数据表

FireEye 邮件安全服务器版本

针对邮件威胁的自适应、智能化、可扩展防护

亮点

- 提供针对恶意附件、凭据 - 网络钓鱼 URL、欺骗、零日和多阶段攻击的全面电子邮件安全
- 支持对 Microsoft Windows 和 Apple Mac OS X 操作系统映像的分析
- 广泛检查邮件中隐藏在密码保护文件、加密附件和 URL 内的威胁
- 从 FireEye DTI Cloud 获取实时威胁情报
- 为警报提供上下文洞察，以便对威胁进行优先级排序并遏制其扩散
- 使用集成或分布式 MVX 服务进行内部部署

图 1. 集成电子邮件安全应用程序，包括 EX 3500、EX 5500 和 EX 8500

概要

邮件是数据量最高的网络入口，因此是最容易受到网络攻击的载体。基于邮件的高级威胁让组织面临越来越多的安全挑战。大多数高级威胁使用电子邮件来传递链接到凭据网络钓鱼站点的 URL 以及武器化文件附件。由于电子邮件具有高度的可定位性和可定制性，因此它成为网络犯罪的主要媒介。

FireEye 邮件安全帮助组织最大程度地降低高成本漏洞风险（由高级邮件攻击引起）。FireEye 邮件安全 - 服务器版本部署在内部，处于行业领先水平，在基于 URL 和附件的攻击进入组织的环境之前，就可以识别、隔离并立即阻止他们。邮件安全采用真实的大数据、可扩展平台，通过结合智能环境和监测插件，区分恶意和良性钓鱼 URL。无特征码 Multi-Vector Virtual Execution™ (MVX) 引擎可针对操作系统、应用程序和网络浏览器的综合性交叉矩阵来分析链接到可下载内容的邮件附件和网址。确定威胁的噪音最小，错误报警几乎不存在。

FireEye 从直接漏洞调查和数百万的传感器中收集大量有关攻击者的威胁情报。邮件安全利用有关攻击和攻击者的真实证据和上下文情报，以便对警报进行优先级排序并实时阻止威胁。

通过整合 FireEye 网络安全和终端安全，组织可实现更高的可视性，从而针对多向量、混合攻击协调实时防护。

防御邮件威胁

凭借在网上可获取的所有个人信息，网络罪犯可以利用网络工程学来引诱几乎任何用户点击网址或者打开附件。

邮件安全可实时检测和抵御凭证盗取、冒充和鱼叉式网络钓鱼攻击，而这些通常可以避开传统的邮件安全防御。如果发现未知和高级威胁隐藏在以下内容中，则会对电子邮件进行分析和隔离（阻止）：

- 附件类型包括但不限于：EXE、DLL、PDF、SWF、DOC/DOCX、XLS/XLSX、PPT/PPTX、JPG、PNG、MP3、MP4 和 ZIP/RAR/TNEF 档案文件
- 密码保护和加密附件
- 密码保护附件，密码通过映像发送
- 邮件内嵌网址、MS Office 文档、PDF 和档案文件（ZIP、ALZip、JAR）以及其他文件类型（Uuencoded、HTML）
- 通过网址 – 甚至 FTP 链接下载的文件
- 混淆式、伪装式、缩短式和动态重定向型网址
- 凭证授权钓鱼诈骗和误植域名网址
- 未知的 Microsoft Windows 和 Apple Mac OS X 操作系统映像、浏览器以及应用程序漏洞
- 鱼叉式网络钓鱼邮件内嵌恶意代码

当恶意软件攻击从邮件开始时，通常需要向控制服务器发送回调指令，以对数据进行加密。邮件安全识别，并阻止难以发现的多级恶意软件活动。

高级威胁检测

邮件安全通过识别和隔离伪装成正常流量的高级、目标性和其他规避性攻击，有助于降低代价高昂的漏洞风险。一旦检测到，这些攻击会立即被阻止、分析和指纹采集，以便更快地识别未来的威胁。

邮件安全的核心是高级 URL 防御、MVX 引擎和 MalwareGuard。这些技术使用机器学习和分析来识别可规避特征码和策略防御的攻击。

作为高级 URL 防御的一个组成部分，PhishVision 是一款映像分类引擎，它使用深度学习来编译和对比可信以及经常受攻击品牌的屏幕截图和电子邮件中 URL 引用的网页。Kraken 与 PhishVision 一起串联工作，它是一种网络钓鱼检测插件，可运用域和页面内容分析来增强机器学习。Skyfeed 是 URL 检测的另一次进化，它是一种专门构建的全自动恶意软件情报收集系统。收集社交媒体帐户、博客、论坛和威胁源以发现误报。高级 URL防御的多方面特性为受到电子邮件安全保护的组织提供功能强大的、针对凭证盗取和鱼叉式网络钓鱼攻击的防御。

MalwareGuard 是一种机器学习实用程序，它将二进制文件作为输入内容，并输出可疑性分数。MalwareGuard 会分析线路上显示的每个可移植可执行文件（PE）文件。根据得分做出决定，并为 MalwareGuard 触发的检测分配名称。

MVX 引擎在安全、虚拟的环境中通过动态、无特征码分析检测零日攻击、多流攻击以及其它隐蔽式攻击。它能识别从未见过的漏洞和恶意软件，以阻止感染和攻击。

规避控制

邮件安全支持受控的实时模式，以防御规避远程对象请求的攻击。MVX 引擎检测需要多次下载的恶意软件，并返回样本二进制文件所请求的远程对象。受控制的实时模式可减少多阶段下载、高级鱼叉式网络钓鱼攻击和高级勒索软件入侵的误报。

攻击者还试图规避用于检测可疑 URL 的技术。作为高级 URL 防御的一部分，针对网络钓鱼站点的规避控制技术也在不断发展。作为高级 URL 防御的一部分，规避控制技术不断得到加强。另一种规避控制技术，可以在潜在的恶意对象被执行时，自定义访客映像，以模拟“已使用”端点。通过确保访客映像再现端点域、域用户、Outlook 数据和浏览器历史记录，可以防止许多规避技术。

集成以提高警报处理效率

邮件安全分析每个附件和网址，以准确地识别现今的高级攻击。整个 FireEye 安全生态系统中的实时更新和针对已知威胁者的警报归因相结合，来提供语境情报，以便对警报进行优先级排序，并对关键警报采取行动，拦截高级邮件攻击。以最小的噪声和误报率识别基于已知、未知和非恶意软件的威胁，将资源投入到真正的攻击上，以降低运营成本。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，从而优先选择警报响应。

快速适应威胁格局的演变

电子邮件安全可帮助您的组织通过 FireEye 动态威胁情报 (DTI) 云的实时威胁情报，不断调整您对电子邮件传播威胁的主动防御。有关威胁和攻击者的深度情报将对抗、机器和受害者情报结合起来，以：

- 针对威胁，提供及时、更高的可视性
- 识别已检测到的恶意软件和恶意附件的具体特性和功能
- 为警报提供上下文洞察，以便进行优先级排序并加速响应
- 确定攻击者的可能身份和动机，并在您的组织内跟踪攻击者的活动
- 重写电子邮件中嵌入的所有 URL，以保护用户免受恶意链接的侵害
- 回溯性地识别交叉式网络钓鱼攻击，并突出恶意网址，以防止访问钓鱼网站

响应工作流集成

邮件安全与 FireEye Helix 和 FireEye Central Management 一起无缝运行。

- 作为安全运行平台中的一个组成部分 — FireEye Helix — 在整个基础架构中提供可视性。FireEye Helix 情报、与终端的关联、自动化以及调查提示来增强邮件和第三方警报。通过这些能力，FireEye Helix 可使看不到的威胁浮出水面，并增强专家决策。
- Central Management 将来自邮件安全和 FireEye 网络安全的警报进行关联，从而对攻击有更全面的了解，并设定拦截规则以防攻击扩散。
- Central Management 支持基于角色的标注，从而知道谁是攻击的对象。
- 根据基于角色的标准，Central Management 支持警报响应和补救。

附加功能

基于 YARA 的规则可实现私人定制

邮件安全可以让分析师指定并测试规则来分析威胁其组织的邮件附件。

管理人员冒充保护

邮件安全 - 服务器版本提供阻止企业电子邮件攻击 (BEC) 的功能，以保护重要员工免受欺骗。制定策略，将入站电子邮件显示名称和已批准的信封发件人所匹配的已批准列表进行对比。

消息队列和警报以及隔离管理

邮件安全 – 服务器版本可高度管理所扫描的邮件消息。对于主动性保护模式的部署，可以跟踪和管理在 MTA 队列中移动的消息。可以利用邮件属性来搜索并验证已被接收、分析和发送到下一跳的消息，而通过直观的仪表盘可以实时监控趋势。显式允许和拦截列表可以定制邮件处理。可以搜索和选择普通警报属性。可以对警报和隔离信息进行批量处理。

主动性防护或仅监控模式

邮件安全可分析邮件，并隔离威胁，以进行主动性防护。关于仅监控模式的部署，组织设定透明的 BCC 规则，将邮件拷贝发送到邮件安全，以进行分析。

灵活的部署选项

邮件安全 – 服务器版本提供多种部署选项，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 邮件安全是一个易于管理的解决方案，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。

  从集成硬件设备到 MVX 智能系统网络的云爆发提供额外的能力，可在信息通量的高峰时期检测和分析邮件威胁。
- **FireEye 云 MVX：**FireEye 托管的 MVX 服务订阅，可通过 Email Smart Node 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）。

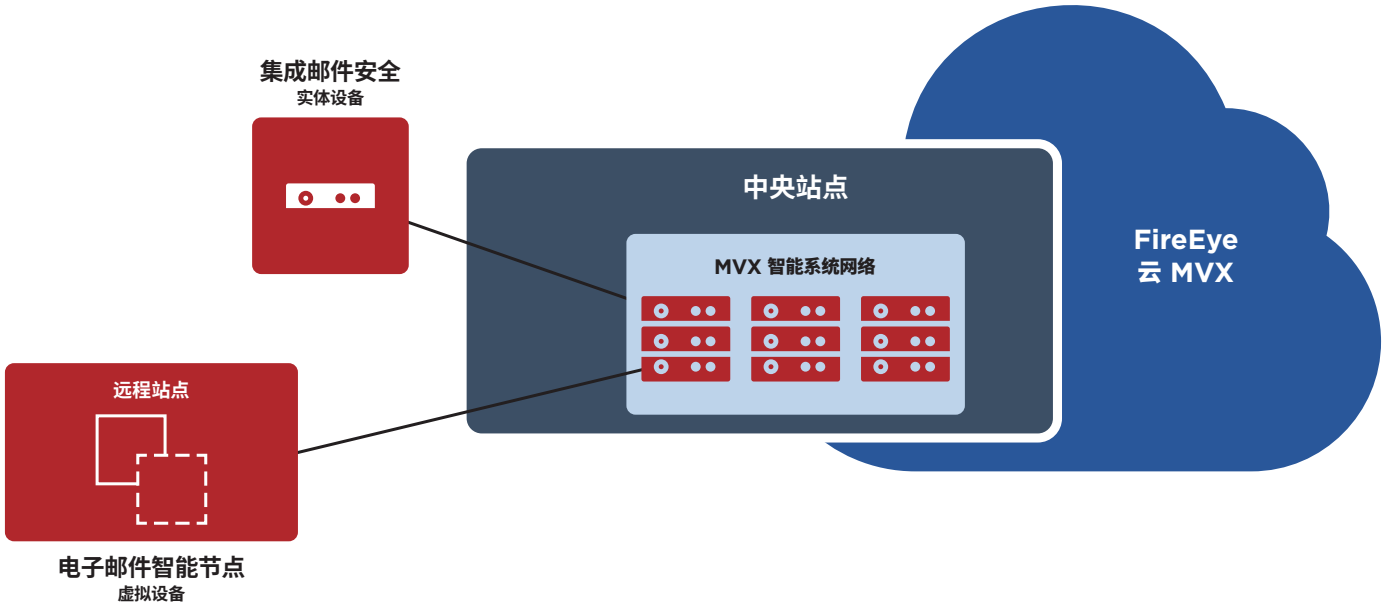

图 2. 邮件安全的分布式和突发部署模式

表 1. 技术规格

	EX 3500	EX 5500	EX 8500
性能*	每小时最多 700 个独特附件	每小时最多 1800 个独特附件	每小时最多 2650 个独特附件
网络接口端口	2x 1GigE BaseT	2x 1GigE BaseT	4x SFP+（支持 10GigE Fiber、10GigE Copper、1GigE Copper）、2x 1GigE BaseT
管理端口	2x 1GigE BaseT	2x 1GigE BaseT	2x 1GigE BaseT
IPMI 监控	包含	包含	包含
VGA 端口（后面板）	包含	包含	包含
USB 端口（后面板）	4x USB 类型 A 后面板	2x USB 类型 A 前面板、 2x USB 类型 A 后面板	2x USB 类型 A 前面板、 2x USB 类型 A 后面板
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 2TB、RAID 10、HDD 3.5 英寸、FRU	4x 2TB、RAID 10、HDD 3.5 英寸、FRU	4x 2TB、RAID 10、HDD 3.5 英寸、FRU
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) 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
DC 电源	不适用	不适用	不适用
最大热功率	245 瓦特（每小时 836 BTU）	456 瓦特（每小时 1556 BTU）	530 瓦特（每小时 1808 BTU）
平均无故障工作时间（小时）	54,200 小时	57,401 小时	53,742 小时
仅设备/发货重量，磅 (kg)	30.0 磅 (13.6 kg)/41.0 磅 (18.6 kg)	44.1 磅 (20.0 kg)/65.3 磅 (29.6 kg)	44.4 磅 (20.2 Kg)/65.6 磅 (29.8 kg)
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
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
安全认证	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1	FIPS 140-2, CC NDPP v1.1
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
运行温度	0 ~ 35 °C (32 ~ 95 °F)	0 ~ 35 °C (32 ~ 95 °F)	0 ~ 35 °C (32 ~ 95 °F)
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	3,000 米/9,842 英尺	3,000 米/9,842 英尺	3,000 米/9,842 英尺

* 根据系统的配置和所处理的邮件流量，所有性能值都会发生变化。根据每小时处理的附件数设计设备的尺寸。

表 2. FireEye MVX 智能系统网络的规格

	VX 5500	VX 12500
支持的操作系统	Microsoft Windows Apple macOS X	Microsoft Windows Apple macOS X
性能*	每小时最多 480 个独特附件	每小时最多 3780 个独特附件
高可靠性**	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 4TB 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	285 瓦特	760 瓦特
最大散热量	每小时 972 BTU	每小时 2594 BTU
MTBF	54,200 小时	38,836 小时
仅设备/发货重量	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	FIPS 140-2 等级 1、CC NDPP v1.1
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

* 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。

表 3. FireEye 邮件安全智能节点、虚拟传感器规范

	EX 5500V
支持的操作系统	Microsoft Windows、Apple macOS X
性能*	每小时最多 1250 个独特附件
网络监控端口	2 个
网络管理端口	2 个
CPU 核心	8 个
内存	16 GB
驱动器容量	384 GB
网络适配器	VMXNet 3、vNIC
支持的 Hypervisor	VMWare ESXi 6.0 或更高

* 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。

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

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