

# Customer Success Story

**MidMichigan**  
Medical Center  
Midland

MidMichigan Medical Center, Midland

*Lumension*® Patch and Remediation provides  
vulnerability management remedy.

June 2010

CS-EN-06-04-10

## Quality Healthcare Mission Extends to IT Security

A family of organizations dedicated to providing quality, comprehensive healthcare, MidMichigan Medical Center – Midland ([www.midmichigan.org](http://www.midmichigan.org)) provides trusted care through coordinated hospitals, home care, nursing homes and urgent care, as well as through physician services and advanced medical and network infrastructure technology.

With responsibility for more than 20 locations, which include service providers and specialty centers, MidMichigan relies heavily on its IT infrastructure to ensure the quality of doctor-patient data assets. As Supervisor for Clinical Desktop Support at MidMichigan, Jim Czyzewski, is frequently reminded of the risks associated with a network infrastructure not current on patching.

MidMichigan's IT goal is to keep its network infrastructure healthy.

## Welchia Worm Hinders MidMichigan Health Business Continuity

In October 2003, MidMichigan — along with a host of other businesses worldwide — received a major wake-up call when the Welchia and Nachia worms brought IT operations and subsequently business continuity to their knees. Czyzewski experienced firsthand the many long days and high costs of reviving MidMichigan's operations.

“We got hit with the first wave of Welchia and spent three days of hardcore worm alleviation using a removal tool and applying Microsoft patches. My team had to seek out the right patches associated with these worms, and that was a lot of work, time and money in and of itself.”

**Jim Czyzewski**

**Supervisor Clinical Desktop Support**

**MidMichigan Medical Center, Midland**

Making matters worse, MidMichigan was struck a second time by Nachia in March 2004.

“Again, we ended up running a removal tool and applying patches,” explained Czyzewski. “I recall applying eight Microsoft patches; even still we were only able to patch 80 percent of our computers. We were just lucky the remaining computers never got infected.”

Eager to withstand future attacks, Czyzewski and his staff sought and researched automated patch and vulnerability management solutions to relieve the IT security pain. When the Nachia worm hit, MidMichigan flipped patch management efforts into high gear, making program completion in 2004 a high priority.

“In November 2003, I read ‘Enterprise Patch Management for Windows’ in Windows IT Pro magazine (formerly Windows & .NET), which included an overview of [Lumension® Patch and Remediation] (formerly PatchLink™) features,” commented Czyzewski. “This story was a key selling point in our decision to move forward with [Lumension] to resolve our patch and vulnerability management issues.”

Czyzewski performed a thorough evaluation in August and September 2004, which included several patch management solutions from vendors like Microsoft (SMS), Lumension, Shavlik and St. Bernard. Based on his analysis, he concluded that SMS was too expensive. Shavlik and St. Bernard offerings didn’t include many of the features that MidMichigan felt were critical to its patch management program’s success, including cross-platform capabilities and enterprise scalability.

Dismissing systems management proposals due to the already-successful implementation of Novell ZENworks and the other patch management vendors due to lack of functionality, MidMichigan declared Lumension its patch and vulnerability management vendor of choice.



## MidMichigan’s IT Wellness Plan In Place

According to Czyzewski, “We were immediately able to stop worrying about getting the most current virus .DAT files because [Lumension® Patch and Remediation’s] mandatory baseline feature allowed us to quickly set up and manage these AV files along with security patches for a wide selection of operating systems applications.”

### MidMichigan had no way of knowing what systems were patched

Previously, MidMichigan had no way of knowing what systems were patched when using home-grown script files for patch management. Now, Czyzewski exceeds IT security expectations with the support of Lumension® Patch and Remediation tracking and enterprise reporting features, which he adds, “really helps put our minds at ease.”

Another solution that puts Czyzewski and his staff at ease is Lumension® Scan, a complete stand-

alone network-based scanning solution that performs a comprehensive assessment of all the devices connected, both managed and unmanaged, to MidMichigan's network. Once all the assets are identified, the solution detects weaknesses on these devices before they can be exploited.

"One of our priorities was being able to identify and inventory assets that didn't or couldn't have the patch installed on them in case we had problems with more viruses and needed to manually remediate those assets," remarked Czyzewski. "[*Lumension*® Scan] gives us the ability to use network access control devices to identify an asset and quarantine it if necessary. "

*Lumension*® Scan provides MidMichigan with a risk-based prioritization of identified threats and a continuously updated vulnerability database. If a virus showed up at one of MidMichigan's facilities that wasn't being identified by its anti-virus solution, the solution would allow Czyzewski and his staff to write their own fingerprint to find that virus, even with the products that were not equipped with a patch.

"This solution has been very beneficial to our staff in getting the correct pieces installed," said Czyzewski. "Also, with the broad security platform provided through the suite, we have one counsel to use for all of the security products we have in place."



**Global Headquarters**

8660 East Hartford Drive, Suite 300

Scottsdale, AZ 85255 USA

phone: +1.888.725.7828

fax: +1.480.970.6323

**[www.lumension.com](http://www.lumension.com)**

Vulnerability Management | Endpoint Protection | Data Protection | Compliance and IT Risk Management