FireEye

Datasheet

EX Series

Threat Prevention Platforms that Combat Advanced Email-based Cyber Attacks

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
- Complements existing email control infrastructure, such as anti-spam and secure email gateways
- Deploys in active protection-mode as an MTA, or monitor-mode (SPAN/BCC)
- Quarantines malicious emails with optional user notifications

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

The FireEye® EX series secures against spear-phishing emails that bypass anti-spam and email reputation-based technologies. As part of the FireEye Threat Prevention Platform, the FireEye EX uses signature-less technology to analyze every email attachment and successfully quarantine the 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 of spear-phishing attacks that easily 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 using the purpose-built FireEye Multi-Vector Virtual Execution™ (MVX) engine that accurately identifies today's advanced attacks. The FireEye MVX engine detonates email attachments against a cross-matrix of operating systems and applications, including multiple Web browsers and plug-ins like Adobe Reader and Flash. If an attack is confirmed, the EX platform quarantines the malicious emails for further analysis or deletion.

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

"In addition to the rapid deployment capabilities, the FireEye platform is an all-in-one solution that effectively halts zero-day attacks across the enterprise. The protection provided is independent of signatures and we enjoy an extremely low false positive rate; from day one the total count remains in the low single digits."

— Information Security Specialist, Global Manufacturer

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 FireEye AV-Suite, each malicious object is analyzed to determine if anti-virus vendors were able to detect the malware stopped by the FireEye EX platform. This enables customers to gain deeper forensic information about the attack and standardize naming terminology for more efficient incident response prioritization.

Usability

The FireEye EX series requires no tuning and can be setup as an MTA, SPAN device, or transparent BCC destination. FireEye supports remote third-party AAA network service access in addition to local authentication.

Technical Specifications

	EX 3400	EX 5400	EX 8400	EX 8420
Form Factor	1U Rack-Mount	1U Rack-Mount	2U Rack-Mount	2U Rack-Mount
Weight	25 lbs (11.4 Kg)	30 lbs (13.6 Kg)	50 lbs (22.7 Kg)	50 lbs (22.7 Kg)
Dimensions (WxDxH)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 25.6" x 1.7" (43.7 x 65.0 x 4.3 cm)	17.2" x 27.9" x 3.5"(43.7 x 70.9 x 8.9 cm)	17.2" x 27.9" x 3.5"(43.7 x 70.9 x 8.9 cm)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack	Fits 19-Inch Rack
Management Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports	(2) 1000 BASE-SX Fiber Optic Ports (LC Multimode)
Performance	Up to 150,000 Emails Per Day	Up to 300,000 Emails Per Day	Up to 750,000 Emails Per Day	Up to 750,000 Emails Per Day
Performance with TLS	Up to 100,000 Emails Per Day	Up to 200,000 Emails Per Day	Up to 500,000 Emails Per Day	Up to 500,000 Emails Per Day
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	8.5–6.0 A	8.5-6.0 A	9.5–7.2 A	9.5–7.2 A
Power Supply/RAID	Dual 700W / 2 SAS HDD in HW RAID1	Dual 700W / 2 SAS HDD in HW RAID1	Dual 1400W / 2 SAS HDD in HW RAID1	Dual 1400W / 2 SAS HDD in HW RAID1
Power Consumption (Max)	887 BTU/hr	1501 BTU/hr	1603 BTU/hr	1603 BTU/hr
Frequency	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Operating Temp	10° C to 35° C	10° C to 35° C	10° C to 35° C	10° C to 35° C

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