IoT and Medical Device Safety

Healthcare networks and devices are becoming significantly more complex, presenting a growing challenge for the IT staff supporting them. Rather than thinking solely in terms of device counts and bandwidth, organizations must now reassess their approach to medical device support and rethink how best to apply business intelligence to the network.

For some IT departments, medical device support is new territory. Best practices formerly included placing all medical devices on a single VLAN protected by a firewall. However, this process is outdated due to a number of factors including:

- Failure to restrict and track internal access by employees, contractors and manufacturer maintenance personnel
- Risk of misconfiguration of one medical device type impacting others

With the rapid adoption of Wi-Fi by medical device manufacturers many hospital IT departments are finding themselves now supporting Wi-Fi enabled IV pumps, blood gas analyzers, telemetry systems, mobile X-ray machines, ultrasound units, hemodialysis devices and glucose meters on their wireless local area networks. As more medical devices are added, the strategy that organizations used during initial rollouts five years ago is no longer adequate. For example, a common approach was to make all medical devices part of a dedicated network, physical or virtual. The theory at the time was that these devices were being protected from outside performance and security risks, but that hasn't always been the case. Over the years, hospitals have experienced challenges supporting wireless medical devices from multiple manufacturers of a single medical device on their virtual network because of:

- Inability of legacy wireless medical devices to support latest authentication and encryption systems
- Unique network configurations to accommodate the devices such as network quality of service parameters or security settings
- Medical Devices and FDA Compliance
- As more medical devices are added, it will no longer be acceptable to simply make all medical devices part of a dedicated network change without notice
- Limiting access to a shared wireless password

With the challenge of supporting a growing variety of medical devices on the same network the U.S. Food and Drug Administration recently released an advisory highlighting the current risks of medical devices on hospital networks along with the following basic recommendations for hospitals

- Restrict unauthorized access to networks and medical devices, and track network activity
- Update antivirus, firewall efforts, and security patches
- Create and evaluate strategies for maintaining functionality during an adverse event

Critical Technology Issues for IoT and Medical Devices in Hospitals

Insufficient Wi-Fi Coverage for Medical Devices

As more medical device manufactures move away from legacy Wireless Medical Telemetry Service (WMTS) bands to Wi-Fi, hospitals require more than just a Wi-Fi coverage model. Whether its connecting workstations on wheels, barcode scanners, IV infusion pumps or phones, the network must be capable of connecting all Wi-Fi enabled devices that hospitals and medical facilities leverage today for real time clinical care. To operate smoothly, there can be no bottlenecks from the Wi-Fi access points, back through the wired infrastructure, and all the way to the broadband Internet connection and the data center. These connections must be highly available or fault tolerant to insure uninterrupted service.

Lack of Medical Device Controls

Medical device adoption really means the growth of Machine-to-Machine (M2M) and Machine-to-People (M2P) automations. With this evolution of clinical workflow, IT operations needs to focus beyond connectivity and to proactive monitoring and management of systems such as nurse call, IV pumps, and telemetry systems that require constant communications with core applications and clinical staff. For every new medical device on the network there is an application data flow between it and a larger system.

Visibility into medical device communications, locations, performance, and patterns of activity are important for optimizing clinical care. This is also vital for optimizing the infrastructure and for both short and long-term planning for medical device automation and support.

- Network analytics equips IT with the capability to understand how well new systems or devices are being adopted, what the baseline is for each application regardless if its hosted onsite or in the cloud, and even when the slowest work times are by department for scheduling change control windows. Network based analytics brings meaningful big data understanding to the health and usage of a hospital's infrastructure.

Unknown Security Risks and Compliance Risks

A constant risk to the network, and ultimately hospitals, are unapproved applications and rogue devices that may appear on the network and either permit unauthorized access or interfere with other devices. A means to monitor all devices and applications that operate across the network is vital. It is not uncommon for one medical device system to incorrectly be configured for DHCP services which can take down an entire medical device VLAN. Network Access Control (NAC) automates onboarding of devices and application of rule-based policies across the entire wired and wireless infrastructure.

Network Segmentation and Partitioning

In order to deliver performance and insure network security, it is necessary to provide network segmentation and partitioning. Fabric Connect offers this through service-based encapsulation and isolation. The secure network segments can be created quickly and easily, end-to-end, without requiring any additional overlay protocols. These networks can be designed to ideally fit the needs of different departments or entities in a traditional multi-tenant environment (say, a clinic or patient records department), to separating different types of devices and users (e.g. smart phones or IoT devices worn by visitors), and even isolating traffic types for security or regulatory compliance (e.g. banking transactions for PCI DSS compliance, or medical imaging devices to comply with HIPAA). The best part is the avoidance of complex configuration issues; this network isolation characteristic is native to Fabric Connect, and therefore deployed quickly and easily via simple edge-only configuration.

24/7 Operational Support

Hospitals never close and neither does Extreme Networks' 100% in-sourced Global Technical Access Center (GTAC.) 24/7 support ensures that all questions can be answered promptly to keep the network functioning at all times. Extreme is the only company in the industry that takes an architectural approach to bringing products to market from R&D to product release. As a result, all of our network products from wireless to wired are managed with a single network management screen for easy management by constrained healthcare IT teams. To learn more visit Extreme Networks Healthcare solutions: http://www.extremenetworks.com/healthcare

Resources

Hospital Network Security Requirements: 5 Steps Beyond Compliance – White Paper

Information Governance Engine for Healthcare – Solution Brief

Extreme Fabric Connect Enables Advanced Paperless Environment at Concord Hospital – Case Study

Required Capabilities	Recommended Solution	How We Do It Better
Stabilization of existing wired and wireless infrastructure to support growth of medical devices	ExtremeSwitching ExtremeWireless ExtremeAI	Single pane of glass management system provides centralized visibility and end-to-end granular control of the unified network
Pervasive Wi-Fi connectivity and bandwidth for clinician workflow and communications	ExtremeWireless ExtremeSwitching ExtremeRouting	Hybrid deployment architectures (bridged at AP or controller), single sign-on to simplify management. Application and device based policy controls. Embedded flow-based ASIC flow sensor technology per port, 3M flows/s collection capability
Automation of device onboarding with audit controls	ExtremeControl Extreme Defender for IoT	Automated, secure, and fast provisioning and control of medical devices on the wired/wireless network
Critical device and agentless application	Extreme Control	Agentless performance and security monitoring of medical device communications
Support and consulting to deliver best of breed IT service delivery	Extreme Services	Extreme services including onsite customer consulting, design, and implementation services as well as comprehensive training curriculum
Determining unknown security risks and meeting government compliance standards	Extreme Management Center Information Governance Engine	Automated and repeatable solution that works in the background 24/7/365, completes assessments in minutes, and yields consistent scoring of a network's compliance
Simple, agile, and secure network infrastructure	Fabric Connect	Network service automation; significantly fewer network touch points enables faster time to service for rolling out application
24/7 Operational Support	Maintenance	Support Center (GTAC) provides technical support 24 hours day, 365 days a year

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact