FireEye 网络威胁防护

为中大型组织有效防护网络入侵

概要

FireEye Network Security 是一种有效的网络威胁防护解决方案，通过准确检测并立即阻止隐藏在网络流量中的高级、有针对性和其他规避性攻击，帮助组织最大限度地降低代价高昂的违规风险。它可以在数分钟内通过确凿的证据、可执行的情报和响应工作流集成来实施有效的解决方案。无论是利用 Microsoft Windows、Apple OS X 操作系统，还是应用程序漏洞；无论是针对总部还是分支机构，或者是隐藏在的大量入站互联网流量中，需要实时检测的威胁，借助 FireEye 网络威胁防护，组织都可以有效地抵御。

FireEye 网络安全的核心是 Multi-Vector Virtual Execution™ (MVX，多向量虚拟执行) 以及动态机器学习和人工智能 (AI) 技术。

MVX 是一种无签名的动态分析引擎，可检查可疑网络流量以识别逃避传统基于签名和基于策略的防御的攻击。它们是多向量机器学习、人工智能和关联上下文动态规则引擎的集合，这些引擎基于最新的机器攻击者和受害者情报，实时和追溯地检测和阻止恶意活动。FireEye 网络威胁防护还包含入侵防御系统 (IPS) 技术，可使用传统特征码匹配来检测常见攻击。

FireEye 网络威胁防护设备有多种外形尺寸、部署方式和性能可供选择。 它通常部署在下一代防火墙、IPS 和安全网关 (SWG) 等传统检测互联网流量的安全设备后面。FireEye 网络威胁防护可快速检测已知和未知攻击，拥有极高的准确性和极低的误报率，让各个警报都能得到有效回应，为传统安全解决方案提供补充支持。

图 1　典型部署 — 网络安全解决方案

性能	优势
检测	
准确检测高级、有针对性和其他规避性网络攻击	将代价高昂的网络入侵风险降至最低
模块化和可扩展的安全架构	提供投资保护并支持业务增长
为多操作系统环境和所有互联网接入点提供相同的保护	在整个组织内为所有类型的设备打造一道强大的防线
集成、分布式、物理机、虚拟机、本地和云多方式部署	提供符合组织偏好和资源的灵活性
与电子邮件和内容安全进行多向量联动	在更广泛的攻击面提供可见性
防御	
以 250 Mbps 至 10 Gbps 线速实时阻止攻击	提供针对逃逸攻击的实时保护
加密流量检测	设备内置 TLS 1.3 解密，不需要额外购买许可
响应	
低误报率，风险软件分类和IPS警报自动验证	降低误报率，节省运营成本
深入调查、警报验证、终端管控以及事件响应	自动化和简化安全工作流程
有效的证据和可执行的威胁情报	针对检测出的安全事件，加速优先化并提出解决方案

技术优势

准确的威胁检测和可执行的建议

FireEye 网络威胁防护使用多重分析技术来检测攻击，具有很高的准确性和较低的误报率：

- **Multi-Vector Virtual Execution™ (MVX) 引擎**在安全的虚拟环境中，通过动态、无签名分析检测零日攻击，多流攻击和其他规避攻击。它可识别前所未有的漏洞和恶意软件，从而阻止网络攻击杀伤链进入感染和损害阶段。

- **多向量机器学习、人工智能和关联引擎**通过从数千小时的事件响应中收集到的实时洞察经验，通过上下文、基于规则的分析来检测和阻止模糊的、有针对性的和其他定制化的攻击。它通过识别恶意入侵、恶意软件、网络钓鱼攻击和命令和控制 (CnC) 回呼，来阻止网络攻击杀伤链进入感染、损害和入侵阶段。它还可以提取可疑网络流量，并将其提交给 MVX 引擎，进行最终判断分析。
  除了终端和服务器流量检测，还同时支持网络横向和垂直流量的检测。

- FireEye 网络威胁防护生成的警报包括具体的实时证据，可快速响应，优先处理和遏制最新出现的，针对性的攻击。

即时和弹性保护

FireEye 网络威胁防护提供灵活的部署模式：

- 通过 TAP/SPAN 旁路镜像，在线镜像或在线拦截。在线拦截模式可自动阻止入站漏洞利用和恶意软件以及出站多协议回呼。 旁路镜像模式下，会生成警报并由组织决定如何响应它们。 在线拦截模式下，FireEye网络威胁防护会对 TCP 或 HTTP 连接进行重定向。

- 部分型号提供主动高可用性 (HA) 选项，以在网络或设备出现故障时提供备份。

覆盖广泛的攻击面

FireEye 网络威胁防护为如今多样的网络环境提供持续防护:

- 支持最常见的 Microsoft Windows 和 Apple Mac OS X 操作系统。
- 能分析包括可移植可执行文件 (PE)、活动 Web 内容、档案、图像、Java、Microsoft 和 Adobe 应用程序以及多媒体在内的 160 多种不同类型文件。
- 能对数千个操作系统、补丁包、物联网应用程序类型和版本组合进行可疑流量分析。
- 能防御无法通过签名检测的高级攻击和恶意软件，包括：Web Shell 上传、现有 Web Shell、勒索软件、加密挖矿等。

验证并列出需要优先处理的告警

除了检测真实的攻击以外，FireEye MVX 技术也可用来判定通过常规特征码相配方式检测出的警报的可靠性，然后识别并优先处理重要的威胁：

- 配备 MVX 引擎验证的入侵防御系统 (IPS)，可减少对基于特征码的检测（通常无法辨别误报）分类时所需的时间。
- 风险软件分类可将真实的漏洞攻击与不受欢迎、但恶意性不高的活动（比如，广告软件和间谍软件）明确区分开来，从而对警报响应进行优化顺序排定。

回应工作流程整合

FireEye 网络威胁防护可以通过多种方式增强防护，从而实现警报响应工作流的自动化：

- **FireEye 集中管理**将来自 FireEye 网络威胁防护的警报，和来自 FireEye 邮件威胁防护的警报进行联动，从而更广泛地了解攻击并设定阻止规则，以防攻击进一步扩散。
- **FireEye 网络取证**与 FireEye 网络威胁防护整合，可以提供与警报关联的详细抓包，实现深入的调查。
- **FireEye 端点安全**可识别、验证并遏制 FireEye 网络威胁防护所检测出的入侵，从而简化受影响端点的管控和修复。

灵活的部署

FireEye 网络威胁防护提供多种部署选项，以相配组织的需求和预算：

- **集成式网络威胁防护：**配备集成 MVX 的，独立、一体化硬件设备，从而在单个站点确保互联网接入点的安全。FireEye 网络威胁防护是一个易于管理的无客户端平台，可以在 60分钟内完成部署。它不需要规则、策略或调试。
- **分布式网络威胁防护：**配备集中共享 MVX 服务的可扩展设备，从而在组织内确保互联网接入点的安全。
  - **网络智能节点：**可通过物理或虚拟设备分析网络流量，以检测和阻止恶意流量，并通过加密连接向 MVX 提交可疑活动，进行最后的判断分析。
  - **MVX 智能系统网络：**本地部署、集中定位、弹性 MVX 服务，可提供透明的可扩展性、内置式 N+1 容错以及自动负载均衡。
  - **FireEye 云 MVX：**FireEye 托管的 MVX 服务订阅，可通过网络智能节点上的网络流量分析来确保隐私安全。仅可疑对象会通过加密连接发送到 MVX 服务，判断为无害代码后会被排除。
  - **本地或云端部署保护：**除了独立物理和虚拟设备外，FireEye 还在提供公共云部署方式，在 Amazon 和 Azure 中均可用。

图 2 集成式网络威胁防护的展示。
包括 NX 2550、NX 3500、NX 5500、NX 6500

图 3

分布式部署模式

图 4

FireEye 网络威胁防护的模块化组件

高性能和可扩展性

FireEye 网络威胁防护以接入互联网带宽为主要参数，为不同大小的分支机构和总部提供各种性能选择：

MVX 智能系统和 FireEye 云 MVX 可扩展架构使 MVX 服务得以支持单个到数千个网络智能节点，在需要时可进行无缝扩展。

部署方式	性能
集成式（物理机单机模式）	50 Mbps to 5 Gbps
物理机智能节点模式	50 Mbps to 10 Gbps
虚机和公有云智能节点模式	50 Mbps to 8 Gbps

业务优势

FireEye 网络威胁防护的设计可满足单站点和分布式多站点组织的需求，具有多种优势：

将网络漏洞的风险降至最低

FireEye 网络威胁防护是一款高效的网络防御解决方案，它可以：

- 通过阻止高级的、有针对性的和其他规避攻击，防止入侵者闯入组织窃取有价值的资产或破坏业务
- 通过具体的证据、可操作的情报、内联阻止和响应工作流自动化，更快地阻止攻击并拦截入侵
- 消除组织网络防御的弱点，能为各种操作系统、应用程序类型、分支机构和中心站点提供保护

缩短投资回报周期

根据 Forrester Consulting[1]的一项研究，FireEye 网络威胁防护客户可以在 3 年内实现 152% 的投资回报率 (ROI)，并在 9.7 个月内回本。FireEye 网络威胁防护：

- 将安全团队资源集中在真正的攻击上，以减少运营费用
- 通过共享的 MVX 服务，以及可调整为最理想部署规模的各种效能点，达成最理想的成本支出
- 当分支机构数量或互联网流量增长时，可以按需进行平滑扩展，确保信息安全投资永不过时
- 通过允许从集成部署到分布式部署的无成本迁移，保护现有投资
- 通过模块化和可扩展的架构减少未来的资本支出

1 Forrester (May 2016). The Total Economic Impact of FireEye.

荣誉和认证

FireEye 网路安全的产品组合已获得多项行业和政府奖项：

- 2020年，FireEye在海军信息战系统司令部（NAVWAR）人工智能网络安全挑战赛中获得第一名[2]
- 2020年，KuppingerCole 授予 FireEye 网络检测和响应领导者[3]
- 2020年，Forrester 认可 FireEye 为网络分析和可视化的大型供应商[4]
- 2018 年，Frost & Sullivan 认定 FireEye 为当之无愧的市场领军企业，其市场份额占到 46%，超过了随后 10 位竞争对手的总市场份额[5]
- FireEye 网络威胁防护拥有 Common Criteria、FIPS 140-2 和 SOC 等认证
- FireEye 网络威胁防护已获得 SANS 机构、SC 杂志、CRN 以及其它机构颁发的各种奖项
- FireEye 网络威胁防护是市面上第一个获得美国国土安全部安全法案认证的安全解决方案

2 FireEye (January 6, 2021). Naval Information Warfare Systems Command (NAVWAR) Awards FireEye First Place in Network Threat Detection Challenge.
3 KuppingerCole (June 10, 2020). Leadership Compass Network Detection and Response.
4 Forrester (June 23, 2020) Now Tech: Network Analysis and Visibility, Q2 2020.
5 Frost & Sullivan (July 5, 2018) Advanced Malware Sandbox (AMS) Solutions Market, Global, Forecast to 2022.

表 1. FireEye 网络威胁防护的规格、集成设备

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
支持的操作系统	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
性能 *	最大 50 Mbps 或 100 Mbps	最大 250 Mbps	最大 500 Mbps	最大 1 Gbps	最大 2.5 Gbps	最大 5 Gbps
网络监控端口	4x 10/100/1000 BASE-T 端口（位于前面板）	4x 10GigE SFP+ 4x 1GigE 旁路	4x 10GigE SFP+ 4x 1GigE 旁路	8x 10GigE SFP+ 4x 1GigE 旁路	8x 10GigE SFP+ 4x 1GigE 旁路	8x 1GigE/10GigE SFP+ 2x 40GigE QSFP+
运行的网络端口模式	内联监控器、故障开型、故障关型（HW 旁路）或 TAP/SPAN	内联监控器、故障开型、故障关型（HW 旁路）或 TAP/SPAN	内联监控器、故障开型、故障关型（HW 旁路）或 TAP/SPAN	内联监控器、故障开型、故障关型（HW 旁路）或 TAP/SPAN	内联监控器、故障开型、故障关型（HW 旁路）或 TAP/SPAN	内联、监控器或 TAP/SPAN
高可靠性 (HA)	不适用	不适用	不适用	不适用	不适用	不适用
高可靠性 (HA) 端口 (后面板)	不适用	不适用	不适用	不适用	2x 100/1000/10G Base-T 端口	不适用
管理端口 (后面板)	2x 10/100/1000 BASE-T 端口（位于前面板）	2x 10/100/1000 BASE-T 端口	2x 10/100/1000 BASE-T 端口	2x 10/100/1000 BASE-T 端口	2x 10/100/1000 BASE-T 端口	4x 1000 基本端口
IPMI 端口 (后面板)	包含	包含	包含	包含	包含	包含
前 LCD 和键盘	不适用	不适用	不适用	不适用	不适用	不适用
VGA 端口	无	有	有	有	有	有
USB 端口	2x 类型 A USB 端口 (前面板)	4x 类型 A USB 端口 前方 2 个、后方 2 个	4x 类型 A USB 端口 前方 2 个、后方 2 个	4x 类型 A USB 端口 前方 2 个、后方 2 个	4x 类型 A USB 端口 前方 2 个、后方 2 个	2x 类型 3 USB 端口
串行端口 (后面板)	115,200 bps、无校验、8 比特、1 停止位 (RJ45 连接器； RJ45-to-Dsub 转接头的线缆包含在内)	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	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
驱动器容量	单个 1TB 3.5 英寸、SATA HDD、内置、固定	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
外接盒	1RU，适合 19 英寸机架	1RU，适合 19 英寸机架	2RU，适合 19 英寸机架	2RU，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)	17.2 英寸 (437 毫米) x 25.6 英寸 (650 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)	17.24 英寸 (438 毫米) x 24.41 英寸 (620 毫米) x 3.48 英寸 (88.4 毫米)	17.2 英寸 (437 毫米) x 31.0 英寸 (787 毫米) x 3.5 英寸 (89 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) 750 瓦特、 100 - 240 V AC 9.0 – 4.5A、50-60 Hz IEC60320-C14 输入、FRU	冗余 (1+1) 800 瓦特、 100 - 240 V AC 10.5 – 4.0A、50-60 Hz IEC60320-C14 输入、FRU	冗余 (1+1) 800 瓦特、 100 - 240 V AC 10.5 – 4.0A、50-60 Hz IEC60320-C14 输入、FRU	冗余 (1+1) 800 瓦特、 100 - 240 V AC 10.5 – 4.0A、50-60 Hz IEC60320-C14 输入、FRU	冗余 (1+1) 1000 瓦特、 100 - 240 VAC 10.5 – 4.0A、50-60 Hz IEC60320-C14 输入、FRU

表 1. FireEye 网络威胁防护的规格、集成设备（续）

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
最大功耗 (瓦特)	85 瓦特	265 瓦特	426 瓦特	519 瓦特	658 瓦特	660 瓦特
最大散热量 (BTU/h)	290 BTU/h	904 BTU/h	1,454 BTU/h	1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
平均无故障工作时间 (小时)	56,400 小时	54,200 小时	65,466 小时	57,766 小时	52,802 小时	54,041 小时
仅设备/发货重量 磅 (kg)	16.2 磅 (7.3 kg)/ 28.2 磅 (12.79 kg)	29.8 磅 (13.5 Kg)/ 40.8 磅 (18.5 Kg)	37.4 磅 (17.0 Kg)/ 58.6 磅 (26.6 Kg)	42.4 磅 (19.2 Kg)/ 63.5 磅 (28.8 Kg)	42.7 磅 (19.2 Kg)/ 63.8 磅 (29.0 Kg)	44 磅 (20 kgs) 71 磅 (32.2Kg)
安全合规性	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
安全认证	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP vw1.1
EMC 合规性	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	安全: EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC: FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
环境合规性	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS、 REACH、 WEEE 冲突矿产
运行温度	0 - 40 °C 32 - 104 °F	0 - 35 °C 32 - 95 °F	0 - 35 °C 32 - 95 °F	0 - 35 °C 32 - 95 °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	-40 - 70 °C -40 - 158 °F	-40 - 70 °C -40 - 158 °F	-40 - 70 °C -40 - 158 °F	-30 - 70°C -22 - 158°F
运行相对湿度	5% - 85% 无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10% - 90% @ 40 °C、无结露
非运行相对湿度	5% - 95% 无结露	10 - 95% @ 60 °C、无结露	10 - 95% @ 60 °C、无结露	10 - 95% @ 60 °C、无结露	10 - 95% @ 60 °C、无结露	10% - 95%@55°C 无结露
运行海拔高度	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺

表 2. FireEye 网络威胁防护的 IPS 性能、集成设备

	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
最大 IPS 性能	最大 50 Mbps 或 100 Mbps	最大 250 Mbps	最大 500 Mbps	最大 1 Gbps	最大 2.5 Gbps	最大 5 Gbps
最大并发连接数	15K 或 80K	80K	160K	500K	1M	2M
每秒 新连接数	750/秒或 4K/秒	4K/秒	8K/秒	10K/秒	20K/秒	40K/秒

表 3. FireEye 网络威胁防护智能节点、物理规格

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
支持的操作系统	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
性能	最大 50 Mbps	最大 100 Mbps 或 250 Mbps	最大 500 Mbps	最大 1 Gbps	最大 2 Gbps	最大 5 Gbps	最大 10 Gbps
网络监控端口	4x 10/100/1000 BASE-T 端口	4x 10/100/1000 BASE-T 端口 (位于前面板)	4x 10GigE SFP+ 4x 1GigE 旁路	4x 10GigE SFP+ 4x 1GigE 旁路	8x 10GigE SFP+ 4x 1GigE 旁路	8x 10GigE SFP+ 4x 1GigE 旁路	8x 1GigE/10GigE SFP+ 2x 40GigE QSFP+
运行的网络端口模式	内联监控器、故障关型或 Tap	内联监控器、故障开型、故障关型 (HW 旁路) 或 TAP/SPAN	内联监控器、故障开型、故障关型 (HW 旁路) 或 TAP/SPAN	内联监控器、故障开型、故障关型 (HW 旁路) 或 TAP/SPAN	内联监控器、故障开型、故障关型 (HW 旁路) 或 TAP/SPAN	内联监控器、故障开型、故障关型 (HW 旁路) 或 TAP/SPAN	内联、监控器或 TAP/SPAN
高可靠性 (HA)	不适用	不适用	不适用	不适用	不适用	不适用	不适用
高可靠性 (HA) 端口 (后面板)	不适用	不适用	不适用	不适用	不适用	不适用	不适用
管理端口 (后面板)	2x 10/100/1000 BASE-T 端口	4x 10/100/1000 BASE-T 端口 (位于前面板)	2x 10/100/1000 BASE-T 端口	2x 10/100/1000 BASE-T 端口	2x 10/100/1000 BASE-T 端口	2x 10/100/1000 BASE-T 端口	4x 1000 BaseT 端口
IPMI 端口 (后面板)	不适用	后面板	包含	包含	包含	包含	包含
前 LCD 和键盘	不适用	不适用	不适用	不适用	不适用	不适用	不适用
VGA 端口	不适用	不适用	有	有	有	有	有
USB 端口	2x 类型 A USB 端口	2x 类型 A USB 端口 (前面板)	4x 类型 A USB 端口 前方 2 个、后方 2 个	4x 类型 A USB 端口 前方 2 个、后方 2 个	4x 类型 A USB 端口 前方 2 个、后方 2 个	4x 类型 A USB 端口 前方 2 个、后方 2 个	2x 类型 3 USB 端口

表 3. FireEye 网络威胁防护智能节点、物理规格（续）

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
串行端口（后面板）	115,200 bps、无校验、8 比特、1 停止位（RJ45 连接器； RJ45-to-Dsub 转接头的线缆包含在内）	115,200 bps、无校验、8 比特、1 停止位（RJ45 连接器； RJ45-to-Dsub 转接头的线缆包含在内）	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	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
驱动器容量	单个 500GB 2.5 英寸 SATA HDD、内置、固定	单个 1TB 3.5 英寸 SATA HDD、内置、固定	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2 x 4TB HDD、3.5"、SAS3、7.2krpm、FRU RAID1	2x 10TB HDD 3.5", SAS3, 7.2krpm FRU RAID1
外接盒	桌面外形尺寸	1RU，适合 19 英寸机架	1RU，适合 19 英寸机架	2RU，适合 19 英寸机架	2RU，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）	11 英寸（280 毫米）x 6.9 英寸（175 毫米）x 1.8 英寸（45.7 毫米）	17.2 英寸（437 毫米）x 19.7 英寸（500 毫米）x 1.7 英寸（43.2 毫米）	17.2 英寸（437 毫米）x 25.6 英寸（650 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）	17.24 英寸（438 毫米）x 24.41 英寸（620 毫米）x 3.48 英寸（88.4 毫米）	17.2 英寸（437 毫米）x 27.9 英寸（709 毫米）x 3.5 英寸（89 毫米）
AC 电源	外置 60 瓦特 12V@5A 输出 AC 适配器、90-264 VAC、50-60 Hz、IEC60320-C14、输入、FRU	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）750 瓦特、100 - 240 VAC 9– 4.5A、50-60 Hz IEC60320-C14 输入、FRU	冗余(1+1) 800 瓦特、100 - 240 VAC 9 – 4.5A、50-60 Hz IEC60320-C14 输入、FRU	冗余(1+1) 800 瓦特、100 - 240 VAC 9 – 4.5A、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	冗余（1+1）1000 瓦特、100 - 240 VAC 10.5 – 4.0A、50-60 Hz IEC60320-C14 输入、FRU
最大功耗（瓦特）	27 瓦特	85 瓦特	265 瓦特	426 瓦特	519 瓦特	658 瓦特	660 瓦特
最大散热量（BTU/h）	92 BTU/h	290 BTU/h	904 BTU/h	1,454 BTU/h	1,771 BTU/h	2,245 BTU/h	2,252 BTU/h
平均无故障工作时间（小时）	95,400 小时	56,400 小时	54,200 小时	65,466 小时	57,766 小时	52,802 小时	54,041 小时
仅设备/发货重量 磅（kg）	3.75 磅（1.7 kg）/ 6.5 磅（2.95 kg）	16.2 磅（7.3 kg)/28.2 磅（12.79 kg）	29.8 磅（13.5 kg)/40.8 磅（18.5 kg）	37.4 磅（17.0 kg)/58.6 磅（26.6 kg）	42.4 磅（19.2 kg)/63.5 磅（28.8 kg）	42.7 磅（19.2 kg)/63.8 磅（29.0 kg）	44 磅（20 kgs）71 磅（32.2Kg）
安全合规性	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2
安全认证	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1	FIPS 140-2 等级 1 CC NDPP v1.1

表 3. FireEye 网络威胁防护智能节点、物理规格（续）

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
EMC 合规性	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	安全：EN 60950; C22.2; UL 60950; IEC 60950; CAN/CSA-C22.2; K 60950; AS/NZS 60950; GB 4943.1; J60950, SI60950 EMC：FCC Part 15 SubPart B Class A; ICES-003; EN55032; VCCI V-3; EN 55024; EN 61000; CNS 13438; CISPR32; KN 32; KN 35
环境合规性	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS、REACH、WEEE 冲突矿产
运行温度	0 - 40 °C 32 - 104 °F	0 - 40 °C 32 - 104 °F	0 - 35 °C 32 - 95 °F	0 - 35 °C 32 - 95 °F	0 - 35 °C 32 - 95 °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	-20 - 80 °C -4 - 176 °F	-40 - 70 °C -40 - 158 °F	-40 - 70 °C -40 - 158 °F	-40 - 70 °C -40 - 158 °F	-40 - 70 °C -40 - 158 °F	-30 - 70ºC -22 - 158ºF
运行相对湿度	5% - 85% 无结露	5% - 85% 无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10 - 95% @ 40 °C、无结露	10% - 90% @ 40 °C、无结露
非运行相对湿度	5% - 95% 无结露	5% - 95% 无结露	10 - 95% @ 60 °C、无结露	10 - 95% @ 60 °C、无结露	10 - 95% @ 60 °C 无结露	10 - 95% @ 60 °C 无结露	10% - 95%@55ºC 无结露
运行海拔高度	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺	3,000 米 9,842 英尺

表 4. FireEye 网络智能节点 IPS、物理规格

	NX 1500	NX 2500	NX 2550	NX 3500	NX 4500	NX 5500	NX 6500
最大 IPS 性能	最大 50 Mbps	最大 100/250 Mbps	最大 500 Mbps	最大 1 Gbps	最大 2 Gbps	最大 5 Gbps	最大 10 Gbps
最大并发连接数	15K	80K	160K	500K	1M	2M	4M
每秒新连接数	750/秒	4K/秒	8K/秒	10K/秒	20K/秒	40K/秒	80K/秒

表 5. FireEye 网络智能节点、虚拟规格

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
支持的操作系统	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
性能 *	最大 50 Mbps	最大 100 Mbps	最大 250 Mbps	最大 500 Mbps	最大 1 Gbps
网络监控端口	1-8	1-8	1-8	1-8	1-8
网络管理端口	1 或 2	1 或 2	1 或 2	1 或 2	1 或 2
运行的网络端口模式	内联、SPAN	内联、SPAN	内联、SPAN	内联、SPAN	内联、SPAN
CPU 核心	3	6	8	8	16
内存	10 GB	16 GB	16 GB	32 GB	32 GB
驱动器容量	384 GB	384 GB	384 GB	512 GB	512 GB
网络适配器	VMXNet 3、vNIC	VMXNet 3、vNIC	VMXNet 3、vNIC	VMXNet 3、vNIC	VMXNet 3、vNIC
支持的 Hypervisor	VMWare ESXi 6.0 或更高	VMWare ESXi 6.0 或更高	VMWare ESXi 6.0 或更高	VMWare ESXi 6.0 或更高	VMWare ESXi 6.0 或更高
安全认证	FIPS 140-2 等级 1 CC NDPP v1.1 （进程）	FIPS 140-2 等级 1 CC NDPP v1.1 （进程）	FIPS 140-2 等级 1 CC NDPP v1.1 （进程）	FIPS 140-2 等级 1 CC NDPP v1.1 （进程）	FIPS 140-2 等级 1 CC NDPP v1.1 （进程）

表 6. FireEye 网络智能节点 IPS、虚拟规格

	VA-NXS 1500	VA-NXS 2500	VA-NXS 2550	VA-NXS 4500	VA-NXS 6500
最大 IPS 性能	最大 50 Mbps	最大 100 Mbps	最大 250 Mbps	最大 500 Mbps	最大 1 Gbps
最大并发连接数	15K	80K	80K	160K	500K
每秒新连接数	750/秒	4K/秒	4K/秒	8K/秒	10K/秒

表 7. FireEye MVX 智能系统网络的规格

	VX 5500	VX 12500
支持的操作系统	Microsoft Windows Mac OS X	Microsoft Windows Mac OS X
性能 *	最大 2 Gbps	最大 14 Gbps
高可靠性 (HA)**	N+1	N+1
管理端口（后面板）	1x 10/100/1000 BASE-T 端口	1x 10/100/1000 BASE-T 端口
群集端口（后面板）	3x 10/100/1000 BASE-T 端口	1x 10/100/1000 Mbps BASE-T 端口、 2x 10 Gbps BASE-T 端口
IPMI 端口（后面板）	包含	包含
前 LCD 和键盘	不适用	包含
VGA 端口	包含	包含
USB 端口（后面板）	4x 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
驱动器容量	2x 2TB 3.5 SAS HDD、RAID 1、热拔插、FRU	2x 2TB 3.5" SAS3 HDD、RAID 1、FRU
外接盒	1RU，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. 2x25.6x1.7 英寸（437 x 650 x 43.2 毫米）	17.2x33.5x3.5 英寸（437 x 851 x 89 毫米）
DC 电源	不适用	不适用
AC 电源	冗余 (1+1) 750 瓦特、100-240 VAC、 8 - 3.8 A、50-60 Hz、IEC60320-C14、输入、 热插拔、FRU	冗余 (1+1) 800W：100-127V、 9.8A-7A 1000W：220-240V、7-5A、50-60Hz、FRU IEC60320-C14 输入、FRU
最大功耗（瓦特）	285 瓦特	760 瓦特
最大散热量 (BTU/h)	972 BTU/h	2594 BTU/h
平均无故障工作时间（小时）	54,200 小时	38,836 小时
仅设备/发货重量 磅 (kg)	33 磅 (15 kg)/48 磅 (21.8 kg)	46 磅 (21 kg)/90 磅 (40.2 kg)
安全认证	FIPS 140-2 等级 1、CC NDPP v1.1（待定）	FIPS 140-2 等级 1、CC NDPP v1.1（待定）
安全合规性	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2	IEC 60950 EN 60950-1 UL 60950 CSA/CAN-C22.2

表 7. FireEye MVX 智能系统网络的规格

	VX 5500	VX 12500
EMC 合规性	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015	FCC Part 15 ICES-003 Class A AS/NZS CISPR 22 CISPR 32 EN 55032 EN 55024 IEC/EN 61000-3-2 IEC/EN 61000-3-3 IEC/EN 61000-4-2 V-2/2015 与 V-3/2015
环境合规性	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU	RoHS 指令 2011/65/EU REACH WEEE 指令 2012/19/EU
运行温度	10 - 35 °C (50 - 95 °F)	0 - 40°C (32 - 104°F)
非运行温度	-40 - 70 °C (-40 - 158 °F)	-30 - 70°C (-22 - 158°F)
运行相对湿度	10% - 85% 无结露	10% - 90% @ 40°C，无结露
非运行相对湿度	5% - 95% 无结露	10% - 95% @ 55°C，无结露
运行海拔高度	3000 米 9842 英尺	3000 米 9842 英尺

表 8. 主动式故障开型交换机的规格

	AFO 10G 交换机
尺寸（宽 x 长 x 高）	6.5 x 14.0 x 1.125 (16.5 x 35.6 x 2.8 厘米)
管理端口	1 X DB9 串行控制台、1 X RJ45 Cat5e 端口 (10/100)
网络端口	1 X Quad LC 连接器
监控端口	2 X XFP 端口
AC 电源输入	100 - 240 VAC、1.0 A、47-63 Hz
运行温度	0 - 40 °C (32 - 104 °F)

*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。
** 附带合理的冗余硬件配置

支持服务

FireEye 提供简易而灵活的支持计划，从而最大限度地为您提升 FireEye 产品及服务的价值。我们提供不同级别的支持服务：白金级、白金优享+级。如果您需要进一步了解 FireEye 支持，请参阅 FireEye 支持服务。

FireEye Network Security is part of FireEye XDR
了解更多信息，请访问 **www.FireEye.com/XDR**

Cyberworld
广州科明大同科技有限公司
FIREEYE
中国区总代理
官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

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

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

© 2019 FireEye, Inc. 保留所有权利。FireEye 是 FireEye, Inc. 的注册商标。其它所有品牌、产品或服务名称是或可能是各个所有者的商标或服务标记。
NS-EXT-DS-ZH-CN-000048-06