

# Unifying Device Management and Cyber Security in the Connected Hospital

General-purpose computing platform reduces the effort and costs associated with deploying, managing and securing medical devices.



## Reducing Complexity

As healthcare providers digitize their medical records and integrate clinical systems and diagnostic data, opportunities are emerging to simultaneously reduce cost, redundancy, administrative burden and medical errors, all while increasing quality of care.

This is the driving force behind the “Connected Hospital”, spanning administration, health monitoring, patient care, imaging and diagnostics, and records management.

But, as the complexity and the number of devices within a clinical environment increase, so do the challenges associated with integrating, managing and securing them. Surveying 74 hospitals across the United States, Identity Force\* found over 60 percent of hospitals had at least one data breach annually, while 20 percent reported ten or more a year.<sup>1</sup> With cyber crime moving from individuals interested in fame to financially motivated criminal organizations, the security risk is increasing, evidenced by the exponential growth in the number of more sophisticated attacks.<sup>2</sup>

Moreover, new security and privacy laws for healthcare, along with heightened enforcement and stiffer penalties, have increased the urgency of protecting data and infrastructure.

Collectively, Intel, Symantec\* and Emerson\* Network Power have developed a Connected Hospital proof of concept (POC) that demonstrates a unified approach for bringing advanced remote management features and enhanced security to healthcare computing platforms. The POC is the basis for the Metro\* medDISPENSE\* Automated Medication Dispensing System featuring the MATXM-CORE-411 platform from Emerson Network Power. This paper discusses how the new technologies featured in the POC can help hospital IT organizations manage medical devices with less effort and secure patient data more effectively.

Healthcare providers seamlessly share clinical information that helps improve care delivery and quality along with patient safety.

### The Connected Hospital

Electronic Medical Records (EMRs) are the cornerstone of the Connected Hospital, where healthcare providers seamlessly share clinical information, stored in vast databases rather than maintained on single-instance paper charts, that helps improve care delivery and quality along with patient safety. At the Connected Hospital, conceptualized in Figure 1, appropriate patient data can be efficiently, reliably and securely shared throughout the hospital and among participating healthcare providers.

For patients, it simplifies the process for receiving quality treatment, while increasing the effectiveness of doctors, nurses and administrators providing and managing their care. For clinicians, the Connected Hospital makes it easier to gather and access patient data wherever and whenever it is critically needed. Administrators can optimize staff utilization and workflows in order to increase operational efficiency, reduce medication errors and lower costs.



Figure 1: The Connected Hospital Concept

## IT Challenges

Yet, with increased integration and reliance on digital systems come increased data security and device management challenges. For the hospital IT department, the big job is integrating a wide range of devices – shared data stores, wired and wireless networking, robust cyber security and efficient device management – into the IT infrastructure. Every device connected to the network requires security to protect against malware and hackers; however, complicating matters, various devices typically use different software platforms, which can make a unified management and security approach difficult to implement.

As the number of devices throughout the hospital increases, so do the number of day-to-day tasks the Biomedical and IT staffs must deal with to manage inventory, configuration, patches, security, as well as providing maintenance and repairing devices. Table 1 lists some of the issues facing clinical engineers and IT and how they impact hospital operations.

Increased integration and reliance on digital systems come with increased data security and device management challenges.

**Table 1: Issues Facing Hospital IT Staffs**

<b>Device Management Issues</b>	<b>Impact on Clinical Engineering and Hospital IT</b>
Lack of a centralized portal for device management	<ul style="list-style-type: none"><li>▪ Device management and security issues are more difficult to monitor and correlate</li><li>▪ Device management is unreliable and less efficient</li></ul>
Incomplete device inventory and configuration data	<ul style="list-style-type: none"><li>▪ Devices cannot be managed from a security perspective when there are inventory tracking deficiencies</li><li>▪ Unknown device configurations may leave security holes due to missing patches, unsecure configuration, etc.</li></ul>
A non-responsive device that typically requires an onsite repair visit	<ul style="list-style-type: none"><li>▪ Onsite repair is expensive and time consuming</li><li>▪ The device may be down for a significant amount of time, slowing down workflow and potentially impacting clinical care</li></ul>
Clinical devices may have no security or use a variety of cyber security applications	<ul style="list-style-type: none"><li>▪ Security inconsistencies lead to gaps in security posture</li><li>▪ The IT staff must spend considerably more time learning and managing different security software</li></ul>

### **medDISPENSE\* AUTOMATED MEDICATION DISPENSING SYSTEM**

In hospitals, nurses need to retrieve patient medications 24/7 – even when pharmacists are not on duty. Providing secure, around-the-clock access to medications, the medDISPENSE\* Series from Metro\* protects drugs and supplies from unauthorized access. Since the system provides full integration with most operations software, medication costs are captured immediately upon dispensing, streamlining operations and ensuring reimbursement. Furthermore, medDISPENSE incorporates Intel® Active Management Technology (Intel® AMT) and the Symantec\* Altiris\* Client Management Suite, which enables the hospital IT staff to wirelessly manage the system throughout the hospital.

The medDISPENSE Series (Figure 2) connects wirelessly to the local area network (LAN), enabling it to share patient information in the Connected Hospital. This gives nurses up-to-date medication history, including adverse clinical events and allergy information, which helps improve patient safety. Staff efficiency increases because inventory and billing are automated, resulting in closed loop medication delivery that reduces waste and saves time – leading to significant cost reductions.

### **A Unified Approach**

Addressing many of the aforementioned IT and device management issues, Intel, Symantec and Emerson Networks have collaborated to show how healthcare devices can be managed and secured more efficiently. They developed a Connected Hospital proof of concept (POC) that reduces the time IT needs to manage devices by utilizing remote management functions and state-of-the-art security software. The POC demonstrates how, from a single console, device management and security can be administered to clinical and diagnostic equipment using the same tools and in the same way as with servers, desktop and laptop PCs – when they are based on Intel® architecture.

### **Key Connected Hospital POC Components:**

- MATXM-CORE-411 compute platform from Emerson Network Power
- Altiris\* Client Management Suite 7.0 from Symantec
- Intel® Active Management Technology (Intel® AMT)<sup>4</sup> administered from a Symantec console

This solution allows administrators to manage users and devices on the network from a central location, consistently maintain software policy (including security), and diagnose and remediate hardware and software issues remotely, regardless of location and distance. These capabilities have been incorporated by Metro, a manufacturer of medication management systems (see sidebar).



**Figure 2:** medDISPENSE\* Automated Medication Dispensing System

## Compute Platform for Medical Devices

The MATXM-CORE-411-B from Emerson Network Power is a MicroATX format motherboard based on the very latest Intel® Core™ i7 processor, giving significant performance and power-saving options over existing Intel® Core™2 Duo processor based MicroATX products. The embedded computing platform provides system integrators with the performance and features needed to power a wide variety of next-generation medical solutions. The MATXM-CORE-411-B can power devices, like bar code scanners, medical sensors and printers, using 12V and 24V USB connections, thus reducing peripheral cost.

The board supports dual independent displays and has VGA/LVDS and HDMI interfaces for connection to the widest possible range of displays, enabling the board to be used in a broad assortment of medical devices, as shown in Figure 3. Acting as the “brain” for the entire system, this stable, long-life platform from Emerson Network Power delivers the multi-core computing headroom needed to run a number of complex and safety-critical medical applications.

Intel AMT enables a remote manager to protect, maintain and manage the board even if it is in a sleep state, its operating system is unresponsive, hardware (e.g., hard drive) has failed, or software agents are missing. This level of remote diagnostic capability enables maintenance costs to be dramatically reduced because systems based on MATXM-CORE-411-B can be updated without requiring a technician to visit.

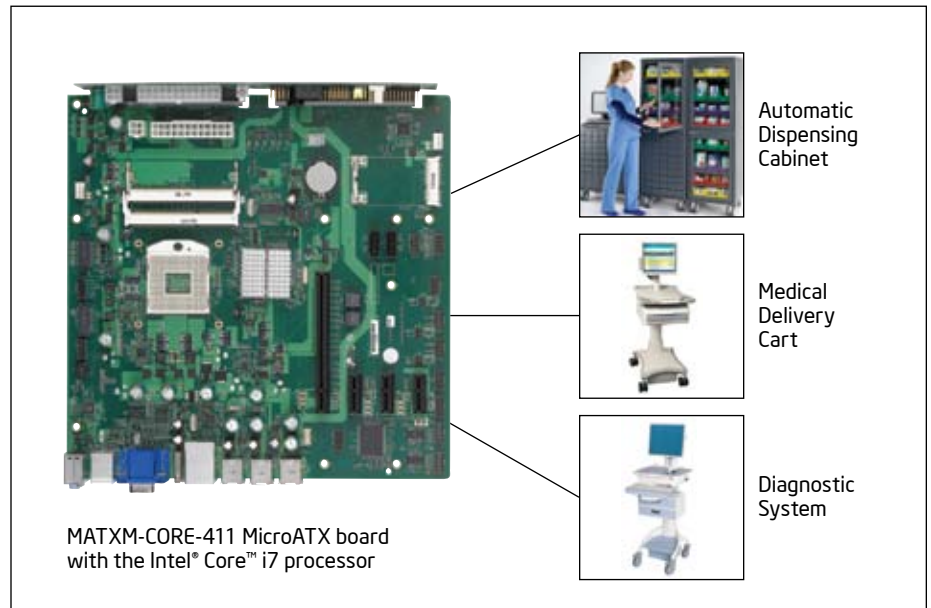


Figure 3: MATXM-CORE-411-B in Medical Applications

## Medical Device Security Challenges

Although not typically the target of cyber attacks, medical devices are still vulnerable to the same cyber threats as traditional IT systems. A device can become “collateral damage” in a malware outbreak or even be the weak link that opens the door to a cyber attack. The healthcare industry needs to be prepared for the possibility that cybercriminals may penetrate devices with the goal of harming patients or threatening harm to our healthcare infrastructure.

Sounding more like fiction than fact, it was reported that a sophisticated computer virus, called Conficker, infected hundreds of MRI devices at dozens of hospitals worldwide.<sup>3</sup> One of the potential risks was the infected machines could be used to leak patient information, or the virus could lead to malfunction and potentially impact patient care.

Medical devices are challenging to protect for a number of reasons, one of which is the difficulty of keeping security

schemes up to date. For instance, U.S. hospital IT staffs cannot modify security software without assistance from the manufacturer, who, according to the U.S. Food and Drug Administration (FDA), must control and approve all device configuration changes. Furthermore, medical devices often have long lifecycles, which means they were designed to defend against a much simpler threat landscape from years back and not the latest attack scenarios.

Another security hurdle is the need to maintain a thorough inventory of devices, tracking hardware, software and manufacturer. It is not enough to know what’s on the network, the IT staff needs a record of the software - applications and operating system by version and configuration - the devices are running. This way, any vulnerability can be identified quickly and mitigated with the cooperation of the manufacturer, or the risk can be reduced by proper network architecture.

Intel® AMT makes it possible to troubleshoot and fix devices based on the Connected Hospital POC from anywhere, often without disrupting end users.

### Utilizing a Management Suite to Improve Medical Device Security

Providing visibility across a healthcare provider's entire network, Altiris Client Management Suite from Symantec enables the IT staff to see the medical device they have, its configuration, and what state it's in. The tool automates time-consuming and redundant tasks to reduce the effort and costs associated with deploying, managing, securing and troubleshooting systems.

The suite's actionable reporting tools not only help identify problems in the healthcare infrastructure, they empower IT to take immediate action to fix the problems from within the reports. Some of the capabilities are illustrated in Figure 4.

### Intelligent Software and Patch Management

For medical devices running an Altiris agent, the Altiris Client Management Suite covers all the bases - software detection, analysis, distribution and compliance. The tool greatly simplifies the effort to update software to any properly architected device in the organization through targeted, policy-based deployment. Even where automated deployment is not feasible, discovering assets and their configuration is essential as it enables reliable manual management. Furthermore, Intel AMT makes it possible to troubleshoot and fix devices based on the Connected Hospital POC from anywhere, often without disrupting end users. The advanced remote assistance features, enabled by Intel AMT, allow IT technicians to rapidly fix end-users' problems without onsite visits.

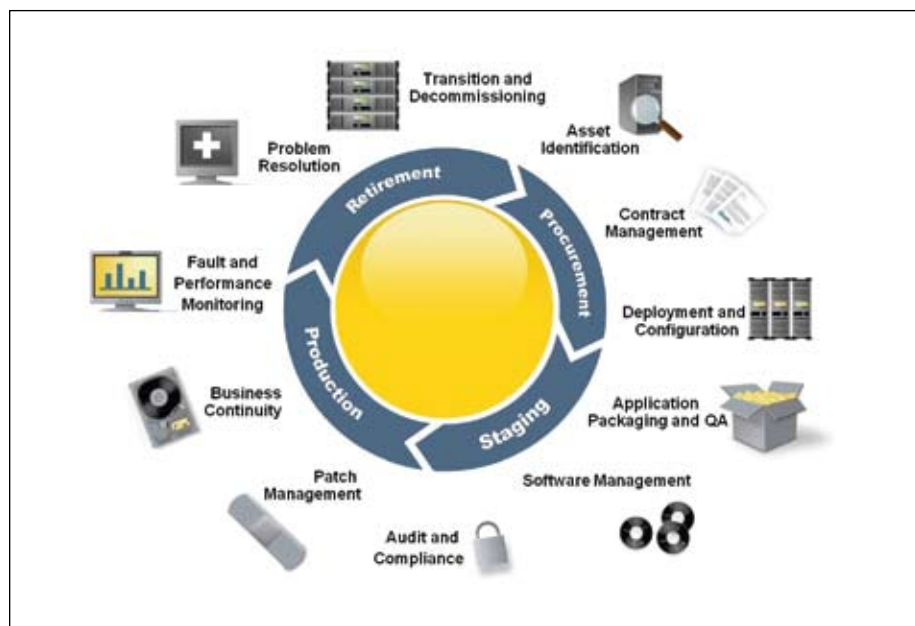


Figure 4: Altiris\* Client Management Suite from Symantec

## Symantec Console with Intel® Active Management Technology (Intel® AMT)

The Connected Hospital POC features unified remote device management and security software, and as a result, an IT staff needs only one graphical user interface (GUI) to manage all their devices. In addition, Intel AMT enables access to medical devices when they crash or are even powered down, leading to increased device accountability and higher utilization rates. For example, if a device has been attacked and is unable to respond, Intel AMT can be used to reboot the system from another hard drive on the network and restore its configuration.

## Deploying, Managing and Securing Medical Devices

While the Connected Hospital will increase staff efficiency and provide opportunities to improve patient care, IT faces the challenge of integrating and managing a rapidly growing number of medical devices. Unifying device security and management allows for a single, advanced management console for managing all devices, thereby saving cost and securing the healthcare infrastructure more effectively. These benefits are realized by the Connected Hospital POC, a joint effort of Intel, Symantec and Emerson Network Power.

The technology employed by the POC was applied to the medDISPENSE system from Metro, including security protection and Intel AMT-enabled remote management from Symantec. The automated medication dispensing system illustrates how unified security and management reduces the effort and costs associated with deploying, managing and securing medical devices.

## WHAT'S MAKES INTEL® ACTIVE MANAGEMENT TECHNOLOGY DIFFERENT?

Intel® Active Management Technology (Intel® AMT)<sup>4</sup> is built into select Intel® processors and chipsets and provides mechanisms for remote discovery, healing and protection of computing systems. It helps software vendors, like Symantec\*, improve the efficiency of remote management and asset inventory solutions by providing persistent connectivity, either wired or wireless, that doesn't require the computing system to be functional.

Traditionally, remote management consoles communicated with devices using their standard networking capability, called "in-band" link. The drawback to this approach is the majority of a device has to be functional (e.g., operating system, hard drive, CPU and network drivers). In contrast, Intel AMT circuitry establishes a new communications channel, called "out-of-band" link, that operates independently of the computing system and enables communication with, and control over nonfunctioning systems.

## UNIQUE INTEL® ACTIVE MANAGEMENT TECHNOLOGY CAPABILITIES†

- Remotely discover medical devices in any operational state: Intel AMT stores hardware asset information in flash memory that can be read anytime, even if the device is powered off.
- Remotely repair computing medical devices: Intel AMT enables the management console to diagnose, control and repair devices after software, operating system or hardware failures.
- Remotely protect medical devices: System security software is remotely updated with the most recent patches. The presence and operation of cyber-protection can be confirmed and monitored centrally.

<sup>†</sup> Requires the medical device to be connected to the network.

To learn more about the MATXM-CORE-411-B board from Emerson Network Power, please visit <http://www.emersonnetworkpower.com/en-US/Products/EmbeddedComputing/EmbeddedMotherboards/Pages/EmbCompMATXMCORE411B.aspx>

To learn more about Symantec\*'s Altiris\* products and services, please visit <http://www.symantec.com/business/theme.jsp?themeid=altiris>

To learn more about Intel's solutions for Medical Embedded Computing, please visit [www.intel.com/go/medical](http://www.intel.com/go/medical).

<sup>1</sup> Source: "Red Flags Rules: Hospital Compliance Report", pg 4 by Identity Force\*: [http://www.identityforce.com/tools/downloads/FINAL\\_IDF\\_RFRF\\_report.pdf](http://www.identityforce.com/tools/downloads/FINAL_IDF_RFRF_report.pdf)

<sup>2</sup> Source: "Symantec Global Internet Security Threat Report: Trends for 2009"  
[http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_internet\\_security\\_threat\\_report\\_xv\\_04-2010.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf)

<sup>3</sup> Source: <http://www.chron.com/disp/story.mpl/tech/news/6402475.html>

<sup>4</sup> Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. With regard to notebooks, Intel AMT may not be available or certain capabilities may be limited over a host OS-based VPN or when connecting wirelessly, on battery power, sleeping, hibernating or powered off. For more information, see [www.intel.com/technology/platform-technology/intel-amt/](http://www.intel.com/technology/platform-technology/intel-amt/).

Copyright © 2010 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel Core are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

