解决方案简介

确保销售点系统的实时终端安全

要点概述

随着网络安全威胁态势不断演变，使得企业越来越难以防御各种维度攻击。高级漏洞利用程序和工具正快速增加，趁虚而入的攻击者也在持续增长。易受攻击的联网销售点(POS)系统和设备为他们提供了有利可图的攻击目标。保护这些POS系统需要具有实时终端响应和检测功能的安全方案，使用人工智能(AI)和机器学习(ML)来处理事件调查和响应机制。FortiEDR帮助安全负责人在感染前和感染后保护其POS终端，有效阻止高级恶意软件攻击和数据泄露风险，确保数据反窃取和系统业务完整性。

瞄准针对 POS 系统的更高级的新型威胁

由于威胁数量、速度和复杂程度不断提升，首席信息安全官 (CISO) 正遭受恶意漏洞利用程序的持续威胁困扰。终端设备仍然是网络犯罪分子的主要攻击目标之一，他们企图利用某些终端的漏洞作为网络接入点。POS 系统和设备是许多 CISO 的关注要点，因为它们往往运行于较旧的或指定的嵌入式操作系统之上。然而，补丁并非持续始终可用，这导致问题进一步恶化。此外，即使它们受到保护，也通常是由基于特征的旧版杀毒解决方案提供，因为大多数更现代的最新杀毒能力与终端检测和响应解决方案都不支持其旧版操作系统。

在 65 个国家或地区的 67 家企业发生的 2,200 多起经证实的数据泄露事件中，约有 14.5% 涉及针对销售点 (POS) 终端和控制器发起的远程攻击，另有约 5% 是通过在 POS 设备上物理植入支付卡盗号软件入侵，包括从气泵终端到 ATM 的所有设备。[1]

POS 系统保护要求

为了保护这些 POS 终端设备，CISO 必须确保其团队能够实现以下能力：

- **保护机器免受攻击**，例如暴力破解、后门恶意软件、窃取凭证利用、网络钓鱼或内存抓取，而无需让机器离线，以便继续运行业务。
- **检测攻击和高级恶意软件**。 对受攻击系统的延迟检测将导致攻击者有更多时间进行横向移动、抓取、窃取并利用客户支付卡信息，进而严重损害品牌声誉。
- 发现未受防御、存在漏洞或正在运行可能不必要应用的系统，有助于收集数据**并控制减少安全隐患性**。
- 在支持传统操作系统的同时，不会给低功率且资源有限的 POS 终端**增加额外的性能负担**。

此外，安全负责人还需要一款轻量级端点安全解决方案，以支持广泛的传统或指定操作系统，包括有效防御能力和检测高级恶意软件、实时规避和遏制威胁、自动阻止漏洞攻击并确保业务连续性，而不会危及业务安全。同时，请切记，防御虽然重要，但无法保证提供全面保护。尽管终端安全持续受威胁，但我们可以防止数据丢失。

高级轻量级终端防御

FortiEDR（终端检测和响应）为安全负责人提供了 AI/ML 驱动型高级防御解决方案，使用获得专利的代码跟踪技术，在入侵前和入侵后检测并阻止恶意软件嵌入。集成 Fortinet Security Fabric 的 FortiEDR 能够让企业完全了解所有终端（包括 POS 系统）情况，并提供直观的用户界面，支持最终用户快速、轻松地管理策略，并在发生感染时及时修复。为此，该解决方案将下一代杀毒 (NGAV)、应用通信控制、虚拟补丁修复和自动化 EDR 结合在一起，实现在单个代理中执行实时拦截、威胁搜寻和事件响应。

FortiEDR 提供了主动式实时安全防御，便于企业保障其 POS 业务系统。核心功能包括：

通过机器学习 NGAV 防御恶意软件。通过异常入侵的内核级可视化，FortiEDR 能够全面掌握可绕过传统杀毒软件及其他防御方法入侵的高级威胁防御。鉴于其无特征性，FortiEDR 可显著降低特征数据库下载和升级软件开销，同时为新式和传统操作系统提供轻量级有效防御。

实时检测并规避威胁。FortiEDR 能够自动识别入侵，可实时检测并规避威胁，从而准确地进行感染后（被攻击后）遏制，防止数据泄露和勒索软件加密终端。因此，客户可以阻止漏洞攻击并防止勒索软件等恶意软件造成的任何相关损害。

借助应用和漏洞可视性来降低风险。FortiEDR 具有高级自动化攻击面策略控制和面向所有联网设备（包括 POS 系统）的漏洞评估和安全保护，可支持安全和运营团队发现和跟踪应用与终端，并将其与 CVE 数据和应用评级数据相关联，以确定 POS 设备是否正在运行易受攻击的应用，并根据此信息执行基于风险的主动策略。借助 FortiEDR，安全运营团队能够轻松找到存在漏洞的应用和系统，并通过虚拟补丁进行修复，在下一个补丁维护窗口前主动修复易受攻击的系统。

轻量级终端安全解决方案支持广泛的传统或指定操作系统，并能够防御和检测高级恶意软件、实时规避和遏制威胁、自动阻止漏洞攻击并确保业务连续性，而不会危及业务安全。

最大限度地降低性能影响。由于 FortiEDR 可实时防御威胁攻击，因此 POS 设备能够持续运行，而不会让企业面临业务中断风险。此外，FortiEDR 的 CPU 开销很小，并且不会生成太多的网络流量。总而言之，FortiEDR 提供了单个轻量级代理，不仅 CPU 资源占用率少于 1%，所需 RAM 容量不到 120 MB，而且每主机网络流量生成速度低于 1kb/分钟。

利用取证分析。此外，FortiEDR 还为网络安全和运营团队提供了深度取证调查功能，不仅有助于全面了解POS 系统上快速演变的安全威胁数据，而且还能够灵活地自动解决安全事件。因此，安全运营中心 (SOC) 团队可在最适合自己的时间窗口进行威胁探测搜索。

此外，安全和运营团队还能够通过 FortiEDR 中量身定制的 Playbook来编排和自动实施事件响应与修复，从而减少威胁响应时间。FortiEDR 采用基于风险评估的方式，支持根据资产价值、终端组和威胁等级分类进行自定义响应。此外，FortiEDR 还允许在特定设备上或整个终端环境（包括 POS 系统）中手动或自动地恢复已遏制恶意软件所做的更改配置。

快速轻松实施。FortiEDR 代理面向每个受支持操作系统提供标准安装程序包，可通过 Microsoft System Center Configuration Manager (SCCM) 等标准远程无人值守部署工具轻松安装，无需本地配置或重启。

总结

FortiEDR 能够帮助安全运营团队预防、检测、遏制和补救修复对 POS 系统发动的快速移动攻击。借助 FortiEDR，他们可以针对性地降低跨 POS 终端检测和修复高级恶意软件的复杂性和成本。此外，FortiEDR 还能够最大限度地降低事件响应时间压力，同时防止往往导致数据泄露的漏洞利用和因网络攻击所致的业务中断，避免警报干扰、滞留终端时间过长或数据泄露。

[1] Joe Stanganelli, "数据漏洞增加表明终端正遭受攻击," Security Now, 2018 年 4 月 16 日。

FORTINET

www.fortinet.com

January 8, 2020 7:17 AM

572439-0-0-EN

D:\Fortinet\Solution Briefs\purple solution briefs\FortiEDR POS\sb-FA-ensuring-real-time-endpoint-security-on-point-of-sale-systems-teal