SECURE YOUR MEDICAL DEVICES

Obtain optimal quality of service—and maintain it
Obtain optimal quality of service—and maintain it

The Situation

When was the last time you were connected to a medical device? It might have been a blood pressure cuff, dialysis machine, or MRI. While you were sitting there waiting for the procedure to conclude, were you thinking about the security of the device you were connected to? No? Chances are that neither was the device vendor. It is this sentiment that has many in the security industry worried about the future safety of the medical device market.

The safety of the patient is obviously the highest priority of medical device vendors and the regulatory agencies that oversee the testing and certification of the devices. That blood pressure cuff you were connected to had to go through rigorous functionality tests to be sure the device could do what it was designed to do. Not only did it have to perform the function properly, but it also had to do so safely in multiple usage scenarios.

Ensuring safety is well and good so long as the device is used as instructed, for the purposes for which it was certified. However, no network cable has been present on a blood pressure cuff before, nor on a dialysis machine. Now that more medical devices are networked together, using IT types of technologies, these devices are vulnerable to hackers and disruption. It is just a matter of time before medical devices enter the sphere of regulator influence, particularly HIPAA and privacy controls.

To lay the groundwork for secure medical devices, vendors and users of medical devices should begin to understand the security issues and implement necessary and compensating controls.

Driving Concerns

The number one priority of a medical device vendor is to provide a safe and operationally sound device. Also important are low failure rates, backed up by redundant systems for when those failures occur. Historically, what wasn’t as important was security, and this vulnerability is now public. A 2011 Black Hat presentation showed the successful hack of an insulin pump.

The main reason that security is such an issue in the embedded device space is the number of attack vectors cropping up as previously proprietary, standalone systems migrate to standard PC-class technologies and connections. More often than not, behind that MRI or X-ray device is a PC platform that allows these medical devices to be networked and easily updated. This platform contains commercial off the shelf hardware, operating systems, and database technologies that don’t differ greatly from other corporate IT assets. When general purpose IT systems are used in health care settings, previously isolated worlds (and networks) collide, with potentially expensive and dangerous consequences.

• General purpose IT policies cannot be easily applied to specialized medical devices. The more that medical devices rely on PCs, the more security and asset administrators in medical facilities treat medical devices like other corporate IT assets. Medical and healthcare facilities have 300 percent to 400 percent more medical equipment than IT devices. Granted, not all the devices are networked, and they may be running real-time operating systems (RTOS) that aren’t managed using the same tools, but the additional device count is still substantial. When these devices are viewed as “just another asset,” the security decisions come from a completely different side of the executive team: the CSO. Where the COO is concerned with job completion, the CSO worries about security. Suddenly, the security standards designed for other corporate IT assets apply to medical devices. This sounds like a positive step until the first time a security patch adversely affects the quality of service of the medical device.
• **Medical devices require a stable environment.** In general, medical devices require a static state unless the vendor has approved a specific update. If the devices are treated as IT assets, the patches meant to make the device more secure end up crippling the device, which leads to health care disruption, support calls, and technicians dispatched to repair if not reimage the software stack.

For example, device vendors spend many hours certifying application and security updates for their own applications as well as those of third party applications that might be present, such as antivirus software. The hours involved to perform these continuous verification and validation checks are represented as part of the cost of the device (potentially multimillions for a single device). The support costs and warranty claims are also built into the cost of the device. If the detection engine of the antivirus software changes, the vendor is forced to completely recertify the device. If an approved patch disrupts the operation of a medical device, the vendor has to cover the cost of the support call. So the vendor's goal is tight control. However, this state conflicts with the directive of the CSO for visibility and standards.

• **Devices may store regulated and confidential data.** Another major concern of medical devices is how they capture, store, and transmit sensitive patient data, as well as the intellectual property of the device manufacturer. Data at rest on a device, however temporarily, presents a security gap if the proper precautions aren’t taken to protect that data. A USB key can be attached to a device and data downloaded, or the storage media can be physically extracted from the system and read from another computer. The most common methods for protecting the data at rest include file read/write protection and device encryption. The IT department has to rely on the vendor to implement these controls on the device and, if necessary, demonstrate to auditors that these protections are sufficient to maintain the privacy of health information.

• **Removable storage devices introduce risks.** Prior to the advent of application whitelisting (AWL) programs, the use of a USB key was the most common method that viruses and malware spread from computer to computer. Where systems deploy AWL technologies, portable media remain a threat due to the data loss that can occur.

• **Devices may store data in separate databases.** Sensitive data may also sit within a database rather than in the device's native file system. If this is the case, the database is in scope for protection equally as much as the device OS. Depending on the architecture, the database may reside on a separate system. Typically database devices are the last to be patched due to the critical requirement for constant availability. From a security perspective, this delay in patching is a nightmare, because OS and database vulnerabilities are exploitable if they have not been patched. An application whitelisting program will protect the OS, but not a separate database. In order to mitigate the risk of database exploitation, these devices must be patched or a compensating control used.

• **Devices may transmit data over vulnerable networks.** Proprietary connection methods have existed for quite some time on these devices to enable the transfer of information from the device to a proprietary console that displays the device status on an HMI (human machine interface). However, as standard connection protocols such as TCP/IP have become ubiquitous, many vendors have embraced these standards, celebrated the lower costs associated with using these standards, and fallen behind in implementing security for the new vectors of attack that these standards allow.

In a sense, medical devices have become no less susceptible to attack than the standard PCs in homes and businesses. The main difference is that the way these devices are used generally limits the attack surface. That said, simply because a device has a capability that isn’t used in a typical “day in the life” of the device doesn’t mean that those attack vectors should be ignored. This approach—security by obscurity—has worked sketchily in the past, and will only work more poorly going forward. The Internet and the criminal black market make it hard for any vulnerability to remain obscure. Every standard technology and protocol used provides a means for these devices to be compromised.

So the battle for precedence is on. The device vendor wants to ensure stability and supportability, and the IT team wants to gain visibility, enforce standards, and ensure data protection. Through the use of the right solution, there can be a happy medium.
Solution Description
Traditional blacklisting approaches such as antivirus scanning are too resource-intensive and signature-dependent to work well in the constrained medical device environment. A review of all of the attack vectors leads us to conclude that we must secure the local device files, data on the device, and the database within the device. The solution must also prevent installation of unauthorized code and malware through removable media. Securing highly regulated medical devices requires a layered approach.

- **Application whitelisting.** Application whitelisting (AWL) programs allow only authorized code to run and maintain the state of the existing code, thus making the code tamperproof. AWL should protect the files on disk as well as the memory space of a device.
  - **Memory protection.** All AWL programs are not created equal. There are some AWL programs that claim to whitelist files, but, if the program doesn’t have memory protection, then it is simply an application inventory tool, offering weak protection. Hackers can use buffer overflows and other memory-based tactics to disrupt device operation and take over a process.
  - **Trusted updates.** The use of a trusted updater—a list of applications or users that are permitted to make software changes—obviates the need for manual intervention and maintenance of the whitelist. Instead, the trusted process updates the whitelist automatically.

- **Data protection.** The data on medical devices can be protected through encryption. Encryption uses an algorithm to make information unreadable to anyone except those possessing the correct key. The importance of encryption on medical devices is twofold: for patient privacy and intellectual property protection. Encryption ensures that the patient data can only be read if the storage medium (such as a hard drive or flash-based storage) remains in the original device. Additionally, encryption ensures that if a device were lost or stolen, the vendor’s software could not be pirated.

- **Database protection.** Even on devices that have some protection, such as antivirus and application whitelisting, more often than not the database is not protected. In order to protect the data within the database, the solution must offer “virtual patching” that will detect attacks on known vulnerabilities and block these activities, even when the database is not yet patched against the vulnerability.

- **Removable media controls.** Finally, the protection of a medical device must include controlling which removable media can be utilized. Encryption will protect the data prior to boot up, but once the key has been entered and the data is decrypted, the next line of defense is controlling what can be plugged into the open ports (including USB and 1394 devices). The use of removable media management ensures that the only media that will operate in an open port is the media approved by policy.

Technologies Used in the McAfee Solution
McAfee offers a suite of products that work together to protect medical device installations. These solutions can be tied together and integrated with other security and IT systems through the open platform of McAfee ePolicy Orchestrator® (McAfee ePO™).

First, to maintain the availability and integrity of the software on the device, McAfee® Embedded Control provides broad visibility into device changes as well as tight control over attempted changes to ensure that medical devices remain up and running and free of malware. This solution integrates application whitelisting, file integrity monitoring, and change management solutions into a single “deploy and forget” solution optimized for medical devices. It is a low footprint, low overhead software solution that runs transparently, without the disruption and updates of file system scanning.

McAfee Integrity Control—which combines McAfee Embedded Control and McAfee ePO—provides integrated audit and compliance reports to help you satisfy multiple compliance regulations. To reduce the chances that users will attempt to use unauthorized removable media or copy data to removable media, McAfee Device Control allows you to restrict use of portable storage devices. For strong data protection, devices can be encrypted with McAfee Endpoint Encryption. To protect the databases in the deployment, McAfee Vulnerability Manager for Databases will scan for vulnerabilities and database-specific threats.
Tight technical controls over software execution can protect the device and data used in medical environments.

**McAfee Embedded Control**

McAfee Embedded Control automatically creates a dynamic whitelist of the “authorized code” on the device. 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.

While preventing execution of unauthorized code—untested patches, scripts, malware, unapproved applications—McAfee Embedded Control also ensures that authorized code cannot be tampered with by preventing changes to selected files, directories, and registry keys. For this reason, vulnerabilities in authorized code cannot be exploited, so the device is safe even when it is unpatched. This benefit is crucial to the security of frontline medical devices.

Memory protection insulates running processes from malicious hijacking. 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.

Authorized updating mechanisms allow granular and selective change control by trusted updaters. For example, the system might approve Windows patches automatically, while preventing changes to critical device configuration files and logging any attempts logged. Authorized updating can occur by opening an update window and authorizing a user or application to make changes.

In addition, the system tracks any authorized changes in real time, allowing automatic and accurate monitoring and reporting of actual changes. You gain visibility into the sources of change and verification that changes were deployed onto the correct target systems. Protection is linked directly to policy, and changes are verified against the change source, time window, or approved change ticket. Changes that are attempted outside of policy are not allowed and attempts are logged. In the event of forensic investigation, activity monitoring can easily identify the time and source of changes, files that were changed, and the user logged in to the system at that time.
McAfee enforces whitelists and blacklists to directly manage execution of software on the medical device.

**McAfee Integrity Control**
McAfee Embedded Control can also be integrated with McAfee ePolicy Orchestrator (McAfee ePO) software. This configuration, McAfee Integrity Control, eases agent deployment, management, and reporting and provides continuous information about change events across the infrastructure. Data captured includes where the change was made (which server), when it was made (time), which user made the change, how the change was made, what content inside the file changed, and whether the change was approved. This deep level of visibility into the device is delivered through the McAfee ePO platform and enables you to continuously verify the security of the device, validate compliance to auditors, and document evidence and an audit trail in the event of a breach.

The single McAfee ePO console also lowers the cost of ownership by consolidating fixed-function device security and compliance management. This saves IT organizations hardware, training, and operational costs, and provides unified control over the policies and protections on each enabled system. You can monitor the authorized changes, which allows proof of due diligence and due care in audit processes required by the Technical Safeguards section 164.312 of HIPAA.

**McAfee Device Control**
McAfee Device Control gives you power over which devices can and cannot be connected to your medical devices. You can make devices read only, so malware cannot be introduced through an attached device. To allow on-site support, you can allow connection by only certain brands of USB keys, or even a specific key using its serial number. Policies are set and maintained using McAfee ePolicy Orchestrator.

**McAfee Endpoint Encryption for PC**
McAfee Endpoint Encryption for PC (EEPC) is your first line of defense against data loss and theft as well as risks when you recycle or retire your hardware. With a standard PC, when the user turns on the machine in the morning, it loads its operating system and then asks for authentication—user ID and password. The user identifies to the OS and then proceeds to a regular workday. On a medical device, instead of user authentication, the decryption key is stored separately from the data on an inaccessible USB key on the device itself. If a thief steals the device and removes the media, the data remains protected.
What if a thief decides to take the drive and put it in another machine? Nothing bad happens. The data is encrypted and unreadable by third parties. Not only is it safe if lost or stolen, it is safe to release for repair or other green initiatives such as recycling or resale of the hardware.

McAfee Vulnerability Manager for Databases, Database Activity Monitoring, and Virtual Patching for Databases

Designed to speed initial vulnerability scans and out-of-the-box reports to reduce risk and address most compliance requirements, McAfee Vulnerability Manager for Databases can discover and scan multiple databases from a single console. It will locate and identify tables containing sensitive information and conduct a quick port scan providing database version and patch status. In addition to basic password strength detection (dictionary, default, and shared passwords), it can even scan encrypted and hashed passwords stored, for example, in SHA-1, MD5, or DES. It will also test for susceptibility to database-specific risks, including SQL injection, buffer overflow, and malicious or insecure TSQL and PL/SQL code. It then presents findings in preconfigured reports for common compliance standards.

Additionally, virtual patching for databases shields databases from the risk presented by unpatched vulnerabilities by detecting and preventing attempted attacks and intrusions in real time, without requiring database downtime or application testing. Using virtual patching for databases, organizations gain protection from threats even if they have not yet installed a vendor-released patch to deal with a known vulnerability.

McAfee ePolicy Orchestrator (McAfee ePO)

The McAfee products utilized in this medical device technology blueprint can all be managed via McAfee ePolicy Orchestrator (ePO). McAfee ePO is a scalable, open platform by which McAfee products can be managed, reported against, and configured.

Optional Integrations

Information feeds that McAfee may not include by default can be sent to the McAfee ePO console through the use of vendor-built custom extensions. For example, a medical device vendor might offer McAfee ePO integration through a custom extension that provides the end customer with a device status, configuration, or security event. Once in the McAfee ePO database, you can mine and report on this event data to acquire actionable and valuable feedback about the device. Not only is this visibility into the device beneficial to the IT department at the medical facility, but it can also serve as a competitive differentiator for the vendor.

Impact of the Solution

This medical device reference architecture defines ways in which the attack surfaces of a medical device can be reduced to allow safe connectivity, improve data security, enable device management and visibility, and make the device compliant with the security directives of IT. Through the use of application whitelisting programs and encryption, the concerns around device security diminish drastically. Not only does the addition of these tools decrease the attack surface available to those who target these devices, but they allow operational optimizations as well.

Every device vendor has concerns around support costs and warranty claims. These costs are generally caused by improper updating of the device or by the addition of third-party software such as antivirus. Application whitelisting greatly reduces these costs because the ability to add or modify those applications goes away. Vendors, manufacturers, and system integrators can see immediate ROI when implementing these security techniques.

Generally, the costs associated with the need for a physical presence are seen as unavoidable. The reason for this is that the vendor or manufacturer doesn’t have visibility into events occurring on the device. They have to rely on the statements being provided by the end customer. Again, through the use of the tools defined in this blueprint, the root cause of why the technician was deployed or truck rolled can be eliminated. Even if technician visits are reduced by just 10 percent, the ROI is immediate and substantial.
Q&A

Do the tools listed in this reference architecture operate in a disconnected or standalone state?
Yes, however not all of the products listed will operate without a management console (ePO). The most critical security component of the architecture is the AWL program, namely McAfee Embedded Control. Embedded Control was designed for devices that operate in a standalone state. All of the functionality discussed—whitelisting, updaters, memory protection, and tamper proofing—still apply. What’s more, should the standalone device become IP connected and central management become a priority, McAfee Embedded Control can be easily upgraded to McAfee Integrity Control, enabling full, centralized management.

What is the main benefit of McAfee’s AWL methodology as compared to others in the industry?
McAfee uses a dynamic whitelisting method. Dynamic whitelisting differs from traditional AWL programs by allowing vendor- or user-defined policies to be the change agents for the device rather than the device administrator. Compared to manual user-defined whitelists, we have found that the use of dynamic whitelisting reduces the headcount required both to manage the solution and to react to events that are generated. And since the policies reside within the central management console (McAfee ePO), they can be updated easily to allow for more processes to be added later.

Can I still comply with regulatory requirements without the use of antivirus?
Yes. Depending on the compliance body's requirements, the regulations dictating antivirus may be avoided. An antivirus program is required to protect against malware and other similar threats. AWL programs paired with memory protection provide the same level of protection. Where antivirus programs rely on a blacklist of known bad files and signatures called a DAT or virus definition (this file can be very large in size and requires constant updating to be effective), instead you will use a whitelist to prescribe which applications are allowed to execute. Since AWL technology is a comparatively new technology, the security assessor might require that the effectiveness of the AWL solution be proven through references or a demonstration.

Additional Resources
www.mcafee.com/embedded
www.mcafee.com/integritycontrol
www.mcafee.com/devicecontrol
www.mcafee.com/endpoint-encryption
www.mcafee.com/vmfordatabases
www.mcafee.com/epo
www.mcafee.com/gti
www.mcafee.com/kb
For more information about the Security Connected Reference Architecture, visit:
www.mcafee.com/securityconnected

About the Author
Michael Cioffi is a solutions architect at McAfee. He is responsible for management of the worldwide technical sales team within the OEM sales organization. Michael’s focus since 2006 has been enhancing endpoint security through the utilization of whitelisting. He has designed and applied the key principles of whitelisting at well-known organizations including Siemens and Phillips Medical and spanning numerous verticals such as medical, industrial automation, retail, and transportation. Prior to McAfee, he was a practice manager for an IBM Global Services partner specializing in monitoring and identity and access management.