DATASHEET

Email Threat Prevention Cloud

Cloud-Based Platform That Identifies, Analyzes, and Blocks Email Attacks

SECURITY REIMAGINED

HIGHLIGHTS

- Complete email security against advanced attacks and anti-spam, anti-virus protection
- Deploys as a cloud-based solution with no hardware or software to install
- Enables operational efficiencies through consolidation
- Integrates with the FireEye NX platform to stop blended attacks across multiple threat vectors
- Analyzes emails for threats, such as zero-day exploits, attacks hidden in ZIP/ RAR/TNEF archives, and malicious URLs
- Provides true file type analysis for all attachment types: EXE, DLL, PDF, SWF, DOC/DOCX, XLS/XLSX,PPT/PPTX, JPG, PNG, MP3, MP4, and many more
- Deploys in active protectionmode as a mail exchanger (MX) destination, or monitor-mode (via BCC)
- In active protection-mode, quarantines malicious emails with optional user notifications
- SOC 2 Type I certification for Security and Confidentiality

Overview

The FireEye® Email Threat Prevention Cloud is a SaaS offering that combats against today's advanced email attacks and provides anti-spam, anti-virus protection. As organizations have embraced the cloud for email needs, the Email Threat Prevention Cloud provides a complete email security for cloud mailboxes.

Organizations face an ever-increasing number of threats from emailbased spam, viruses, and advanced threats. Email-based attacks, in particular spear phishing, remain one of the primary methods used to initiate an advanced persistent threat (APT) attack because of the complexity involved in detecting them. To protect against malicious emails, organizations simply route messages to the Email Threat Prevention Cloud. The cloud analyzes the emails for spam and known viruses first. It then uses the signature-less FireEye Multi-vector Virtual Execution™ (MVX) engine to analyze every attachment and URL to detect threats and stop APT attacks in real time.

Easy deployment and cross-enterprise protection

With no hardware or software to install, the Email Threat Prevention Cloud is a particularly good fit for organizations seeking to move their infrastructure into the cloud. This eliminates the complexity of procuring, installing, and managing a physical infrastructure.

Email Threat Prevention Cloud integrates with the entire FireEye deployment for real-time threat intelligence sharing. This rich correlation of threat intelligence provides organizations several unique capabilities, such as:

- Identifying previous targets of spear-phishing emails
- Locating copies of the malicious email in target inboxes
- Finding out if the message is being forwarded to new targets
- Highlighting URLs that become malicious after message deliveryFor added accessibility and ease-of-use, the NX series dashboard shows region- and industry-based malware trends, has customizable widgets, RBAC, and audit logging.

Operational effectiveness

Email Threat Prevention Cloud consolidates advanced threat prevention with traditional security to optimize spending, reduce false positives, and enable operational efficiencies through consolidation.

Multi-vector virtual execution in the cloud

Email Threat Prevention Cloud uses the MVX engine in the cloud to detonate email attachments against a cross-matrix of operating systems and applications, including multiple Web browsers and plug-ins like Adobe Reader and Flash. Like the on-premise EX series platforms, the cloud-based FireEye MVX engine does not use signatures to stop advanced attacks exploiting unknown OS, browser, and application vulnerabilities as well as malicious code embedded in file and multimedia content.

Real-time quarantine of malicious emails

To block spear-phishing emails, Email Threat Prevention Cloud analyzes every attachment using the MVX engine to accurately identify today's advanced attacks. When an attack is confirmed, Email Threat Prevention quarantines the malicious emails for further analysis or deletion by administrators.

Security across email and Web threat vectors

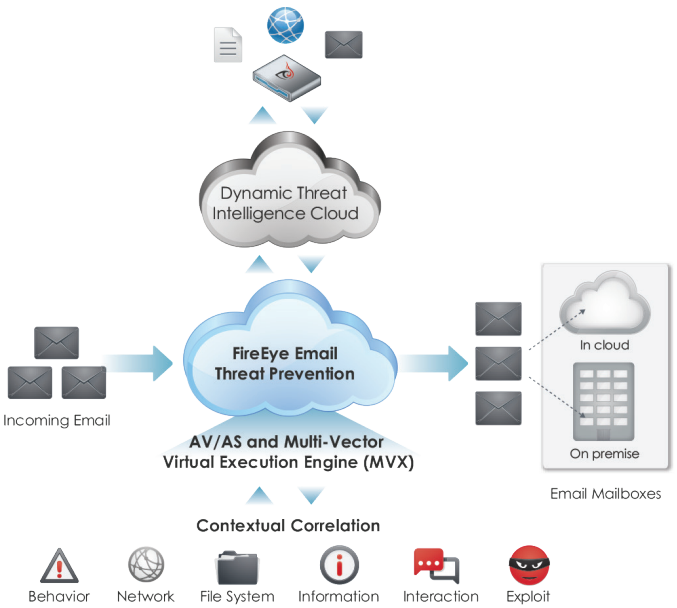
Today's advanced attacks use email as a primary delivery mechanism for malicious content. While some attacks use an attachment with embedded malicious code, it is common for cybercriminals to use a malicious link thereby blending attack tactics in the hopes of bypassing today's traditional defense silos. FireEye Email Threat Prevention Cloud integrates with onpremise FireEye NX platforms to coordinate real-time protections against multi-vector, blended attacks.

Deploy in active protection-mode or monitor only

FireEye Email Threat Prevention Cloud can analyze emails and quarantine threats for active protection. Organizations simply update their MX records to route messages to FireEye. For monitor-only deployments, organizations just need to setup a transparent BCC rule to send copies of emails to FireEye for MVX analysis.

Easy-to-use management portal

Organizations have access to the FireEye Email Threat Prevention portal to view real-time alerts and generate reports.



FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@FireEye.com | **www.FireEye.com**