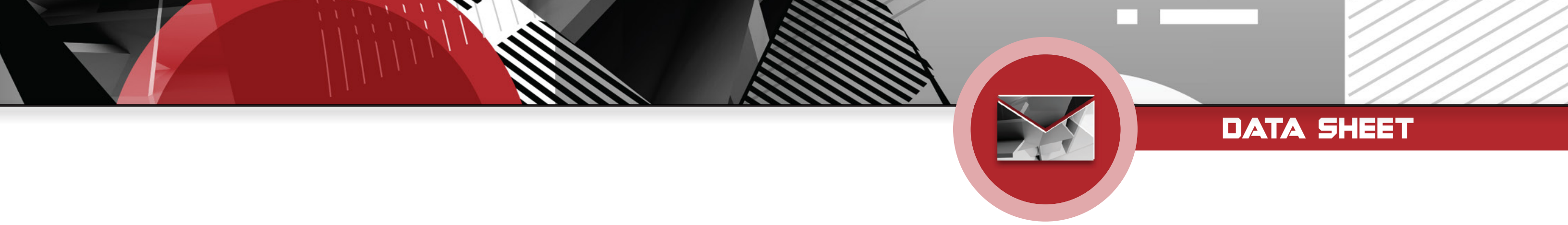


DATA SHEET

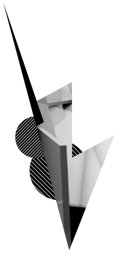
FireEye

FireEye Email Security Cloud Edition

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

HIGHLIGHTS

- Offers comprehensive email security against spear phishing and other advanced, multi-stage and zero-day attacks, as well as anti-spam and antivirus protection
- Analyzes emails for threats hidden in files including password-protected and encrypted attachments and malicious URLs
- Automatically detects and reduces or entirely prevents credential phishing
- Provides contextual insights for alerts to prioritize and contain threats
- Integrates with Office 365, Google Mail and a variety of FireEye technologies
- Deploys in active protection or monitor-only mode
- Meets the FedRAMP security requirements and complies with SOC 2 Type II certification



> "Because we have such confidence in knowing that FireEye Email Security provides the protection we are looking for, we don't spend a lot of time fixating on the possibility of an attack."
>
> **Shaun Guthrie**
> Director of Information Technology
> Go Auto

Overview

Email is the most vulnerable vector for cyber attacks because it is the highest volume data ingress point. Organizations face an ever-increasing number of threats from email-based spam, viruses and advanced threats. The majority of threats arrive by email in the form of weaponized file attachments, malicious links, wire-transfer fraud and credential phishing. While anti-spam and antivirus software are good at catching traditional mass email phishing attacks with known malicious attachments, links and content, they cannot catch sophisticated and targeted spear-phishing attacks designed to bypass these legacy solutions. Email remains the primary method used to initiate an advanced attack or deliver ransomware because it can be highly targeted and customized to increase the odds of exploitation.

FireEye Email Security helps organizations minimize the risk of costly breaches. Deployed in the cloud, it accurately detects and can immediately stop advanced and targeted attacks, including spear phishing and ransomware before they enter your environment. Email Security uses the signature-less Multi-Vector Virtual Execution™ (MVX) engine to analyze 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, firsthand breach investigations and through millions of sensors. Email Security draws on this real evidence and contextual intelligence about attacks and attackers to prioritize alerts and block threats in real time.

Email Security integrates with FireEye Network Security for broader visibility to coordinate real-time protection against multi-vector, blended attacks.

Effective threat detection

Email Security is an effective cyber threat protection solution that helps organizations minimize the risk of costly breaches by accurately detecting and immediately stopping advanced, targeted and other evasive attacks hiding in email traffic.

At the core of Email Security is the MVX engine that inspects suspicious email traffic to identify attacks that evade traditional signature- and policy-based defenses. The MVX engine detects zero-day, multi-flow and other evasive attacks by using dynamic, signature-less analysis in a safe, virtual environment. It stops the infection and compromise phases of the cyber attack kill chain by identifying never-before-seen exploits and malware.

Email Security – Cloud Edition is available with anti-spam and antivirus protection to detect common attacks that use conventional signature matching.

Defense against email borne threats

With all the personal information available online, a cyber criminal can socially engineer almost any user into clicking a URL or opening an attachment.

Email Security provides real-time detetion and prevention of spear-phishing, ransomware, sender impersonation and credential-phishing attacks that evade traditional defenses. It reduces credential phishing with detection of “like but not equal” domains (typosquatting).

If an attack is confirmed, Email Security quarantines the malicious email for further analysis or deletion. It conducts analyses for malware 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 embedded in emails
- 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.

Efficient response to alerts

Email Security analyzes every attachment and URL to accurately identify today’s advanced attacks. Real-time 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 spear-phishing emails. 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 by using deep intelligence about threats and attackers. It 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 highlighting malicious URLs

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

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 Google Mail.

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

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.

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.

Compliance certfications

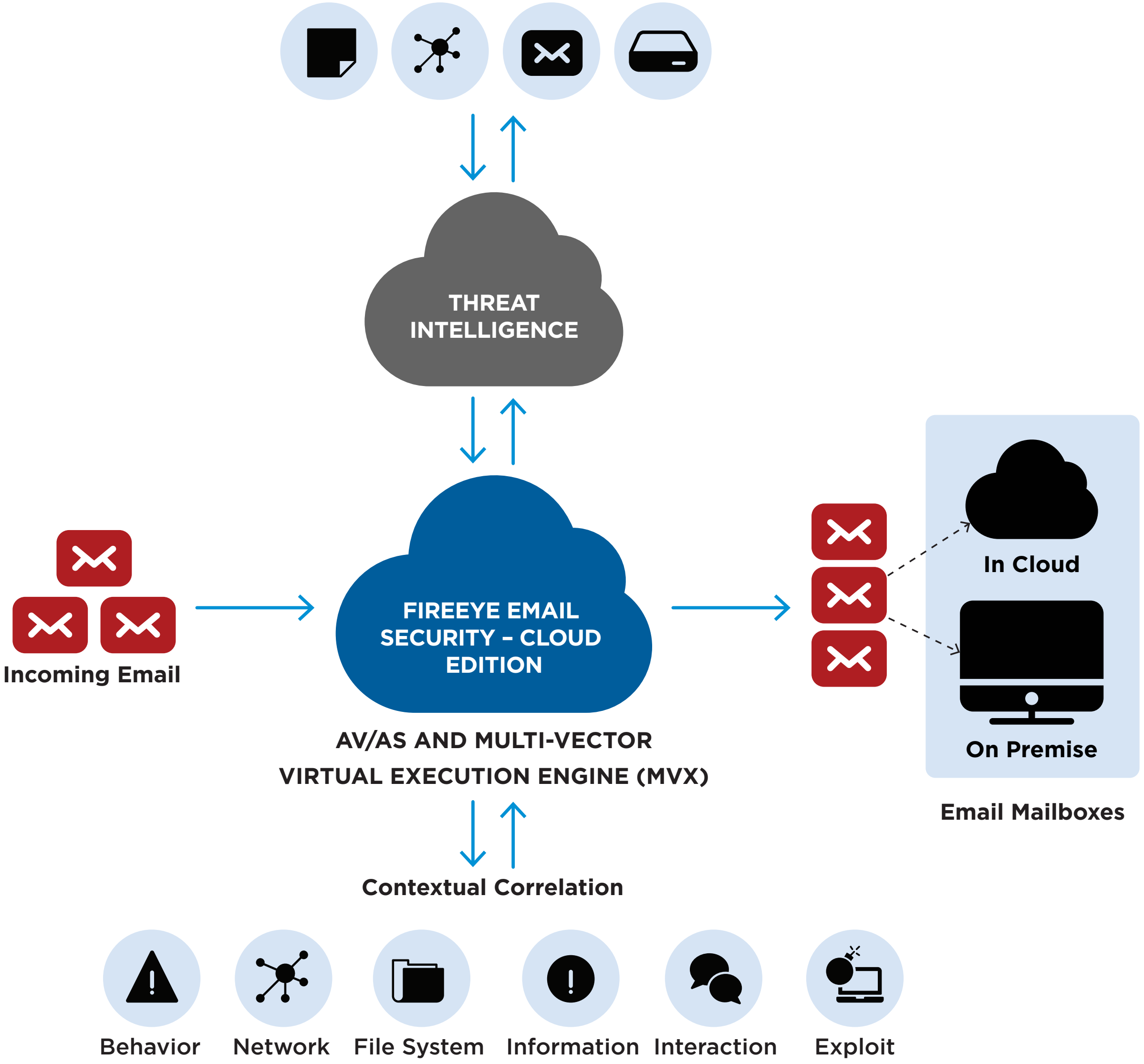
FedRAMP

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

SOC 2 Type II

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

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. FireEye has over 6,600 customers across 67 countries, including more than 45 percent of the Forbes Global 2000.