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.

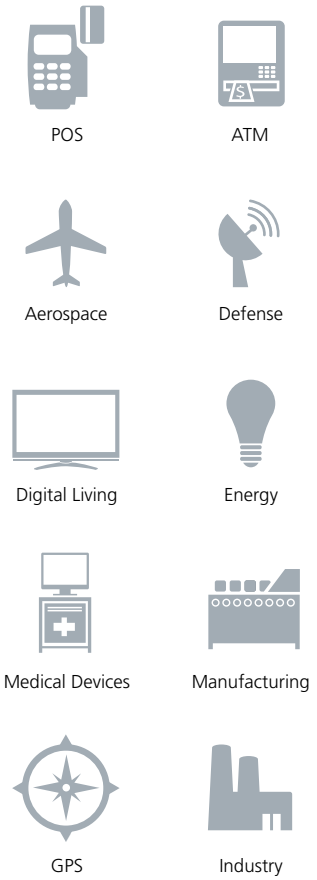
In addition, McAfee Embedded Control enables centralized management through McAfee ePolicy Orchestrator® software. This powerful web-based console helps you easily deploy software and automatically manage configurations and policies from a single location. It also lets you monitor events in real time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