FireEye

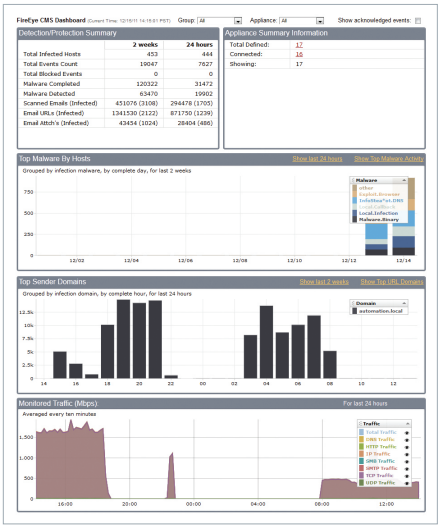
Datasheet

Central Management System

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

Highlights

- Offers integrated controls for multiple appliance deployments
- Enables blended threat protection through multi-vector correlation
- Purpose-built appliance that can be deployed in less than 60 minutes
- At-a-glance security dashboard provides advanced targeted attack protection status
- Consolidated security event storehouse speeds reports and audits
- Streamlined centralized management of multiple FireEye appliances reduces time spent managing configurations, threat updates, and software upgrades



The FireEye CMS 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 the FireEye Malware Protection System™ (MPS) in an easy-to-deploy, network-based appliance.

Within the FireEye deployment, the FireEye CMS enables real-time sharing of the auto-generated malware intelligence to identify and block advanced attacks targeting the organization. It also enables centralized configuration, management, and reporting of FireEye appliances.

Real-time sharing of local malware intelligence

FireEye appliances generate real-time advanced malware protections using the FireEye Multi-Vector Virtual Execution™ (MVX) engine. These protections are distributed within the deployment via the FireEye CMS which is a distribution hub that ensures the entire FireEye deployment has the dynamic protections against the advanced targeted attack underway. In addition, subscribers to the FireEye Dynamic Threat Intelligence™ (DTI) cloud can use the FireEye CMS to centralize the sending and receiving of anonymized threat intelligence across FireEye appliances deployed within customers, technology partners, and service providers.

At-a-glance security dashboard, plus drilldowns

The FireEye 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.

"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

FireEye™

Datasheet

Unified analysis of advanced targeted attacks

By deploying the FireEye Web MPS, Email MPS,™ File MPS,™ and Malware Analysis System™ (MAS) with the FireEye CMS, detailed analysis of blended threats such as pinpointing the spear phishing email used to distribute malicious URLs, become 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 CMS 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 scoped 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 appliances to view 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, all FireEye appliance upgrades can be deployed to all managed appliances, ensuring the latest security capabilities across all appliances.

Consolidated storehouse and detailed reporting

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

The 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 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 Ports	(2) 10/100/1000 BASE-T Ports	(2) 10/100/1000 BASE-T Ports
Monitoring Ports	N/A	N/A
AC Input Voltage	Auto-switching 100 ~ 240 VAC Full Range	Auto-switching 100 ~ 240 VAC Full Range
AC Input Current	8.5–6.0 A	8.5–6.0 A
Power Supply/RAID	Dual 700W / 3 SAS HDD in HW RAID5	Dual 700W / 3 SAS HDD in HW RAID5
Frequency	50–60 Hz	50–60 Hz
Operating Temp	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.