WHITE PAPER

McAfee Embedded Control

Built-in protection for bulletproof peace of mind

McAfee Embedded Control

Built-in protection for bulletproof peace of mind

Today, embedded devices are all around us—in kiosks, point-of-sale (POS) terminals, ATMs, medical equipment, and more. For far too long, however, protecting the integrity of these devices and the sensitive information they contain has been an afterthought. McAfee® Embedded Control enhances embedded device integrity, maximizing uptime, reducing support costs, and helping to ensure compliance throughout the lifecycle of your devices.

The Rise of Embedded Devices

Embedded devices are flourishing in verticals such as banking, aerospace, automotive, healthcare, manufacturing, retail, and entertainment. Kiosks, point-of-sale devices, ATMs, medical devices, entertainment equipment, and more are all growing in number and variety. This phenomenon is a direct result of faster and easier development enabled by commercial off-the-shelf (COTS) and open-source hardware, firmware, operating systems, and even application software. Many of these components are supported by industry best practices, sound development cycles, and functional validation testing—making them very attractive to manufacturers like you.

Risky Business

Unlike the closed, proprietary systems and networks of past generations, today's embedded devices, after they are deployed, are prime targets of cybercriminals. And the frequency of attacks is on the rise. In fact, through McAfee Global Threat Intelligence, technicians at McAfee Labs have seen an exponential growth in cybercrime since 2005, including multipronged attacks. Today, McAfee Labs is identifying more than 60,000 new pieces of malware every day, and 80% of that cybercrime activity is motivated by the potential for profit.

The fact is, these kinds of events will always take place. Without the proper defenses in place, malware and cyberattacks will continue to jeopardize the security and integrity of embedded devices and destroy their performance in many cases. Moreover, these events can occur anytime within the long lifespan of your devices with varying repercussions to your business, your partners, and your customers. Bad news travels fast. Today, we have more real-time information about products and services available through specialty industry news, blogs, and community groups than ever before. The impact of "likes" and "dislikes" via social networks can quickly make or break a manufacturer's

brand and affect customer loyalty for better or worse. Even alleged security issues pose huge risks until disproven.

The ramifications of weak embedded device security become even more daunting when you consider the broad spectrum of industries that provide embedded systems to critical infrastructure and processing networks. Vulnerabilities in these embedded devices could be devastating for millions of people and could even impact national security. In healthcare, such vulnerabilities could potentially threaten lives.

The Root of the Problem

So what makes COTS-based embedded devices prone to attack? The primary culprit is the operating system. In many cases, the operating systems are simply some version of Microsoft Windows, and the applications are therefore Windows-compatible. As we all know, without frequent patching, strong firewalls, and antivirus packages, such systems are ripe targets for bad guys.

Connectivity complicates matters

Many devices these days require internal networking or external Internet access through Ethernet, Bluetooth, Wi-Fi, or other means. This connectivity increases their susceptibility to unexpected threats and possible compromise. Often, such interconnectedness is built into business revenue models. When a customer purchases a device, they are then able to license and use a specialized subscription service, increasing the vendor's business revenues. In these cases, security here that prevents unauthorized changes to the device not only protects the equipment but also the revenue stream that the device enables.

Long lifecycle doesn't help

Despite the fact that the development cycle of most of these embedded devices is shorter than it used to be, the product lifespan is still quite long. In some industries, these devices remain functional for up to 10 years—sometimes even longer. Some manufacturers continue to try to maintain and support their legacy devices with leading-edge service models. However, many are simply unprepared when vulnerabilities and threats against these older systems arise.

Preparing for the full lifecycle of an embedded device is a challenge. From the time the device leaves the manufacturing floor until it becomes obsolete, it is always at risk of having a vulnerability exploited. Some manufacturers have even used this situation to scare customers into continually upgrading to the latest release or next generation to shirk their responsibility for supporting aging legacy systems.

It's worth noting that embedded devices aren't simply at risk once they're installed. They are vulnerable from the very moment they leave the factory—during transportation and through the distribution chain. Trusted distributors, resellers, and integrators typically ensure that systems maintain their integrity throughout distribution. But truth be told, there never is a moment when the device is completely "safe."

So what can you do?

Depending on the criticality and performance requirements of a particular embedded device, antivirus protection might well be the first line of defense. However, it falls short in providing protection for:

- Targeted malware
- Unauthorized software changes
- Configuration file or registry alterations

Patching embedded devices also presents its own regulation-related problems. Mandates such as PCI, HIPAA, NERC, and Sarbanes-Oxley all have unique quirks. And then there's the FDA. When an embedded device leaves the factory, the manufacturer has it configured and running just the right way for maximum performance and compliance with regulatory requirements. However, out of a sense of responsibility for maintaining compliance or simply just doing what they think is right, customers then apply patches to the embedded devices, often hindering device performance, affecting compliance status, and sometimes outright breaking the devices. This requires a truck roll and putting a technician on the scene. The manufacturer's or service provider's costs go up, and affected end users usually aren't too happy that the device they need to use right then and there is down or on its way back to the shop.

In some industries, the maintenance of embedded systems is commonly outsourced. However, that often just means that the manufacturer or distributor will be rolling trucks on a more regular schedule. That's often due to the fact that outsourced maintenance personnel are contractually obligated to regularly patch the systems they are responsible for. Their intentions are good. They are trying to make sure that the devices are up to date with the latest security patches to safeguard the devices and any data they contain as well as maintain regulatory compliance. Unfortunately, these actions likely have just the opposite effect. If you are an embedded device manufacturer, you understand the issue all too well.

What's Not Working

Many embedded device manufacturers deal with the risk of malware and hacker attacks in three basic ways:

- **Change nothing**: Continue with current development and manufacturing processes and ignore or downplay the growing risks in the market
- **Deflect**: Insist that the security and integrity of the embedded devices are the responsibility of the buyer once they leave the manufacturer's control
- **Mitigate**: Identify the most common threat models, and implement security development and processes to accommodate risks

Manufacturers that have adopted sophisticated approaches talk about risk mitigation and sell their wares based partially on that abstract concept. These companies are on the right path, but many fall short by looking at only positive use cases and security controls. For example, a kiosk manufacturer might limit risk by designing a restricted user interface without administrative rights for the browser or operating

system, expecting a threat to come from user interaction with the kiosk interface. But what if this device was proven to be vulnerable through another threat vector? For example, maybe the kiosk was found to be poorly secured against network attacks. In that case, the restricted user interface wouldn't really provide much protection at all.

Other manufacturers have simply taken little action toward building security into their embedded devices, mostly due to a lack of awareness that they can provide more value to their customers by doing so.

The Growing Need

When margins are cooling down and the competition is heating, many manufacturers look for other, more profitable ways to drive business. As you have probably seen in other industries, value-added services beyond the simple break-fix paradigm are well received by purchasers. The same business model can be applied to embedded device manufacturing. In fact, you build trust with your customers as you evolve from a simple get-it-to-market model to building a portfolio of value-added services and developing strong, deep relationships with your customer base.

Security that absolutely prevents unauthorized changes from occurring on embedded devices needs to be designed right into new systems from the start. Current devices that are already deployed in the field also need to be retrofitted with the same built-in security. This way, equipment manufacturers can ensure that malicious code doesn't enter or execute on their embedded devices, maintaining system security and integrity.

Manufacturers who operate this way find that they can reduce support costs, improve customer satisfaction, and increase their company's brand value.

McAfee Embedded Control

Today, McAfee Embedded Control helps embedded device makers integrate dynamic security right into their products during the manufacturing process. It works for operating systems, applications, and other software components provided by the manufacturer. This security goes well beyond malware protection, yet signature updates or other secondary steps are never needed to initiate it.

The whitelisting nature of this security technology blocks unwanted changes and executables to the system, preventing security control workarounds. If an application or process isn't on the list, it can't run. It's as simple as that. For authorized executables, McAfee Embedded Control provides memory protection, mitigating associated exploit risks.

McAfee Embedded Control protects embedded systems from both known and zero-day vulnerabilities and reduces the need to immediately provide patch updates. In fact, many manufacturers rely on the control afforded by McAfee Embedded Control to limit system updates to a quarterly or even biannual basis, greatly reducing the overhead and stress of multiple version support.

Using McAfee solutions from McAfee, manufacturers benefit from reduced support costs, enhanced security in their products, and the ability to develop services that give them distinct market advantages.

Let's take a closer look at the capabilities of McAfee Embedded Control.

Application whitelisting

Application whitelisting protects the applications and related binaries at the kernel level without a dependency on operating system (OS) services. It's this kernel integration that allows McAfee Embedded Control to control software installation and modification. It's also the kernel integration that protects these same files when they are on disk and in memory. This memory-based protection is crucial for preventing zero-day exploits.

Even if one of your embedded devices were to fall into the wrong hands, McAfee solutions can protect the intellectual property residing on the system and even block specific access to critical files that might provide hackers with more insight than they should have.

Change control

The second feature of McAfee Embedded Control is change control. This mechanism uses a trust-model approach for allowing or disallowing change. Change control restricts who can change what, how they can change it, and when it can be changed. In other words, change can only enter the system through the expected means. Unexpected changes are prevented and logged—and administrators are alerted. This same mechanism can also provide file system monitoring.

Change control and validation are key requirements of most industry regulations, which often prescribe the specific type of controls required and how changes in the field are to be made. Regardless of how in-field support changes are executed, we can assist in providing the security and validated integrity of the applied updates.

- **Customer-driven, downloadable updates**: If you allow customers to download and implement their own updates, we can ensure that only these updates are installed, blocking any changes that may be out of scope of an acceptable change. Through the use of digital certificates, you can ensure that only the appropriate updates will be applied to a targeted device version. This reduces the risk of applying patches or updates to inappropriate systems or models.
- **Third-party, manufacturer-validated updates**: If you rely on third parties to manage devices in the field, we provide the controls to ensure that only your authorized updates are applied. In this scenario, we use digital certificates and updates prepackaged on removable media. This model is ideal for supporting remote locations and devices like ATMs, which reside on tightly closed networks. Field technicians don't need to have a robust skill set either, as the prepackaged updates virtually self-install. This technology ensures that only your authorized updates are made and that any other attempted changes will be blocked.
- **Manufacturer-provided, remote updates or device-initiated updates**: If you're venturing into value-added services, having the technical ability to manage your embedded devices remotely is a must. Through network access, you can update your remote devices with the latest software to increase functionality and performance while ensuring the

highest system integrity. You can block changes from all sources that can't be implicitly trusted. And you can even design your devices to automatically check in for updates and download and install them from a trusted source. These controls remain intact even if network connectivity is disabled.

How it works

McAfee Embedded Control is based on the principle of solidification. What that means is that, as a manufacturer, you deploy your software into a controlled state. The solidification process only adds about 10 minutes to your manufacturing time, and copies of solidified images can be distributed to other devices even quicker. Here's how it works:

1. Automatically create a baseline inventory of all software installed on the embedded device, including binaries, scripts, DLLs, and driver files.
2. Enable McAfee Embedded Control.
3. Rest assured. Once McAfee Embedded Control is enabled, the device is solidified. Only authorized code will run. The system can't be tampered with or hijacked after that. Any attempts to change protected program files or run an exploit in memory are blocked and logged—and an alert is sent to administrators. Best yet, there are no signatures to update, no applications to patch, and no databases to maintain.

Audit and compliance ready

As mentioned earlier, many industries deploying embedded devices are regulated by mandates such as PCI, HIPAA, Sarbanes-Oxley, and even NERC. McAfee Embedded Control 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.

McAfee ePolicy Orchestrator® (McAfee ePO™) Software

Today's embedded devices are part of the overall business infrastructure. Since this is the case, you and your customers need a way to easily manage these systems, which are most often distributed far and wide.

McAfee ePO technology offers performance, configuration, operations, and security management of embedded devices from a centralized console. Using McAfee ePO software, you and your customers can manage security policy, configure authorized updates (people, processes, and packages), report on image deviation, and provide reports and dashboards covering the controls required for compliance with PCI-DSS, HIPAA, and other regulations.

McAfee ePO software can be configured to simply cover the scoped devices or feed this data into a master McAfee ePO console. Any customer using our security solutions for their enterprise business can easily incorporate this data for a comprehensive view of the overall security of their organization.

The Final Word

More industries are relying on embedded systems, and the limitations on computing, control, and communication are no longer obstacles. The challenge now is to protect these devices and systems from being used in unintended ways, minimize possible vulnerabilities and exploits of openly sourced components, and secure these devices over their extended life spans.

McAfee Embedded Control software is the industry's first and only solution to secure embedded devices and automate the enforcement of software change control policies on them. It increases device integrity while reducing risk and long-term support costs for manufacturers and their service channels. McAfee Embedded Control is deployed by major manufacturers of automated teller machines, POS terminals, medical devices, thin clients, storage appliances, and other devices. These customers have realized significant and rapid returns on their investments by reducing ongoing in-field support and breakage incidents due to unauthorized changes, and developing new services that give them distinct market advantages.

About McAfee Embedded Security

McAfee Embedded Security solutions are a part of the McAfee product family. They help manufacturers ensure that their products and devices are protected from cyberthreats and attacks. Our 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.

Next Steps

For more information, visit **www.mcafee.com/embedded**.

About McAfee

McAfee is one of the world's leading independent cybersecurity companies. Inspired by the power of working together, McAfee creates business and consumer solutions that make the world a safer place. By building solutions that work with other companies' products, McAfee helps businesses orchestrate cyber environments that are truly integrated, where protection, detection and correction of threats happen simultaneously and collaboratively. By protecting consumers across all their devices, McAfee secures their digital lifestyle at home and away. By working with other security players, McAfee is leading the effort to unite against cybercriminals for the benefit of all.

www.mcafee.com.

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