数据表

FireEye 终端威胁防护 (Endpoint Security)

利用实时响应知识阻止攻击

亮点

- 防止大多数针对环境终端的网络攻击
- 检测并阻止已发生的数据外泄，以减少数据外泄的影响
- 通过发现威胁，而不是追踪警报来提高生产力和效率
- 使用单个小型代理，大幅减少对最终用户的影响
- 通过可下载模块提供一定的保护和功能
- 符合规定，如 PCI-DSS 和 HIPAA
- 本地部署或云端部署

传统的终端防护对现代威胁无效；无法处理复杂或高级持续性威胁（advanced persistent threat, APT）攻击。若要保证终端安全，必须采用可快速洞察威胁、并具有最高效响应技术的解决方案。

FireEye 终端威胁防护结合了最佳传统安全产品，强化了 FireEye 技术、专业知识和智能化，以用于防护当今的网络威胁。终端威胁防护根据深度防御模型，采用配备默认引擎和可下载模块的模块化结构，以保护、检测和管理代理。

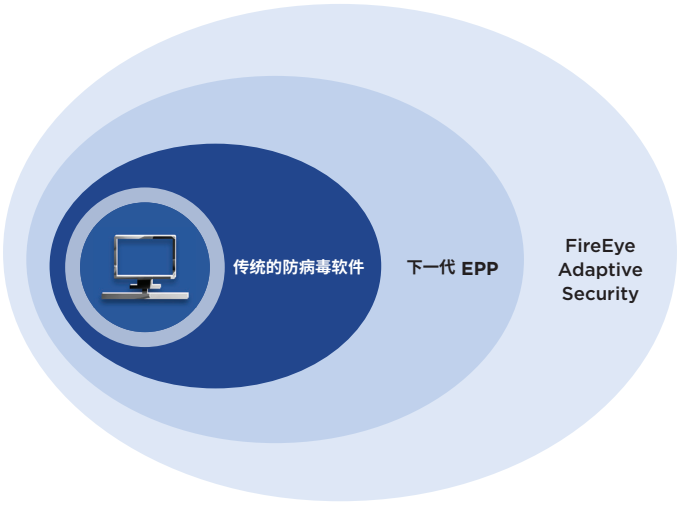
为防止常见恶意软件，终端威胁防护使用基于特征码术的终端保护平台 (endpoint protection platform, EPP) 引擎。为查找尚未存在特征码的威胁，MalwareGuard 使用机器学习功能，以获取来自网络攻击的最新信息。为了应对高级威胁，可以通过基于行为分析的引擎启用终端检测和响应 (endpoint detection and response, EDR) 功能。根据当前实时情报生成的妥协指标 (indicators of compromise, IOC) 引擎有助于发现隐藏的威胁。若要添加新引擎和功能，您可从 FireEye Market 下载模块。

即使有最好的保护，遭受攻击也是不可避免的。为确保实时响应可大幅度减少业务中断，终端威胁防护提供的工具可以：

- 在数分钟内搜索并调查成千上万个终端上的未知及已知威胁
- 识别并详述攻击入侵终端时所使用的向量
- 确定攻击是否已在具体的终端上出现（并持续）
- 建立终端损坏的时间表和持续时间，并跟踪事件
- 清楚识别需要遏制哪些终端和系统以防进一步入侵

IT 是一种战略推动器，可以有效提高我们的教育能力。利用 FireEye 终端威胁防护确保我们的 IT 资产可用、高度运行和安全，这对于实现我们的任务至关重要。

— James D. Perry II
南卡罗来纳大学首席信息安全官



通常，管理层认为任何病毒几乎都是世界末日。通过 FireEye，我们可以了解问题的本质，以及我们能够管理和控制这些问题的证据。快速了解所有这些未知因素，有助于减轻组织中所有人的压力。

— Michael Hennessy, Alpha Grainer Manufacturing, Inc
技术服务总监

主要功能

- 单个代理采用深度防御旨在最大程度减少配置，最大化检测和阻止功能
- 终端威胁防护的单集成工作流程，可分析并响应威胁
- 完全集成的恶意软件防护，附带防病毒 (antivirus, AV) 机器学习、行为分析、攻击指示器 (IOC) 和终端可见性
- Triage Summary 和 Audit Viewer 用于彻底检查和分析威胁

其他功能

- Enterprise Security Search 可快速查找和阐明可疑活动和威胁
- Data Acquisition，以在特定的时间框架内进行详细、深入的终端检查和分析
- 端到端的可见性，允许安全团队快速搜索、识别和发现威胁级别
- 检测和响应功能可快速检测、调查和纳入终端，以加快响应速度
- 易于理解的界面，可快速解释和响应任何可疑的终端活动

支持操作系统和环境	
Windows	Windows 7、8、8.1、10 服务器 2008R2、2012R2、2016、2019
Mac	OS X 10.9+
Linux	RedHat Enterprise Linux 6.8+、7.2+、8 CentOS 6.8+、7.2+、8 Ubuntu 14.04、16.04、18.04 SUSE 11.3、11.4、12.2、12.3、15 Open SUSE 15.1 Amazon AMI 2018.3、AMI2 Oracle Linux 6.10 和 7.6

部署选项： 现场物理设备、现场虚拟设备、FireEye Cloud Service

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。

EP-EXT-DS-US-EN-000018-05