Trellix

Cyberworld

Trellix 终端安全 (HX)

运用前线响应的知识阻止攻击

每天都会出现新的网络攻击、新的漏洞和新的勒索软件目标。安全团队发现现有的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，不能对高级威胁提供充分的检测和响应。另外，响应者有太多无法协同工作的工具，并且产生很多误报，这些误报的数量比有效警报还要多。

Trellix 终端安全 (HX) 使用深度防御模型来防御当今的网络攻击。终端安全 (HX) 的模块化架构将默认引擎和可下载模块结合起来，以保护、检测、响应和管理终端安全。

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，而不是使用追踪警报。
- 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。

为了防止常见的恶意软件，终端安全(HX)使用了基于特征码的终端保护平台(EPP)引擎。为了找到尚未存在特征码的威胁，恶意软件保护(MalwareGuard)使用机器学习，其中包含来自网络攻击前线的知识。对于针对常见软件和浏览器的漏洞利用的攻击，漏洞利用防护(ExploitGuard)使用了行为分析引擎，该引擎可以确定是否正在使用漏洞，并阻止其执行。此外，Trellix不断开发模块来检测攻击技术，加速对新兴威胁的响应。例如，开发了进程保护(Process Guard)来阻止凭证泄露。

即使有最好的保护，也有可能被入侵。为了确保做出实质性响应，最大限度地减少业务中断，终端安全(HX)包括终端检测和响应功能，这些功能依赖于前线实时发布的 IoC。Trellix工具也有以下功能：

- 在几分钟内，搜索并调查数万个终端上已知和未知的威胁。
- 识别并详细说明用于渗透终端的攻击向量。
- 确定特定终端上是否发生了、并持续存在的攻击，以及攻击的传播范围。
- 创建终端入侵的时间表，确定入侵持续时间并跟踪事件。

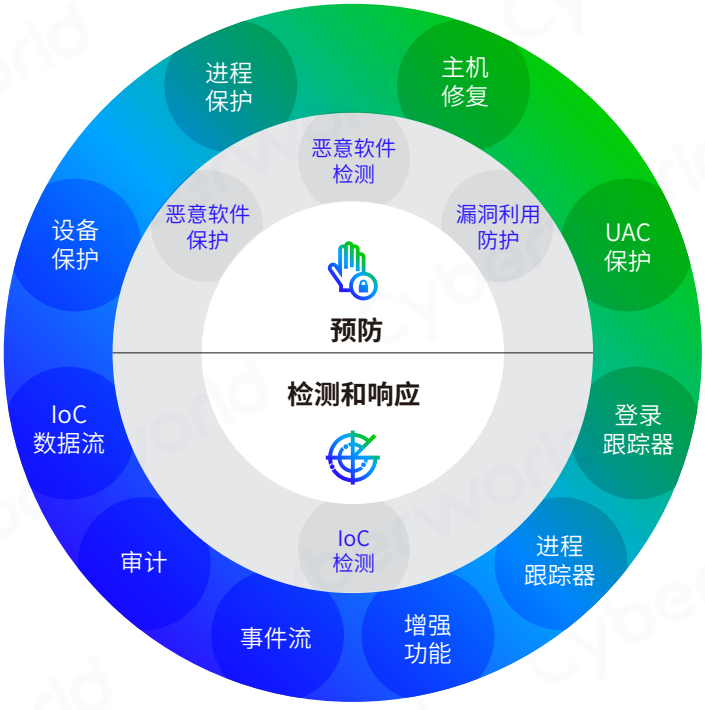

图 1：Trellix 终端安全 (HX) 的核心引擎（中心）和可用模块（外环）

现代威胁不会只发生在单个终端上。因此，只在单个终端进行修复，不能解决大多数由入侵导致的问题。全面的修复能够有效地通信和指向可能隐藏威胁的所有设备，并实时关联这些信息。终端安全 (HX) 与 Trellix XDR 本地集成，无缝连接所有 Trellix 技术和服务，以检测和响应所有复杂的威胁。

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。
- 终端安全 (HX) 集成了威胁分析和响应的工作流程。
- 恶意软件保护，包括反恶意软件防护、机器学习、行为分析、IoC 和终端可视化。
- 与 Trellix XDR 本地集成，以获得更多可视化和控制，全面修复企业中的所有威胁。

附加功能

- Enterprise Search 可快速查找和阐明可疑活动和威胁。
- Data Acquisition 可在特定时间范围内进行详细且深入的终端检查和分析。
- 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
Mac	10.9 - 10.15、11、12、13
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：物理设备、虚拟设备、云托管设备。

Trellix

关于 Trellix
Trellix是一家重新定义网络安全未来的全球性公司。它的开放式原生扩展检测和响应 (XDR) 平台，可帮助企业抵御当今最先进的网络威胁攻击，并保护其业务不受影响。Trellix安全团队和庞大的合作伙伴生态系统，运用人工智能、机器学习和自动化加速技术创新，为 40,000 多家企业客户提供服务。