Lumension SECURITY™

John C. Lincoln

Health Network Finds Sanctuary for Thousands of Patients' Confidential Data

Background

Phoenix, Ariz.-based John C. Lincoln Health Network is a not-for-profit organization that includes two hospitals, thirteen physician practices and a number of outreach programs. John C. Lincoln employs more than 3,000 staff and 1,400 physicians, all of whom are dedicated to providing the highest-quality patient care possible. For CIO Rob Israel, ensuring quality care also includes maintaining a secure environment for patient data.

The Challenge

Devices such as USB memory sticks, scanners and PDAs give John C. Lincoln physicians and other staff instant access to information for increased productivity, but Israel explains that these devices also pose a serious threat to the confidentiality of patient data as devices as small as a thumb that hold up to 80 MB of data can easily be lost or stolen. Data leakage isn't the only risk; not only can employees drag-and-drop information from a company's network onto a device, but they can also inadvertently introduce viruses and other malware from a device.

In 2003, an employee inserted a floppy disk and inadvertently exposed John C. Lincoln to the Slammer virus—the pandemic worm that used a known buffer overflow in Microsoft's SQL Server database to generate massive amounts of network packets, overloading servers and routers and slowing down network traffic. While the organization recovered from this incident, portable media continued to cause problems.

"We were experiencing lots of problems with people downloading or uploading from thumb drives, CD-ROMs, burners and floppy disks, and adding peripheral devices, such as modems, without our knowledge," says Israel. "The modems were bypassing our firewalls and connecting to things like AOL. We weren't sure what was being uploaded or downloaded. We had people loading games, bringing in term papers and using our machines for non-work activities."

While John C. Lincoln defined a computer use policy for all employees, the firm was unable to enforce that policy. The policy stated that, "you cannot save anything to a hard drive," says Israel, but employee activity stood in direct violation. "We were continually performing reactive maintenance," he adds.

Israel could not individually inspect the 2,000 machines across 15 locations, yet he could not ignore the unknown threats to his network that could potentially put the organization at risk of non-compliance with the Health Insurance Portability & Accountability Act (HIPAA) privacy laws, which mandate the protection of confidentiality and security of health data through setting and enforcing standards. Israel began his search for an effective, yet flexible device management solution to prevent unauthorized user activity.

"We wanted a process that would allow us to take better control of our peripherals without making it impossible for the people who needed devices to do their jobs because there are some instances where those devices are appropriate," he says. "Secondly, we wanted to take control of our hard drives."

The Solution

According to Israel, he found, "an immediate fix to the glaring problem," of unauthorized device use when, in 2005, he implemented Sanctuary Device Control from Lumension Security to dramatically simplify the device management process and proactively secure his organization from threats, such as data leakage, malware and

spyware. "Lumension Security came highly recommended from a trusted vendor," he says. "The product was not oversold. It does exactly what it is supposed to do." Israel requires John C. Lincoln employees to fill out a 'device approval' form to plug devices into their work machines and those who try to use devices that are not sanctioned by the organization are automatically blocked by Sanctuary.

He also needed a way to identify unauthorized applications running on his network, stop them, and then assign permissions to enforce his application control policies. In 2006, Israel added the other primary component of Sanctuary by purchasing Sanctuary Application Control to regulate Company application use. Sanctuary's unified console allows Israel to centrally manage and monitor both device and application control across the organization.

"Sanctuary provides a single, seamless view of everything accessing or attempting to access the network through corporate endpoints from a device and application perspective, providing a new level of visibility into the network then was previously possible," he says.

Sanctuary's unique combination of endpoint application and device control protects the enterprise from a host of security threats, including data leakage and malware, and assures compliance with evolving regulations that govern privacy and internal controls. While John C. Lincoln has strict security policies in place to prevent use of unauthorized applications or devices, Sanctuary is needed to stop those who would break the rules. "We could not rely on policies alone any more," says Israel. "Sanctuary put meaning behind our procedures."

If employees can justify a need to use an application or connect a device such as a USB stick to the IT network, Israel can easily use Sanctuary to grant access rights. Enabling access rights at a high level or all the way down to device class, specific device or application to users, user groups, a particular computer and much more, Sanctuary provides Israel with the control he needs while giving his users the flexibility to access applications and devices that are required to effectively do their job. Permission settings include read/write, scheduled access, temporary access, online/offline, specific busses, HDD/non-HDD devices and more.

"By rolling out Sanctuary to all of our desktops, we were able to set policies based on either a user's role or a user's identity," says Israel. For example, he adds, "A user could get full thumb drive access, just keyboard access or access to read from a thumb drive or CD-ROM, but not be able to save anything to the machine."

The Benefits

Following the October 2006 news that some Apple iPods had been infected with malware, Israel felt further justified in his decision to implement Lumension Security's Sanctuary. He spends minimal time updating his whitelist of authorized applications and devices. "It comes pre-populated and identifies every type of removable media, so there's not much custom definition that needs to be done," he says. In turn, Israel has the guarantee that virus-laden iPods or other devices will not impair the organization because they will never succeed in connecting to the network if plugged in to any of his 2,000 workstations. On average, Israel says he saves 10 hours per week due to a substantial decrease in the number of work orders for trouble shooting related to device dilemmas.

"Tons of things can happen with iPods if you don't have the proper security measures in place," he says. "People could take up valuable disc space with music and video uploads. There's a risk of copyright infringement and you could also upload malware." There's also the risk that someone could load confidential network data onto an iPod, he notes.

John C. Lincoln saw a definite need to add to its software control arsenal already in place. Sanctuary Application Control allowed John C. Lincoln to add a layer of protection that would prevent people from installing software without IT involvement not only reducing the risk of software conflicts, but also assisting with software license compliance.

Israel says that organizations often have hundreds of IT policies and many times employees unintentionally violate policies they are not aware of, so he used Sanctuary to audit his network and evaluate all device activity. Sanctuary's patent-pending I/O bi-directional Shadowing tracks information as it is read from or written to a floppy, CD/DVD or removable device, and provides a comprehensive audit log of every event, whether allowed or attempted—including those by unauthorized code—and all writes to removable media and specific ports. Optionally, a full copy of

the data written to or from a device can be captured and retained as well.

"We were surprised when we rolled out the Sanctuary software at how many devices were out there," says Israel. "We found devices we didn't even know about." Not only is the audit log invaluable in measuring and enforcing policy compliance, it also bundles the information Israel needs as proof of HIPAA compliance.

Equally as important to Israel is Sanctuary's encryption functionality, which encrypts removable media so that it can be safely used and transported to ensure that sensitive data is not inadvertently exposed to those without authorized access. "Every day you pick up the newspaper and hear about another hard drive or laptop or PC that was stolen out of the Hospital Corporation of America, the Veterans Administration or TriWest containing tons of patient data," he says. With Sanctuary, John C. Lincoln can enforce policies so that if a removable device with sensitive data is lost or stolen, the data is encrypted.

Conclusion

As incidents of mobile malware and device theft make headlines in growing numbers, John C. Lincoln will continue to utilize Sanctuary to proactively enforce its device usage policies. The organization will also regulate application use with Sanctuary and thus proactively avoid problems of malware, spyware, keyloggers, Trojans, rootkits, worms and viruses. "We chose the option of safety through technology," says Israel. "With Sanctuary, we don't have to worry about patient data being exposed."

Israel cautions of the impending danger for organizations without policy enforcement in place. "A lot of people are assuming their policies and procedures are covering them. There is going to be a lot of 'I told you so'," he says. "Policies are nice, but if you have a choice between a policy and a technology such as Sanctuary that enforces a policy, you're safer to go with the technology because people are human and they're going to make mistakes."

"As long as your end users know what you're doing and why you're doing it, they're usually more than willing to help you out," he adds.

About Lumension Security™, Inc.

Lumension Security, a company formed by the combination of PatchLink® Corporation and SecureWave® S.A., is a recognized, global security management company, providing unified protection and control of enterprise endpoints for more than 5,100 customers and 14 million nodes worldwide. Leveraging its proven Positive Security Model, Lumension enables organizations to effectively manage risk at the endpoint by delivering best-of-breed, policy-based solutions that simplify the entire security management lifecycle. This includes automated asset discovery, vulnerability assessment, remediation and validation; application and device control; extensive policy compliance reporting; and integration with leading network access control solutions. Headquartered in Scottsdale, Arizona, Lumension has offices worldwide, including Virginia, Florida, Luxembourg, the United Kingdom, Spain, Australia, Hong Kong and Singapore.

Lumension SECURITY™

Lumension Security
15880 N. Greenway-Hayden Loop, Suite 100
Scottsdale, AZ 85260
480.970.1025 / www.lumension.com