数据表

Malware Analysis（恶意软件分析）

以 360 度视角分析攻击

亮点

- 通过 FireEye MVX 引擎，在整个攻击周期内执行深入取证分析
- 简化和批量分析可疑的 Web 代码、可执行文件和其他文件
- 有关文件系统、内存和注册表进行系统级操作系统和应用程序更改的深入报告
- 提供实时模式或沙盒分析，以确认零日攻击
- 通过与 FireEye Central Management 集成，动态生成威胁情报，以立即进行本地保护
- 采集数据包，以允许分析恶意 URL 会话和代码执行
- 包括 FireEye AV-Suite，用于简化事件响应的优先级
- 包括支持 Windows 和 MacOS X 环境

图 1. FireEye 恶意软件分析设备 AX 5550。

概要

FireEye Malware Analysis 是一种取证分析解决方案，便于安全分析师控制强大的自动配置测试环境，以安全执行和检测嵌入在网页页面、电子邮件附件和文件内的高级恶意软件、零日攻击和高级持续威胁 (APT) 攻击。

随着网络罪犯针对特定业务进行渗透攻击，用户帐户、系统或分析师需要易于使用的取证工具，以帮助其快速解决有针对性的恶意活动。

评估操作系统、浏览器和应用程序攻击

Malware Analysis 通过 FireEye Multi-Vector Virtual Execution™ (MVX) 引擎，使内部分析师可 360 度了解攻击，范围从最初利用的回拨目的地，到随后的二进制下载尝试。

通过预配置、仪表化的 Microsoft Windows 和 Apple MacOS X 虚拟分析环境，MVX 引擎完全执行可疑代码，以允许深入检查常见 Web 对象、电子邮件附件和文件。Malware Analysis 通过 MVX 引擎检查单个文件或批量文件内的恶意软件，追踪出站多个协议的连接尝试。

花费时间分析（非管理）

Malware Analysis 使管理员摆脱了费时的设置，基准设置和还原手动恶意软件分析中使用的虚拟机环境。通过内置自定义和精细控制负载爆炸，Malware Analysis 可使取证分析师全面了解攻击，以适用于企业客户的需求。

选择实时分析或沙盒模式

Malware Analysis 为用户提供两种分析模式，即实时分析和沙盒模式。Malware 分析师采用实时、网络模式，以全面进行恶意软件周期分析，以允许外部连接。据此，Malware Analysis 可追踪多个阶段和不同途径的高级攻击。在沙盒模式下，特定恶意软件样本的执行路径已完全包含在虚拟环境中，并且在虚拟环境中可见。

在两种模式下，用户可生成动态和匿名攻击配置文件，该文件可通过 FireEye Central Management 分享至其他 FireEye 解决方案。Malware Analysis 生成的恶意攻击配置文件包括恶意软件代码标识符、利用 URL 以及其他感染和攻击来源。同时还可通过 FireEye Dynamic Threat Intelligence™ (DTI) 分享恶意软件通信协议特点，以动态阻止整个 FireEye 部署组织的数据泄露尝试。

基于 YARA 的规则可实现自定义

Malware Analysis 支持自定义 YARA 规则导入，以指定比特级规则，快速分析可疑对象，以了解组织指定威胁。

全球恶意软件保护网络

Malware Analysis 可通过 Central Management，利用其他 FireEye 解决方案，自动分享恶意软件取证数据，阻止出站数据泄露尝试，并阻止入站已知攻击。来自 Malware Analysis 的威胁数据可通过 FireEye DTI 云端共享，以阻止新出现的攻击。

借助预先配置的 FireEye MVX引擎，无需进行启发式调整，Malware Analysis 可节省管理员的设置时间和配置问题。威胁研究员可通过该解决方案分析高级目标攻击，无需增加网络和安全管理开销。

表 1. 技术规格。

	AX 5550
性能 *	每日最多 8200 次分析
支持的操作系统	Microsoft Windows / Apple Mac OSX
网络接口端口	2x 10/100/1000BASE-T 端口
IPMI 端口（后面板）	包含
键盘	包含
DB15 VGA 端口（后面板）	包含
USB 端口（后面板）	4x 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
驱动器容量	2x 4 TB HDD、RAID 1、3.5 英寸、FRU
外接盒	1RU，适合 19 英寸机架
机箱尺寸（宽 x 长 x 高）	17.2 英寸（437 毫米）x 25.6 英寸（650 毫米）x 1.7 英寸（43.2 毫米）
DC 电源	不适用
AC 电源	冗余 (1+1) 750 瓦特、 100 – 240 VAC、 8–4.5A，50–60 Hz， IEC60320-C14 入口，FRU
最大功耗	225 瓦特
最大散热量	768 BTU/h

表 1. 技术规格。

	AX 5550
MTBF	54,200 小时
仅设备/发货重量 磅 (千克)	26.8 磅 (12.2 千克) /37.8 磅 (17.2 千克)
安全认证	IEC 60950、EN 60950、CSA 60950-00、CE 标示
EMC/EMI 认证	FCC (Part 15 Class-A)、CE (Class-A)、CNS、AS/NZS、VCCI (Class A)
合规性	RoHS、REACH、WEEE
运行温度	0–40 °C (32–104 °F)
运行相对湿度	10 ~ 95% @ 40 °C、无结露
运行海拔高度	3000 米 / 9842 英尺

注意:性能数据基于 Malware Analysis 的默认分析次数,但是会根据系统配置和处理流量配置文件的不同而异。

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。