CM Series

Real-time exchange of dynamic threat intelligence and unified management of enterprise deployments

Figure 1. CM 4500 and CM 9500 (not pictured CM 7500).

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 products 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
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.

FireEye

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.

Table 1. Appliance specifications.

	CM 4500	CM 7500	CM 9500
Network Interface Ports	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
Management Ports (rear panel)	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
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 2TB HDD, RAID 10, 3.5 inch, FRU	4x 2TB HDD, RAID 10, 3.5 inch, FRU	8x 2TB HDD, RAID 10, 3.5 inch, FRU
Enclosure	1RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack	2RU, Fits 19 inch Rack
Chassis Dimensions (WxDxH)	17.2in(437mm) x 25.6in(650mm) x 1.7in(43.2mm)	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) 750W AC PSUs	Redundant (1+1) 800W AC PSUs	Redundant (1+1) 800W AC PSUs
Power Consumption Maximum (watts)	245 watts	456 watts	612 watts
Thermal Dissipation Maximum (BTU/h)	836 BTU/h	1556 BTU/h	2088 BTU/h

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

Table 2. Appliance specifications continued.

	CM 4500	CM 7500	CM 9500
MTBF (h)	35,200 h	60,700 h	60,700 h
Appliance Alone / As Shipped Weight lb. (kg)	30.0 lbs (13.6Kg) / 41.0 (18.6Kg)	44.1 lbs (20.0 kg) / 65.3 lbs (29.6 kg)	50.4 lbs (22.9 Kg) / 71.6 lbs (32.5 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 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;"	"FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;"	"FCC Part 15 SubPart B Class A; ICES-003 Class A; EN 61000-3-2 Class A; EN 61000-3-3; CISPR22 Class A;"
Regulatory Compliance	RoHS, REACH, WEEE	RoHS, REACH, WEEE	RoHS, REACH, WEEE
Operating Temperature	0 ~ 35° C	0 ~ 35° C	0 ~ 35° C
Operating Relative Humidity	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 40° C, 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.

Table 2. Virtual appliance specifications.

Model	CPU Cores	RAM	Virtual NICS	Hard Disk Space
CM2500V	4	32 GB	4 (total): 1 (management) 1-3 (for future use)	512 GB
CM7500V	16	128 GB	4 (total): 1 (management) 1-3 (for future use)	1200 GB

Note: Each virtual appliance must meet the following spcifications.

For more information on FireEye, visit:
www.FireEye.com

FireEye, Inc.
1440 McCarthy Blvd. Milpitas, CA 95035 tel: 408.321.6300 / 877 FIREEYE (347.3393) / info@FireEye.com

www.FireEye.com

FireEye® is the leader in intelligence-led security-as-a-service. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nation-state grade threat intelligence and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks. FireEye has over 5,000 customers across 67 countries, including more than 940 of the Forbes Global 2000.

FireEye