SECURE YOUR POINT-OF-SALE (POS) SYSTEMS

Lock down point of sale/service (POS) systems
Lock down point of sale/service (POS) systems

The Situation
So convenient to use. So easy to abuse. Point of sale/service systems support every purpose from warehouse inventory to retail price checks to mini-ATM machines. Although each device typically has an active connection into corporate data systems—enterprise resource planning applications, customer account data, sales databases—these devices have poor protections against physical attack and system compromise. Poorly tested software updates can crash a device. In addition, if the network umbilical cord to the mother ship uses Wi-Fi, it is possible to break into the device, or sniff traffic for unencrypted data and weak network access controls.

While many organizations are trying to extract as much value as possible from existing fixed-function POS systems, other groups are moving to new devices running on general purpose (and vulnerable) PC operating systems. In either situation, standard AV and security controls are too cumbersome and complex for typical retail and point of service situations with limited compute resources and local IT expertise. Especially if your organization is thinking of new ways to employ POS systems—perhaps to enable custom production or just-in-time distribution—you have to get in front of these risks.

Driving Concerns
With their high utilization, specialized features, far-flung locations, and undertrained employees, retail POS kiosks and handheld devices take constant abuse. They are (mis)handled by multiple people (both employees and customers), serviced infrequently and with difficulty, and sit out in the open, exposed to malware, viruses, and other attacks. For instance, an uncontrolled USB port is a simple way to introduce a keylogger or remote administration tool. Alternatively, a replacement mouse with a malicious microcontroller could be used to capture credentials and break into the corporate network. In addition to the loss of confidential and regulated data that requires costly cleanup and embarrassing public disclosure, you face the loss of productivity and sales revenue if a device crashes or must be taken out of service.

Organizations need to wrap these POS endpoints in strong security, just as you would a laptop carrying a customer database or a cash register full of sales data and cash. However, limited budgets and compute resources, atypical attack vectors, and remote operational models mean these devices require specialized protection—not just off-the-shelf antivirus. POS security tools must respect and serve unique POS requirements:

- **Limited CPU and memory resources.** Installed on a fixed-function POS system, traditional processor-intensive antivirus software can overload the CPU during basic scanning. This monopolization of resources interferes with the intended purpose of the POS device. Without malware protection, criminals are able to attack the memory in these devices with buffer overflows, heap overflows, stack execution, and other exploits. These exploits allow criminals to overwrite functions and manipulate the device and its data. The system also has few resources to offer up to logging and audit activities that might help support security processes. Newer POS devices built on full-featured PCs provide more resources for security, but also introduce more vulnerabilities and related patching overhead.
• **Poor connectivity and maintenance hurdles.** Field, store, and shop floor devices may not have the connectivity, bandwidth, and service models to receive updates that maintain security protections, such as regular DAT updates for new malware. Devices typically go unpatched longer than other enterprise devices, meaning they are more susceptible to attack. Since remote and field sites often lack technical experts capable of detecting, diagnosing, or repairing a problem, any issue that needs more than a reboot could take days to fix. Further, even when a service call or over-the-network remediation is possible, vendors may have discontinued support for older (legacy) systems, so no patch will ever be available.

• **Gold image or baseline configuration drift.** Over time, these systems can drift from their approved baseline build. Whether it’s from falling behind on updates, introduction of new code, or change in configuration, baseline drift can introduce security weaknesses that can be exploited.

• **Physical compromise.** Unlike traditional high-value endpoints protected with layers of security—physical safeguards, encrypted hard drives, access and device controls, network segmentation, and gateway security systems—these POS devices are very accessible to criminals and malicious (or inept) insiders. Anyone with hands-on system access can attach portable storage and other peripherals that introduce malware directly into the system. If the device retains or processes data, that data can be sniffed, downloaded, and stolen.

• **Network-based compromise.** Wireless networks remain a security soft spot. Criminals can use poor wireless security to break into POS devices to install a worm or keylogger or take over device operations through a memory operation like a buffer overflow. With a criminal controlling the device, any data processed by it is at risk.

• **Poor accountability and compliance.** Many point-of-service systems such as ATMs, POS terminals, and kiosks are in scope for meeting PCI DSS compliance. Any personal data they process needs to be protected for compliance with privacy laws. Yet these devices are handled by many people over different shifts. In the event of a compromise or loss it may not be possible to figure out what happened, and if it was a deliberate or malicious act. Value-added resellers or supply chain relationships complicate audit trails that might explain what was done, by whom, when. If you don’t know what happened, you can’t be sure you have cleaned up the problem, or prevented its reoccurrence.

**Solution Description**

To secure POS devices, McAfee suggests locking down the software that can run on the device, blocking data theft, configuration changes, and compromise. In this model, instead of using bulky scanners to respond to the introduction of malware, you proactively restrict the software on the device to the functions that you have tested and approved, preventing malware from executing. Of course, some maintenance and update functions are necessary, and these should be tightly controlled, too.

• **Low CPU and memory resource utilization.** The security software (controls and logging) should consume a minimal portion of the resource footprint of fixed-function devices to operate without impairing the primary function of the device. For example, memory and CPU utilization should be minimal as compared to antivirus software. The software should run on multiple platforms to allow compatibility with the installed base of devices, including legacy platforms.

• **Offline operation and whitelisting.** The security solution should work without a network connection, so that locations connected by intermittent and low-bandwidth networks are not left unprotected when the network is unavailable. By locking down a trusted image to an approved whitelist, the security controls should be active and effective without dependency on software and signature updates. This “golden master” baseline should protect the devices in both zero day situations and where patches are no longer available.

• **Gold image or baseline drift.** A solution should prevent systems from unintentional change in code, configuration, or updates that could cause a system to drift from a known good or gold image. This is imperative to ensure expected operation as well as helping with auditing and compliance reporting.
• **Protection against direct physical compromise.** The solution should prevent execution of any unapproved software, including malware, keyloggers, or device drivers for new accessories.

• **Protection against network-based compromise.** The solution should prevent attackers taking over the POS device via the network, exploiting the system or its memory.

• **Clear accountability and compliance.** The system should only permit updates by approved users. It should also maintain precise, detailed audit trails of changes and change attempts. Reports should make it easy to track down the root cause of issues and be specific enough—users, times, activity sequence—to be actionable in educating users on policy or providing evidence in the case of wrongdoing.

**Technologies Used in the McAfee Solution**

Traditional blacklisting approaches such as antivirus scanning are too resource-intensive and signature-dependent to work well in the constrained point of service environment. McAfee has integrated application whitelisting, file integrity monitoring, and change management solutions into a single “deploy and forget” solution optimized for POS devices. McAfee® Embedded Control provides broad visibility into changes as well as tight control over attempted changes to ensure that POS devices remain up and running and free of malware. It is a low footprint, low overhead software solution that runs transparently, without the disruption and updates of file system scanning.

McAfee Embedded Control automatically creates a dynamic whitelist of the “authorized code” on the POS system. Once the whitelist is created and enabled, the system is locked down to the known good baseline. No program or code outside the authorized set can run, and no unauthorized changes can be made. McAfee Integrity Control—which combines McAfee Embedded Control and the McAfee ePolicy Orchestrator® (McAfee ePO™) console—provides integrated audit and compliance reports to help you satisfy multiple compliance regulations.

While preventing execution of unauthorized code—untested patches, scripts, malware, unapproved applications—it also ensures that authorized code cannot be tampered with by preventing changes to selected files, directories, and registry keys. For this reason, vulnerabilities in authorized code cannot be exploited, so the device is safe even when it is unpatched. This benefit is crucial to the security of frontline POS devices and may be the only reliable protection for systems running legacy software.

Memory control protects running processes from malicious hijacking. Unauthorized code injected into a running process is trapped, halted, and logged. This way, attempts to gain control of a system through buffer overflow, heap overflow, stack execution, and similar exploits are rendered ineffective and are logged.

Authorized updating mechanisms allow granular and selective change control by trusted updaters. For example, Windows patches might be approved automatically, whereas changes to the inventory application will be prevented from executing. Authorized updating can occur by opening an update window and authorizing a user or application to make changes. In addition, it tracks any authorized changes in real time, allowing automatic and accurate monitoring and reporting of actual changes. It provides visibility into the sources of changes and verifies that changes were deployed onto the correct target systems. Protection is linked directly to policy, and changes are verified against the change source, time window, or approved change ticket. Changes that are attempted outside of policy are not allowed and attempts are logged. In the event of forensic investigation, activity monitoring can easily identify the time and source of changes, files that were changed, and the user logged in to the system at that time.
5
Securing POS Systems

Figure 1. McAfee enforces whitelists and blacklists to directly manage execution of software on the POS device.

Figure 2. Enterprises can manage the security of a variety of POS systems using the familiar McAfee ePO console.
McAfee Integrity Control
For organizations like enterprises that need to manage POS systems alongside other enterprise infrastructure, McAfee Integrity Control integrates McAfee Embedded Control with McAfee ePolicy Orchestrator (McAfee ePO) software. This configuration eases agent deployment, management, and reporting and provides continuous information about change events across the point-of-service infrastructure, which includes where the change was made (which server/servers), when it was made (time), which user made the change, how the change was made, what content inside the file changed, and whether the change was approved. This deep level of visibility into the point-of-service environment is delivered through the McAfee ePO platform and enables you to continuously verify the security of POS systems, validate compliance to auditors, and document evidence and an audit trail in the event of a breach.

The single McAfee ePO console also lowers the cost of ownership by consolidating fixed-function device security and compliance management. This saves IT organizations hardware, training, and operational costs, and provides unified control over the policies and protections on each enabled ATM, kiosk, or POS system. You can monitor the authorized changes and correlate them with change requests in Remedy, which allows proof of due diligence and due care in audit processes required by PCI and ISO 27002.

Impact of the Solution
Deploying McAfee Embedded Control (or McAfee Integrity Control with McAfee ePO) provides a way to ensure the software running on your POS devices is software that you approve and trust. When you are ready to update these systems and expand their features, you have a controlled, predictable production environment.

These McAfee solutions help security controls live within the challenging climate of POS environments. Consuming just 15-20 megabytes of system memory and less than one percent of the CPU, even older fixed-function systems can accommodate the software footprint. Since it does not require signature updates, this proactive approach provides comprehensive protection in both connected and disconnected environments. It eliminates emergency patching and reduces the number and frequency of patching cycles, allowing testing and validation and reducing risk for hard to patch POS devices.

Locking down the system protects devices against both physical and network-based compromise and prevents the configuration from drifting off the approved baseline. Unapproved software cannot execute on the device, and device integrity, memory, and data cannot be compromised through direct or drive-by access to the system.

To help with audits and accountability, McAfee Embedded Control integrates closed-loop, real-time compliance and audit with a tamperproof system of record for the authorized activity and unauthorized attempts.
Q&A

How are applications added to the whitelist?
Applications are added to the dynamic whitelist during the solidification process, which takes an initial snapshot of the software implemented on a system and creates an inventory of program code.

What types of executable files can be whitelisted?
McAfee Embedded Control can whitelist a wide variety of files including binary executables (such as .exe or .dll), and scripts (.bat, .cmd, and .vbs) for the Windows platform and binary executables (elf format) and scripts (containing #!) for supported local file systems for UNIX platforms.

Can the user disable the whitelisting function?
McAfee Embedded Control runs in memory as a kernel driver below the User Mode of the operating system. By running in this memory space, the user is denied the ability to disable the application code protection and memory protection.

Does the solution have canned industry regulatory reports such as PCI?
McAfee Embedded Control solution ships with more than 25 predefined queries. Many of these reports are designed with standard regulations such as PCI in mind. Existing reports can easily be modified or used as templates for new custom reports. All reports can be scheduled and emailed to business stakeholders in HTML or PDF format.
Additional Resources
www.mcafee.com/embedded
www.mcafee.com/integritycontrol
www.mcafee.com/epo
www.mcafee.com/kb
www.mcafee.com/gti

For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author
Joe McMahon is an enterprise solutions architect for McAfee. Joe provides technical direction, training, and support to enterprise, education, and government customers worldwide. He also assists with project scoping, solution selection, proof-of-concept pilots, and production implementation for McAfee application control and change control products.

Joe has 18 years of IT experience and holds a bachelor’s degree in Information Systems Management from Eastern Michigan University. Joe specializes in enterprise information security and compliance and has worked at leading-edge technology firms such as IBM and Lockheed Martin prior to coming to McAfee. Areas of specific focus include network management, endpoint and server security, policy compliance auditing, and risk assessment.