Trellix

Cyberworld

Trellix
网络取证 (PX)

通过高性能的数据包捕获和调查分析
最大限度地减少网络攻击的影响

Trellix网络取证(PX)结合了业界最快的无损网络数据捕获和检索解决方案，并提供集中分析和可视化。它通过单一工作台加速网络取证过程，从而简化调查并降低风险。

您的企业需要尽早发现事件并迅速展开调查，以确定范围和影响，有效地遏制威胁，重新确保您的网络安全。

网络取证可让您通过高速捕获和索引完整的数据包，更快地识别和解决安全事件。借助网络取证，您可以检测各种安全事件，提高响应质量，并准确量化每个事件的影响。

作为网络取证的一部分，调查分析设备通过添加具有易于使用的分析界面的集中工作台，揭示隐藏的威胁，加速事件响应。

分析师可以在攻击前、攻击中和攻击后查看特定的网络数据包和会话。通过重建和可视化触发恶意软件下载或回调的事件，您的安全团队可以有效且迅速地做出响应，以防止再次发生。他们还可以通过解码通常用于在网络中横向传播攻击的协议，扩大对攻击者活动的可视化。

这种高性能的数据包捕获和深入分析的独特组合，可以帮助您的企业快速识别和监察攻击的每个元素。

Trellix

Cyberworld

数据包捕获亮点

高性能：连续无损数据包捕获，带时间戳，记录速度高达 20 Gbps。

高保真度：使用时间戳和连接属性对所有捕获的数据包进行实时索引；以JSON格式导出流索引和连接元数据；流索引可转换为 NetFlow v9、IPFIX 和 SiLK 数据格式。

快速结果：使用专利索引架构对目标连接和数据包进行超快速搜索、检索。

丰富的上下文：基于Web的深入式GUI，用于搜索和检查数据包、连接和会话。

广泛的可视化：会话解码器支持查看和搜索网页、电子邮件、FTP、DNS、聊天、SSL 连接详细信息和文件附件。

智能捕获：选择性过滤捕获的流量，以消除流视频、大文件传输、加密有效载荷等。

提高效率：使用自动化流程识别数据盗窃，使用专有算法诊断潜在的异常网络行为。

表 1. 数据包捕获设备

型号	捕获端口配置	管理端口	最大记录速度	总板载存储	规格	电源/典型工作负载
PX 1004S-6	4 x 1GE	1 x 1GbE	500 Mbps	6 TB	1U；17.2in(437mm)x19.7in (500mm) x1.7in(44mm)；18 lbs (8.2 kg)	AC, Fixed AC 100–240 V @ 50–60 Hz, IEC60320-C14 inlet
PX 2060ESS-96	4 x 10GE SFP+	2 x 1GbE	2 Gbps	96 TB，可扩展的SAS附加存储	2U；17.24in (438mm) x 24.41in (620mm) x 3.48in (88.4mm)；57.3 lbs (26.0 kg)	Redundant (1+1) 800 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU
PX 2060ESS-120	4 x 10GE SFP+	2 x 1GbE	7.5 Gbps	120 TB，可扩展的SAS附加存储	2U；17.24in (438mm) x 24.41in (620mm) x 3.48in (88.4mm)；57.3 lbs (26.0 kg)	Redundant (1+1) 800 watt, 100–240 VAC 10.5–4.0A, 50–60 Hz IEC60320-C14 inlet, FRU

请注意：根据系统的配置和所处理的网络流量，所有性能值都会发生变化。

Trellix

Cyberworld

表 2. 下一代数据包捕获设备

型号	捕获端口配置	管理端口	最大记录速度	总板载存储	规格	电源/典型工作负载
7600PX-HW	2p*40G FPGAQSFP 可选8x10G光纤端口	2p*10GT+2p*SFP	10-20 Gbps	192 TB 原始存储， 122 TB 用于PCAP 存储，可扩展的 SAS附加存储	17.2in (437mm) x 25.5in (437mm) x 3.5in (89mm)； 81.2 lbs (36.8 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH
7620PX-HW	2p*40G FPGAQSFP 可选8x10G光纤端口	2 x 1GbE	14-20 Gbps	无板载存储； 光纤 HBA 连接到 外部 SAN 存储	17.2in (437mm) x 25.5in (437mm) x 3.5in (89mm) 63 lbs (28.6 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH
5000SX-HW	-	-	-	704 TB 原始存储， 465 TB 用于 PCAP 存储	17.2in (437mm) x 25.5in (437mm) x 7in (89mm) 78 lbs (35.4 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH
5600PX-HW	4p*10G FPGA-QSFP 端口	2p 10/100/1000 BASE-T端口	6-10 Gbps	120 TB 原始存储， 80 TB 用于 PCAP 存储	17.2in (437mm) x 25.5in (647mm) x 3.5in (89mm) 42 lbs (19.05 kg)	Redundant (1+1), FRU, 920W with Input 100-240V, 11-4.4A, 50-60 Hz IEC60320-C14 inlet

*根据系统的配置和所处理的网络流量，所有性能值都会发生变化。

- 7600PX 和 7620PX 可支持高达 20 Gbps 的连续数据包捕获速率，无需进行元数据分析，至少连接一个存储阵列。
- 7600PX 和 7620PX 可以支持高达 16 Gbps 的连续数据包捕获速率，并进行元数据分析，至少连接一个存储阵列。
- 7600PX 和 7620PX 可以支持高达 14 Gbps 的连续数据包捕获速率，并进行元数据分析，加载多达 10,000 条 Suricata 规则，至少连接一个存储阵列。
- 7600PX 支持高达 10 Gbps 的连续数据包捕获速率，并进行元数据分析，未连接存储阵列。
- 5600PX 可以支持高达 10 Gbps 的连续数据包捕获速率，并进行元数据分析，至少连接一个存储阵列。
- 5600PX 支持高达 6 Gbps 的连续数据包捕获速率，并进行元数据分析，未连接存储阵列。

表 3. 下一代数据包捕获设备的合规性

型号	EMC合规性	安全合规性	环境合规性
7600PX-HW 7620PX-HW	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	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368 EN 62368 BS EN 62368	RoHS, REACH, Conflict Minerals
5600PX-HW	“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”	“CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368, EN 62368 BS EN 62368”	“RoHS REACH”

表 4. 虚拟数据包捕获设备（支持 Azure、ESXi、KVM 和 AMI）

虚拟 PX 设备规格	最低要求	Trellix 建议的要求	性能要求
CPU 核心	4 核	8 核	16 核
内存	16 GB RAM	32 GB RAM	64 GB RAM
网络接口控制器 (NIC)	管理专用网卡 用于数据包捕获的专用网卡	管理专用网卡 用于数据包捕获的专用网卡	管理专用网卡 用于数据包捕获的专用网卡
硬盘	80 GB 硬盘用于 Linux 操作系统 200 GB 硬盘用于存储捕获的数据	80 GB 硬盘用于 Linux 操作系统 200 GB 硬盘用于存储捕获的数据	80 GB 硬盘用于 Linux 操作系统 200 GB 硬盘用于存储捕获的数据
大概的捕获速率	25 Mbps（规则数量有限）	100 Mbps（具有标准设备限制）	1,000 Mbps（具有标准设备限制）

调查分析亮点

Trellix调查分析设备支持单节点和分布式架构的多种配置，以优化带宽和元数据聚合、查询和分析的性能。

可视化：通过易于创建的自定义仪表板查看并共享网络元数据和活动。

快速响应：对所有警报、捕获的流量和元数据进行集中的应用程序级关键字、正则表达式和通配符查询。

灵活的界面：立即为感兴趣的会话切换，并下载单个或批量的 PCAP 数据。

强大的搜索功能：使用HTTP、SMTP、POP3、IMAP、SSL、TLS、DNS 和 FTP 等协议的索引元数据加速搜索。

IOC 聚合：将Trellix网络威胁防护、电子邮件安全和终端安全产品的警报以及所有网络元数据整合到一个单一的工作台中，只需单击一下，即可从警报切换到会话数据。

回顾性威胁搜寻：将Trellix威胁情报、STIX 和 OpenIOC 数据源与自动 IA 搜索功能集成，进行回溯的IOC威胁分析，并自动告警您网络中出现的IOC，这些IOC可能早在数天或数周前就存在。

一键文件重建：快速且安全地重建可疑文件、网页和电子邮件，以供进一步分析。

表 5. 下一代调查分析设备

型号	总板载存储	规格	电源/典型工作负载
2600IA-HW*	120 TB，82 TB 用于元数据存储	17.2in (437mm) x 25.5in (437mm) x 3.5in (89mm)；79.4 lbs (36 kg)	AC 1200W, Titanium Level, Redundancy, PMBus 1.2, +12V/+5Vsb, 360x76x40 mm, HF, RoHS/REACH

请注意：摄入速率为每秒 50,000 个事件。
*可配置为主节点或数据节点

表 6. 下一代调查分析设备的合规性

型号	EMC合规性	安全合规性	环境合规性
2600IA-HW	FCC Part 15 Class-A, CE (Class-A), CNS 13438, CISPR 32, VCCI-CIS PR32, EN 55035, EN 55032, EN 61000, ICES-003, KN 32, KN 35	CAN/CSA 22.2 No. 62368 UL 62368 IEC 62368 EN 62368 BS EN 62368	RoHS REACH Conflict Minerals

表 7. 虚拟调查分析设备（支持 Azure、ESXi、KVM 和 AMI）

	最低要求	虚拟 IA 主节点	虚拟 IA 数据节点
CPU 核心	16	16	64
内存 (RAM)	32 GB	64 GB	256 GB
网络接口控制器（NIC）	1	1	2 (multibox 聚类)
硬盘	2.5 TB (IO 吞吐量 > 100 MB/秒)	1 TB	48 TB (IO 吞吐量) > 1GB/秒
性能	4–5k/秒	不适用	25–30K/秒 (single box 集群)
保留时间	7 天	无	30 天

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。