DATA SHEET

FireEye Email Security Cloud Edition

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

HIGHLIGHTS

- Offers comprehensive inbound and outbound email security
- Consolidates the email security stack with a comprehensive single vendor solution
- Supports custom YARA rules to enhance threat detection efficacy
- Enables auto remediate for Office 365 to remove emails that become malicious after delivery
- Integrates with any third party email provider
- Provides in-depth knowledge about attacks and attackers from frontline investigations and observations of adversaries
- Meets the FedRAMP security requirements

"Email is fundamental to all collaborative environments, so deploying FireEye Email Security gives us the ability to mitigate the risks of compromise from this highly exploited channel using a single solution."

Nils Göldner
Managing Partner and Cloud Advisor
Blackboat GmbH

Overview

Email is the most vulnerable vector for cyber attacks as it is the highest volume data ingress point. Organizations face an ever-increasing number of threats from email-based spam, malware and advanced threats. The majority of advanced threats arrive by email in the form of URLs linked to credential-phishing sites, fraudulent wire transfer requests and weaponized file attachments. The highly targeted and customizable nature of email allows cyber criminals to successfully exploit it, making email the primary choice for cyber crime.

FireEye Email Security can reduce cost and increase employee productivity through a single email security solution that minimizes the risk of costly breaches caused by advanced email attacks. Deployed in the cloud, FireEye Email Security is a fully featured secure email gateway that leads the industry in identifying, isolating, and immediately stopping URL, impersonation, and attachment-based attacks, before they enter an organization's environment. With auto remediate for Office 365, emails that become retroactively malicious after delivery to an user's inbox can be extracted. FireEye Email Security also scans outgoing email traffic for advanced threats, spam and viruses.

Using a confluence of intelligence-led context and detection plug-ins, malicious URLs are unearthed on a true big data, scalable platform. Sender names and email addresses are checked for authenticity and content is examined for impersonation tactics to stop CEO fraud and other malware-less attacks. The signatureless Multi-Vector Virtual Execution™ (MVX) engine analyzes email attachments and URLs against a comprehensive cross-matrix of operating systems, applications and web browsers. Threats are identified with minimal noise, and false positives are nearly nonexistent.

FireEye collects extensive threat intelligence on adversaries, through firsthand breach investigations and millions of sensors. Email Security draws on this real evidence and contextual intelligence about attacks and bad actors to prioritize alerts and block threats in real time.

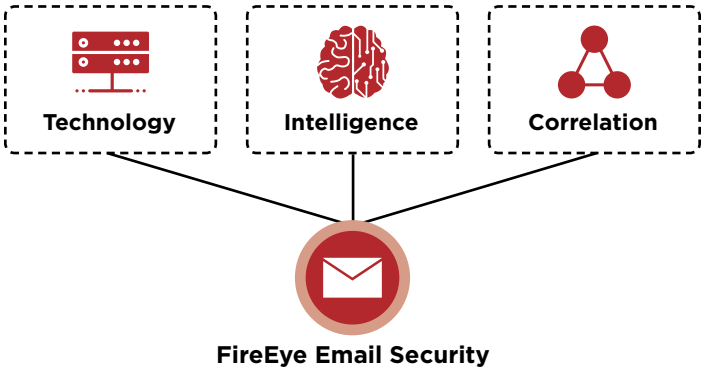

Figure 1. A secure email gateway.

By integrating with FireEye Network Security organizations can get broader visibility into multi-vector blended attacks and coordinate real-time protection.

Defense against email borne threats
With personal information readily available online, a cyber criminal can use social engineering to trick almost any user into taking an action, clicking a URL or opening an attachment.

Email Security provides real-time detection and protection against credential harvesting, impersonation, and spear-phishing attacks that typically evade traditional email security services. Emails are analyzed and quarantined (blocked) if unknown and advanced threats are found hidden in:

- All attachment types, including EXE, DLL, PDF, SWF, DOC/ DOCX, XLS/XLSX, PPT/PPTX, JPG, PNG, MP3, MP4 and ZIP/RAR/TNEF archives
- Password-protected and encrypted attachments
- URLs embeded in emails, PDFs and Microsoft Office documents
- Credential-phishing and typosquatting URLs
- Unknown OS, browser and application vulnerabilities
- Malicious code embedded in spear-phishing emails

While ransomware attacks start with an email, a call back to a command-and-control server is required to encrypt the data. Email Security identifies and stops these hard-to-detect multi-stage malware campaigns.

Superior threat detection

Email Security helps mitigate the risk of costly breaches by identifying and isolating advanced, targeted, and other evasive attacks camouflaged as normal traffic.

Once detected these attacks are immediately stopped, analyzed, and fingerprinted for faster identification of future threats.

At the core of Email Security are Advanced URL Defense and the MVX engine. These technologies use cutting edge machine learning and analytics to identify attacks that evade traditional signature and policy-based defenses.

An integral part of Advanced URL Defense, PhishVision is an image classification engine that uses deep learning to compile and compare screenshots of trusted and commonly targeted brands against web and login pages referenced by URLs in an email. Working in tandem with PhishVision, Kraken is a phishing detection plug-in that applies domain and page content analytics to augment machine learning. Another advance in URL detection is Skyfeed, a purpose-built, fully automated malware intelligence gathering system. Social media accounts, blogs, forums and threat feeds are collected for false negative discovery. The multifaceted nature of Advanced URL Defense offers organizations protected by Email Security unparalleled defense against credential harvesting and spear-phishing attacks.

An email may start out as benign to get past security defenses. Only after it has been delivered to a recipient's inbox does the email become malicious. Email Security—Cloud Edition retroactively analyzes and alerts when an email becomes malicious post delivery. Via the Office 365 API, emails that become retroactively malicious can be automatically extracted from the inbox by creating an auto remediate policy.

The MVX engine detects zero-day, multi-flow and other evasive attacks by using dynamic, signature-less analysis in safe virtual environments. It stops the infection and compromise phases of the cyber attack kill chain by identifying never-before-seen exploits and malware.

Enhanced AVAS protection

Email Security—Cloud Edition is available with anti-spam and antivirus (AVAS) protection to detect both common attacks that use conventional signature matching as well as impersonation techniques.

Impersonation attacks, such as CEO fraud (often called business email compromise) continue to significantly impact businesses financially. This is due in part to the lack of traditional threat indicators such as malicious attachments or links since the attacks are malware-free and rely on social engineering techniques. To combat these attacks and protect customers, FireEye has developed innovative algorithms, systems and tools specializing in impersonation detection and defense.

A common indicator of an email attack is the age of the sender's domain. When creating an impersonation campaign, cyber criminals send out attack emails from a domain similar to that of the person or company they are impersonating, usually within a few hours of that domain's creation.

Email Security is able to accurately determine the age and maturity of a domain using in-house developed Newly Existing Domains (NED) and Newly Observed Domains (NOD) tools. Domains determined to be newly created are treated suspiciously and extensively inspected for other attack indicators, such as typosquatting and sender display or username spoofing.

Instead of having to go through the process of buying and registering a domain, cyber criminals can simply change the display name or username of the sender making the email appear to come from a trusted source. Email Security defends against this sender spoofing by determining a display name's and username's authenticity using friendly name identification.

Outbound scanning

Email Security detects unknown advanced threats, including malicious attachments and phishing URLs delivered via outbound email messages. Outgoing email traffic is also scanned for malware and spam to protect an organization's domains from being blacklisted.

Integration to improve alert handling efficiencies

Email Security analyzes every email attachment and URL to accurately identify today's advanced attacks. Realtime updates from the entire FireEye security ecosystem combined with attribution of alerts to known threat actors provide context for prioritizing and acting on critical alerts and blocking advanced email attacks. Known, unknown and non-malware-based threats are identified with minimal noise and false positives so that resources are focused on real attacks to reduce operational expenses.

Rapid adaptation to the evolving threat landscape

Email Security helps your organization continually adapt your proactive defense against email-borne threats. Email Security creates its own threat intelligence rather than relying on lagging third-party feeds. In-house, email-specific threat intelligence (or Smart DNS), data collection capabilities, email security experts and threat analysts provide the underlying infrastructure for enhanced anti-spam technologies and impersonation detection. Deep intelligence about threats and attackers combines adversarial, machine and victim intelligence to:

- Deliver timely and broader visibility to threats
- Identify specific capabilities and features of detected malware and malicious attachments
- Provide contextual insights to prioritize and accelerate response
- Determine the probable identity and motives of an attacker and track their activities within your organization
- Retroactively identify spear-phishing attacks and prevent access to phishing sites by rewriting malicious URLs

Organizations have access to the Email Security portal to view real-time alerts, create Smart Custom Rules and generate reports. Smart Custom Rules allow your organization to create policies and rules based on multiple granular conditions.

Response workflow integration

Email Security works with several other FireEye solutions to help automate alert response workflows:

FireEye Central Management correlates alerts from both Email Security and Network Security for a broader view of an attack and to set blocking rules to prevent the attack from spreading.

The FireEye Helix platform works smoothly with Email Security and is specifically designed to simplify, integrate and automate security operations.

Easy deployment and cross-enterprise protection

Email Security—Cloud Edition is cloud-based, with no hardware or software to install. It's ideal for organizations migrating their email infrastructure to the cloud. This shift eliminates the complexity of procuring, installing and managing a physical infrastructure.

Email Security—Cloud Edition integrates seamlessly with cloud-based email systems such as Microsoft Office 365 with Exchange Online Protection and G Suite.

To protect against malicious and fraudulent emails, organizations simply route messages to Email Security, which analyzes the emails for spam, known malware and impersonation tactics first. It then uses the URL defense technology and signature-less detonation chamber, MVX engine, to analyze every attachment and URL for threats and stop advanced attacks in real time.

Additional capabilities

YARA-based rules enable customization

Email Security enables analysts to use custom YARA rules to manage and enhance detections, stop the latest threats and identify ongoing campaigns.

Active-protection or monitor-only mode

Email Security 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 set up a transparent BCC rule to send copies of emails to FireEye for MVX analysis.

Authorization and compliance certfications

ISO 27001

Email Security—Cloud Edition meets the ISO 27001 information security standard that ensures data centers are securely managed.

FedRAMP

Email Security—Cloud Edition with AVAS protection meets the FedRAMP security requirements for cloud services operated by government and public education entities.

SOC 2 Type 2

Email Security—Cloud Edition complies with the American Institute of Certified Public Accountants (AICPA) Service Organization Controls (SOC 2) Type 2 Certification for Security and Confidentiality.

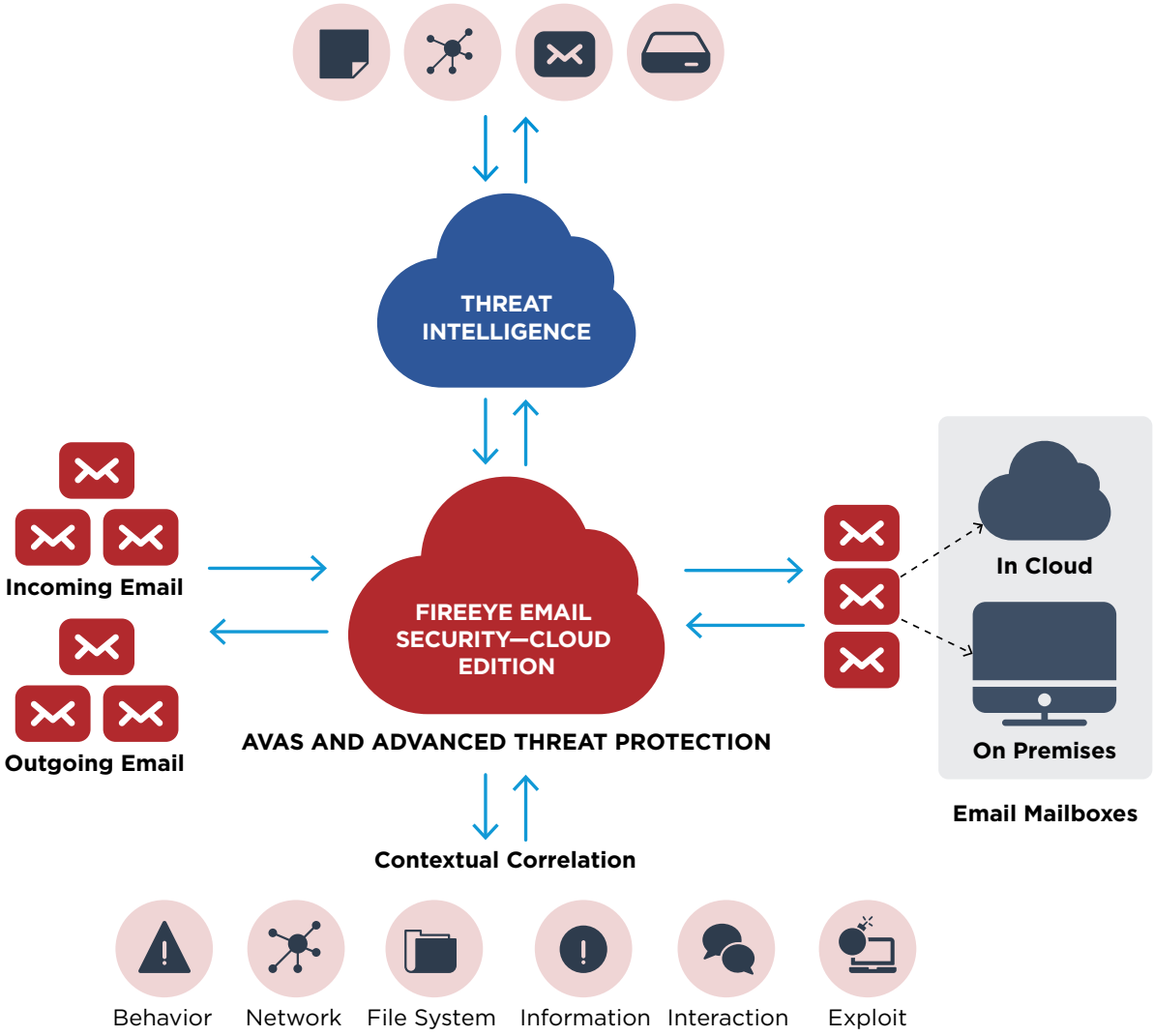

Figure 2. FireEye Email Security – Cloud Edition.

To learn more about FireEye, visit: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About FireEye, Inc.

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.