Strengthen POS Security from Transaction to Data Center

Protect sensitive store and customer data with a holistic approach that goes beyond PCI and EMV

“Larger (POS) breaches tend to be a multi-step attack with some secondary system being breached before…”

Verizon 2015 Data Breach Investigation Report

Industry Strategic Challenges

In the retail business, trust is everything. Customers and partners rely on retailers to protect their personally identifiable information and payment data. It takes years and a lot of effort to build trust in a brand and business but only moments to see it all vanish in a major security breach.

With the recent, rapid growth in organized cybercrime, consumers and retailers and their data have come under increasingly frequent and sophisticated attack. In 2014, there were 801 weekly malware attacks reported worldwide on retail enterprises. In 2015, in the US alone, 650 data breaches were reported, and 175.7 million records were known to have been stolen. And it’s no longer just payment card data at risk. Shopper personal data, proprietary financial and vendor data, and product and services development data all are vulnerable. Data breach investigations reveal that the vast majority of attacks—70% from 2013 to 2015— were done via the Point of Sale (POS). This is true despite the fact that 100% of the top retail data theft victims reported that they were in compliance with PCI standards.

The new realities of retail data security delivery make protecting the POS while delivering the critical data the organization needs to improve its operations and meet its customers’ needs more challenging than ever before. Mobile payment has become the norm, and new mobile POS payment methods are emerging all the time. POS systems—even those that are PCI compliant— feature multiple “open” USB ports that make it possible for malware to enter the system via peripherals, and most POS deployments do not lock the BIOS or encrypt the hard drive. Furthermore, a new world of industry partnerships means that retailers are sharing inventory and information across multiple channels.

For cybercriminals, these new realities translate to new opportunities. For retailers, they mean that PCI and EMV—while a critical starting point—are not enough. Retailers can pass their most recent PCI assessment and still be breached—don’t confuse being compliant with being secure. Securing the POS requires an end-to-end security strategy.
**Business Drivers and Desired Outcomes**

- Break the data breach cycle with a protect-detect-correct approach and security tools that work in unison.
  - Prevent attacks from becoming formal breaches either by keeping sensitive data out of vulnerable hardware or by detecting and blocking via deployed countermeasures.
  - Find attacks that were not prevented via an iterative process of hunting, assessing scope and impact, and prioritizing.
  - Remediate any attack quickly; restore normal operations; and report impact.
  - Adapt countermeasures to prevent similar attacks in the future.

- Minimize the time between breach and detection and between detection and remediation.

- Integrate new security solutions seamlessly into existing systems.

- Make better strategic decisions with real-time data that enables right-time insight and analysis.

- Scale up or down with hardware-enabled security platforms.

**Digital Transformation and Business Innovation**

As traditional attacks on applications give way to malware that implants below anti-virus software, threats are becoming harder to find and more persistent. To protect against them effectively, retailers need security solutions embedded deeper in the platform. This begins with the recognition that security is no longer an option or an afterthought that can be addressed through software. Security is critically important and should be designed into the platform from the ground up. What is needed is a shift towards a hardware-enabled model where security is an integral part of the entire end-to-end solution and goes all the way down to the chip level of all endpoints. Built-in security technologies can help secure personal data and credit/debit card information from the moment a transaction is initiated all the way through to the storage of the encrypted information in the retailer datacenter and bank server networks.

**Enabling Transformation**

Protecting sensitive data in today’s environment requires a connected, end-to-end solution that enables retailers to block attacks, keep sensitive data out of vulnerable hardware, isolate breaches when they occur, and limit the impact on customers and brand. Starting with the POS, Intel® Data Protection Technology for Transactions (Intel® DPT for Transactions) brings forward an end-customer, policy-based approach to securing both personal data (loyalty program, insurance information, age verification data, etc) and credit/debit card information traveling through transaction networks. With Intel DPT for Transactions, sensitive data is routed away from vulnerable hardware, retailer transaction network updates and changes are automated, POS station equipment authentication and asset tracking are managed electronically and transaction data is available to the retailer in real time. (Figure 1).

---

**Figure 1. Intel® Data Protection Technology for Transactions: Advanced Protection for Consumer Information.**
Key components of enterprise architecture for the new POS include (Figure 2):

1. More secure, flexible local store transactional operations.
2. More secure, flexible data center business systems.
4. No matter the source, the payment portion of the POS functionality, the actual transaction is serviced via secure connection to a common payment service provider.
5. Linkage to cloud-based SaaS business components to support the data center.
6. Linkage to cloud-based SaaS applications to support the store.

Intel’s security-by-design approach can help retailers reach that optimized, end-to-end state to protect customers, data and infrastructure—from POS to data center to event management:

1) Security software solutions, such as Intel Data Protection Technology for Transactions, take an active role in security, providing below-the-OS protection—at the point of sale and throughout the POS system—for transactions initiated on peripherals. Retailers can move encrypted information through the system without leaving sensitive data behind in the POS’s memory or in other hardware elements that are vulnerable to breach. Policy-driven transaction management software enables access to useful transaction information. Working together, these solutions help retailers defend against attacks and maintain control over sensitive data.

2) Hardware-enabled security built in at the chip level helps POS processes start secure, run secure and stay secure. These technologies provide secure access to enterprise resources and protect payment card data in motion and at rest. Should a breach occur, built-in anti-malware features accelerate detection while remote management capabilities enable rapid patching and recovery.

3) New security solutions and ecosystems enable the retail industry not only to innovate, to develop security posture against targeted cyber-attacks, but to be better orchestrated for enhanced efficiency and profitability.

**Intel Recommendations for Best-in-Class Retail Endpoint Security**

**Deploy whitelisting technology**

Built-in application whitelisting and change control technology, such as McAfee Integrity Control, improves anti-malware protection by locking down devices, protecting against unauthorized malware and changes that could take a system offline, negatively impacting your customers’ experience and your reputation. With security integrated into your device, you avoid incidents that can result in high maintenance and service costs, such as:

- Zero-day attacks
- Unauthorized software changes that impact system availability
- High partner support costs related to device security problems
- Frequent, costly OS patching
- High field maintenance costs tied to unauthorized changes
Use strong encryption practices to protect data at rest and in motion

- Specify self-encrypting drives such as Intel® Solid State Drive for your endpoint devices like POS, self-serve kiosks, vending machines, etc.
- Enable full disk encryption with network-based pre-boot authentication and management with McAfee® Drive Encryption and McAfee ePolicy Deep Command.

Streamline security management

Enable Remote Access and Power On with Intel® Active Management Technology powered by Intel® vPro™ technology.

Deploy KVM visibility and remote management to facilitate timely updates and ensure greater device resiliency.

Easily monitor, manage, and maintain large, globally dispersed deployments of embedded devices with McAfee® ePolicy Orchestrator® (McAfee® ePO™) software which also provides dashboards and reports to help you meet compliance requirements. McAfee Embedded Control delivers integrated, closed-loop, real-time compliance and audit, complete with a tamper-proof system of record for authorized activity and unauthorized attempts.

Protect IO ports

Data Loss Prevention (DLP) solutions including MSFT Device Guard* and McAfee Device Control are effective in providing the needed protection of USB ports.

- Centrally deploy and manage security policy to protect POS and prevent confidential data loss
- Complete content-aware and context-aware device-blocking capability
- Control how users exchange data with external removable media devices or peripherals
- Regulate how users exchange data with external devices

Enable Secure Boot & deploy BIOS password management

Helps resist below-the-OS attacks and tampering of BIOS settings, boot loaders, key operating system files, and unauthorized option ROMs.

Lock down the BIOS by enabling BIOS password. Use security management software such as McAfee ePO Deep Command to manage and change BIOS passwords periodically.

Deploy Intel® DPT for Transactions

Provides below-the-OS protection of retail transactions including payment and personal identifiable information. Works to prevent sensitive personal and payment data from entering hardware vulnerable to breach as well as streamlines deployment and management of trusted payment peripherals.

Deploy multifactor authentication

Provides HW-enabled, secure access to enterprise resources and helps protect login credential theft.

Intel® Identity Protection Technology includes a multifactor authentication framework to allow consumers to easily log in to their cloud-based accounts and enterprises.

Intel Technology Foundation

Intel has pioneered retail technologies, connectivity and security solutions and has powered the innovative POS devices that are enabling transformation of the retail industry today.

- Intel® Core™ vPro™ Technology
- Intel® Data Protection Technology for Transactions
- Intel® Authenticate Technology
- McAfee® Integrity Control
- Intel® Software Guard Extensions (Intel® SGX)
- Intel® Active Management Technology
- McAfee® ePolicy Orchestrator® (McAfee® ePO™)
- McAfee® Device Control
- Intel® Solid State Drive
- Open Network Insight Software
- Intel® Identity Protection Technology
- McAfee® Data Loss Prevention
- McAfee® Network Security Platform
- Intel® Platform Protection Technology with OS Guard
- McAfee® Application Control
- VirusScan® Enterprise Software
- McAfee® Host Intrusion Prevention
- Intel® Trusted Execution Technology

For more information about building a stronger, more optimized security posture, visit Intel.com/retail/transactionsecurity