Trellix

Cyberworld

Trellix IVX

在工作流程中的任何阶段扫描对象以查找威胁

Trellix IVX 如何运作

为了准确检测和阻止动态的、前所未见的漏洞和恶意软件，企业需要以情报为主导的威胁检测，这种检测能够随着威胁空间的变化而不断发展。企业还需要洞察上下文，以便通过确凿的证据、可操作的情报和顺畅的工作流程集成来加速解决安全事件。

IVX (Intelligent Virtual Execution) 是一种无特征码的动态分析引擎，可捕获和确认零日攻击和有针对性的 APT 攻击。IVX 通过在专有虚拟机管理程序中引爆可疑文件、Web 对象、URL和电子邮件附件，识别规避传统基于特征码的防御的攻击，该虚拟机管理程序可同时执行 200 多次。IVX 使分析师能够直观地了解恶意软件在虚像中的行为方式，并与恶意软件进行安全交互，以测试对策的有效性，从而加速事件响应。

亮点

- 检测已知和未知的恶意软件。
- 与所有主流的云存储解决方案、许多Web应用程序集成。
- 支持的操作系统包括Windows、Mac和Linux，能分析操作系统中的威胁。
- 深入分析详细信息，包括MITRE ATT&CK 映射、提取的对象、IOC等。
- 支持浏览器和云存储插件。
- 以JSON格式提供检测到的恶意软件的上下文分析。

Trellix IVX可在本地部署或作为云原生服务使用，提供经过验证的灵活分析功能。它能够快速检查和判定潜在的恶意内容。SOC分析师可以手动提交对象以供检查和洞察，或者将IVX与企业构建或购买的应用程序无缝集成，实现持续且无摩擦的保护。

Trellix IVX 的工作原理

Trellix IVX通过揭露前所未见的漏洞和恶意软件来阻止入侵。

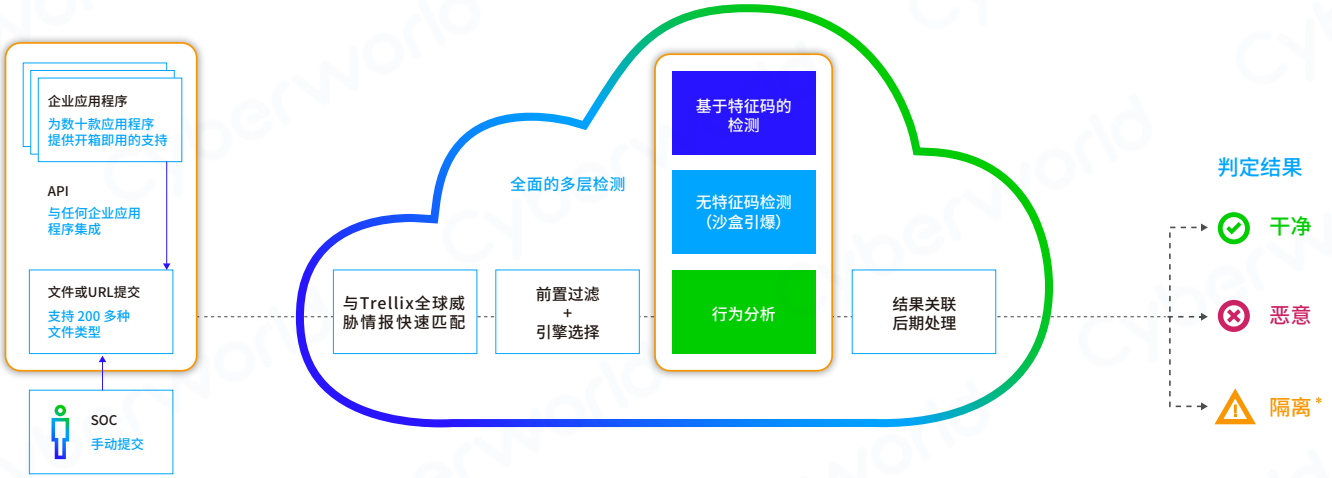
IVX引擎使用与许多Trellix产品相同的经过验证的检测方法，通过引爆可疑文件、Web对象、URL和电子邮件附件来捕获与确认零日攻击、多流攻击和其他规避攻击。

首先，IVX使用从Trellix全球40,000多家用户和合作伙伴那里收集的Trellix全球威胁情报，将您提交的内容与最新已知的威胁行为、其他潜在的恶意行为进行比较。

然后，IVX使用统计分析、人工智能和机器学习进行一对多分析。在分析时，IVX决定如何分析对象，并实时组成多个独特的执行环境。IVX可同时执行200多次，涵盖多个操作系统、服务包、应用程序和应用程序版本。

Trellix IVX 与专注于单一攻击对象的检测解决方案不同，它执行多流分析来分解并全面了解多阶段攻击的完整上下文。状态攻击分析对于触发整个攻击生命周期（从初始攻击到数据泄露）的分析至关重要。Trellix 还确定了攻击生命周期多个阶段产生次要或组合效应的可能性，以发现前所未见的漏洞和恶意软件。

如果判定该对象是恶意的，则发送警报。这样您就会知道该对象需要注意。



主要技术特点：

- **主动分析未知代码和可疑Web对象**
  对象针对各种浏览器、插件、应用程序和操作环境执行。无特征码IVX引擎可识别零日漏洞的利用情况，确认正在进行的Web攻击，阻止通过多种协议进行的回调和后续恶意软件下载。

- **在虚拟环境中引爆所有电子邮件附件**
  安全且准确地分析所有附件，以识别零日漏洞。除了基于特征码和信誉系统，IVX引擎还可以检测以前合规的文件是否已被武器化、是否通过鱼叉式网络钓鱼电子邮件发送来渗透企业防御。

- **分析网络文件共享上的武器化文件**
  IVX引擎可用于扫描与CIFS兼容的文件共享，以检测和阻止嵌入在武器化的 Microsoft Office 文件、图像、PDF、Flash或ZIP/RAR/TNEF档案中的高级针对性攻击。

- **检查URL**
  包括：嵌入在电子邮件、MS 365文档、PDF和存档文件中的URL；通过URL（包括FTP链接）下载的文件；混淆、欺骗、缩短和动态重定向的URL；凭据式网络钓鱼和仿冒URL。

- **专有虚拟化技术**
  IVX引擎分析并确认真正存在的零日恶意软件，例如特洛伊木马、针对性攻击、Bots攻击、虚拟机感知式恶意软件和高级持续性威胁(APT)。

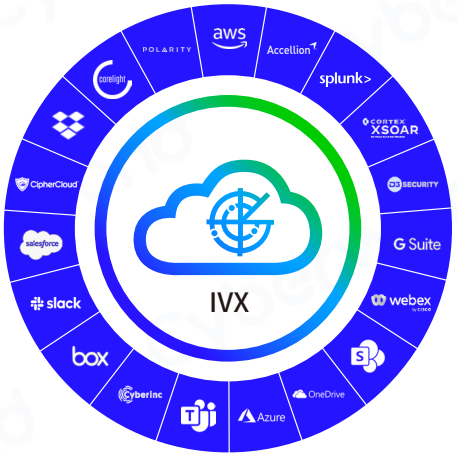
- **多阶段检查、拦截引擎**
  判定已知攻击和零日攻击，同时消除误报。多阶段的检查过程将虚拟化和网络安全结合起来，准确拦截用于渗透网络、窃取资源和敏感数据的高级恶意软件。

- **定制的虚拟机管理程序**
  内置专门为恶意软件分析而设计的对策。此虚拟机管理程序可实现峰值性能，能够检测许多复杂恶意软件对象所使用的沙盒感知和规避策略。

加速调查和响应

IVX可在本地部署或作为云原生服务使用，快速扫描提交的内容，识别恶意软件。

您可以通过API轻松配置对IVX的访问，以便轻松集成到您的安全运营中心(SOC)工作流程中。



您不仅可以得到判定结果，还可以获取支持性的上下文详细信息，例如文件、注册表、进程和网络更改，以及 MITRE ATT&CK 映射和来自不断更新的 Trellix 全球威胁情报的其他相关发现。

保护协作平台和企业应用程序

IVX 与 AWS 、Azure 等云服务、Slack、MS 365 和 Google Workspace 等协作平台以及 Dropbox 、Box 、OneDrive 等云存储工具集成。

它还与许多企业应用程序集成，例如 Salesforce 、Webex 、Slack 、Microsoft Teams 等。您可以通过 Trellix 易于使用的 API ，轻松地与尚无插件的应用程序集成。

灵活的部署选项

Trellix 的云原生 IVX 可通过 Trellix 渠道或直接通过 AWS Marketplace 获取。如果您在本地部署，Trellix 也提供了选项：

表 1. 在 AWS 上的 Trellix Virtual Execution 型号

型号	吞吐量	vCPU	内存	网络接口	AWS实例类型
Trellix VX Bare-Metal	14 Gbps (类似于 VX 12550)	96	192GB	一个管理端口，4个集群端口	C5.metal

表 2. Trellix Virtual Execution 智能系统网络的规格

	VX 5600	VX 12600
支持的 操作系统	Linux macOS X Microsoft Windows	Linux macOS X Microsoft Windows
性能	11 subs/min	85 subs/min
高可用性	N+1	N+1
管理端口（后面板）	(1) 10/100/1000BASE-T 端口	1x 1G/10G Base-T
集群端口（后面板）	(3) 10/100/1000BASE-T 端口	1x 1G/10G Base-T 4x 1G/10G SFP+
IPMI 端口（后面板）	包含	包含
前 LCD 和键盘	不适用	不适用
VGA 端口	包含	包含
USB 端口（后面板）	2 个 USB 2.0、2 个 USB 3.2	2 个 USB 3.1 端口
串行端口（后面板）	115200 bps、无奇偶校验、8 个数据位、1 个停止位	115200 bps、无奇偶校验、8 个数据位、1 个停止位
驱动器容量	(2) 4TB SAS SED, RAID 1	4x 4TB 3.5 SAS3 HDD, RAID10, hot swappable, FRU
外接盒	1 RU，适合19英寸机架	2 RU，适合19英寸机架
机箱尺寸 宽x长x高	17.2 x 19.98 x 1.7 英寸 (437 x 507 x 43 毫米)	19 x 26 x 3.5 英寸 (482.6 x 660.4 x 89 毫米)
DC 电源	不适用	不适用
AC 电源	Redundant (1+1), FRU, 400W with Input 100 240VAC / 6.0-3.0A 200-240VDC / 3.4- 3.2A, 50-60 Hz IEC60320- C14 inlet	Redundant (1+1),FRU,1000W/1200W with Input 100-127/200 - 240Vac, 15-12A/8.5- 7A, 50-60 Hz IEC60320-C14 inlet
最大功耗（瓦）	300 瓦	948 瓦
最大散热量（BTU/h）	1024 BTU/h	3232 BTU/h
平均无故障时间（小时）	即将推出	即将推出
设备本身/发货重量 磅（kg）	24 磅 (10.9 kg) / 37 磅 (16.8 kg)	44 磅 (20 kg) / 70 磅 (31.8 kg)
安全认证	FIPS 140-2 等级 1（待定），CC NDcPP v2.2e（待定）	FIPS 140-2 等级 1, CC NDcPP v2.2e（待定）

表 2. Trellix Virtual Execution 智能系统网络的规格（续）

	VX 5600	VX 12600
安全合规性	EN IEC 62368-1:2018+A11:2020	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368
EMC 合规性	EN 55032:2015/A11:2020, EN 55035:2017/A11:2020, EN 61000-3-2:2014, EN 61000-3-3:2013	FCC Part 15 Class-A, CE (Class-A) CNS 13438 CISPR 32 VCCI-CISPR32 EN 55035 EN 55032 EN 61000 ICES-003 KN 32, KN 35
环境合规性	RoHS: 指令 2011/65/EU	RoHS REACH
运行温度	5°C - 35°C (41°F - 95°F)	10–35°C (50–95°F)
非运行温度	-40°C - 70°C (-40°F - 158°F)	-40–70°C (-40–158°F)
运行相对湿度	8–90% (无结露)	8–90% (无结露)
非运行相对湿度	5–95% (无结露)	5–95% (无结露)
正常运行的海拔高度	1524 米 (5000 英尺)	1524 米 (5000 英尺)

表 3. 在 VMware 上的 Trellix Virtual Execution 型号

型号	吞吐量	vCPU	内存	网络接口	VM实例类型
IVX-VM300	3 subs/min (类似于 VATD)	16	32GB	一个管理端口，4个集群端口	VMware ESXi

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。