



MidMichigan Medical Center - Midland

PatchLink Update™ Provides Patch & Vulnerability Management Remedy

Quality Healthcare Mission Extends to IT Security

A family of organizations dedicated to providing quality, comprehensive healthcare, MidMichigan Medical Center – Midland (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. The senior information systems specialist responsible for desktop patch management at MidMichigan, Jim Czyzewski is frequently reminded of the risks associated with a network infrastructure not current on patching.

“I am mostly concerned with users exploiting vulnerabilities by misuse of the Internet or email,” explains Czyzewski. “No matter how much you try to educate your users, there are still those who will open every attachment or go to every link they receive in their email.”

“ No matter how much you try to educate your users, there are still those who will open every attachment or go to every link they receive in their email. ”

Jim Czyzewski - Sr. Info. Systems Specialist

MidMichigan’s IT goal is to keep its network infrastructure well.

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,” said Czyzewski. “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.”

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,” explains 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.”

MidMichigan
Medical Center
Midland

KEY FACTS:

- IT infrastructure supporting more than 20 locations
- Welchia worm attack required three days to repair multitude of critical systems
- Nachia worm attack infected nearly 80% of all systems
- Required a cross-platform and enterprise level patch & vulnerability management solution

PATCHLINK®

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) that included an overview of PatchLink Update™ features. This story was a key selling point in our decision to move forward with PatchLink to resolve our patch and vulnerability management issues."

Czyzewski performed a thorough evaluation in August and September 2004, that included several patch management solutions from vendors including Microsoft (SMS), PatchLink, Shavlik, and St. Bernard. His analysis 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 PatchLink Update its patch and vulnerability management vendor of choice.

MidMichigan's IT Wellness Plan In Place

"Immediately, we were able to stop worrying about getting the most current virus .DAT files because PatchLink Update'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."

“ PatchLink Update'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 ”

Jim Czyzewski - Sr. Information Systems Specialist

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 PatchLink Update's tracking and enterprise reporting features, which he adds, "Really helps put our minds at ease."