DATA SHEET

FireEye Email Security Server Edition

Adaptive, intelligent, scalable defense against email borne threats

HIGHLIGHTS

- Offers comprehensive email security against malicious attachments, credential-phishing URLs, spoofing, zero-day and multi-stage attacks
- Supports analysis against Microsoft Windows and Apple macOS X operating system images
- Extensively examines email for threats hidden in password-protected files, encrypted attachments, and URLs
- Acquires real-time threat intelligence from the FireEye DTI Cloud
- Prioritizes and contains threats by providing contextual insights for alerts
- Deploys on-premises with integrated or distributed MVX service

Figure 1. Integrated Email Security appliances include EX 3500, EX 5500 and EX 8500.

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 security challenges from email-based advanced threats. Most advanced threats use email to deliver URLs linked to credential phishing sites and weaponized file attachments. Because it is highly targetable and customizable, email is the primary medium for cyber crime.

FireEye Email Security helps organizations minimize the risk of costly breaches caused by advanced email attacks. Deployed on premises, FireEye Email Security – Server Edition leads the industry in identifying, isolating and immediately stopping URL and attachment-based attacks, before they enter an organization's environment. Email Security combines intelligence-led context and detection plug-ins to unearth malicious and benign phishing URLs on a big data, scalable platform. The signatureless Multi-Vector Virtual Execution™ (MVX) engine analyzes email attachments and URLs linked to downloadable content 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 both concrete evidence and contextual intelligence about attacks and attackers to prioritize alerts and block threats in real time.

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

Defense against email borne threats
With all the personal information 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 prevention against credential harvesting, impersonation and spear-phishing attacks that typically evade traditional email security defenses. Emails are analyzed and quarantined (blocked) if unknown and advanced threats are found 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
- Password-protected attachments with password sent via image
- URLs embedded in emails, MS Office documents, PDF and archive files (ZIP, ALZIP, JAR), and other file types (Uuencoded, HTML)
- Files downloaded through URLs – and even FTP links
- Obfuscated, spoofed, shortened and dynamically redirected URLs
- Credential-phishing and typosquatting URLs
- Unknown Microsoft Windows and Apple macOS 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.

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, the MVX engine and MalwareGuard. These technologies use 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 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. Skyfeed, another advance in URL detection, is a purpose-built, fully automated malware intelligence gathering system. Social media accounts, blogs, forums and threat feeds are collected to discover false negatives. The multi-faceted nature of Advanced URL Defense offers organizations protected by Email Security unparalleled defense against credential harvesting and spear-phishing attacks.

MalwareGuard is a machine learning utility that takes binary files as input and outputs a suspiciousness score. Every Portable Executable (PE) file seen on the wire is analyzed by MalwareGuard. A decision is made based on the score and detections triggered by MalwareGuard are assigned a name.

The MVX engine detects zero-day, multi-flow and other evasive attacks by using dynamic, signature-less analysis in a safe, virtual environment. It identifies never-before-seen exploits and malware to stop infection and compromise.

Evasion mitigation

Email Security supports a controlled live mode feature to defend against attacks that evade requests for remote objects. The MVX engine detects malware requiring multiple downloads and returns the remote objects requested by the sample binary. Controlled live mode reduces false negatives for multistage downloads, advanced spear-phishing attacks and advanced ransomware intrusions.

Attackers also try to evade technology used for detecting suspicious URLs. As part of Advanced URL Defense, evasion mitigations for phishing sites are continually evolving. Evasion mitigations are continually enhanced as part of Advanced URL Defense. Another evasion mitigation, Guest Images can be customized to mimic a “used” endpoint when a potentially malicious object is executed. Many evasion techniques are prevented by ensuring the Guest Image reproduces an endpoint domain, domain user, Outlook data and browser history.

Integration to improve alert handling efficiencies
Email Security analyzes every email 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 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. 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 via real-time threat intelligence from the FireEye Dynamic Threat Intelligence (DTI) Cloud. 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
- Rewrite all URLs embedded within an email to protect users from malicious links
- Retroactively identify spear-phishing attacks and prevent access to phishing sites by highlighting malicious URLs

Response workflow integration
Email Security works seamlessly with FireEye Helix and FireEye Central Management.

- As a component of the security operations platform — FireEye Helix — it provides visibility across the entire infrastructure. FireEye Helix augments email and third-party alerts with intelligence, correlation to the endpoint, automation, and investigative tips. With these capabilities, FireEye Helix surfaces unseen threats and empowers expert decisions.
- 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.
- Central Management supports role-based tagging to know who is being targeted.
- Central Management supports alert response and remediation based on role-based criteria.

Additional capabilities

YARA-based rules enable customization
Email Security enables analysts to specify and test custom rules to analyze email attachments for threats targeting their organization.

Executive impersonation protection
Email Security – Server Edition offers the capability to block business email compromises (BEC) to protect important employees from being spoofed. A policy is created that compares inbound email display names to an approved list that matches approved envelope senders.

Message queue, alert and quarantine management
Email Security – Server Edition 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.

Active-protection or monitor-only mode
Email Security can analyze emails and quarantine threats for active protection. For monitor-only deployments organizations just set up a transparent BCC rule to send copies of emails to Email Security for analysis.

Flexible Deployment Options

Email Security – Server Edition offers various deployment options to match an organization's needs and budget:

- **Integrated Email Security:** standalone, all-in-one hardware appliance with integrated MVX service to secure an email ingress point at a single site. FireEye Email Security is an easy-to-manage solution that deploys in under 60 minutes. It doesn't require rules, policies or tuning.
- **Distributed Email Security:** extensible appliances with centrally shared MVX service to secure email ingress points within organizations
- **Email Smart Node:** virtual sensors analyze email traffic to detect and block malicious traffic and submit suspicious activity over an encrypted connection to the MVX service for definitive verdict analysis
- **MVX Smart Grid:** on-premise, centrally located, elastic MVX service that offers transparent scalability, built-in N+1 fault tolerance and automated load balancing.

  Bursting from an integrated hardware appliance to an MVX Smart Grid provides added capacity for detecting and analyzing email-borne threats during peak message throughput periods.
- **FireEye Cloud MVX:** MVX service subscription that ensures privacy by analyzing traffic on the Email Smart Node. Only suspicious objects are sent over an encrypted connection to the MVX service, where objects revealed as benign are discarded.

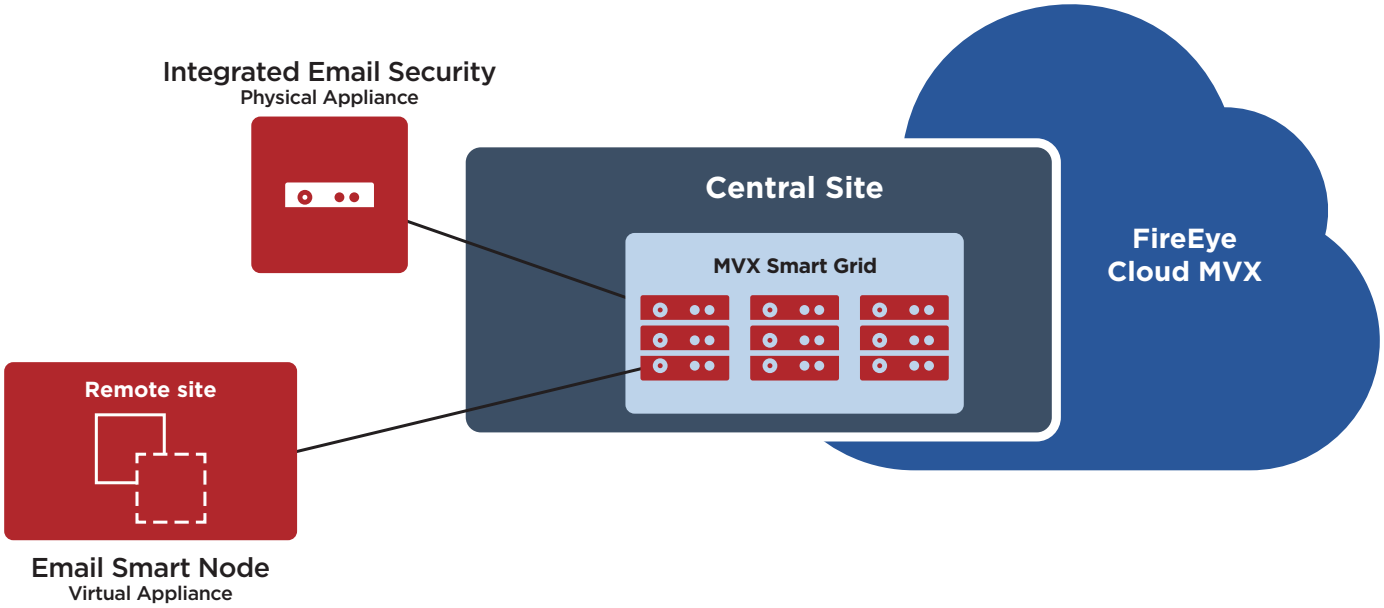

Figure 2. Distributed and bursting deployment models for Email Security.

Table 1. Technical specifications.

	EX 3500	EX 5500	EX 8500
Performance*	Up to 700 unique attachments per hour	Up to 1,800 unique attachments per hour	Up to 2,650 unique attachments per hour
Network Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+ (supporting 10GigE Fiber, 10GigE Copper, 1GigE Copper), 2x 1GigE BaseT
Management Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI Monitoring	Included	Included	Included
VGA Port (rear panel)	Included	Included	Included
USB Ports (rear panel)	4x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear	2x USB Type A Front, 2x USB Type A Rear
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	245 watts (836 BTU per hour)	456 watts (1,556 BTU per hour)	530 watts (1,808 BTU per hour)
MTBF (h)	54,200 hours	57,401 hours	53,742 hours
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	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
Compliance EMC	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 & V-3/2015
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 Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU	RoHS Directive 2011/65/EU; REACH; WEEE Directive 2012/19/EU
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	3,000 m / 9,842 ft	3,000 m / 9,842 ft	3,000 m / 9,842 ft

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

Table 2. FireEye MVX smart grid specifications.

	VX 5500	VX 12500
OS Support	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
Performance*	Up to 480 unique attachments per hour	Up to 3,780 unique attachments per hour
High Availability**	N+1	N+1
Management Ports (rear panel)	1x 10/100/1000 Mbps BASE- T Ports	1x 10/100/1000 Mbps BASE- T Ports
Cluster Ports (rear panel)	3x 10/100/1000 Mbps BASE-T Ports	1x 10/100/1000 Mbps BASE-T Ports, 2x 10 Gbps BASE-T Ports
IPMI Port (rear panel)	Included	Included
Front LCD & Keypad	Not Available	Included
VGA Ports	Included	Included
USB Ports (rear panel)	4x Type A USB Ports	2x Type A USB Ports
Serial Port (rear panel)	115,200 bps, No Parity, 8 bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Drive Capacity	2x 2TB 3.5 SAS HDD, RAID 1, hot-swappable, FRU	4 x 4TB 3.5" SAS3 HDD, RAID 1, FRU
Enclosure	1RU, Fits 19-inch Rack	2RU, Fits 19-inch Rack
Chassis Dimensions (WxDxH)	17. 2x25.6x1.7 Inches (437 x 650 x 43.2 mm)	17.2x33.5x3.5 Inches (437 x 851 x 89 mm)
DC Power Supply	Not Available	Not Available
AC Power Supply	Redundant (1+1) 750 watt, 100-240 VAC, 8 - 3.8 A, 50-60 Hz, IEC60320-C14, inlet, hot-swappable, FRU	Redundant (1+1) 800W: 100-127V, 9.8A-7A 1000W: 220-240V, 7-5A, 50-60Hz, FRU IEC60320-C14 inlet, FRU
Power Consumption Maximum	285 watts	760 watts
Thermal Dissipation Maximum	972 BTU per hour	2594 BTU per hour
MTBF	54,200 hours	38,836 hours
Appliance Alone / As Shipped Weight	33 lb (15 kg) / 48 lb (21.8 kg)	46 lb (21 kg) / 90 lb (40.2 kg)
Security Certification	FIPS 140-2 Level 1, CC NDPP v1.1	FIPS 140-2 Level 1, CC NDPP v1.1
Regulatory Compliance Safety	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

* All performance values vary depending on the system configuration and traffic profile being processed.

** With appropriate redundant hardware configurations.

Table 3. FireEye Email Security smart node, virtual sensor specifications.

	EX 5500V
OS Support	Microsoft Windows, Apple macOS X
Performance*	Up to 1,250 unique attachments per hour
Network Monitoring Ports	2
Network Management Ports	2
CPU cores	8
Memory	16 GB
Drive Capacity	384 GB
Network Adapters	VMXNet 3, vNIC
Hypervisor Support	VMWare ESXi 6.0 or later

* All performance values vary depending on the system configuration and traffic profile being processed.

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

Telecom Liechtenstein AG
Schaanerstrasse 1
9490 Vaduz / Liechtenstein
security@telecom.li
+423 237 90

About FL1

FL1 provides Next Generation Managed Security Services to international customers.
FL1 supplies residential and business customers in the area with highly innovative products and services. The company is the first and leading full-service provider, operates its own mobile network, and is thus able to bundle landline, mobile and internet services, as well as TV. Furthermore, a wide range of cloud and ICT services are provided.