McAfee
An Intel Company

McAfee Embedded Control for Healthcare

A single solution for system integrity, change control, and policy compliance

McAfee® Embedded Control for healthcare maintains the integrity of your system by only allowing authorized code to run and only authorized changes to be made to a system. It automatically creates a dynamic whitelist of the "authorized code" on the embedded system. Once the whitelist is created and enabled, the system is locked down to the current, known good baseline and no program or code snippet outside the authorized set can run and no unauthorized changes can be made. McAfee secures all of the medical devices and the data on those devices routinely used in a healthcare setting.

Key Advantages

- Minimize your security risk by controlling what runs on your embedded devices and protecting the memory in those devices.
- Give access, retain control, reduce support costs.
- Selective enforcement.
- Deploy and forget.
- Make your devices compliance- and audit-ready.
- Real-time visibility.
- Comprehensive audit.
- Searchable change archive.
- Closed-loop reconciliation.

McAfee Embedded Control is a small-footprint, low-overhead, application-independent solution that provides deploy-and-forget security on embedded systems by converting a system built on a commercial operating system into a "black box" with the characteristics of a closed proprietary operating system. It prevents any unauthorized program on disk or injected into memory from executing and prevents unauthorized changes to an authorized baseline.

Assured System Integrity

Executional control

With McAfee Embedded Control enabled, only programs contained in the McAfee dynamic white-list are allowed to execute. Any other programs are considered unauthorized, their execution is prevented, and the failure is logged by default. This enforcement prevents unauthorized programs such as worms, viruses, and spyware from executing.

Memory control

Memory control ensures that running processes are protected from malicious attempts to hijack them. Unauthorized code injected into a running process is trapped, halted, and logged. Attempts to gain control of a system through buffer/heap overflow, and similar exploits are rendered ineffective, and logged.[1]

Change Control

McAfee Embedded Control detects changes in real time. It provides visibility into the sources of change and verifies that changes were deployed onto the correct target systems, provides an audit trail of all changes, and allows changes to be made only through authorized means.

McAfee Embedded Control allows you to enforce change control processes by specifying the authorized means of making changes. You may control who (people or processes) can apply changes, which certificates are required to allow changes, and when changes may be applied.

Audit and Policy Compliance

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

McAfee GTI Integration: The Smart Way to Deal with Global Threats for Air-Gap Environments

McAfee Global Threat Intelligence (McAfee GTI) is an exclusive McAfee technology that tracks the reputation of files, messages, and senders in real time using millions of sensors worldwide. This feature uses cloud-based knowledge to determine the reputation of all files in your computing environment, classifying them as good, bad, and unknown. With McAfee GTI integration, you'll know with certainty when any malware has been inadvertently whitelisted. The GTI reputation is accessible in Internet connected as well as isolated McAfee ePO software environments.

McAfee Embedded Security Addresses HIPAA Requirements

HIPAA Administrative Safeguard Requirements

- 164.308(a)(1)(i)—Security Management Process
- 164.308(a)(1)(ii)(B)—Risk Management
- 164.308(a)(1)(ii)(C)—Sanction Policy
- 164.308(a)(1)(ii)(D)—Information System Activity Review
- 164.308(a)(3)(i)—Workforce Security
- 164.308(a)(4)(i)—Information Access Management
- 164.308(a)(5)(ii)(B)—Protection from Malicious Software
- 164.308(a)(5)(ii)(C)—Login Monitoring
- 164.308(a)(6)(ii)—Response and Reporting
- 164.308(a)(8)—Evaluation

HIPAA Technical Safeguard Requirements

- 164.312(a)(2)(i)—Unique User Identification
- 164.312(b)—Audit Controls
- 164.312(c)(2)—Integrity

HIPAA Physical Safeguard Requirements

- 164.310(a)(2)(ii)—Facility Security Plan
- 164.310(a)(2)(iii)—Access Control and Validation Procedures
- 164.310(b)—Workstation Use
- 164.310(d)(2)(iii)—Accountability

Healthcare

Healthcare systems are increasingly under attack for the simple reason that the information contained in healthcare systems has tremendous value. Exploits are growing more sophisticated, and time to exploit is accelerating. Antivirus does not protect against zero-day attacks, insider attacks, or local hospital staff who make errors or do not adhere to security policies. Medical devices are often not regularly updated with new .DAT files because they are not always on the network. Despite the progress that the IT industry has made in protecting organizations from external threats and the standard practices now in place at most healthcare organizations, misuses of protected information have spread rampantly in recent years. Indeed, according the Computer Security Institute, insider breaches have recently surpassed viruses as the most-reported information security incident.

By mandate, the information that both healthcare professionals and hackers try to access is now in electronic form across an array of devices in nearly every medical arena and department. The Health Insurance Portability and Accountability Act (HIPAA) of 1996, along with the American Recovery and Reinvestment Act of 2009, have legislated investments in Electronic Health Records (EHRs). They have enacted privacy, enforcement, and administrative provisions that imbue trust in EHRs. These provisions have a far-reaching impact on the way HIPAA-covered entities and their partners handle and protect patient information.

Complicating matters, the FDA also has specific requirements for embedded systems deployed in the healthcare system:

- Systems must do only what they are designed to do.
- Systems cannot perform other functions.
- When systems need to change, only manufacturers can change them.
- All of the above are always true and can always be proven.

The FDA calls out two areas where proactive, selective, auditable control is essential.

Documentation for Commercial Off-the-Shelf Software in Medical Devices (US FDA)	Summary
• What are the computer system specifications for the commercial off-the-shelf (COTS) software?	Address via documentation.
• What does the COTS software do? How do you know it works?	
• How will you assure appropriate actions are taken by the end user?	Requires specific control infrastructure with accompanying audit and compliance assurance reporting.
• What components can and/or must be installed/configured?	
• What steps are permitted or must be taken to install/configure?	
• How often will the configuration need to be changed?	
• What education and training are required for end users?	
• What measures are taken to prevent operation of non-specified software on medical devices?	
• How will you keep track of (control) the COTS software?	
• How will you ensure that no incorrect versions/patches are introduced?	
• How will you maintain your COTS software configuration?	
• Where and how will you store your COTS software?	
• How will you ensure proper installation of the COTS software?	
• How will you ensure proper maintenance of lifecycle support for COTS software?	

"Children's Hospital of Philadelphia uses McAfee Embedded Control on their thin client systems to reduce the total cost of ownership by reducing the number of support calls and by reducing the need for emergency patching."

—Tim Conners
Director, IT Operations
The Children's Hospital of Philadelphia

McAfee Embedded Control specifically addresses many of the requirements imposed by HIPAA and the FDA by controlling what software can run and what software can change on any system. It ensures that any software change can happen only via authorized mechanisms—for example, authorized change control time windows, authorized updaters, or only secure signed updates. It can help keep the production environment of medical systems in a known predictable state while keeping them secure against any external malicious threat or internal personnel unauthorized change threats.

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 white-listing, antivirus and anti-malware protection, device management, encryption, and risk and compliance—and all leverage the industry-leading McAfee GTI. Our solutions can be tailored to meet the specific design requirements for a manufacturer's device and its architectures.

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, reduces security risk for difficult-to-patch systems. • Reduces security risk from zero-day, polymorphic attacks via malware such as worms, viruses, and Trojans and 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 gives the flexibility to disable 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.

(continued)

Feature	Description	Benefit
	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.
	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, the process/program that affected it.	• Validate approved changes, quickly identify unapproved changes, and 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—a favorable choice for a low-OPEX security solution configuration.
Rules-free, signature-free, no learning period, application independent	Does not depend on rules or signature databases; is 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 application's 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.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60742ds_emb-ctrl-health-arrow-kontron_1014_kg