FireEye

Datasheet

Central Management System

A Real-Time Local Exchange of Threat Data and Unified Management of Enterprise Deployments

Highlights

- Purpose-built appliance that can be deployed in about 30 minutes
- Ideal for organizations with five or more FireEye appliances to manage, or those using FireEye Web MPS, Email MPS, File MPS, and/or MAS together.
- Two models available to accommodate growing FireEye deployments
- Streamlined centralized management of multiple FireEye appliances reduces time spent managing configurations, threat updates, and software upgrades
- At-a-glance security dashboard provides advanced targeted attack protection status
- Consolidated security event storehouse speed reports and audits

The dashboard provides a real-time view into the network's security state and appliance workloads

The FireEye Central Management System (CMS) consolidates the management, reporting, and data sharing of FireEye Malware Protection Systems (MPS) in an easy-to-deploy, network-based appliance.

The CMS enables real-time sharing of malware intelligence auto-generated within your FireEye deployment to stop advanced attacks targeting the organization. It also enables centralized configuration, management, and reporting of FireEye security appliances.

Real-time sharing of local malware intelligence

FireEye appliances generate real-time advanced malware protections using the Virtual Execution (VX) engine. The CMS is a distribution hub ensuring the entire FireEye deployment has dynamic protections against the advanced targeted attack underway. In addition, subscribers to the Malware Protection Cloud (MPC) can use the CMS to centralize sending and receiving malware intelligence.

At-a-glance security dashboard, plus drilldowns

The CMS 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 FireEye Web MPS, Email MPS, File MPS, and Malware Analysis System (MAS) with the FireEye CMS, it enables the detailed analysis of blended threats, such as pinpointing the spear phishing email used to distribute malicious URLs. Security analysts now have

"Our college takes user security seriously, hence we enforce patches and antivirus 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

the ability to connect the dots of a blended attack for the actionable intelligence necessary to protect organizations against advanced targeted attacks.

Enterprise–class console and alerting

Events can be searched and filtered, and real-time alert notifications can be sent via SMTP, SNMP, syslog or HTTP POST or seen within the CMS' Web GUI console. Administrators can filter by events, dates, or IP ranges and results are scoped to only show data accessible based on the administrator's IT operational role. Notifications can also be sent to third-party SIEM tools such as ArcSight, Nitro Security, Splunk, and RSA.

From the CMS console, administrators can click on an event link and connect seamlessly to specific FireEye appliances to view the local management system and review the network segment being protected.

Central configuration and appliance upgrades

For efficient enterprise deployments, the FireEye CMS features dynamic configurations. Settings can be determined centrally and then distributed appropriately. Administrators can remotely configure and view settings for a single appliance or a group of appliances. Plus, appliance upgrades can be deployed to all managed appliances, ensuring the latest security capabilities across all appliances. Upgrades to the VX engine (such as new guest images to get the latest Service Pack) can be pushed out with a click of a button.

Consolidated storehouse and detailed reporting

Larger and regulated organizations can leverage the CMS' central security data storehouse for efficient, consolidated reporting. The CMS provides a means to collect and store audit-relevant security events to meet long-term data retention requirements.

FireEye CMS provides convenient ways to search for and report on specific types of threats by name or type. Customers can also view summaries such as the top infected hosts and top malware and callback events, including geo-location details. Trending views can help demonstrate progress in reducing the number of compromised systems.

Technical Specifications

	CMS 4310	CMS 7300
Form Factor	1U Rack-Mount	1U Rack-Mount
Weight	30 lbs (13.6 Kg)	30 lbs (13.6 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)
Enclosure	Fits 19-Inch Rack	Fits 19-Inch Rack
Management Interfaces	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Interfaces	N/A	N/A
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	8.5-6 A	8.5-6 A
Power Supply/RAID	Dual / 3 SAS HDD in HW RAID5	Dual / 3 SAS HDD in HW RAID5
Frequency	50-60 Hz	50-60 Hz
AC Power	700 W Max	700 W Max
Ambient Temp	40° C	40° C

© 2012 FireEye, Inc. All rights reserved. FireEye is a trademark of FireEye, Inc. All other brands, products, or service names are or may be trademarks or service marks of their respective owners. – DS.CMS.022012