SOLUTION BRIEF

Ensuring Real-time Endpoint Security on Point-of-sale Systems

Executive Summary

The threat landscape continues to evolve, making it increasingly more difficult for organizations to defend against attacks. Advanced exploits and tools are proliferating, and the number of bad actors with access to them continues to grow. Vulnerable internet-connected point-of-sale (POS) systems and devices provide them with a lucrative target. Protecting these POS systems requires a security approach with real-time endpoint response and detection that uses artificial intelligence (AI) and machine learning (ML) to orchestrate incident investigation and response. FortiEDR gives security leaders the ability to protect their POS endpoints pre- and post-infection, stopping advanced malware and data breaches before they impact data and system integrity.

POS Systems Targeted by New, More Advanced Threats

Due to the growing volume, velocity, and sophistication of the threat landscape, CISOs are under a constant barrage of malicious exploits. Endpoints remain a prime target for cyber criminals, who seek to exploit the vulnerabilities of certain endpoints as a network access point. POS systems and devices are a key concern for many CISOs, as they tend to run on older or designated embedded operating systems. Exacerbating the issue is the fact that patches are not always available. Additionally, if they are protected, they often are protected by older, signature-based antivirus solutions, as most of the latest, more modern antivirus and endpoint detection and response solutions do not support their older operating systems.

About 14.5% of more than 2,200 confirmed data breaches across 67 enterprises spanning 65 nations involved remote attacks against point-of-sale (POS) terminals and controllers, while about 5% more occurred through the physical implantation of payment-card skimmers on POS devices, which includes everything from gas-pump terminals to ATMs.[1]

POS Systems Protection Requirements

To protect these POS devices, CISOs must ensure that their teams are able to:

- **Protect machines against attacks** such as brute-force hacking, backdoor malware, use of stolen credentials, phishing, or memory scraping, without needing to take them offline so they can continue to conduct business.
- **Detect attacks and advanced malware.** Delayed detection of a compromised system gives attackers more time to move laterally, scrape, exfiltrate, and exploit customer payment card information and tarnish a brand's reputation.
- **Gain visibility and control security hygiene** by discovering systems that are not protected, have vulnerabilities, or are running potentially unwanted applications.
- **Add no additional performance burden** on POS machines that are already low-powered and resource-constrained while also supporting legacy operating systems.

In addition to the above, security leaders need a lightweight endpoint security solution that supports broad legacy or designated operating systems, including the ability to prevent and detect advanced malware, defuse and contain threats in real time, automatically stop breaches, and ensure business continuity without risk to the business. At the same time, it is important to remember that prevention, while important, does not guarantee 100% protection. Notwithstanding, even though security compromises are inevitable, data losses can be prevented.

Advanced, Lightweight Endpoint Protection

FortiEDR (endpoint detection and response) provides security leaders with an AI/ML-driven advanced endpoint protection solution that uses patented code-tracing technology to detect and stop malware—both pre- and post-intrusion. Integrated within the Fortinet Security Fabric, FortiEDR provides organizations with transparent visibility across all endpoints—including POS systems—and an intuitive user interface that gives end-users the ability to quickly and easily manage endpoint policies and remediate infections when they do occur. To do so, the solution combines next-generation antivirus (NGAV), application communication control, virtual patching, and automated EDR for real-time blocking, threat hunting, and incident response in a single agent.

FortiEDR delivers proactive, real-time security that organizations can use to protect their POS systems. Core capabilities include:

Prevent malware with machine-learning NGAV. Through kernel-level visibility of anomalous intrusions, FortiEDR has full visibility of advanced threats that can bypass traditional antivirus and other prevention methods. Because it is signatureless, FortiEDR reduces the overhead of downloading and updating the signature database while offering lightweight, effective protection for modern and legacy operating systems.

Detect and defuse threats in real time. FortiEDR automates the identification of intrusions so that it can detect and defuse threats in real time by surgically containing them post-infection (post-compromise) to prevent data exfiltration and ransomware encryption. As a result, customers stop the breach and any associated damage from malware such as ransomware.

Reduce risk with visibility into applications and vulnerabilities. FortiEDR includes advanced automated attack surface policy control with vulnerability assessment and security for all internet-connected devices—including POS systems. This enables security and operations teams to discover and track applications and endpoints, correlate them with CVE and application rating data to determine if POS devices are running vulnerable applications, as well as run proactive risk-based policies based on that information. With FortiEDR, security operations teams can easily find applications and systems with vulnerabilities and remediate them with virtual patching—proactively protecting vulnerable systems until the next patching maintenance window.

> A lightweight endpoint security solution supports broad legacy or designated operating systems and enables prevention and detection of advanced malware, diffusion and containment of threats in real time, automatic breaches prevention, and business continuity without risk to the business.

Minimize performance impact. Because FortiEDR contains attacks in real time, POS devices can continue working uninterrupted without risk to the organization. In addition, FortiEDR consumes a minimum amount of CPU power and does not generate excess network traffic. In sum, FortiEDR offers a single, lightweight agent that consumes less than 1% CPU, requires under 120 MB of RAM, and generates less than 1kb/minute of network traffic per host.

Leverage forensics analysis. In addition, FortiEDR provides security and operations teams with in-depth forensic investigation, not only giving full visibility into rapidly evolving threats on POS systems but also providing the flexibility to address security issues automatically. As a result, security operations center (SOC) teams can hunt on their own time, when it is best suited for them.

Additionally, security and operations teams can reduce the time to respond to threats with tailor-made playbooks in FortiEDR to orchestrate and automate incident response and remediation. Taking a risk-based approach, FortiEDR enables a customized response based on asset value, endpoint groups, and threat categorization. FortiEDR also makes it easy to roll back the changes done by contained malware, either manually or automatically on selected devices or across the entire endpoint environment—including POS systems.

Implement quickly and easily. The FortiEDR agent comes as a standard installer package for each supported operating system and is easily installed via standard remote unattended deployment tools such as Microsoft System Center Configuration Manager (SCCM). No local configuration or reboot is required.

Conclusion

FortiEDR helps security and operations teams prevent, detect, contain, and remediate fast-moving attacks on POS systems. With FortiEDR, they can strategically reduce the complexity and cost associated with the detection and remediation of advanced malware across POS endpoints. In addition, FortiEDR minimizes incident response time pressures, while also preventing vulnerability exploitation that commonly leads to data breaches and the disruption caused by cyberattacks—with no alert fatigue, excessive dwell time, or breach anxiety.

[1] Joe Stanganelli, "Data Breach Increase Shows Endpoints Are Under Attack," Security Now, April 16, 2018.

FURTINET

www.fortinet.com