FireEye
SECURITY REIMAGINED

EX Series

Threat Prevention Platforms that Combat Advanced Email-based Cyber Attacks

DATASHEET

HIGHLIGHTS

- Protects against spear-phishing email attacks
- Integrates with the FireEye NX series 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
- Deploys in active protection-mode as an MTA, or monitor-mode (SPAN/BCC)
- Quarantines malicious emails with optional user notifications
- Integrates with the FireEye cloudbased anti-virus and anti-spam protection engine for complete email security
- Associates alerts with actionable threat intelligence
- Provides visibility, tracking, and management of messages

EX 5400 and EX 8420
(not pictured EX 3400, EX 8400)

Overview

The FireEye® EX series secures against advanced email attacks. As part of the FireEye Threat Prevention Platform, the FireEye EX uses signature-less technology to analyze every email attachment and successfully quarantine spear-phishing emails used in advanced targeted attacks.

With all the personal information available online, a cybercriminal can socially engineer almost any user into clicking a URL or opening an attachment. The FireEye EX series provides real-time threat prevention for spear-phishing attacks that evade traditional defenses. The EX also delivers a new level of threat prevention against blended attacks by working with the FireEye NX platform to quarantine emails with malicious URLs and trace Web-based attacks back to the original spear-phishing email.

Real-time quarantine of malicious emails

To block spear-phishing emails, the FireEye EX series analyzes every attachment and URL using the purpose-built FireEye Multi-vector Virtual Execution™ (MVX) engine that accurately identifies today's advanced attacks. If an attack is confirmed, the EX series quarantines the malicious email for further analysis or deletion.

Comprehensive email security

FireEye EX series can be extended with the FireEye cloud-based antispam, anti-virus engine to provide complete email security against traditional and advanced email attacks. The incoming emails are analyzed and quarantined by the anti-spam, anti-virus engine in the cloud to thwart known threats while the on premise EX series combats the advanced unknown threats and zero-day attacks.

Fights blended attacks across Web and email threat vectors

Advanced attacks use spear phishing as the opening salvo of a multi-vector attack strategy. In order to reveal the entire attack life cycle, the EX series is often deployed along with the FireEye NX and CM series to correlate malicious URLs with the originating emails and the intended targets. The CM then locally distributes new malware intelligence to the entire FireEye deployment in real time.

Dynamic analysis of zero-day email attacks

The EX series uses the signature-less FireEye MVX engine which stops advanced attacks exploiting unknown OS, browser, and application vulnerabilities as well as malicious code embedded in common file and multimedia content. The FireEye MVX engine reports forensic details of the threat, such as the vulnerability exploited in a buffer overflow and callback coordinates used to exfiltrate data.

Threat intelligence sharing across the enterprise

The resulting dynamically generated, real-time threat intelligence can help all FireEye products protect the local network through integration with the FireEye CM platform. This intelligence can be shared globally through the FireEye Dynamic Threat Intelligence™ (DTI) cloud to notify all subscribers of emerging threats.

YARA-based rules enables customization

The EX series supports importing custom YARA rules to enable security analysts to specify rules to analyze email attachments for threats specific to the organization.

Streamlined email threat management

With the integrated offering of FireEye Email Threat Prevention using cloud-based anti-virus, anti-spam protection, and on premise EX series, organizations can gain operational effectiveness. The consolidation of advanced threat prevention with traditional security enables organizations to optimize spending, reduce false positives, and realize operational efficiencies.

Technical Specifications

	EX 3400	EX 5400	EX 8400	EX 8420
Performance *	Up to 150,000 emails per day	Up to 300,000 emails per day	Up to 600,000 emails per day	Up to 600,000 emails per day
Network Interface Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports	2x 1000BASE-SX Fiber Optic Ports (LC Multimode)
Management Ports	1x 10/100/1000BASE-T Ports	1x 10/100/1000BASE-T Ports	1x 10/100/1000BASE-T Ports	1x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included	Included	Included	Included
Front Panel LCD & Keypad	Included	Included	Included	Included
PS/2 Keyboard and Mouse, DB15 VGA ports (rear panel)	Included	Included	Included	Included
USB Ports (rear panel)	2x Type A USB Ports	2x Type A USB Ports	2x 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	115,200 bps, No Parity, 8 Bits, 1 Stop Bit	115,200 bps, No Parity, 8 Bits, 1 Stop Bit
Storage Capacity	2x 600 GB HDD, RAID 1, 2.5 inch, FRU	2x 600 GB HDD, RAID 1, 2.5 inch, FRU	2x 600 GB HDD, RAID 1, 2.5 inch, FRU	2x 600 GB HDD, RAID 1, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2 mm)	17.2" x 27.8" x 1.70" (437 x 706 x 43.2 mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.6 mm)	17.2" x 28.0" x 3.41" (437 x 711 x 86.6 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) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU	Redundant (1+1) 750 watt, 100 - 240 VAC, 9 – 4.5A, 50-60 Hz, IEC60320-C14 inlet, FRU
DC Power Supply	Not Available	Not Available	Not Available	Not Available
Power Consumption Maximum (watts)	296 watts	468 watts	509 watts	509 watts
Thermal Dissipation Maximum (BTU/h)	1010 BTU/h	1597 BTU/h	1737 BTU/h	1737 BTU/h
MTBF (h)	35,400 h	34,600 h	59,800 h	59,800 h
Appliance Alone / As Shipped Weight lb. (kg)	31 lb. (14 kg) / 46 lb. (21 kg)	32 lb. (15 kg) / 47 lb. (21 kg)	42 lb. (19 kg) / 58 lb. (26 kg)	42 lb. (19 kg) / 58 lb. (26 kg)
Security Certifications	CC NDPP v1.1	CC NDPP v1.1	CC NDPP v1.1	CC NDPP v1.1
Operating Temperature	10° C to 35° C	10° C to 35° C	10° C to 35° C	10° C to 35° C
Operating Relative Humidity	10% to 85% (non-condensing)	10% to 85% (non-condensing)	10% to 85% (non-condensing)	10% to 85% (non-condensing)
Operating Altitude	5,000 ft.	5,000 ft.	5,000 ft.	5,000 ft.

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

Actionable Threat Intelligence

Alerts generated by the FireEye EX Series can be optionally combined with the FireEye Advanced Threat Intelligence (ATI) to understand the source, severity, risk, mitigation options, and other contextual information about the attack. Meaningful intelligence from ATI results in a faster and more effective responses to threats.

Message Queue Management

FireEye EX Series provides 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.

LEARN MORE

FireEye offers a comprehensive portfolio of services. For full details, contact us at services@FireEye.com or +1 855.692.2052.

Contact Accumuli Security at info@accumuli.com or +44 (0) 1256 303 700.

WHY FIREEYE?

Expertise. Technology. Intelligence.

FireEye provides a combination of expertise, technology, and targeted, relevant intelligence that is unmatched in the security industry. FireEye security professionals partner with each client to understand and resolve their specific security challenges, providing rapid response from the top experts in the field. The FireEye threat protection platform provides FireEye with unique insight into the world of advanced persistent threats, targeted attacks, and cybercrime, allowing FireEye to provide clients with industry-specific dynamic threat intelligence. FireEye provides the expertise and intelligence organizations need to protect their businesses from today's threats.

FireEye, Inc. | 1440 McCarthy Blvd. Milpitas, CA 95035 | 408.321.6300 | 877.FIREEYE (347.3393) | info@fireeye.com | www.fireeye.com