

# FireEye 网络威胁防护

## 为中型组织有效防护网络漏洞

### 概要

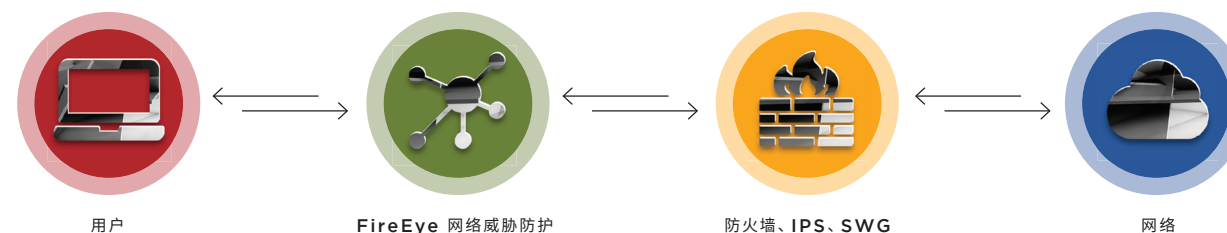
FireEye 网络威胁防护是一款高效的网络威胁防护解决方案，可准确地检测，并立即阻止先进针对性攻击，以及其它隐藏于网络流量中的逃避性攻击，从而帮助组织大幅度降低漏洞所带来的高成本风险。针对已检测出的安全事件，它可以在数分钟内通过确凿的证据、可行动情报以及响应工作流集成来实施有效的解决方案。无论威胁是入侵 Microsoft Windows、Apple OS X 操作系统漏洞，还是应用程序漏洞；无论是直接指向总部或分支机构；或者是隐藏于大规模的入站互联网流量内，并需要进行实时检查，FireEye 网络威胁防护都可以让组织有效防御这些威胁。

FireEye 网络威胁防护的核心是 Multi-Vector Virtual Execution™ (MVX, 多向量虚拟执行) 和情报驱动分析 (IDA) 技术。MVX 是一款无特征码、动态分析引擎，可以检查可疑的网络流量，从而识别可躲避基于特

征码和策略的传统型防御攻击。IDA 是一系列情境型动态规则引擎，可根据最新的机器、攻击者以及受害者情报来实时、追溯性地检测和阻止恶意活动。FireEye 网络威胁防护还包含入侵预防系统 (IPS) 技术，以利用传统特征码相配来检测常见的攻击。

FireEye 网络威胁防护提供各种外形尺寸、部署以及性能选项。它通常位于新生代防火墙、IPS、网络安全网关 (SWG) 等传统网络安全设备后方的互联网流量路径中。FireEye 网络威胁防护可快速地检测已知和未知攻击，拥有很高的准确性和较低的误报率，同时促进对各个警报的有效回应，从而为这些解决方案提供补充支持。

图 1. 典型配置 — 网络安全解决方案。



性能	优势
检测	
准确检测先进针对性攻击以及其它躲避性网络攻击	将代价高昂的网络漏洞风险降至最低
可扩展、模块化的安全架构	提供投资保护
为多操作系统的环境以及所有互联网接入点提供始终如一的防护	为整个组织内所有类型的设备打造一道强大的防线
集成、分布式、实体、虚拟、本地以及云部署选项	提供符合组织偏好和资源的灵活性
与邮件以及内容安全进行多向量关联	在更广泛的攻击面提供可视性
防御	
以 10 Mbps 到 8 Gbps 的线路速率立即阻止攻击	实时防范躲避性攻击
响应	
较低的误报率、风险软件分类以及 IPS 警报自动验证	降低分类不可靠警报所需的运营成本
深入调查、警报验证、端点管控以及事件响应	自动化和简化安全工作流程
凭借情境洞察处理证据和可行动的威胁情报	针对检测出的安全事件，加速优先化并提出解决方案
可从单个站点扩展到数千个站点	支持业务成长

技术优势

准确的威胁检测

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)** 引擎通过动态、无特征码分析在安全、虚拟环境中检测零日攻击、多流攻击以及其它躲避性攻击。它通过识别从未见过的入侵和恶意软件，从而阻止网络攻击杀伤链进入感染和损害阶段。
- **情报驱动分析 (IDA)** 引擎凭借从数百万的 MVX 判定中收集的最前沿、实时洞察以及 Mandiant (一家 FireEye 企业) 和上百位 iSight 威胁研究人员所积累的数千小时的事件响应经验，进行基于规则的情境分析，从而检测并阻止混淆的、针对性攻击以及其它个性化攻击。它通过识别恶意入侵、恶意软件以及指挥与控制 (CnC) 回呼，从而阻止网络攻击杀伤链进入感染、损害以及入侵阶段。它还可以提取可疑的网络流量，并将其提交给 MVX 引擎，以便进行最后的垂直分析。
- **结构化威胁情报 eXpression (STIX)** 使用行业标准格式将自定义的威胁指标添加到 IDA 引擎中，从而允许采取第三方威胁情报。

及时、弹性防护

FireEye 网络威胁防护提供灵活的配置模式，包括：

- 通过 TAP/SPAN 的带外监控、内联监控或内联主动阻止。内联阻止模式可自动阻止入站攻击、恶意软件以及出站多协议回呼。在内联监控模式下，会生成警报，组织需要决定如何应对警报。在带外防御模式下，FireEye 网络威胁防

护 Essentials 会进行 TCP 重置，以带外阻止 TCP、UDP 或 HTTP 的连接。

- 与 FireEye 主动式故障开型 (AFO) 交换机相结合，以确保网络不中断。
- 选择性模式提供一个主动的高可靠性 (HA) 选项，具有应对网络或设备故障的弹性。

广泛的攻击面覆盖

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
- 分析包括可移植执行体 (PE)、网页内容、档案、图像、Java、Microsoft 及 Adobe 应用程序、多媒体在内的 140 多种不同文件
- 针对数千个操作系统、补丁包、应用程序类型和版本处理可疑的网络流量

验证并优先化警报

除了检测真实的攻击意外，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关键威胁：

- 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先化

可行动威胁见解

FireEye 网络威胁防护所生成的警报, 包括确凿的证据和情境情报, 有助于快速应对、优先处理和遏制威胁:

- **动态威胁情报 (DTI):** 具体、实时、全球共享数据, 有助于快速、主动阻止针对性攻击和新发现的攻击
- **高级威胁情报 (ATI):** 有关攻击的情境洞察, 有助于加速响应并提供说明性指导, 以遏制威胁

响应工作流集成

FireEye 网络威胁防护可通过几种方式加以增强, 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关联, 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 网络取证集成了 FireEye 网络威胁防护, 以提供与警报关联的详细抓包, 实现深入的调查
- FireEye 终端安全可识别、验证并遏制 FireEye 网络威胁防护所检测出的损害, 从而简化对受影响端点的管控和修复

灵活的部署选项

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:

- **集成网络威胁防护:** 配备集成 MVX 服务的独立、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:** 分析网络流量的物理或虚拟设备, 有助于检测和阻止恶意流量, 并通过加密连接向 **MVX** 服务提交可疑活动, 以便进行最后的垂直分析
  - **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** 容错以及自动负载平衡
  - **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。仅可疑对象会通过加密连接发送到 **MVX** 服务 (良性对象会被排除)。



图 2. 集成网络威胁防护的范例包括 NX 2550、NX 3500、NX 5500、NX 6500。

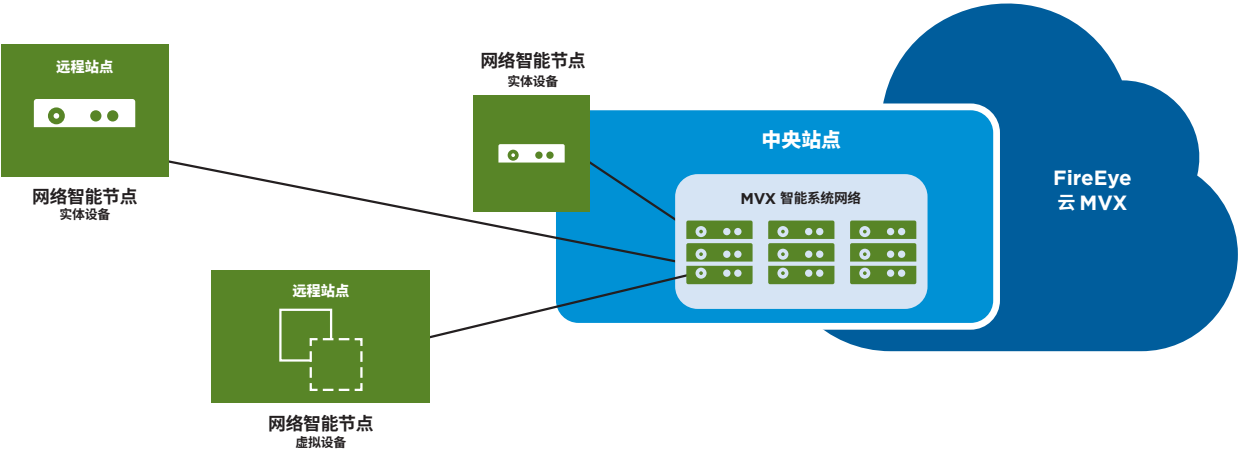


图 3. 针对网络威胁防护的分布式部署模式。



图 4. FireEye 网络威胁防护的模块化组件。

可扩展架构

FireEye 网络智能节点拥有模块化、可扩展的软件架构以及系统设计，从而作为软件模块提供多重威胁防范。

高性能和可扩展性

FireEye 网络威胁防护以线路速率保护互联网接入点，并为不同大小的分支和总部机构提供性能选项：

MVX 智能系统网络和 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，并在需要时进行无缝扩展。

外形尺寸	性能
集成网络威胁防护	50 Mbps 到 5 Gbps
物理网络智能节点	50 Mbps 到 10 Gbps
虚拟网络智能节点	50 Mbps 到 1 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：

- 通过阻止先进针对性攻击和其它躲避性攻击，阻止入侵者闯入组织窃取有价值资产或扰乱业务
- 凭借确凿的证据、可行动情报、内联阻止以及响应工作流程自动化，更快速地阻止攻击和遏制入侵
- 从组织的网络防御中排除弱点，并为各种操作系统、应用程序、分支机构以及中心站点提供始终如一的防护

较短的投资回收期

根据最近的 Forrester 咨询研究<sup>1</sup>，FireEye 网络威胁防护的客户可以在 3 年内实现 152% 的投资回报率 (ROI)，并在 9.7 个月内初步回本。FireEye 网络威胁防护：

- 将安全团队的资源投入到真正的攻击上，以降低运营成本
- 通过共享 MVX 服务优化资本支出，并通过多种性能点合理调整部署的规模，以满足需求

- 当分支机构或网络流量增加时，可顺利进行扩展，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
- 凭借模块化和可扩展建构，可减少未来资本支出

荣誉和认证

FireEye 网络安全的产品组合已获得多项行业和政府奖项：

- 2016 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 56%，超过了随后 10 位竞争对手的总市场份额<sup>2</sup>
- 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



<sup>1</sup> Forrester (2016 年 5 月)。FireEye 的总经济效益。  
<sup>2</sup> Frost & Sullivan (2016 年 10 月)。网络威胁防护沙盒市场分析

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 A 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 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 A USB 端口



表 3. FireEye 网络威胁防护智能节点、物理规格。(继续)

[illegible]



表 3. FireEye 网络威胁防护智能节点、物理规格。（继续）							
	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 ~ 70°C -22 ~ 158°F
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% @ 55°C 无结露
运行高度	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 10 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	4 x 900GB HDD、RAID 10、2.5 英寸、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/装船重量 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)	10 ~ 35 °C (50 ~ 95 °F)
非运行温度	-40 ~ 70 °C (-40 ~ 158 °F)	-40 ~ 70 °C (-40 ~ 158 °F)
运行相对湿度	10% ~ 85% 无结露	10% ~ 85% 无结露
非运行相对湿度	5% ~ 95% 无结露	5% ~ 95% 无结露
运行高度	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

若要了解更多关于 FireEye 的信息，请访问：[www.FireEye.com](http://www.FireEye.com)

#### FireEye, Inc.

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

© 2018 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。  
DS.NX.ZH-CN-082018

#### 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 为弹精竭虑地防备、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。FireEye 在 67 个国家/地区拥有 5,300 多家客户企业，包括福布斯全球 2,000 强中的超过 845 家企业。

#### 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、白金重点+级、政府级以及政府重点+级。如果您需要进一步了解 FireEye 支持，请参阅 FireEye 支持服务。

