数据表

FireEye Detection On Demand (FireEye 侦测即服务)

在工作流程中随时扫描威胁

亮点

- 随时检测和阻止已知和未知的恶意软件
- 为浏览器和云端存储部署 FireEye 支持的插件
- 获取已检测到的、JSON 格式恶意软件的背景分析

简介

威胁确实可能来自任何位置，而且每个公司都可根据自身需求、行业和环境，以不同的方式处理威胁防护问题。但是公司都需要由情报支持、成熟的威胁检测能力，且应可执行足够的背景分析。

借助通过 API (Advanced Threat Intelligence) 向 FireEye 客户提供的 FireEye 侦测即服务，组织可以在受保护的状态下提交文件，以确保免受当今的威胁，无论这些威胁是利用 Microsoft Windows、Apple OS X 操作系统还是应用程序漏洞。

FireEye 侦测即服务利用现有的 FireEye Multi-Vector Virtual Execution™ (MVX) 检测引擎和情报驱动分析 (Intelligence Driven Analysis, IDA) 来快速对提交的文件作出裁定。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。

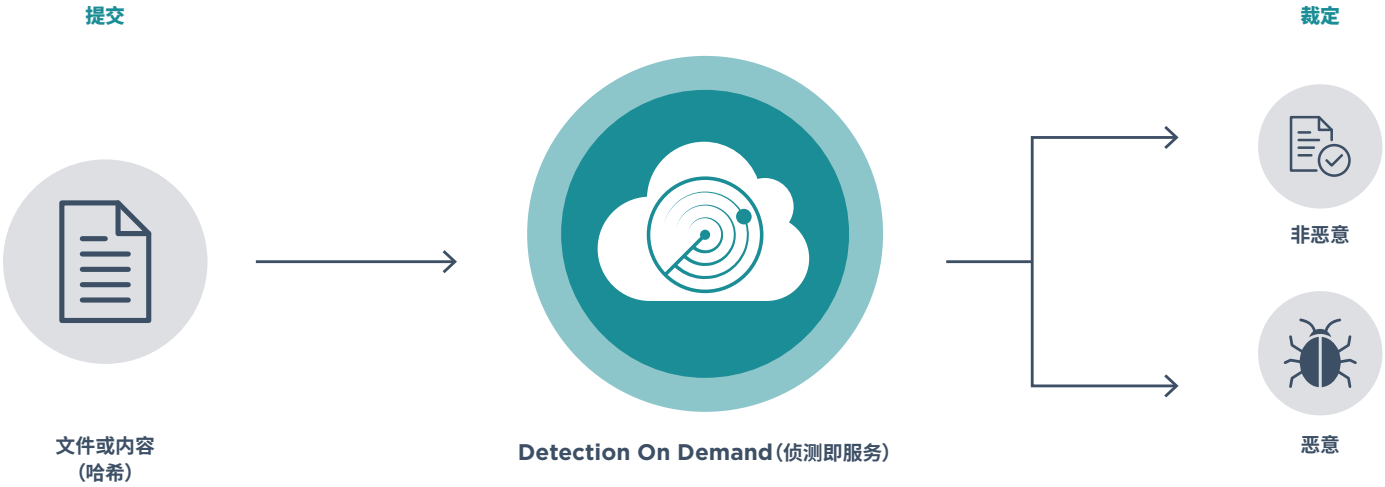
任何威胁防护体系结构中的高级威胁检测

FireEye 侦测即服务是一种云原生威胁检测服务，可快速扫描提交的内容以识别驻留恶意软件。与基于文件完整性算法、内部威胁策略控制或静态检查机制威胁防护解决方案不同，该服务在处理您的提交项时，采用的技术与众多成熟 FireEye 产品相同。

通过 API 可以轻松配置对 FireEye 侦测即服务的访问。其可以集成至您的安全运营中心 (Security Operations Center, SOC) 工作流、SIEM [Security Information and Event Management (安全事件和事件管理)] 分析、数据存储库、客户 Web 应用程序等。本品提供了灵活的文件和内容分析功能，可识别必要的企业恶意行为。

通过侦测即服务，您不仅可以收到对所有已提交文件和内容的裁定，还可收到支持背景详情，如文件、注册表、流程和网络，以及持续更新的 FireEye Dynamic Threat Intelligence (FireEye 动态威胁情报) 的相关查找结果。

侦测即服务的工作原理



FireEye 侦测即服务通过静态分析、人工智能和机器学习，将您的提交项与威胁制造者的最新已知策略和签名进行比较。FireEye 还可确定攻击周期多个阶段的次级或组合效应，以发现前所未有的漏洞和恶意软件。

图 1. 侦测即服务的工作原理。

FireEye Developer Hub（FireEye 开发人员中心）

您可通过 https://fireeye.dev 访问 FireEye Developer Hub（FireEye 开发人员中心），以了解插件和样本代码，并通过侦测即服务与 FireEye 开发社区合作。

购买方式

可通过常规的 FireEye 通道或直接通过 AWS（Amazon Web Services）Marketplace（针对小批量文件的提交）访问侦测即服务。

购买该服务时，您可根据每年预计提交的文件数量，指定您的需求。AWS Marketplace 购买提供按年计费的每月提交配额。文件提交速率限制为 100/分钟。哈希提交速率限制为 200/分钟。

提交给侦测即服务的文件和其他材料可能会分配到大小不同的提交速率；FireEye 会告知您标准提交速率。

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。