SECURE YOUR ATMs
Protect automated teller machines against attacks and noncompliance
Protect automated teller machines against attacks and noncompliance

The Situation
It is easier to steal from a bank electronically than physically. Imagine if you had to send a letter to all affected customers stating that they couldn’t access their funds due to a security breach. Would that drive your customers away? How would an attack or compromise of your automated teller machine (ATM) system change your PCI audit burden and budget?

Barnaby Jack shook the ATM industry when he caused an ATM to spew its entire reservoir of cash across the stage in Las Vegas during the 2010 Black Hat Conference. Since that hack, the affected ATMs have been updated. However, known and new vulnerabilities can allow similar payoffs, as well as data loss, account theft, and system downtime.

Driving Concerns
Because ATMs process both financial and personally identifiable data, they attract both criminals and regulators. Criminals attack vulnerabilities in the ATM software, and regulators (both industry and government) layer restrictions and audit requirements on the ATM supply chain.

ATMs are vulnerable because they are both high-tech and low-tech. Sophisticated ATM systems handle deposits, withdrawals, account services, cash advances, and payment processing. While advanced features are great for customers, they require new code and PC-class systems. New code invariably brings new vulnerabilities that criminals can target. PC-class systems offer a large attack surface.

At the low-tech end, many ATM systems have very limited resources for running security software or other technical controls. They aren’t easy to service and are optimized for rough handling rather than avid hackers.

ATM vulnerabilities must be addressed in system design and implementation to ensure that your customer data and your ability to service their needs are not affected. Effective ATM security must compensate for:

- **Limited CPU and memory resources.** Most ATM systems have minimal memory and CPU processing power. Processor-intensive security software such as antivirus (AV) can create a CPU overload, where resource utilization on the ATM system is taxed to the limit just for AV scanning. Standard solutions based on logging and alerting may slow down processing and impair the user experience or prevent the collection and distribution of money and information.

- **Targeted attack vectors.** The trend in ATM devices is to build on a customized version of Microsoft Windows. Advanced malware targets these devices and cannot be detected using standard AV programs.

- **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.

Security Connected
The Security Connected framework from McAfee enables integration of multiple products, services, and partnerships for centralized, efficient, and effective risk mitigation. Built on more than two decades of proven security practices, the Security Connected approach helps organizations of all sizes and segments—across all geographies—improve security postures, optimize security for greater cost effectiveness, and align security strategically with business initiatives. The Security Connected Reference Architecture provides a concrete path from ideas to implementation. Use it to adapt the Security Connected concepts to your unique risks, infrastructure, and business objectives. McAfee is relentlessly focused on finding new ways to keep our customers safe.
• **Operating system security patch updates.** Due to the distributed locations of these devices and their often nonstop operation, patches are difficult to implement, and are seldom performed on an emergency basis. It’s more efficient (but less safe) to upgrade at planned intervals after updates and patches have been tested and verified. When a critical security patch is shipped by a vendor (like Microsoft) organizations are faced with trading off security risk for revenue.

• **Poor accountability and compliance.** ATMs run payment applications and process cardholder data, making them subject to PCI DSS regulations. Yet these devices are handled by multiple people over different shifts. In the event of a compromise, it may not be possible to figure out what happened, and if it was a deliberate or malicious act. Value-added relationships complicate audit trails that might explain what was done, by whom, when. If you don’t know what happened, you can’t scope the loss, reassure auditors you have cleaned up the problem, or prevent its reoccurrence.

• **Management complexity.** These devices are often managed using specialized processes outside standard IT security operations, which adds a layer that can delay protection, complicate incident response, and add to the cost of compliance.

**Solution Description**

To address the unique challenges of the ATM environment, the heavy footprint of traditional security solutions must be replaced by an approach that operates within the limited resources of an ATM system and service model. McAfee recommends a whitelisting model to proactively restrict the software on the device to the baseline functions that you have tested and approved, preventing malware and unapproved software from executing. Maintenance and update functions can be tightly controlled and documented for accountability and proof of compliance.

• **CPU and memory resource utilization.** A whitelisting approach can drastically reduce the security software footprint on an ATM system. The reason for this is a complete shift in how the technologies work. In a standard AV environment, one must be concerned about the infinite and ever-evolving threats in the wild. As threats are discovered and protection mechanisms developed, a new signature needs to be added to the ever-increasing library on every system. This process repeats every day until it becomes unsustainable for ATM systems. A whitelisting approach, however, is only concerned about what is truly allowed to run for the device to function. This list is finite and does not need to be updated unless new functionality is required, providing greater protection at a fraction of the system resources.

• **Attack vectors.** A whitelisting approach will only allow code that has been designated as trusted to run. New malware or executables that have not been granted rights cannot execute.

• **Gold image or baseline drift.** Whitelisting should protect systems from unintentional changes in code or configuration, as well as updates that could cause the system to drift from a known good or gold image. This predictability is imperative to ensure expected operation as well as enable auditing and compliance reporting.

• **Operating system security patch updates.** A whitelisting approach will allow your organization to patch on your schedule and not that of the vendor. Since whitelisting prevents new malware from running, it provides a window of protection. Administrators have time to test new patch sets thoroughly before applying them.

**Decision Elements**

These factors could influence your architecture:

• What process do you use for ATM software updates?
• Do you manage ATM devices centrally or as standalone systems?
• What change management processes do you currently follow?
• Do you have different types of administrator roles?
• Are any of your devices or their applications subject to PCI regulations?
• Does your ATM connect directly to the Internet for data transmission?
• Is your ATM system connected to a wireless network?
• Is your ATM environment patched on a regular basis?
• **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.

• **Management complexity.** A security solution for ATM devices must be integrated into the broader security and compliance management platform and existing processes. This consistency facilitates policy management, continuous compliance, incident response, auditing, and reporting for PCI. Integrated reports and dashboards improve monitoring and reduce the cost of operations.

**Technologies Used in the McAfee Solution**

McAfee has integrated application whitelisting with other important controls—file integrity monitoring and change management—into a single “deploy and forget” solution optimized for ATM devices. McAfee® Embedded Control provides tight control over attempted changes as well as broad visibility into changes to ensure that ATM devices remain up and running and free of malware. It is a low footprint, low overhead software solution that runs transparently, without the heavy resource utilization, disruption, and constant updates of traditional file system scanning.

McAfee Integrity Control—which combines McAfee Embedded Control and the McAfee ePolicy Orchestrator® (McAfee ePO™) management console—provides integrated audit and compliance reports to help you satisfy PCI and other compliance regulations. This environment connects your ATM security into your broader security management infrastructure, eliminating duplication and reducing management complexity.

![Diagram](image.png)

Figure 1. A centrally managed whitelisting approach can reduce the attack surface of ATM systems.
McAfee Embedded Control
For McAfee embedded partners, McAfee Embedded Control automatically creates a dynamic whitelist of the “authorized code” on the ATM system. Once the whitelist is created and enabled, the system is locked down to the “golden master” baseline. No program or code outside the authorized set can run, and no unauthorized changes can be made. 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 ATM 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. The software protects against remote and local memory-based attacks in three unique ways:

- Critical address space protection prevents any code running in non-code areas from making API calls such as CreateProcess and LoadLibrary. This is a non-intrusive, yet very effective, way of dealing with shellcode running from a non-code area.
- API mangling obfuscates API names, hence malware will not be able to execute
- By randomizing stack and heap addresses and DLL rebasing, the software makes it harder for malicious code to find a way in

Malware and zero-day attacks are unlikely to be able to bypass all three forms of memory protection.

Authorized updating mechanisms allow granular and selective change control by trusted updaters. For example, Windows patches might be approved automatically, whereas changes to the credit card authorization 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, McAfee Embedded Control tracks any authorized changes in real time, allowing automatic and accurate monitoring and reporting of actual changes. It provides visibility into the sources of change 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 audit or 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.
McAfee Integrity Control
Some organizations, especially enterprises, may prefer to purchase McAfee Integrity Control, which includes McAfee Embedded Control integrated with the McAfee ePolicy Orchestrator (McAfee ePO) management platform. This configuration eases agent deployment, management, and reporting and provides continuous information about change events across the ATM infrastructure. Details include 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 ATM environment is delivered through the McAfee ePO platform and enables you to continuously verify the security of ATM systems, validate compliance to auditors, and document evidence and an audit trail in the event of a breach.

Figure 2. Enterprises can manage the security of ATMs using the familiar McAfee ePO console.

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 ATM 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. You can:

- Identify the running application on the ATM systems and compare to the gold image to detect deviation
- Protect ATM systems from remote (drive by attacks) and local exploits
- Prevent unauthorized changes and applications from executing
- Support accountability and audits by identifying the time and source of changes, files that were changed, and the user logged in to the system at that time
- Implement and automate a change management process, patching systems automatically through an approved source of change without any human intervention
- Defer patching until software is fully tested without compromising on security
- Manage, monitor, and report on the ATM environment alongside other enterprise security

**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 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/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.