Industrial Computing
Products and Services

Panel PC's

Industrial PC's

SBC's

Industrial Displays

Electronic Design

dsl
Embedding the future

Why Choose DSL?

- ✓ Lifetime technical support
- ✓ Fully customisable products
- ✓ Product branding (bezel colours + company logos)
- ✓ Free pre-installation of OS and your software

Our Services

- ✓ Electronic Design
- ✓ Production Management
- ✓ Assembly and test
- ✓ Bespoke BIOS creation

sales@dsl-ltd.co.uk

or call us on +44 (0)1462 675530

DSL Ltd. | 4 Aylesford Court, Works Road, Letchworth Garden City, Hertfordshire, SG6 1LP

McAfee®
An Intel Company

McAFEE EMBEDDED CONTROL

Enhanced security for today's embedded systems

Business Brochure

These days, embedded systems have something in common with networks: they're vulnerable to attacks. It didn't used to be this way. Until fairly recently, virtually all embedded systems were proprietary and closed—ATMs, point-of-sale (POS) terminals, medical systems, self-checkout systems, handheld devices in retail stores, thin clients, SCADA systems, and others. They were secure in isolation. But in today's interconnected computing environments, many embedded systems are enabled by Microsoft Windows, Linux, or Google Android operating systems as well as commercial off-the-shelf (COTS) and open-source hardware, firmware, and application software. This has brought products to market faster and at lower costs, but it has also increased risk. And, since many of these systems contain industrial secrets or confidential data, they are prime targets.

Traditional Security Approaches Fall Short

So, what's wrong with status quo security implementations? Nothing—except that they are incomplete solutions that provide little or no security. In embedded environments, antivirus software can't protect against targeted malware and zero-day exploits, and it doesn't guard against unauthorized software changes either.

Control and Configuration Management Challenges Loom Large

Maintaining control is especially difficult when systems are offline or when access is available to service technicians. Bank of America learned this the hard way in 2010, when an employee placed rogue code on ATMs and withdrew more than $300,000 before he was caught. Proper access controls would have neutralized that threat. Image manipulation is another major concern. It's one of the most common (and costly) reasons for systems being sent back to the manufacturer for support.

Regulatory Compliance Isn't Getting Any Easier

You can be vigilant about every detail in an effort to comply with PCI, HIPAA, NERC, Sarbanes-Oxley, and any other regulations that might apply to your system prior to shipment. But what good does it do you when customers or service channel technicians start patching or make other unauthorized changes? Even if they have the best intentions, there's a good chance their actions will affect your system's compliance status. Of course, the alternative is to insist on having your people apply all patches. But that could require putting technicians on the scene several times per year. That's not exactly a money-making proposition, and it still wouldn't protect your system against zero-day attacks.

So, how can you deliver locked-down, regulation-compliant embedded systems to your customers with the assurance that they are shipping at their optimized best, with the strongest possible protection for the long haul?

McAfee Embedded Control Is the Answer

It may be the only answer. It both protects embedded system integrity and automates the enforcement of software change control policies at the same time.

McAfee® Embedded Control secures embedded systems and the sensitive information they contain while maximizing uptime, reducing support costs, and helping ensure compliance throughout the lifecycle of your systems. It lets you build security right into your manufacturing process—easily and cost effectively. You create a dynamic whitelist of programs authorized for the system, including binaries and scripts, DLLs, Java, and more. No programs or code snippets outside the authorized set can run and no unauthorized changes—not even Microsoft patches—can be made. Plus, an audit trail logs all access attempts.

McAfee Embedded Control includes the following key components and offers these benefits.

Application whitelisting

McAfee Embedded Control shields applications and related binaries at the kernel level—protecting files on disk or in memory, preventing malware and zero-day exploits, and minimizing the need to patch your operating system (OS) or applications. Reducing patching frequency is especially useful for systems that are remote and distributed in areas with little or no local support. It's one important way that application whitelisting reduces the cost of operations while increasing embedded system availability.

The trend is for embedded devices to become more interconnected and IP connected. However, the protection capabilities of the whitelist and, more importantly, the zero-day threat protection (by protecting the system memory) requires no .DAT updates, unlike traditional embedded security. This means that the systems that are still "closed" or stand-alone can also benefit from this protection capability. Because the whitelist defines what can execute and what can make modifications, these same systems can be protected from internal threats as well.

Change control

McAfee Embedded Control only allows policy-based changes that are expected and authorized. Files are monitored, and unexpected changes are prevented and logged for compliance. The product provides complete visibility and accountability through the automated, continuous collection of audit data. Using the data collected by McAfee Embedded Control, you and your customers can verify that no changes have been made to critical system files, directories, or registries—and report these findings to regulatory officials to help meet compliance requirements.

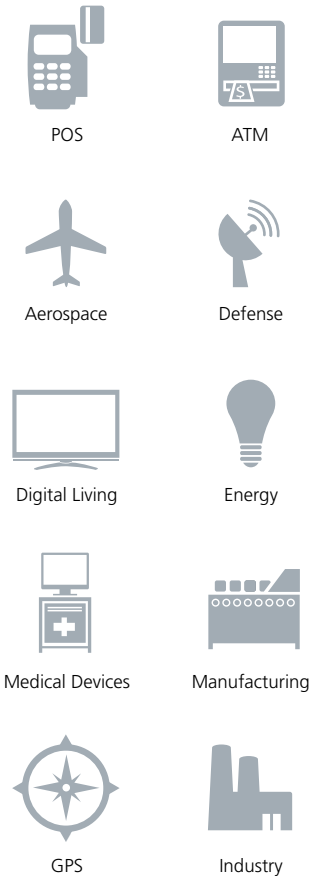
In addition, McAfee Embedded Control enables centralized management through McAfee ePolicy Orchestrator® software. This powerful web-based console helps you easily deploy software and automatically manage configurations and policies from a single location. It also lets you monitor events in real time and generate reports automatically.

A Key Differentiator and Major Value-Add

McAfee Embedded Control is ideal for designing change control and overall security into your manufacturing process, or retrofitting embedded systems that are already deployed in the field with the same built-in security. It's the powerful way to reduce support costs, maintain compliance, improve customer satisfaction, and increase your company's brand value.

Adding McAfee Embedded Control can be accomplished in as little as 10 minutes on your production line. Retrofitting existing systems by updating them online can be accomplished even more quickly. Once installed, there are no signatures to update, no applications to patch, and no databases to maintain. And security for the entire lifecycle of your product is assured.

McAfee Secures Multiple Devices



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 architectures.

http://www.mcafee.com/embedded

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe.

http://www.mcafee.com

McAfee
An Intel Company

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

35101br_embedded-security_0911

McAfee Embedded Control

System integrity, change control, and policy compliance in one solution

McAfee® Embedded Control maintains the integrity of your system by only allowing authorized code to run and only authorized changes to be made. 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 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.

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, and 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 focuses on solving the problem of increased security risk arising from the adoption of commercial operating systems in embedded systems. McAfee Embedded Control is a small-footprint, low-overhead, application-independent solution that provides "deploy-and-forget" security. McAfee Embedded Control converts a system built on a commercial operating system into a "black box" so it looks like a closed proprietary operating system. It prevents any unauthorized program that is on disk or injected into memory from executing and prevents unauthorized changes to an authorized baseline. This solution enables manufacturers to enjoy the benefits of using a commercial operating system without incurring additional risk or losing control over how systems are used in the field.

Assured System Integrity

Executable control

With McAfee Embedded Control, only programs contained in the McAfee dynamic whitelist can execute. Other programs (exes, dlls, scripts) are considered unauthorized. Their execution is prevented, and the failure is logged by default. This prevents worms, viruses, spyware, and other malware that install themselves from executing illegitimately.

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. 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.[1]

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.

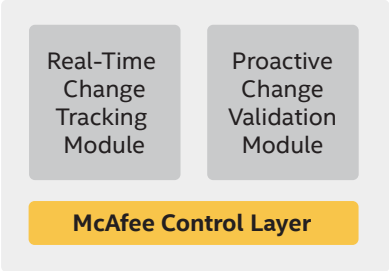
Change control

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. It also provides an audit trail of 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 can apply changes, which certificates are required to allow changes, what may be changed (for example, you may restrict changes to certain files or directories), and when changes may be applied (for example, update Microsoft Windows may only be opened during certain times of the week).

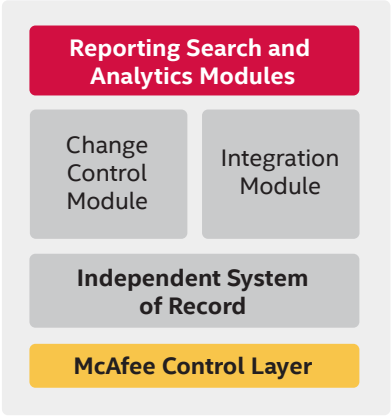
Proactive change verifies each change before it is applied on target systems. With this module enabled, updates to software systems may only be made in a controlled manner.

The real-time change tracking module logs all changes to system state, including code, configuration, and the registry. Change events are logged as they occur, in real time, and sent to the system controller for aggregation and archival purposes.



Change Agent Deployed on Endpoints

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.



Change Agent Deployed on Endpoints

Audit and Policy Compliance

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 UI 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.

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 the industry-leading McAfee Global Threat Intelligence. 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 the cost of operations by limiting unplanned patching and 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.
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.

Feature	Description	Benefit
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, thereby 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, and 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.

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

60745ds_embedded-control_1213B_ETMG