

CM Series

Real-time Exchange of Dynamic Threat Intelligence and Unified Management of Enterprise Deployments

DATASHEET

SECURITY
REIMAGINED

HIGHLIGHTS

- Offers integrated controls for multiple platform deployments
- Enables blended threat prevention through multi-vector correlation
- Provides a purpose-built platform that can be deployed in less than 60 minutes
- Displays an at-a-glance security dashboard that provides advanced targeted attack protection status
- Speeds reports and audits through a consolidated security event storehouse
- Streamlines management of multiple FireEye platforms and reduces time spent managing configurations, threat updates, and software upgrades

Overview

The FireEye® CM series is a group of management platforms that consolidates the administration, reporting, and data sharing of the FireEye NX, EX, FX, HX and AX series in one easy-to-deploy, network-based platform. Within the FireEye deployment, the FireEye CM enables real-time sharing of the auto-generated threat intelligence to identify and block advanced attacks targeting the organization. It also enables centralized configuration, management, and reporting of FireEye platforms.

Real-time sharing of local threat intelligence

FireEye platforms generate real-time threat intelligence using the FireEye Multi-Vector Virtual Execution™ (MVX) engine. The FireEye CM distributes threat intelligence to the entire FireEye deployment, ensuring that each platform has the same dynamic protections against the advanced attack underway. In addition, subscribers to the FireEye Dynamic Threat Intelligence™ (DTI) cloud can use the FireEye CM to centralize the sending and receiving of anonymized threat intelligence across FireEye platforms deployed within customers, technology partners, and service providers around the world.

At-a-glance security dashboard, plus drilldowns

The FireEye CM consolidates activities and improves situational awareness with

a unified security dashboard.

The dashboard gives administrators a real-time view to see the number of infected systems and drill directly down to infection details to determine next steps.

Unified analysis of advanced targeted attacks

By deploying the FireEye NX, EX, FX, HX and AX series together with the FireEye CM series, the analysis of blended threats, such as pinpointing a spear-phishing email used to distribute malicious URLs, and correlating a perimeter alert to the endpoint, becomes possible. Security analysts now have the ability to connect the dots of a blended attack, giving them the actionable intelligence necessary to protect organizations against advanced targeted attacks.

Enterprise-class console and alerting

The FireEye CM series provides a Web GUI console where events can be seen, searched, and filtered, and real-time alert notifications can be sent via SMTP, SNMP, syslog, or HTTP POST. Administrators can filter by events, dates, or IP ranges and results are displayed to only show data based on the administrator's IT operational role. Notifications can also be sent to third-party SIEM tools. In addition, administrators can click on an event link and connect seamlessly to specific FireEye platforms to view the network segment being protected.



CM 4400 and CM 9400
(not pictured CM 7400)

Central configuration and platform upgrades

For efficient enterprise deployments, the FireEye CM series features dynamic configurations. Settings can be determined centrally and then distributed across an organization accordingly. Administrators can remotely configure and view settings for a single or multiple platforms. Plus, all upgrades can be simultaneously deployed to all managed platforms, ensuring all products have the latest security capabilities.

Consolidated storehouse and detailed reporting

Larger and regulated organizations can leverage the FireEye CM series' central security data for efficient, consolidated reporting. The FireEye CM series provides a means to collect

and store audit-relevant security events to meet long-term data retention requirements. For added accessibility and ease-of-use, the NX series dashboard shows region- and industry-based malware trends, has customizable widgets, RBAC, and audit logging.

The FireEye CM series offers convenient ways to search for and report on specific types of threats by name or type.

Organizations can also view summaries such as the top infected hosts and malware and callback events, including geo-location details. In addition, trending views can help demonstrate progress in reducing the number of compromised systems

Technical Specifications

	CM 4400	CM 7400	CM 9400
Network Interface Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports
Management Ports (rear panel)	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports	2x 10/100/1000BASE-T Ports
IPMI Port (rear panel)	Included	Included	Included
Front Panel LCD & Keypad	Included	Included	Included
PS/2 Keyboard and Mouse, DB15 VGA Ports (rear panel)	Included	Included	Included
USB Ports (rear panel)	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
Storage Capacity	4x 600 GB HDD, RAID 10, 2.5 inch, FRU	4x 600 GB HDD, RAID 10, 2.5 inch, FRU	4x 800 GB SSD, RAID 10, 2.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2" x 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
DC Power Supply	Not Available	Not Available	Not Available
Power Consumption Maximum (watts)	313 watts	351 watts	565 watts
Thermal Dissipation Maximum (BTU/h)	1068 BTU/h	1198 BTU/h	1928 BTU/h
MTBF (h)	35,200 h	60,700 h	60,700 h
Appliance Alone / As Shipped Weight lb. (kg)	32 lb. (15 kg) / 47 lb. (21 kg)	42 lb. (19 kg) / 57 lb. (26 kg)	42 lb. (19 kg) / 58 lb. (26 kg)
Safety Certifications	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking	IEC 60950, EN 60950, CSA 60950-00, CE Marking
EMC/EMI Certifications	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)	FCC (Part 15 Class-A), CE (Class-A), CNS, AS/NZS, VCCI(Class A)
Regulatory Compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Operating Temperature	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)
Operating Altitude	5,000 ft.	5,000 ft.	5,000 ft.

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

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.

