Interfaith Medical Center

Executive Summary

Industry

- Healthcare

Environment

- 287 beds, 6 satellite locations
- 1,500 employees
- 4,000 networked devices

Technology Needs

- Wired infrastructure
- Simple network management
- Secure patient information
- Medical device management
- Network segmentation
- Zero trust environment

Extreme Solution Components

- ExtremeSwitching™
- ExtremeManagement™
- ExtremeControl™
- Extreme Intrusion Prevention System (IPS)

Results

- Increased network performance and nearly eliminated latency in their wireless network
- Implemented policies that allow essential communications, while effectively putting each PC into its own micro-segment
- Successful deployment of a zero trust network environment
- Enhanced network and device security

ExtremeControl™ Enables "Zero Trust," Micro-Segmented Network to Reduce Security Threats

Interfaith Medical Center is a not-for-profit organization dedicated to providing quality healthcare to the residents of Brooklyn, NY. The 287-bed hospital offers a wide-range of preventive, diagnostic, and treatment services and educates its community to achieve optimal health outcomes and quality of life. Interfaith's 1,500 employees provide a total of over 200,000 outpatient clinic visits, 50,000 emergency department visits and 11,000 discharges each year.

In order to deal with the management challenges and security threats that come with the increasing number of medical devices on the hospital's network, Interfaith partnered with Extreme Networks to deliver a "zero trust" environment that uses micro-segmentation to eliminate threats and improve patient safety.

No Tolerance for Security Threats

The recent changes in healthcare brought on by the onslaught of networked medical devices have caused additional security challenges. Within the last couple of years, cyber-attacks, and in particular, ransomware attacks, have brought many hospitals to their knees. The National Health Service (NHS) in the UK was crippled by the WannaCry ransomware attack.

In the face of these ransomware attacks, Interfaith Medical Center moved to protect not just their medical devices and patient data, but also the safety of patients. They created a plan for securely on-boarding and

managing their 4,000 networked devices, including telemetry monitors, CAT scan machines, X-ray machines, MRI machines, lab equipment, and EKGs. The plan called for building in network segmentation as a critical security control to mitigate threats. To go a step further in protecting their mission-critical network, the hospital also strategically decided to move to a zero trust environment where devices can only interact with other devices or systems they explicitly need to communicate with.

Zero Trust Becomes a Reality

In their quest for a networking solution to achieve a zero trust environment, Interfaith evaluated several vendors. They selected an Extreme switching solution, including Extreme Intrusion Prevention System (IPS), ExtremeManagement, and ExtremeControl, because not only did the products work well in their environment, they also delivered the best value.

"The use of ExtremeControl has allowed me to do for my physical network what I've been doing for my virtual network," said Christopher Frenz, Director of Infrastructure, Interfaith Medical Center. By working with Extreme, a zero trust model has become a reality. The hospital deployed ExtremeControl in one week and had several thousand devices protected.

Using Extreme Networks' Access Control (NAC) appliance, ExtremeControl, the hospital implemented policies to allow essential communications, while effectively putting each PC into its own micro-segment and making lateral movement between PCs extremely challenging. "We wanted to minimize the potential for a malware outbreak or other cyber attack to spread through our organization," says Frenz.

Aside from using ExtremeControl to securely connect the hospital's medical devices and business-related IoT devices such as IP video cameras, printers, and HVAC, the new Extreme solution has increased network performance and nearly eliminated latency in their wireless network. "The use of EMR has made IT one of the most critical departments in any hospital. A high-performing network is essential to patient care in this day and age and Extreme delivers," said Frenz.

Beyond Saving Patient Data, Saving Patient Lives

Frenz has been very happy with the sales and support he has received from Extreme, and says it is better than the vendors he has dealt with in the past. He also notes that the solution has made his job, and that of his 10-person networking team, much easier.

Looking into the future, Interfaith Medical Center anticipates the challenge of keeping up with the growing number of devices coming on to the network and the need to replace older equipment with new versions that require a network connection. Their plan? To continue their current security initiatives and keep building in network isolation.

According to Frenz, "In the interest of protecting the patient, and not just their data, my goal is to keep everything as separate as possible, so if a threat breaks out we won't lose whole systems. The last thing we want is to find out that a piece of surgical equipment is suddenly brought down by ransomware and a patient dies on the table because the surgeon lost access. With the help of ExtremeControl, we can prevent something like that from happening."

"Healthcare IT is challenged with trying to balance the risk of securing medical devices within a budget, all the while taking into consideration patient care and the security of the hospital. ExtremeControl has enabled us to cost-effectively secure our medical devices with network segmentation and create a zero trust environment."

Christopher Frenz, Director of Infrastructure
Interfaith Medical Center

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact / Phone +1-408-579-2800