FireEye

Datasheet

Email Threat Prevention

Cloud-based platform that identifies, analyzes, and blocks email attacks

Highlights

- Protects against spear-phishing email attacks
- Deploys as a cloud-based solution with no hardware or software to install
- 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
- Complements existing email hygiene offerings, such as anti-spam and secure email gateways
- Deploys in active protection-mode as a mail exchanger (MX) destination, or monitor-mode (via BCC)
- In active protection-mode, quarantines malicious emails with optional user notifications

The FireEye® Email Threat Prevention cloud-based platform secures against today's advanced email attacks. As organizations have embraced the cloud for email needs, the Email Threat Prevention platform addresses the missing piece, advanced email security for cloud mailboxes.

Email-based attacks, in particular spear phishing, remain one of the primary methods used to initiate an advanced persistent threat (APT) attack because they can easily evade traditional defenses. To start protecting against malicious emails, organizations simply route messages to the Email Threat Prevention. The cloud 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 platform 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.

Like the on-premise FireEye EX platforms, the cloud-based Email Threat Prevention platform 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 delivery

"FireEye Email Threat Prevention is a critical component of our security strategy. As a provider of critical infrastructure, it's essential we put in place the most effective security solution available on the market to block email attacks—and FireEye does just that."

— Chief Information Officer for U.S. state-run utility

FireEye™

Datasheet

Multi-vector virtual execution in the cloud

The Email Threat Prevention platform 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. The MVX analysis environment accounts for evasion tactics, such as archiving the attachment multiple times, password protecting the ZIP/RAR, or embedding malicious code within legitimate documents.

Real-time quarantine of malicious emails

To block spear-phishing emails, Email Threat Prevention 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 will 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. The FireEye Email Threat Prevention integrates with on-premise FireEye NX platforms to coordinate real-time protections against multi-vector, blended attacks.

Deploy in active protection mode or monitor only

The FireEye Email Threat Prevention cloud-based platform 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.