Point of View

Three Key Imperatives for Enhanced Endpoint Resilience

Point-of-Fail: How Store Systems Could Be Your Weakest Security Link

Increasing Complexity of Security Risks

The security threats enterprises face have grown in **volume, variety and velocity**.

IT decision makers face increasingly complex security threats. Not only are threats growing rapidly in number and type, the speed at which new threats are emerging is also increasing.

Security threats are no longer a peripheral reality that only impact the unsophisticated. More than 80% of U.S. businesses expect a critical breach in 2019[1].

Volume

More enterprises across more industries are experiencing a higher number of threats and attacks today than ever before.

Variety

There has been a significant increase in the different types of attacks across various layers of the enterprise.

Velocity

The speed at which malware spreads and the rate at which new threats are born are both at an all-time high.

There were over **206 million** ransomware attacks in 2018.[2]

Users receive an **average of 16** malevolent e-mails per month.[3]

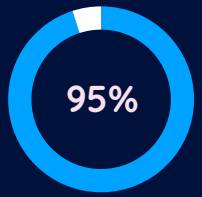
There are over **350,000** new malware variants every day.[4]

1. Trend Micro, 2. 2019 SonicWall Security Threat Report, 3. Symantec, 4. AV-TEST Institute

Retail & Restaurants Are Most Targeted

U.S. retail is the **most targeted industry**, followed by restaurants and hospitality. Combined, they account for 42% of all incidents.[5]

3 in 4 retailers have been breached some time in their past, with 50% of those breaches occurring in the past year.[5]



of retailers believe they are vulnerable to data breaches.[5]

Even as retail enterprises strengthen network, application and data security, their defenses are only as strong as their weakest link. **Compromised POS systems have been a major source of data breaches**, such as at Checkers, Darden restaurants and Russell Stover.

Point-of-sale vulnerabilities continue to be a major source of retail data breaches.

Malware planted by hackers collected credit card information from systems at over 100 **Checkers** locations. Almost 15 percent of locations were compromised from software that was installed in September of 2018.

Darden was targeted in a cyber attack statewide. Hackers accessed payment information of customers who went to the restaurant from November 3, 2017 to January 2, 2018.

Store customers of **Russell Stover's** Chocolates who used a payment card between February and August 2019, could have had their information captured by machines that were infected by malware.

5. Thales 2018 Data Threat Report

Data Breaches Are Costly

The aftermath of a POS breach includes damage to brand reputation, lost sales due to downtime and increased legal and IT costs.

33%
of customers will take a temporary break from doing business with a retailer who has suffered a data breach.[6]

19%
of customers will permanently stop shopping at a retailer who has suffered a data breach.[6]

A point-of-sale breach can be catastrophic. Depending on the severity of the breach, costs can run into the hundreds of millions of dollars. The Home Depot's point-of-sale breach is estimated to have cost over **$179 million**.[7]

Loss of brand reputation.

A **class-action suit** was filed against Macy's for failing to protect personally identifiable information (PII), and waiting for almost a month to notify customers after discovering a breach.

Downtime and productivity loss.

In 2019, Target lost an estimated **$110 million**[8] in sales during a point-of-sale outage that lasted ten hours spread over two days.

Legal, compliance and IT cost.

Marriot International incurred an estimated cost total of around **$1 billion**[9] to recover from the customer data breach in 2018.

6. KPMG, 7. Cybersecurity News, 8. CNBC, 9. Bloomberg Intelligence

Three Imperatives for Enhanced Endpoint Resilience.

Retailers can build resilience through a **holistic approach** to prevention, detection and recovery.

Comprehensive Protection

Protect against all attack vectors with multiple layers of security for your store systems.

Intelligent Detection

Amplify protection against the growing threat of unknown and zero-day attacks through continuous monitoring.

Accelerated Self Recovery

Reduce the time it takes to recover from destructive malware.

Comprehensive Protection

Protect against all attack vectors with multiple layers of security for your store systems.

From unintended human error to sophisticated rootkit attacks delivered via malicious emails, there are threats lurking around every corner. Your store systems must be comprehensively protected.

1 in 10 web requests lead to malware.[10]

Insecure browsers and malicious attachments.

HP Sure Click[15] is a secure virtual container that protects against the most common attack methods: malicious websites and attachments.

Lower immunity via compromised security apps.

HP Sure Run[16] ensures your store systems' key security processes and critical applications are protected against compromise through an additional layer of hardware protection.

Unauthorized access of store mobile devices.

HP Engage Go Smart Dock protects against unauthorized removal of mobile POS through a smart locking system with advanced authentication.

Outdated software or untimely updates.

Intel vPro® performs remote software updates, discovers and heals software-related issues, and eliminates the need for expensive service calls and truck rolls for various types of repairs.

10. Sumantec, 11. Accenture, 15. Refer disclaimer #1, 16. Refer disclaimer #2

Intelligent Detection

Detect known and unknown attacks in real-time with minimal performance impact.

It takes more than a traditional approach to keep up with the rapid pace of threat evolution. For instance, a zero day attack - an attack that exploits vulnerability in software before the developer either knows about it or is able to fix it - is impossible to detect through traditional means.

Zero-day attacks can outsmart traditional antivirus.

HP Sure Sense[17] harnesses the power of deep learning AI to provide real-time detection and prevention of zero-day threats coupled with behavioral detection of ransomware activity.

Stronger protection can mean slower performance.

HP Sure Sense[17] is a lightweight agent that requires minimal updates, works online or offline, and detects known and unknown threats in milliseconds with less than 1% CPU load.

In 2018, 76%
of successful attacks on organization endpoints were zero-day.[12]

Traditional antivirus solutions can stop just **43%** of zero-day attacks.[12]

12. Ponemon Institute, 17. Refer disclaimer #3

Accelerated Self-Recovery

Recover quickly from attacks and minimize the impact of worst-case scenarios.

However strong your defenses, you are never 100% protected. The question then becomes: How quickly can you recover from the most debilitating attacks, such as a BIOS rootkit? How prepared are you to respond to a security-breach-induced POS outage across your stores?

NotPetya, one of the world's deadliest Wiper attacks, spread globally within hours of its first appearance in Ukraine. It crippled multinational companies including Maersk, pharmaceutical giant Merck, FedEx's European subsidiary TNT Express, French construction company Saint-Gobain, Mondelēz, and Reckitt Benckiser. It even spread back to Russia, striking the state oil company Rosneft. The result was more than $10 billion in total damages, according to a White House assessment.[13]

Protect against BIOS tampering.

In the event of a malware attack on the BIOS, **HP Sure Start**[18] automatically detects the change, notifies the user and IT, and restores the most recent good version of the BIOS.

Restore to last known stable state.

HP Sure Recover[19] lets you quickly and easily reimage your device using only a network connection—and can even enable IT to schedule reimaging for the entire fleet.

13. Wired.com , 18. Refer disclaimer #4 , 19. Refer disclaimer #5

When it comes to cybersecurity attacks, retailers and restaurants are the most heavily targeted[14]. And, their point-of-sale and store systems are in hackers' crosshairs constantly.

There is no foolproof way of preventing an attack. You can, however, reduce vulnerability against the most common threat vectors through **comprehensive protection**, be better prepared against unknown zero-day attacks through **intelligent detection**, and minimize the impact of worst-case scenarios through **accelerated self-recovery**.

14. Thales 2018 Data Threat Report

With a broad portfolio of point of sale devices, HP helps retailers and hospitality operators meet customers' needs anytime, anywhere. From traditional to mobile point of sale devices, HP is reinventing the customer experience with technology solutions that empower employees and engage customers. Discover how HP is designing devices with built-in security. Learn more at **www.hp.com/go/retail**

Intel vPro® platforms with Intel® AMT empowers HP Retail and Hospitality customers to embrace new experiences that require complex device management by remotely performing software updates, discovering and healing software-related issues, eliminating the need for expensive service calls and truck rolls for various types of repairs, and adding an extra layer of hardware-based security that complements and augments existing HP security solutions.

Disclaimers:

1. HP Sure Click is available on most HP PCs and HP Engage retail products and supports Microsoft® Internet Explorer, Google Chrome, and Chromium™. Supported attachments include Microsoft Office (Word, Excel, PowerPoint) and PDF files in read only mode, when Microsoft Office or Adobe Acrobat are installed.

2. HP Sure Run is available on HP Elite products and HP Engage retail products equipped with 8th generation Intel® or AMD® processors.

3. HP Sure Sense requires Windows 10. See product specifications for availability.

4. HP Sure Start Gen5 is available on select HP PCs and retail products with Intel processors. See product specifications for availability.

5. HP Sure Recover Gen2: See product specifications for availability. Requires an open, wired network connection. Not available on platforms with multiple internal storage drives. You must back up important files, data, photos, videos, etc. before using HP Sure Recover to avoid loss of data. HP Sure Recover (Gen1) does not support platforms with Intel® Optane™.

4AA7-6632ENW, December 2020.