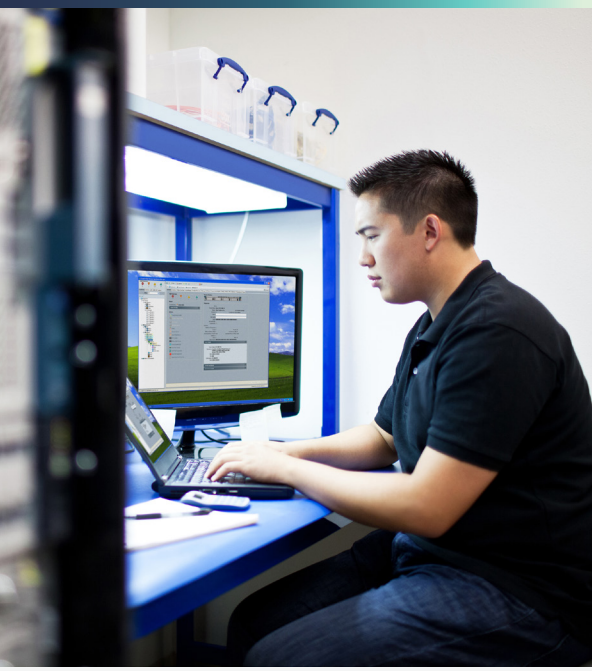
At-a-Glance



Advanced Malware Protection for Cisco Email Security

Protect Against the Most Stealthy Email-Based Attacks

Organizations face an ever-increasing number of email-based attacks. From spear phishing to targeted attacks, cyber attackers use email as a primary method to infiltrate the network. After malware is inside, traditional detection tools provide limited or no visibility into the activity of potential threats. IT security teams are left blind and unable to quickly respond. As a result, organizations are being breached every day.

It is critical to deploy an email security solution that provides visibility across the entire attack continuum: before, during, and after an attack. Only Advanced Malware Protection (AMP) for Cisco® Email Security can address the full lifecycle of advanced malware on email gateways and protect against the most stealthy email attacks that evade traditional defenses.

Benefits

- **Protects** against phishing email attacks such as ransomware and cryptoworms
- **Analyzes emails for threats** such as zero-day exploits and attacks hidden in attachments and malicious URLs
- **Stops blended attacks** across multiple threat vectors by integrating with other AMP deployments
- **Uncovers stealthy malware** and understands how it works with advanced sandboxing capabilities
- **Reduces time to detection** with retrospective alerting
- **Tracks unknown files** after they have traversed the email gateway with continuous analysis of files

Why Advanced Malware Protection for Email Security?

Adding AMP to Cisco's email security solutions adds advanced threat capabilities alongside traditional email security features like antivirus and antispam tools to take your threat protection to the next level.

Together, these solutions can inspect email content and transactions and analyze them using real-time threat intelligence. They can also deploy retrospective detection alerts so you can track malware that made it through your initial defenses and later turned malicious.

Protection Before, During and After an Attack

Add an AMP subscription to your Cisco Email Security solution and take advantage of the following capabilities:

Before: Strengthen your defenses with real-time threat intelligence from Cisco Talos. Email content and transactions will be inspected and malicious content will be automatically blocked.

During: Using 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. Advanced sandboxing technology can also be used to detect malware, allowing security administrators to glean precise details about a file's behavior and threat level.

After: Using continuous analysis of files, AMP finds malicious files that have passed through the gateway and were subsequently deemed a threat. AMP will then send a retrospective alert that gives you visibility into who on the network may have been affected and when.

Next Steps

Learn more at www.cisco.com/go/ampforemail or talk to a Cisco sales representative or channel partner about how AMP for Email Security can help you defend your organization against the most advanced cyber attacks.

C45-730848-03 07/16