FireEye 终端安全

利用来自一线响应积累的知识经验和情报阻止攻击

亮点

- 防止绝大多数针对终端的网络攻击
- 检测并阻止入侵行为以减少其影响
- 通过发现威胁来提高生产力和效率，而不是利用追踪警报
- 使用单个空间占比较小且单一的终端代理，从而将对最终用户的影响降至最低
- 通过可下载的模块获得额外的保护和功能
- 符合 PCI-DSS 和 HIPAA 等法规要求
- 支持本地或云部署方式

每天都会有新的网络攻击，新的漏洞或新的勒索软件出现。安全团队发现现有的安全解决方案难以对其用户、公司数据和知识产权进行有效保护。安全团队有太多无法协同工作的工具，并且会产生更多的误报，这些误报的数量比有效警报还要多。现有解决方案往往不能对高级威胁提供充分的检测和响应。

FireEye 终端安全通过利用 FireEye 技术、专业知识和智能增强安全产品的最佳组合来防御当今的网络攻击。FireEye 终端安全的模块化架构使用深度防御模型，将默认引擎和可下载模块结合在一起，以保护、检测和响应，并管理终端。

为了防止常见的恶意软件，FireEye 终端安全使用基于特征码的终端保护平台 (EPP) 引擎。MalwareGuard 使用含有来自网络攻击前线知识的机器学习，发现尚不存在特征码的威胁。 对于针对常见软件和浏览器中的漏洞利用的攻击，ExploitGuard 使用行为分析引擎来确定是否正在使用漏洞并阻止它执行。此外，FireEye 不断创建模块来检测攻击技术并加速对新兴威胁的响应。例如，开发了 Process Guard 来阻止凭证泄露。

IT 是一种战略推动力，可以有效提高我们的教育能力。使用 FireEye 终端安全，可确保我们的 IT 资产可用、功能强大且安全，这对于实现我们的使命至关重要。

— James D. Perry II
南卡罗来纳大学首席信息安全官

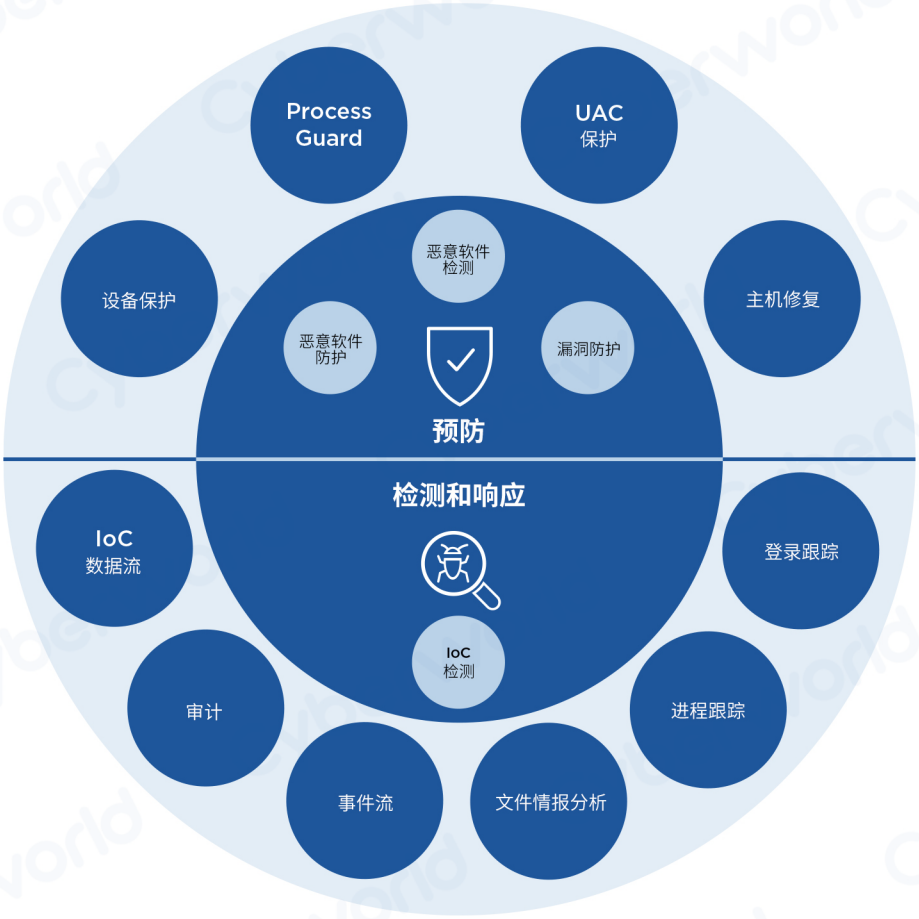
即使有最好的保护，也有可能会被入侵。为了最大限度地减少业务中断造成的影响，FireEye 终端安全包括终端检测和响应 (EDR) 功能，这些功能依赖于在一线响应者的帮助下开发实时危害指标 (IOCs)。 FireEye 还可以做到：

- 在数分钟内搜索和调查数万个终端上的已知和未知威胁
- 能识别并详细分析终端的攻击
- 确定攻击是否在特定终端上发生（并持续存在）及其传播方向
- 创建终端入侵的时间表，确认入侵持续时间并跟踪事件

现代安全威胁往往不会只发生在一个终端上，因此在单个终端上进行事后补救是不能解决大部分入侵导致的问题。FireEye 终端安全能全面修复有问题的终端，同时会指出可能隐藏威胁的所有设备，并进行实时关联。它是 FireEye XDR 的一个组成部分，可以无缝连接所有 FireEye 技术和服务，以检测和响应所有最复杂的威胁。

图 1

FireEye 终端安全核心引擎（中心）和可用模块（外环）



通常，管理层认为任何病毒入侵都几乎是世界末日。
借助 FireEye ，我可以提供真实的证据来展示问题以及我们已经能够管理和控制它。
快速了解所有未知因素，有助于减轻组织中每个人的压力。

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

主要功能

- 使用单一代理深度防御，以最小化配置实现最大化的检测和拦截
- FireEye 终端安全中集成了威胁分析和响应的工作流程
- 包含病毒 (AV) 防护、机器学习、行为分析、危害指标 (IOCs) 和终端可视化功能的恶意软件保护
- FireEye 终端安全作为 XDR 的组件，用于全面修复组织中的所有威胁

其他功能

- Enterprise Security Search 可快速查找和阐明可疑行为和威胁
- Data Acquisition 可在特定时间范围内进行详细的深入终端检查和分析
- 端到端可视化，使安全团队能够快速搜索、识别和辨别威胁级别
- 检测和响应功能，可快速检测、调查和控制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

支持的操作系统和环境	
Windows	Windows 7, 8, 8.1, 10, 11 Server 2008R2, 2012R2, 2016, 2019, 2022
Mac	10.9 - 10.15, 11, 12
Linux	RHEL 6.8 - 6.10, 7.2 - 7.9, 8.0 - 8.3 CentOS 6.8 - 6.10, 7.2 - 7.7, 8.0 SUSE 11 SP3, SP4, 12 SP2 - SP5, 15 GA Open SUSE Leap 15.1, 15.2 Ubuntu 14.04, 16.04, 18.04, 19.04, 20.04 LTS Amazon Linux AMI 2018.3, AM2, Amazon Linux 2 Oracle Linux 6.10, 7.6, 8.1, 8.2

部署选项：本地物理设备、本地虚拟设备、FireEye 云服务

广州科明大同科技有限公司

官方网站 www.cyberworld.com.cn
业务电邮 info@cyberworldchina.com
服务专线 400-9988-792

FireEye, Inc.
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

FireEye Endpoint Security is part of FireEye XDR
Learn more at **www.FireEye.com/XDR**