WHITE PAPER

The Challenge of Securing Hard to Patch Servers in Health Care Environments

BlueLane

InfoWorld 2007 TECHNOLOGY OF THE YEAR AWARD

WINNER BEST OF INTEROP Computing

Overview

The healthcare industry has benefited from the breakneck pace of digitization - spanning everything from payments to patient records to X-ray film- but it has also been increasingly exposed to greater risk. Efforts to increase healthcare provider productivity via increased digitization and system interconnectivity have to be counterbalanced against the growing concerns for patient privacy and a backdrop of increasing liability.

In the wake of these concerns, a number of regulations have emerged for IT professionals in the healthcare industry to navigate. Beyond the standard set of IT security concerns that most IT departments must confront, many of the systems utilized in healthcare not only require special vulnerability management efforts but also fall under the auspices of the US Food and Drug Administration (FDA), which complicates things further. Another pain point specific to the industry is the proliferation of embedded systems or medical devices that operate with their own unique set of security challenges.

An inline patch mimics the corrective action of the security patch for network-accessible vulnerabilities, no matter how complex, to address the vulnerability at the root cause.

To manage these challenges, IT professionals in the healthcare industry turn to the typical array of security solutions used by their counterparts across other industries. Network intrusion prevention systems (IPS) are utilized to segment and defend the network. Patch management tools are used to quickly roll out security patches. Unfortunately, perimeter-oriented network IPS require ongoing operational resources, from constant tuning to the management of "noise" due to false alarms. Security patches may mitigate vulnerabilities but are resource intensive to install, require time to test and validate, and may introduce new risks and problems.

Blue Lane's patch protection gateway, PatchPoint™, provides inline vulnerability remediation for server operating systems, databases, enterprise applications and medical devices, offering instant application protection with zero footprint, zero downtime, and zero tuning. PatchPoint utilizes inline patches that are functionally equivalent to software security patches. An inline patch mimics the corrective action of the security patch for network-accessible vulnerabilities, no matter how complex, to address the vulnerability at the root cause.

PatchPoint utilizes inline patches that are functionally equivalent to software security patches.

Regulatory Compliance

Unlike other industries that may experience inconveniences or financial losses that stem from security events, healthcare organizations in the United States are directed by several federal initiatives that mandate the implementation of rigorous security and privacy controls. The most widely publicized initiative of recent years is the Health Insurance Portability and Accountability Act (HIPAA). If the healthcare organization also happens to be a public company then additional efforts must be devoted to IT security in order to achieve Sarbanes-Oxley (SOX) compliance. Additionally, the Food and Drug Administration and its policies also require the attention of IT professionals because usage (and security) of most medical devices falls under the guidance of the FDA. Below is a brief synopsis of each initiative and its impact on healthcare providers:

- HIPAA is perhaps the most widely recognized regulation that directly impacts healthcare providers. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the use of electronic

data interchange in the US health care system. There are two sets of standards stemming from HIPAA: Privacy standards that seek to protect patient data from improper disclosure or use and security standards that safeguard patient data from unauthorized access. The security portion is further subdivided into three safeguard standards: administrative, technical and physical. Among the key applicable HIPAA standards that pertain to the patching challenges mentioned above, organizations must:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Implement policies and procedures to protect electronic protected health information from improper alteration or destruction; and
- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

- SOX (specifically Section 404) requires that public companies have "adequate internal controls" and that the controls be well documented. These requirements refer to business continuity planning and risk mitigation. Although the regulations do not specifically require the installation of patches or reasonable steps toward vulnerability mitigation, they are designed to ensure that reasonable steps are taken to mitigate risk, measure these efforts over time and document procedures.

- The FDA was stuck in the middle of a public confrontation a couple of years ago between healthcare IT professionals and the major manufacturers of medical devices. The manufacturers, who built their software products on top of commercial operating systems such as Microsoft Windows, instructed customers not to patch underlying operating systems because the FDA had to approve the patch first. The FDA clarified its rules in 2005, stating that there was no FDA legal requirement that would prevent the user from installing patches without prior approval from the device manufacturer. Although this has helped clear up the legal misconception, additional challenges face those who seek to eliminate vulnerabilities by patching these embedded systems.

Embedded Systems: Medical Devices

As more and more healthcare computer systems are networked, those systems are increasingly exposed to more threats and greater risk.

As more and more healthcare computer systems are networked, those systems are increasingly exposed to more threats and greater risk. Despite the fact that software patching will eliminate nearly 100% of vulnerabilities, one of the biggest obstacles to creating and maintaining a secure healthcare IT environment is the ability to patch systems in a timely manner. While stretched IT staffs, 24x7 operation, and limited budgets are typical impediments, the proliferation of embedded systems, specifically medical devices, is one of the most daunting.

The most well known manufacturers of medical devices include General Electric, Phillips, Siemens, Kodak, McKesson and Agfa. These devices host critical functions

for healthcare providers, including oncology systems, CAT scans, and even emergency systems such as echo and EKG. All of these systems typically combine some proprietary software (written by the manufacturer) and some off-the-shelf software. The off-the-shelf components typically consist of an operating system, database, web server, or some combination of several components.

Running any off-the-shelf application has its own set of patch-related headaches, but running those same underlying applications within embedded systems tends to complicate things even further. The medical device manufacturer ships its product after extensively testing it on top of a baseline of the underlying apps. Over time however, the underlying applications require security patches, which could create incompatibilities and even break the medical device. So the medical device manufacturers are reluctant to patch until they have performed adequate testing, but in the meantime the systems are vulnerable.

This creates a significant dilemma for the customer. If the device manufacturer has not yet certified the security patch, the system is at risk of attack. Compounding the problem, the healthcare provider may even run afoul of regulatory issues or fail an audit by not patching the system in a timely manner. Even in the face of these significant consequences, it is not an easy decision to patch. If the device manufacturer has not yet certified the patch, it could be because the patch introduces a problem. In some cases, it is common that the manufacturer chooses to support only certified versions of underlying applications. The customer faces the difficult choice between the risk of patching and the risk of waiting.

The customer faces the difficult choice between the risk of patching and the risk of waiting.

Alternative Solutions

Mitigating server application vulnerabilities quickly to prevent data breaches and financial losses is mandatory. Unfortunately, most approaches to server security are inadequate:

- Security patches from software vendors mitigate vulnerabilities but are resource intensive to install, require significant time for the vendor to certify, and ultimately can disrupt availability of the system;

- Host-based security products require the installation of intrusive local agents, are complex to manage, and often require lengthy “learning periods” in order to function properly. These products are almost impossible to deploy within an embedded system without the express consent of the device manufacturer. The device manufacturer also has very little incentive to certify these solutions; and

- Perimeter-oriented network intrusion prevention systems require constant tuning and generate inordinate amounts of “noise” due to false alarms. These products may function as a compensating control for the inability to patch but the benefit is outweighed by the additional management burden and the potential for the device itself to block legitimate network traffic.

Blue Lane Patch Protection Gateway

Blue Lane's patch protection gateway, PatchPoint, provides inline vulnerability remediation for server operating systems, databases and enterprise applications, offering instant application protection with zero footprint, zero downtime, and zero tuning.

Zero Footprint:

Appliance-based approach to server security provides instant protection without agent installation, server configuration changes or reboots. This is significant for protecting medical devices because the devices themselves will not be touched, eliminating the possibility of disturbing the applications and preserving availability, which is critical in the healthcare environment.

Zero Downtime:

Inline corrective actions applied after deterministic problem detection instantly remediate unpatched vulnerabilities without incurring maintenance-related downtime or blocking legitimate application usage. Unlike signature-based products that may misinterpret legitimate network behavior as malicious activity, the Blue Lane solution fixes any problem within the data stream just as patch would do and ensures that legitimate use is preserved.

Zero Tuning:

Application-centric user interface and asset-awareness eases deployment and eliminates the need for tuning. The solution is deployed extremely quickly, relying solely on information about the host and the patches necessary for the underlying applications. Unlike other products that require advanced knowledge about exploits, PatchPoint inherently provides the appropriate patch-equivalent protection and eliminates all guesswork.

The patch protection gateway utilizes inline patches that are functionally equivalent to software security patches for network-accessible vulnerabilities. An inline patch mimics the corrective action of the security patch, no matter how complex, to address the vulnerability at the root cause. The primary difference between an inline patch and an actual software patch is that the inline patch operates in the network and does not require any software to be installed on the server.

The primary difference between an inline patch and an actual software patch is that the inline patch operates in the network and does not require any software to be installed on the server.

Benefits of Inline Patches

- Emulates even complex security patch functionality to ensure that applications continue to function properly;
- Deploys simultaneously across hundreds of servers to provide immediate protection across even the largest server deployments with no code or configuration changes required on any of the servers;
- Promotes uptime and business continuity by performing corrective action inline with zero footprint on the protected servers, which eliminates the possibility of overwriting shared files or disturbing server configurations;

- Eliminates any guesswork during deployment and subsequent maintenance through the correlation between an inline patch and its corresponding vendor security patch; and

- Provides protection for a wide variety of applications, databases and operating systems.

Summary

As the healthcare industry continues to benefit from increasing interconnectivity among disparate systems, such as patient record systems and medical devices, new risks will continue to emerge. Most significant among those risks today are the proliferation of networked medical devices and the inability of administrators to quickly mitigate vulnerabilities. Patient privacy is at risk, healthcare provider reputation is at risk, and the fate of ongoing audits are at risk.

In the face of this inability to patch quickly, most of the solutions on the market today are poorly suited to mitigate the vulnerabilities and provide an adequate compensating control, without compromising system availability, flooding administrators with noisy false-positive alerts, or requiring significant and ongoing tuning. PatchPoint is uniquely suited to address this problem. The solution protects the underlying applications of an embedded system without tuning, without requiring an agent or intrusive software to be installed, and without compromising the availability of critical medical infrastructure. Zero tuning. Zero footprint. Zero downtime.

Blue Lane Customer Q&A: Spotlight on Healthcare

Blue Lane interviewed one of our early customers to determine how they used the PatchPoint system. The customer interviewed is an engineer for a west coast based public health organization. Here is what they had to say:

Q: Please tell us about your organization.

A: I work for an organization who's mission is to protect and promote the health of all citizens in the City. We oversee fifteen primary care health centers.

Q: Why did you deploy Blue Lane?

A: We have lots of critical servers and we've had some difficulty keeping our patches deployed in the timely manner. Blue Lane allows us to instantly mitigate those vulnerabilities without putting availability at risk.

Q: Was there anything unique to your environment that made it particularly difficult to deploy patches on servers in a timely manner?

A: A big challenge faced by all healthcare organizations is the widespread use of embedded systems, which are difficult to patch. These systems are typically built upon some base operating system, such as Microsoft NT Server. Many of the embedded system vendors are not providing patches in a timely manner due to the testing requirements. Obviously, if we don't have an approved patch then we can't install it. When they do release a patch, we have to go through out own series of regression tests which can extend the window of vulnerability even further.

Q: How far behind are some of these vendors?

A: Some are reasonably quick but others may be months or years behind. Our paging system is only supported on NT 4.0 and patches aren't readily available since the official Microsoft End-of-Life.

Q: You mentioned the regulatory environment. What are the implications?

A: HIPAA is the big one. The embedded system vendors address their own product vulnerabilities so that they may claim HIPAA compliance but they often can't keep up with patches for the underlying operating systems so they aren't necessarily accountable. Failure to patch the OS could result in fines or jail time, so we take it very seriously.

Q: What other approaches did you consider?

A: We honestly felt like we were out of options. We couldn't afford to deploy additional personnel. We tried to implement network IPS but it generated way too many false positives and generated an onerous amount of log data that we had no time to analyze. The degree to which you have to tune those products to eliminate the noise is far too costly for an organization with our resources.

Q: What other benefits have you realized with Blue Lane in place?

A: We have since moved to a quarterly patching cycle as opposed to before when we simply reacted to everything. We never kept up under the previous model so there's far less chaos now. We implemented the product as a security solution but it's actually had a terrific operational benefit.

About Blue Lane Technologies

Blue Lane provides the only inline patch proxy systems for enterprise servers that checks for the same conditions and applies the same corrective action as the software vendor security patch to fix application-specific vulnerabilities at the root cause. Solving the dilemma of "patch now or patch later," PatchPoint instantly secures critical applications and preserves the uptime of the business while eliminating the cost and risks associated with unscheduled patching. Founded in 2002, Blue Lane is headquartered in Cupertino, California. For more information, contact the company at www.bluelane.com.

Blue Lane
10450 Bubb Road
Cupertino, CA 95014

www.bluelane.com
info@bluelane.com
408-200-5200