数据表

FireEye 中央管理平台

集中设备和情报管理，以关联多个攻击矢量数据

亮点

- 为多平台部署提供集成控制
- 通过多向量相关性实现混合威胁预防
- 提供一个可在 60 分钟内部署的专用平台
- 提供一个一目了然的安全仪表板，显示高级针对性攻击的防护状态
- 通过一个合并安全事件库加快报告和审核的速度
- 精简多个 FireEye 解决方案的管理，同时减少配置管理、威胁更新、软件升级所需的时间

图 1 CM 4500 和 CM 9500（CM 7500 不在图片之中）。

概要

FireEye® 中央管理平台（CM 系列）是一组管理平台，将 FireEye 产品的管理、报告以及数据共享整合到一个可轻松部署的网络型平台中。中央管理平台可确保实时共享自动生成的威胁情报，以识别并阻止针对组织的先进攻击。它还可以实现 FireEye 解决方案的集中配置、管理和报告。

本地威胁情报的实时共享

FireEye 解决方案通过 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎生成实时威胁情报。中央管理平台将该威胁情报分发到您系统中的多个 FireEye 部署，确保所有解决方案均配备相同的动态保护，以防范先进攻击。FireEye Dynamic Threat Intelligence™ (DTI) 云端的订阅用户可以使用中央管理平台在全世界的客户、技术合作伙伴、服务提供商所部署的 FireEye 解决方案中，集中发送和接收匿名威胁情报。

一目了然的安全仪表板，附带向下钻取功能

中央管理平台通过统一的安全仪表板整合活动，并提升情景感知。该仪表板为管理员提供实时视图，使之能够看到受影响的系统数量，并深入了解详情，以决定后续措施。

对先进针对性攻击的统一分析

针对混合威胁的分析，例如，可实现准确定位用来散发恶意网址的钓鱼邮件，并将外围警报关联到终端。安全分析师现在可以将混合攻击的各个点连接起来，从而获得必要的可行动情报，以确保组织免受高级针对性攻击的威胁。

企业级控制台和警报

中央管理平台系列提供网络 GUI 控制台，可以从中查看、搜索和过滤事件，并可通过 SMTP、SNMP、syslog 或 HTTP POST 发送实时警报通知。管理员可以通过时间、日期或 IP 范围进行过滤，而在过滤结果中，只会根据管理员的 IT 操作职责显示数据。通知也可以发送到第三方的 SIEM 工具。管理员可以点击事件链接，从而无缝连接到指定的 FireEye 解决方案，查看正受保护的网段。

集中配置和平台升级

中央管理平台系列拥有动态配置的特性，可实现高效的企业部署。可先集中决定设置，然后据此发布到整个组织。管理员可远程配置和查看一项或多项 FireEye 安全解决方案的设置。另外，可同时对所有受管理的平台进行升级，以确保所有产品获得最新的安全性能。

合并事件库和详细报告

规模较大且受监管的组织可以使用中央管理平台来有效地整合安全数据报告。中央管理平台系列为审核相关安全事件的收集和存储提供一种有效的方式，以满足长期保留数据的需求。

中央管理平台为您提供便利的方式，按名称或类型即可搜索和报告威胁。组织也可以查看最受影响的主机、恶意软件以及回调事件等汇总信息，包括详细地理位置。趋势图有助于显示受影响系统的数量减少进度。

表 1 设备规格。

	CM 4500	CM 7500	CM 9500
网络接口端口	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
管理端口（后面板）	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI 端口（后面板）	包含	包含	包含
前面板 LCD 和键盘	包含	包含	包含
PS/2 键盘和鼠标、DB15 VGA 端口（后面板）	包含	包含	包含
USB 端口（后面板）	2x 类型 A USB 端口	2x 类型 A USB 端口	2x 类型 A USB 端口
串行端口（后面板）	115,200 bps、无校验、8 比特、1 停止位	115,200 bps、无校验、8 比特、1 停止位	115,200 bps、无校验、8 比特、1 停止位
存储容量	4x 4 TB HDD、RAID 10 可用；8TB	4x 4 TB HDD、RAID 10 可用；8TB	4x 4 TB HDD、RAID 10 可用；8TB
外接盒	1RU，适合 19 英寸机架	2RU，适合 19 英寸机架	2RU，适合 19 英寸机架
机箱尺寸（宽 x 长 x 高）	17.2" x 25.6" x 1.7"（437 x 650 x 43.2 毫米）	17.24" x 24.41" x 3.48"（438 x 620 x 88.4 毫米）	17.24" x 24.41" x 3.48"（438 x 620 x 88.4 毫米）
AC 电源	冗余 (1+1) 750W AC PSU	冗余 (1+1) 800W AC PSU	冗余 (1+1) 800W AC PSU
最大功耗（瓦特）	245 瓦特	456 瓦特	612 瓦特
最大散热量（BTU/h）	836 BTU/h	1556 BTU/h	2088 BTU/h
平均无故障工作时间（小时）	35,200 小时	60,700 小时	60,700 小时
仅设备/发货重量 磅（千克）	30.0 磅 (13.6 Kg)/41.0 (18.6 Kg)	44.1 磅 (20.0 kg)/65.3 磅 (29.6 kg)	50.4 磅 (22.9 Kg)/71.6 磅 (32.5 kg)

注意： 根据系统的配置和所处理的网络流量，所有性能值都会发生变化。

表 1 设备规格。

	CM 4500	CM 7500	CM 9500
安全认证	IEC 60950、EN 60950、CSA 60950-00、CE 标示	IEC 60950、EN 60950、CSA 60950-00、CE 标示	IEC 60950、EN 60950、CSA 60950-00、CE 标示
EMC/EMI 认证	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
合规性	RoHS、REACH、WEEE	RoHS、REACH、WEEE	RoHS、REACH、WEEE
运行温度	0 - 35°C	0 - 35°C	0 - 35°C
运行相对湿度	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露
运行海拔高度	5,000 英尺 (1,524 米)	5,000 英尺 (1,524 米)	5,000 英尺 (1,524 米)

注意: 根据系统的配置和所处理的网络流量，所有性能值都会发生变化。

表 2 虚拟设备规格。

型号	CPU 核心	RAM	虚拟网卡	硬盘空间
CM2500V	4	32 GB	4 (总共)： 1 (管理) 1-3 (备用)	512 GB
CM7500V	16	128 GB	4 (总共)： 1 (管理) 1-3 (备用)	1200 GB

注意: 每个虚拟设备必须满足以下规格。

若要了解更多关于 FireEye 的信息，请访问：**www.FireEye.com**

FireEye
26/F Time Square93 Middle Huaihai,
HuangpuShanghai, China
China@FireEye.com

关于 FireEye, Inc.
FireEye 是一家情报主导型安全企业。FireEye 为客户提供无缝式、可扩展的讯息安全解决方案，提供一个将创新型安全技术、国家级威胁情报以及闻名于世的 Mandiant® 咨询集成于一体的平台。通过这种方式，FireEye 为殚精竭虑防备、阻止和应对网络攻击的组织，消除了网络安全的复杂性和负担。