the malware from infecting and spreading into the internal network. This rich, multilayered defense reduces the detection-to-protection timeframe and alleviates the ever-increasing workload facing security professionals. The benefits to customers are better protection with fewer resource requirements.

Cisco Email Security Technologies protect against ransomware, business email compromise, spoofing, and phishing. It uses advanced threat intelligence and a multilayered approach to protect inbound messages and sensitive outbound data. With a choice of physical appliance, virtual, cloud-based, or hybrid deployment, Cisco Email Security helps customers stay several steps ahead of threats, keep inboxes highly secure, and protect vital business assets.

McAfee Advanced Threat Defense offers interoperability with Cisco Email Security Appliance to enhance detection of advanced, zero-day email threats. With minimal configuration and single-click activation, McAfee Advanced Threat Defense works with Cisco Email Security to provide in-depth analysis capabilities that detect even highly camouflaged, evasive threats disguised in email attachments.

Solution Reference Architecture

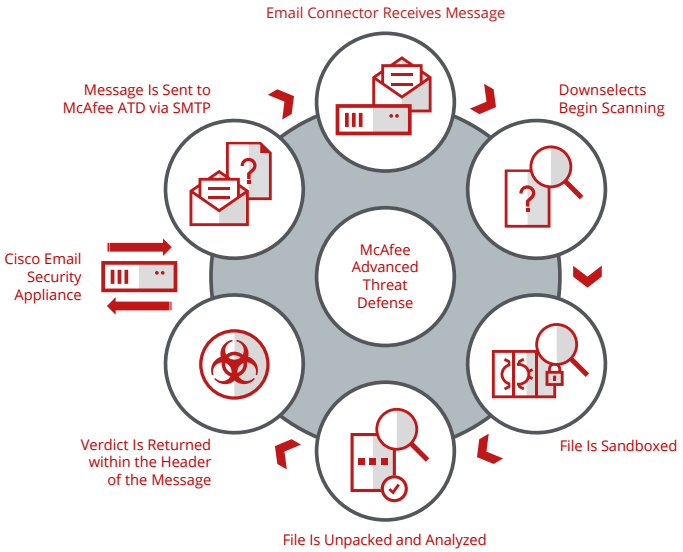

Figure 1. Inline deployment example demonstrates interoperability of McAfee Advanced Threat Defense and Cisco Email Security.

How It Works

Interoperability between Cisco Email Security Appliance and McAfee Advanced Threat Defense enhances detection of malicious attachments and enables investigation. The Cisco Email Security Appliance receives an email with a suspicious attachment that its inspection engine cannot fully determine, so it forwards the message to McAfee Advanced Threat Defense for further analysis.

Two deployment modes for McAfee Advanced Threat Defense offer flexibility.

- Inline mode prevents messages with attachments from reaching a user's inbox until McAfee Advanced Threat Defense analysis is complete and results are forwarded to Cisco Email Security Appliance.
- Offline mode allows messages to be sent immediately to a user's inbox while McAfee Advanced Threat Defense analyzes the file. Administrators view analysis results through the McAfee Advanced Threat Defense user interface.

With either mode deployed, McAfee Advanced Threat Defense in-depth analysis begins:

- Through dynamic analysis, the attachment file is executed within the McAfee Advanced Threat Defense sandbox environment. The file's actions are recorded and evaluated.
- Running in parallel is static code analysis. McAfee Advanced Threat Defense unpacks the file, looks at the instruction sets to determine intended behaviors, and then compares those to instruction sets of known malware families. Since malicious code is often reused but slightly modified to create new variants, this analysis engine is especially effective.
- In the final step of the analysis, McAfee Advanced Threat Defense specifically looks for malicious indicators that have been identified through machine learning in the form of a deep neural network.
- The reputation score of the file is determined.

For inline mode:

- The severity level of the attachment is placed into an X-header in the email. McAfee Advanced Threat Defense then sends the message back to the Cisco Email Security Appliance where the X-header is scanned for the "verdict." The Cisco Email Security Appliance then acts appropriately on this information by delivering the message to the intended recipient (if the attachment is determined to be clean) or by enforcing user-defined policies to handle the message based on the user's requirements.
- Reports and indicators of compromise (IoCs) are also available through McAfee Advanced Threat Defense and are searchable via file hash, recipient email, subject line, and other fields.

For offline mode:

- The copy of the mail and its attachments are deleted from McAfee Advanced Threat Defense. The severity level of the attachment, analysis reports, and IoCs are available for administrators through McAfee Advanced Threat Defense.
- Cisco Email Security Appliance does not receive an analysis verdict from McAfee Advanced Threat Defense.

About Cisco

Cisco (NASDAQ: CSCO) is the worldwide technology leader that has been making the internet work and is a member of the McAfee Security Innovation Alliance Partner Program. Cisco Email Security has been certified as McAfee Compatible to securely interoperate with McAfee Advanced Threat Defense software.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly interoperable, where protection, detection, and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.
www.mcafee.com

Learn More

Cisco Email Security Appliance at **http://www.cisco.com/go/esa**. Evaluate how Cisco products will work for you with a Cisco sales representative, channel partner, or systems engineer.

McAfee Advanced Threat Defesnse Cisco ESA How to Guide: Use this guide to implement an instance of Cisco Email Security Appliance and McAfee Advanced Threat Defense.

Learn more about McAfee Advanced Threat Defense at **www.mcafee.com/atd**. Contact your McAfee sales representative or partner, and learn how McAfee products, like McAfee Advanced Threat Defense can help you orchestrate a safer environment with enhanced security.

1. http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

McAfee Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com