FIREEYE™

解决方案简述

Managed Defense for Endpoint Security 终端安全托管防御

专家驱动的保护，免受影响性网络攻击

亮点

- **快速威胁阻止：**集成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
- **最先进的威胁情报：**由先进的威胁研究人员利用尖端检测技术支持
- **答案，非警报：**分析师彻底调查关键威胁，提供详细的调查报告，以加快响应速度，从而做出有效响应。
- **Managed Defense 顾问：**安全专家充当您的主要联络点，以方便其他支持，例如恶意软件样本分析、深入的取证分析或现场事件响应。

据报告，2018 年，78% 的组织受到成功的网络攻击的影响。虽然组织需要主动进行有效的网络防御，但大多数组织仍然依赖基于技术的响应性安全解决方案保护其最有价值的资产。

为了更好地配备以抵御网络攻击，您需要一个值得信赖的合作伙伴，通过主动的分析师驱动方法全天候监控您的网络和终端，该方法利用了从前线经验中培养的最新威胁情报。

您需要 FireEye Mandiant 终端安全托管防御。

专家推动的检测和响应

终端安全托管防御具有行业领先的终端安全和托管检测与响应，使企业能够提高企业安全计划的有效性。

终端安全托管防御为托管检测和响应服务，充分利用 FireEye 的全部力量，将 FireEye Mandiant 一线专业知识与业界领先的威胁情报和 FireEye Endpoint Security 相结合。这些功能增强了您的安全团队，可推动检测和调查活动，甚至可以揭示最复杂的攻击者。

Managed Defense 分析师与安全运营中心合作，提供对攻击者活动的深入审查以及自定义的响应建议，提供采取明确行动所需的背景。

工作原理

终端安全托管防御利用 FireEye 终端技术实时查看企业情况，包括 ICS 和云基础架构。

当泄密证据导致调查时，您会立即收到通知，在我们的分析师继续调查该事件时，您可以通过一个安全的门户网站跟踪其状态。

您还将收到详细的摘要报告，该报告提供威胁背景以及补救建议，以形成有效的响应并帮助防止攻击者完成任务。

选定功能

- 产品检测：实时检测引擎、攻击防护
- 分析师检测：Webshells 检测（识别服务器上基于 Web 的后门、上传工具和 Command Shells）
- 终端搜寻和调查数据收集：处理内存列表、注册表配置单元列表、服务列表、端口列表、计划任务、事件日志、Windows 服务、预处理条目
- 通过 Managed Defense 门户一键式阻止

为何选择 FireEye Mandiant

自 2004 年起，FireEye Mandiant 始终走在网络安全防护和网络威胁情报领域的前列。我们的事件响应产品不断用于处置全球最复杂的违规事件。我们可深入了解原有和新兴威胁制造者，及其快速多变的策略、技术及程序。

为何选择 MANAGED DEFENSE

- **经验**
  借鉴 Mandiant 事件响应团队的经验，他们每年花费 200,000 多个小时在最具影响力的漏洞事件上
- **快速检测**
  Managed Defense 调查和响应平均时间为 67 分钟
- **成本效益**
  开发和维护内部功能可能需要大量时间、资金和资源
- **情报**
  访问由 150 多名情报分析师支持的国级情报收集
- **强大的防御**
  融合 FireEye 技术和情报的专有技术堆栈
  - 1.5 亿 FireEye 产品检测
  - 接收 2.2 亿 Managed Defense 警报
  - 17 万分析师调查
  - 快速响应解决 91% 的高优先级威胁
  - 未完全响应事件的情况下解决 98% 的事件响应

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

FireEye
中国上海市黄浦区淮海路东段淮海中路 99 号大上海时代广场 26 楼
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。

MD-EXT-SB-US-EN-000202-02