FireEye™

Datasheet

CM Series

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

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

The FireEye® CM series is a group of management platforms that consolidates the administration, reporting, and data sharing of the FireEye NX, EX, FX, 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.

CM 4400 and CM 9400
(not pictured CM 7400)

> **"Our college takes user security seriously, hence we enforce patches and anti-virus on the desktop and use firewalls and IPS systems on the gateway. But because of remote users who are infected outside our gateway, compounded by the reality of spear phishing, zero-day and targeted attacks, we realize that a signature-based solution does not provide complete protection against today's Web exploits and botnets."**
>
> *— Systems and Server Manager, Liberal Arts College*

Unified analysis of advanced targeted attacks

By deploying the FireEye NX, EX, FX, 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, 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.

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.

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
Form Factor	1U Rack-Mount	2U Rack-Mount	2U Rack-Mount
Weight	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 3.4" (43.7 x 65.0 x 8.9 cm)	17.2" x 25.6" x 3.4 (43.7 x 65.0 x 8.9 cm)
Enclosure	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
AC Input Voltage	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	8.5–6.0 A
Power Supply/RAID	Dual 700W / 4 SAS HDD in HW RAID10	Dual 700W / 4 SAS HDD in HW RAID10	Dual 700W / 4 SATA SSD in HW RAID10
Power Consumption (Max)	1057 BTU/hr	1143 BTU/hr	1876 BTU/hr
Frequency	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

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