McAfee Embedded Control—Retail

System integrity, change control, and policy compliance for retail point-of-sale systems

McAfee® Embedded Control for retail maintains the integrity of your point-of-sale (POS) systems, kiosks, or other embedded systems by only allowing authorized code to run and authorized changes to be made. It is the cost-effective, quick-to-deploy software solution that resolves software security, change control, and compliance issues for the lifetime of your retail system.

Key Advantages

McAfee Embedded Control enables retailers to maintain the integrity of POS devices, kiosks, and other embedded systems by:

- Preventing malware through dynamic whitelisting.
- Solidifying gold standard images to make devices tamperproof.
- Auditing retail system configurations.
- Automatically unlocking systems for signed updates.

McAfee Embedded Control is a small-footprint, low-overhead, application-independent solution that provides "deploy-and-forget" security. McAfee Embedded Control converts potentially vulnerable embedded systems built on commercial operating systems into rock-solid "black boxes" to look like closed proprietary operating systems. It prevents any unauthorized program that is on a disk or injected into memory from executing and prevents unauthorized changes to an authorized baseline.

Executional Control

With McAfee Embedded Control enabled prior to product shipment, only programs contained in the McAfee dynamic whitelist are allowed to execute. Any other programs are considered unauthorized. Their execution is prevented, and the failure is logged by default. This prevents worms, viruses, spyware, and malware that install themselves from executing illegitimately.

Memory Control

Memory control ensures that running processes are protected from attempts to hijack them. 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 logged.[1]

Change Control

McAfee Embedded Control detects changes in real time and provides visibility into the sources of change by:

- Verifying that changes were deployed or attempted.
- Providing an audit trail of all changes.
- Allowing changes to be made only through authorized means.

McAfee Embedded Control enables change control enforcement by specifying the authorized means of making changes. You designate the people or processes that can apply changes, which certificates are required to allow changes, and when changes may be applied.

Change control agents are deployed on each node for which change data is needed. Those agents work in conjunction with these modules:

- Real-time change tracking module logs all changes to system state, including code, configuration, and the registry.

intel Security

Change events are logged as they occur, in real time, and sent to the system controller for aggregation and archival purposes.

- The proactive change validation module verifies each change before it is applied on target systems. With this module enabled, updates to software systems may only be made in a controlled manner.
- The system controller module manages communication between the system controller and the agents. It aggregates and stores change event information from the agents in the independent system of record (ISR).

Audit and Policy Compliance

McAfee Embedded Control and McAfee ePolicy Orchestrator® (McAfee ePO™) software—bundled as McAfee Integrity Control—provides dashboards and reports that help you meet compliance requirements. These are generated through the McAfee ePO console, which provides a web-based user interface. McAfee Embedded Control delivers integrated, closed-loop, real-time compliance and audit, complete with a tamperproof system of record for authorized activity and unauthorized attempts.

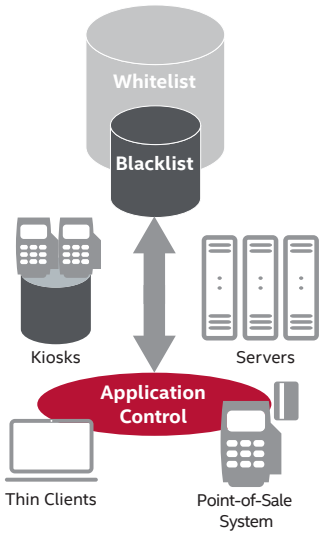

Figure 1. McAfee Embedded Control software extends a layer of protection to fixed-function devices such as kiosks, POS terminals, and legacy platforms to reduce customer risk exponentially.

The Current Retail Environment

Many of today's POS terminals, kiosks, and other retail systems are running popular Microsoft Windows, Linux, and Android operating systems. What's more, they are interconnected via Ethernet, Bluetooth, Wi-Fi, or other means. As a result, there are significant control, security, and compliance challenges.

Operational challenges

Too many people in the distribution channel have access to the inner workings of retail systems. As a result, it is difficult to enforce a validated, "as shipped" image. And yet manufacturers must still honor warranties when unauthorized changes are made.

Support challenges

Retail systems come with their own unique set of support challenges:

- Retail systems are vulnerable to existing and zero-day security threats, which are now key causes of in-field breakage or unavailability. Antivirus software is not sufficient to defend against these threats and degrades retail system performance.
- Many systems are accessed by on-site support personnel with administrative privileges for applying software updates and for break-fix support, which makes compliance auditing and assurance difficult.
- The product lifespan of retail systems can be 10 years or more. Even with a topnotch service model, it's difficult to defend against the constant barrage of threats to these older systems.
- Patching and other unauthorized changes can impede performance and affect system compliance status. Far too often, this requires putting a technician on the scene. Costs go up, and customers start looking for another vendor.

Revenue stream challenges

Several retail system manufacturers charge for adding or certifying that a new hardware, application, or utility version is compatible and can be installed on the retail system during production. However, these system manufacturers

do not have a way to enforce this other than owning the entire professional services and support role of the distribution channel.

End-customer expectation challenges
Retailers expect and deserve systems that offer high availability, regulatory compliance, and foolproof security. However, when systems are vulnerable, it is difficult for system manufacturers to satisfy these expectations.

Next Steps

For more information, visit **www.mcafee.com/embeddedsecurity,** or contact your local McAfee representative.

About McAfee Embedded Security

McAfee Embedded Security solutions help manufacturers ensure that their products and devices are protected from cyberthreats and attacks. McAfee solutions span a wide range of technologies, including application whitelisting, antivirus and anti-malware protection, device management, encryption, and risk and compliance—and all leverage industry-leading McAfee Global Threat Intelligence. Our solutions can be tailored to meet the specific design requirements for a manufacturer's device and its architecture.

Feature	Description	Benefit
Guaranteed System Integrity		
External threat defense	Ensures that only authorized code can run. Unauthorized code cannot be injected into memory. Authorized code cannot be tampered with.	• Eliminates emergency patching, reduces number and frequency of patching cycles, enables more testing before patching, and reduces security risk for difficult-to-patch systems. • Reduces security risk from zero-day, polymorphic attacks via malware such as worms, viruses, Trojans, along with code injections like buffer-overflow, heap overflow, and stack-overflow. • Maintains integrity of authorized files, ensuring the system in production is in a known and verified state. • Reduces cost of operations via both planned patching and unplanned recovery downtime and improves system availability.
Internal threat defense	Local administrator lockdown offers the flexibility to prevent even administrators from changing what is authorized to run on a protected system, unless presented by an authentic key.	• Protects against internal threat. • Locks down what runs on embedded systems in production and prevents change even by administrators.
Advanced Change Control		
Secure authorized updates by manufacturer	Ensures that only authorized updates can be implemented on in-field embedded systems.	• Ensures that no out-of-band changes can be deployed on systems in the field. Prevents unauthorized system changes before they result in downtime and generate support calls. • Manufacturers can choose to retain control over all changes themselves or authorize only trusted customer agents to control changes.
Verify that changes occurred within approved window	Ensure that changes were not deployed outside of authorized change windows.	• Prevent unauthorized change during fiscally sensitive time windows or during peak business hours to avoid operational disruption and/or compliance violations.
Authorized updaters	Ensure that only authorized updaters (people or processes) can implement changes on production systems.	• Ensure that no out-of-band changes can be deployed on production systems.

(continued)

Real-Time, Closed-Loop Audit and Compliance		
Real-time change tracking	Track changes as soon as they happen across the enterprise.	• Ensure that no out-of-band changes can be deployed on production systems.
Comprehensive audit	Capture complete change information for every system change: who, what, where, when, and how.	• An accurate, complete, and definitive record of all system changes.
Identify sources of change	Link every change to its source: who made the change, the sequence of events that led to it, and the process/ program that affected it.	• Validate approved changes, quickly identify unapproved changes, increase change success rate.
Low Operational Overhead		
Deploy and forget	Software installs in minutes, no initial configuration or setup necessary. No ongoing configuration necessary.	• Works out of the box. Effective immediately after installation. Does not have any ongoing maintenance overhead, so it is a favorable choice for a low operating expenses (OPEX) security solution configuration.
Rules-free, signature-free, no learning period, application independent	Does not depend on rules or signature databases; effective across all applications immediately with no learning period.	• Needs very low attention from an administrator during server lifecycle. • Protects server until patched or unpatched server with low, ongoing OPEX. • Its effectiveness does not depend on quality of any rules or policies.
Small footprint, low runtime overhead	Takes up less than 20 MB disk space. Does not interfere with applications' runtime performance.	• Ready to be deployed on any mission-critical production system without impacting its run-time performance or storage requirements.
Guaranteed no false positives or false negatives	Only unauthorized activity is logged.	• Accuracy of results reduces OPEX as compared to other host intrusion prevention solutions by dramatically reducing the time needed to analyze logs daily/weekly. • Improves administrator efficiency, reduces OPEX.

1. Only available on Microsoft Windows platforms.

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com

Intel and the Intel logo are registered trademarks of the Intel Corporation in the US and/or other countries. McAfee, the McAfee logo, ePolicy Orchestrator, and McAfee ePO are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the US and other countries. Other marks and brands may be claimed as the property of others. The product plans, specifications and descriptions herein are provided for information only and subject to change without notice, and are provided without warranty of any kind, express or implied. Copyright © 2012 McAfee, Inc.
35402ds_embedded-control-retail_0312B_ETMG