数据表

FireEye SmartVision Edition

检测企业网络中的可疑横向移动

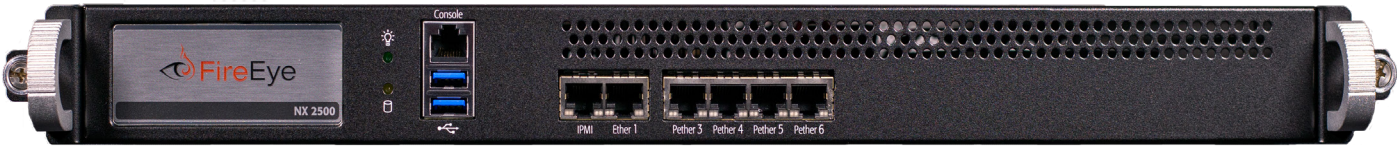

图 1. NX 2500 SmartVision 硬件。

优势

- 检测以前无法检测到的可疑横向流量
- 减少检测违规后活动的时间
- 提供灵活性，以在整个网络中扩展
- 查看网络分段计划
- 改善网络取证和事件响应
- 减少攻击者停留时间

FireEye SmartVision Edition 为网络流量分析 (NTA) 解决方案，可检测企业网络中的可疑横向移动。与其他网络安全解决方案在外围阻止恶意攻击不同的是，FireEye SmartVision Edition 可在整个网络内部署—无论是在核心、网络分段，还是在关键服务器资产之前—都能检测恶意内部流量。

安全分析师和管理员可通过 FireEye SmartVision Edition，了解和观察防火墙和其他安全网关遗漏的可疑横向流量。通过使用易于部署、轻型传感器结合 FireEye 在业界领先的 Cloud MVX™ 技术，客户可扩大在整个网络的 SmartVision Edition 可见性—范围从数据中心到远程办公室位置。

SmartVision Edition 的核心是高级威胁检测软件，其中包括高级关联和分析引擎和机器学习模块，通过 120 多条入侵检测规则检测数据泄露可能性，识别出安全性较弱的指标。

SMARTVISION EDITION 组件

SmartVision Edition 的启用需要三种组件：

- 至少一个或多个 SmartVision 传感器（硬件或虚拟）
- 连接至 FireEye MVX 引擎（本地、智能网格或通过 Cloud MVX *）
- SmartVision 激活的 FireEye 操作系统版本 8.1.2 或以上版本

表 1. SmartVision Edition 功能。

功能	描述
检测可疑横向网络流量	将高级关联和分析引擎与机器学习模块与 120 多条独特规则关联，以检测隐藏横向（东西向）流量
通过 SMB/SMB2 协议引爆对象	使用 FireEye MVX 技术引爆 WannaCry 等恶意软件和勒索软件，以及通过 SMB 协议在内部移动的可疑文件和对象
可视化警报以快速分类事件	提供 10 分钟（+/- 5分钟）的 L4 和 L7 警报环境，以快速调查攻击者活动并进行取证分析
支持广泛的元数据协议	生成用于综合分析的元数据，包括以下协议：FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS
补充现有的 FireEye Network Security 部署	采用第 4 代和第 5 代网络安全设备的 FireEye 客户易于将 SmartVision Edition 集成至现有架构，进一步增加其投资收益
与 FireEye Helix 集成	为团队之间的协作提供额外的威胁情报环境和集成警报分类

FireEye SmartVision Edition 可识别横向攻击周期的独特威胁活动，进一步减少违规后的停留时间和损失风险。

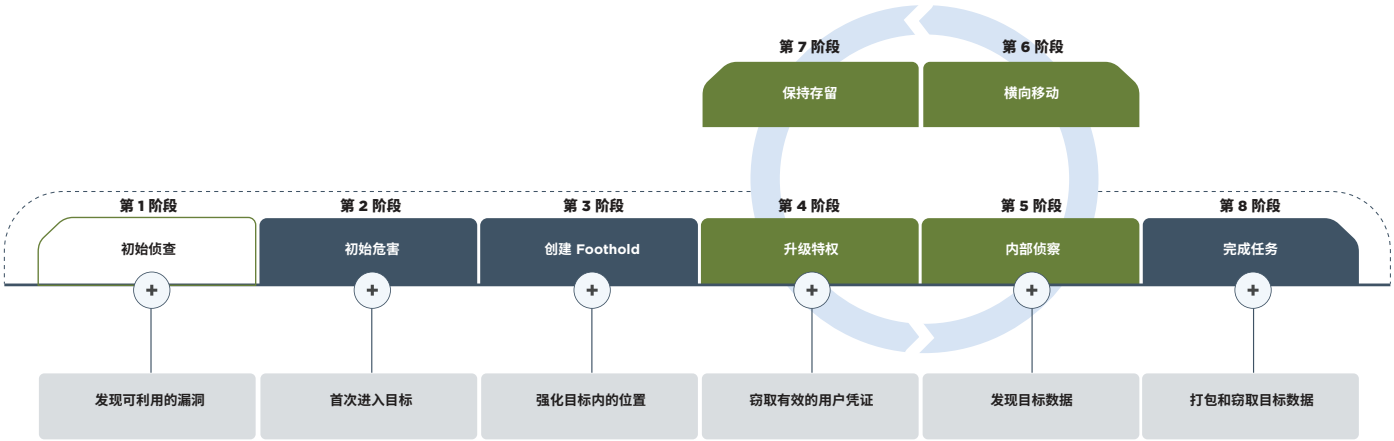

表 2. SmartVision Edition 规格，按硬件型号。

型号	SV-2500-HW	SV-5500-HW	SV-6500-HW
传感器模式性能**	最大 500 Mbps	最大 10 Gbps	最大 15 Gbps
集成或混合模式性能**	最大 200 Mbps	最大 5 Gbps	最大 10 Gbps
网络监控端口	4x 10/100/1000 BASE-T 端口	8x 10GigE SFP+4x 1GigE 旁路	8x 1GigE/10GigE SFP+ 2x 40GigE QSFP+
管理端口	2x 10/100/1000 BASE-T 端口（位于前面板）	2x 10/100/1000 Base-T 端口	4x 1000 BaseT 端口
存储容量	单个 1TB 3.5 英寸、SATA HDD、内置、固定	2 x 4TB HDD、3.5英寸、SAS3、7.2krpm、FRU RAID1	“2x 10TB HDD、3.5英寸、SAS3、7.2krpm、FRU RAID1”
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 英寸（437 毫米）x 19.7 英寸（500 毫米）x 1.7 英寸（43.2 毫米）	17.24 英寸（438 毫米）x 24.41 英寸（620 毫米）x 3.48 英寸（88.4 毫米）	17.24 英寸（438 毫米）x 24.41 英寸（620 毫米）x 3.48 英寸（88.4 毫米）
AC 电源	单个 250 瓦特、90-264 VAC、3.5-1.5 A、50-60 Hz、IEC60320-C14、输入、内置、固定	冗余 (1+1) 800 瓦特、100- 240 VAC 10.5 - 4.0A、50-60 Hz IEC60320-C14 输入、FRU	冗余 (1+1) 800 瓦特、100- 240 VAC 10.5 - 4.0A、50-60 Hz IEC60320-C14 输入、FRU
最大功耗	85 瓦特	658 瓦特	660 瓦特
仅设备/装船重量，磅 (kg)	16.2 磅（7.3 千克）28.2 磅（2.95 千克）	42.7 磅（19.2 千克）63.8 磅（29.0 千克）	44 磅（20 千克）71 磅（32.2 千克）
运行温度	0°- 40°C 32°-104°F	0-35°C 32-95°F	10°C 到 35°C，保险起见，以 0°C 到 40°C 进行测试
非运行温度	-20-80°C -4-176°F	-40-70°C -40-158°F	-30-70°C -22-158° F
支持元数据协议	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

表 3. SmartVision Edition 传感器规格，按虚拟型号。

型号	2550v	6500v
性能**	最大 500 Mbps	最大 2 Gbps
网络监控端口	1-8	1-8
管理端口	1 或 2	1 或 2
CPU 核心	6 个	16 个
内存	16 GB	64 GB
驱动器容量	384 GB	512 GB
支持的监控程序	VMWare ESXi 6.0 或更高	VMWare ESXi 6.0 或更高
支持元数据协议	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS	FTP, HTTP, IMAC, IRC, POP3, RDP, RTSP, SMB, SMB 2, SMTP, SSH, TLS

* Cloud MVX 旨在确保已知和未知威胁的简单、实时监测和引爆。与通用的云端沙箱不同，Cloud MVX 并不仅是简单地分析文件类型和对象，而是重放网络流量，以识别跨越多个网络流的攻击。

** 性能数据将根据各个网络条件而有所不同。

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

FireEye, Inc.
26/F Times Square, 93 Middle Huaihai,
Huangpu Shanghai, 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。