Security and PCI Compliance for Retail Point-of-Sale Systems

In the retail business, certain security issues can impact customer confidence and the bottom line—regulatory penalties, breaches, and unscheduled downtime. Retailers know they need to address these issues, but the security solutions they deploy cannot come with increased labor costs and require system or network upgrades. In fact, the ideal security solution should accomplish quite the opposite: it needs to extend the ROI of the existing IT infrastructure. McAfee is able to offer a comprehensive approach to securing retail store point-of-sale (POS), also know as point-of–service, and back-office solutions across various platforms, regardless of whether those platforms are legacy, end-of-life (EOL), or recently purchased. Our solutions are equally effective in environments where network bandwidth is constrained, purpose-built POS and back-office systems have limited resources, and frequent patching and updates are not an option.

McAfee solutions expand beyond retail stores, integrating a comprehensive security strategy for the entirety of the retailer's IT infrastructure, including stores, main offices, and supply chain assets across desktops, servers, network devices, and data. McAfee achieves this by combining several core aspects of security, including discovery, management, threat intelligence, protection, monitoring, response, and audit within comprehensive solution suites. McAfee can also work with existing qualified security assessors (QSAs) and/or offer consulting services and its own QSAs to help deploy and customize a personally crafted solution efficiently and effectively.

Unique Retailer Requirements

Retail IT infrastructure is complex and distributed. It includes stores with POS checkout terminals, self-check units, cash drawers, information/web kiosks, PCs, and back-office servers. These systems are generally connected to a main office, which includes desktops, servers, network devices, and data. In addition to the retailer's operational environment, there are increasing IT dependencies on supply chain relationships, ranging from wholesalers and distributors to manufactures and suppliers.

Retail organizations are concerned about striking a balance between reducing risks, reducing costs, and delivering optimized security to their constituents and customers. At the same time, they also want to improve the customer experience, reinforcing brand identity, generating customer loyalty, and increasing sales. There are two areas that make this balance particularly challenging for retailers—compliance mandates and today's resource-constrained retail environment.

- Compliance mandates:
  - » PCI DSS
  - » PCI-related state legislation (Nevada, Washington, and Minnesota)
  - » The European Union Privacy Directive
- Today's resource-constrained retail environment:
  - » Newer POS systems have the power, extensibility, and vulnerabilities of a PC
  - » Legacy and EOL systems are still very common and are needed to keep critical systems and services available while maintaining security
  - » Downtime must be minimized, and patches and updates are difficult across all retail stores
  - » Resources remain constrained in terms of IT staff, system resources, and network bandwidth

Mandates

Problem

Retailers must be able to demonstrate PCI compliance within their stores across all IT systems that store, transmit, or track credit card data. This generally includes POS and back-office systems. Failure to comply with PCI requirements can result in penalties or sanctions from members of the payment card industry. In addition to PCI, there are several states with PCI-related legislation, and the European Union Privacy Directive has many controls that overlap with PCI requirements as they relate to the storage and transmission of credit card information. These mandates taken collectively amplify the need for retailers to be able to demonstrate compliance.

Solution

Purpose-built security solutions for retail store environments from McAfee are focused specifically on security controls, reports, and dashboards for POS, back-office systems, and related in-store systems. McAfee integrity control solutions provide the security controls and reports for demonstrating compliance with PCI sections 10.5.5 and 11.5, which specify the use of file integrity monitoring. These integrity controls also help address other sections within PCI, including 1, 2, 6, and 8. Because many retail environments can't run anti-malware solutions on their in-store systems, McAfee solutions can act as a compensating control for PCI anti-malware requirements which has been accepted by QSAs.

McAfee also has partnerships with log management companies and database security companies. Log management is another PCI requirement relevant to in-store operations that is applicable to PCI sections 1, 2, 6, 7, 8, 10, and 11. Databases are common within retail store back offices and tend to contain the most sensitive data. PCI controls for databases are relevant to PCI sections 3 and 11.

Those areas directly supported by McAfee® Integrity Control software, as well as McAfee partners for log management and database security, are highlighted in the following PCI DSS requirements table. While the solutions outlined here are specific to the retailer's in-store environment, McAfee has a complete range of IT security and compliance solutions and services that work together to address every PCI requirement across the retailer's stores, main office, and supply chain. McAfee also has consulting services with QSAs that can help design, deploy, and manage solutions for even the most complex retail environments and put in place solutions that will demonstrate PCI compliance while reducing risk, reducing operational expenses, and maximizing IT asset ROI.

PCI DSS Requirements	McAfee Integrity Control	McAfee Log Management Partners	McAfee Database Security Partners
1: Install and maintain a firewall configuration to protect cardholder data	✓	✓	
2: Do not use vendor-supplied defaults for system passwords and other security parameters	✓	✓	
3: Protect stored cardholder data			✓
4: Encrypt transmission of cardholder data across open, public networks			
5: Use and regularly update anti-virus software			
6: Develop and maintain secure systems and applications	✓	✓	
7: Restrict access to cardholder data by business need-to-know		✓	
8: Assign a unique ID to each person with computer access	✓	✓	
9: Restrict physical access to cardholder data			
10: Track and monitor all access to network resources and cardholder data	✓	✓	
11: Regularly test security systems and processes	✓	✓	✓
12: Maintain a policy that addresses information security			

The Modern Retail Environment and Resource Constraints

Problem

Retailers are upgrading their POS to take advantage of add-on modules that promise the building of stronger ties to the consumer at the point of checkout. Not wanting to fall behind the competition in terms of features and functions and needing the broadest possible application support, retailers are moving to commercially popular operating systems and applications.

As purpose-built solutions, these POS systems and the back-office systems that reside at the remote stores are often resource constrained. They often have dial-up or low bandwidth connectivity to regional or main offices, and that bandwidth is primarily reserved for business operations, backups, pricing updates, new applications, order fulfillment, marketing pattern analytics, and other retail functions. These stores do not have local IT support and, generally, the retailers have such limited IT resources that they depend on third-party contractors to perform hands-on IT activities as needed. This results in an environment that is not well suited to downloading and installing patches for core operating systems, critical applications, or anti-malware .DATs. With a desire to get the most ROI out of their initial POS investment while at the same time achieving the benefits that today's solutions offer, many retail environments will also have a mix of current solutions with existing, legacy solutions—each with its own risks.

Solution

McAfee solutions for in-store retail operations:

- Are not scan based, so they are not system resource intensive
- Do not require .DAT downloads, so they are not network intensive and do not require frequent updates
- Can be deployed and managed centrally by leveraging McAfee management solutions, reducing demands on IT staff
- Can run on multiple platforms, including Microsoft Windows XPe (embedded), which cannot run traditional anti-malware
- Reduce patch cycles for operating systems and applications and extend the life of legacy/EOL systems
- Provide a broad range of protections from zero-day vulnerabilities and targeted malware to dynamic whitelisting authorized executables (drivers, Java, binaries) and blocking unauthorized user or browser installs
- Prevent malware from being installed through USB access

- Prevent the installation and propagation of unapproved software
- Prevent changes by unauthorized users
- Provide visibility into changes across all POS and back-office systems

While the most pressing area of focus for retailers remains stores, retail infrastructures, are, of course, much more than this. As shown in Figure 1, retailers also have complex main offices leveraging mission critical assets from accounting controls and enterprise resource planning (ERP) to loss prevention and replenishment. They also depend on interconnected supply chain management systems with suppliers, warehouse operations, and the like. The complexity, criticality, and sensitivity of these environments are similar to those found in the financial industry and even government agencies. Unfortunately, in comparison, retailers generally have much smaller IT staffs to manage their environments because of the thin margins.

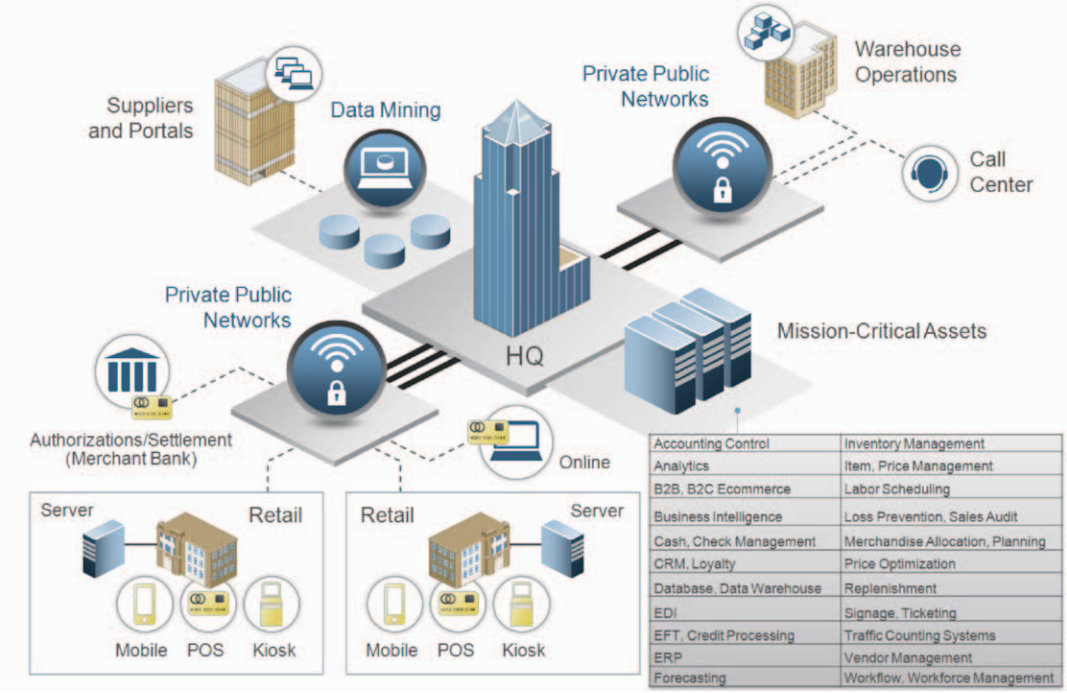

Figure 1. Interconnected retail environment.

McAfee is unique in its ability to offer products, services, and added value through partnerships to address the complete spectrum of retailer needs across various mandates and security requirements. This is achieved by combining several core aspects of security, including discovery, management, threat intelligence, protection, monitoring, response, and audit within comprehensive solution suites. McAfee solutions allow retailers to lower risk, reduce operational costs, demonstrate compliance, and maximize IT infrastructure ROI, so that retailers can focus on the business of doing business without additional staff or changes to systems or networks.

For more information about McAfee solutions for security and PCI compliance for retail POS systems, please visit: www.mcafee.com/pci.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

9625brf_retail_0710_ETMG