FireEye Email Security (EX Series)

Adaptive, intelligent, scalable defense against email borne threats

Figure 1. EX 3500, EX 5500 and EX 8500.

HIGHLIGHTS

- Offers comprehensive email security against spear phishing and other advanced, multi-stage and zero-day attacks
- Cloud bursting provides added detection analysis capacity during peak message throughput periods
- Supports analysis against Microsoft Windows and Apple Mac OS X operating system images
- Analyzes email 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 a variety of FireEye technologies
- Deploys on-premises in active-protection or monitor-only mode
- Provides visibility, tracking and management of messages and alerts

OVERVIEW

Email is the most vulnerable vector for cyber attacks because it's the highest volume data ingress point. Organizations face an ever-increasing number of security challenges from email-based spam and viruses to advanced and targeted threats. The majority of threats arrive by email in the form of weaponized file attachments, malicious links and credential phishing. While anti-spam filters 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. Email Security (EX Series) on-premises appliances, accurately detect and can immediately stop advanced and targeted attacks, including spear phishing and ransomware before they enter your environment. Email Security uses the signatureless 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 and Endpoint Security for broader visibility to coordinate real-time protection against multi-vector, blended attacks.

FireEye

Effective threat detection

FireEye 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 Multi-Vector Virtual Execution™ (MVX) engine. MVX is a signatureless, dynamic analysis 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, signatureless 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.

Cloud bursting to a FireEye MVX Smart Grid provides added capacity for detecting and analyzing email-borne threats during peak message throughput periods.

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 detection and prevention of spear-phishing, ransomware 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:

- Attachment types including, but not limited to: 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, MS Office documents, PDF and archive files (ZIP, ALZip, JAR), and other file types (Uuencoded, HTML)
- Files downloaded through URLs
- Obfuscated, spoofed, shortened and redirected URLs
- Credential-phishing and typosquatting URLs
- Unknown Microsoft Windows and Apple Mac OS X operating system images, 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 typically 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. Riskware categorization separates genuine breach attempts from undesirable, but less malicious activity (such as adware and spyware) to prioritize alert response.

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

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. It then uses the signatureless detonation chamber, the MVX engine, to analyze every attachment and URL for threats and stop advanced attacks in real time.

For monitor-only deployments organizations set up a transparent BCC rule to send copies of emails to Email Security for analysis by the MVX engine.

Elevation of security operations

Email Security is a component of FireEye Helix and works with FireEye Central Management.

- As a component of FireEye Helix, it empowers organizations to go from detecting a threat to defeating it quickly at a low cost.
- FireEye Central Management correlates alerts from both Email Security and FireEye Network Security for a broader view of an attack and to set blocking rules to prevent the attack from spreading.

YARA-based rules enable customization

Email Security supports custom YARA rules to enable security analysts to specify and test rules for analyzing email attachments containing threats targeting their organization.

Message queue and alert and quarantine management

Email Security provides a high degree of control over the email messages it scans. For active protection-mode deployments, messages can be tracked and managed as they move through the MTA queue. Email attributes can be used to search and verify that messages were received, analyzed and delivered to the next hop and trends over time can be monitored through an intuitive dashboard. Explicit allow and block lists provide custom control over email processing. Common alert attributes can be searched and selected. And bulk operations can be performed on alerts and quarantined messages.

Table 1. Technical specifications

	EX 3500	EX 5500	EX 8500
Performance*	Up to 700 unique attachments/h	Up to 1,800 unique attachments/h	Up to 2,650 unique attachments/h
Network Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+, 2x 1GigE BaseT
Management Ports	LSI9341-4i, 2x 1GigE BaseT	LSI9341-4i, 2x 1GigE BaseT	LSI9341-4i, 2x 1GigE BaseT
IPMI Monitoring	Supported	Supported	Supported
PS/2 keyboard and Mouse, DB15 VGA ports (rear panel)	Included	Included	Included
USB Ports (rear panel)	2x USB2, 2x USB3	2x USB2, 2x USB3	2x USB2, 2x USB3
Serial Port (rear panel)	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU	4x 2TB, RAID 10, HDD 3.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 25.6" x 1.7" (437 x 650 x 43.2 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)	17.24" x 24.41" x 3.48" (438 x 620 x 88.4 mm)
AC Power Supply	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 800 watt, 100 - 240 VAC, 9 – 4.5A,50-60 Hz, IEC60320-C14 inlet, FRU
DC Power Supply	Not Available	Not Available	Not Available
Thermal Maximum Power watts (Btu/h)	245 watts (836 Btu/h)	456 watts (1,556 Btu/h)	530 watts (1,808 Btu/h)
MTBF (h)	54,200	19,970	11,880
Appliance Alone / As Shipped Weight, lb (kg)	30.0 lbs (13.6 kg) / 41.0 lbs (18.6 kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	44.4 lbs (20.2 Kg) / 65.6 lbs (29.8 kg)
Compliance Safety	UL 60950-1-2014; CAN/ CSA C22.2 No. 60950-1-07, Am.1:2011+Am.2:2014; AS/NSZ 60950.1- 2011	EN 60950-1, 1:2006+A1 1:2009+A1:2010+A12:20 11+A2:2013; IEC 60950- 1:2005 + Am 1:2009 + Am 2:2013	EN 60950-1, 1:2006+A1 1:2009+A1:2010+A12:20 11+A2:2013; IEC 60950- 1:2005 + Am 1:2009 + Am 2:2013

Table 1. Technical specifications

	EX 3500	EX 5500	EX 8500
Compliance EMC	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN55022 Class A; VCCI V-3 Class A; EN 55024; EN 61000-3-2 Class A; EN 61000-3-3; CNS 13438 (2006) Class A; CISPR22 Class A; AS/NZS CISPR 22 Class A; KN 32; KN 35	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;	FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;
Security Certifications**	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
Environmental Compliance	RoHS; REACH; WEEE	RoHS; REACH; WEEE	RoHS; REACH; WEEE
Operating Temperature	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)	0 ~ 35° C (32 ~ 95° F)
Operating Relative Humidity	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing
Operating Altitude (ft)	5,000	5,000	5,000

* All performance values vary depending on the system configuration and email traffic profile being processed. Size appliance(s) based on unique attachments per hour.
** In progress.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. 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 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye