Extreme™
Customer-Driven Networking

White Paper

Table of Contents

Becoming an Intelligent Hospital: From Smart Building Technologies to Connected Medical Devices

Impacts and Opportunities of IoT

IoT is nothing new in healthcare, and it has created a growing sea of connected devices, both medical and end user, that are revolutionizing how care is being delivered. Meanwhile, the wireless network continues to advance in software-driven capabilities including insight, analytics, and automation, all melding together to form an open, comprehensive ecosystem. Crucial to enabling a digital transformation is having a clinical-grade infrastructure to properly support the innovative medical devices and smart building technologies being used. The ultimate goal: becoming an intelligent hospital by harnessing the power of advanced wireless network infrastructure, as well as interconnected assets, to create new, better clinical processes, management systems, and deliver better patient outcomes. (HealthcareITNews).[1]

The Connected Environment of the Modern Medical Facility

- The IoT healthcare market will reach $136.8 billion worldwide by 2021.
- Today, there are 3.7 million medical devices in use that are connected to and monitor various parts of the body to inform healthcare decisions (Allied Market Research).[2]

There's a profound need to identify ways to successfully execute on building management and all IoT device functions. On the medical side, IoT enables a more data rich experience by collecting all sorts of useful patent information. How can healthcare organizations make the most of that data and use it in a practical manner?

Security has also become an increasing priority as a result of IoT; healthcare has failed to adopt basic security protections, and its attack surface is increasing as a consequence (Frost and Sullivan).3 Cyberattacks and data breaches are on the rise, designed by malicious hackers looking to make quick money on a network reliant industry. Advanced strains of malware and IoT vulnerabilities remain pressing issues, as well. New efforts have been made to shore up security, initially aimed primarily at pre-market devices. However, as legacy medical devices remain in use, post-market guidelines, regulations, and recalls are emerging.

Connected medical devices play an integral role in patient rooms, from clinics to birthing suites. Being able to connect to those devices with agility, security, and minimal complexity is difficult, but it's what hospitals should be aiming for.

Solving Agility and Security Challenges with Devices and Sensors

Examining the Continuum of Smart Building Technology

A continuum of technology advancements exists within the building space as smart buildings and connected solutions evolve. The fast pace of IoT continues at light speed, and with increasing frequency, manufacturers are releasing technology solutions for buildings, both generic and healthcare-specific. In fact, healthcare is the fastest growing industry when it comes to IoT and smart building technology, as seen in Figure 1 (Memoori).[4]

Up to **30B**

connected IoT and medical devices in the healthcare ecosystem by 2020

60%

...of all medical devices are unpatchable (6 million-11 million)

6.2

...vulnerabilities per medical devices on average

Growth in Smart Building Connected Devices Over Time
(millions of devices)

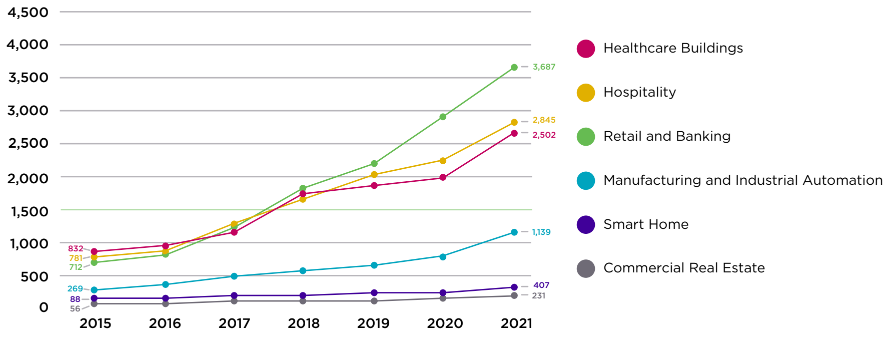

Figure 1

Security and safety surveillance systems now feature the ability to tie in video with larger coverage, bringing in analytics to detect anomalous behavior, search, and conduct forensic analysis easily. The goal is to improve security and access control while creating a better experience for hospital occupants.

For example, simply being able to unlock doors with a smart phone as opposed to having to use a physical badge is a big transformation as the need for higher levels of situational awareness grows. Consider your own experiences, whether in a hospital or other medical facility, in which you walk into a room with typical access to a light switch and thermostat. If either have a problem, who do you call? Smart building technology, thanks to IoT, can deliver solutions to operational problems like this through a mobile connected solution interface. Visitors, patients, and clinicians become more connected and empowered by gaining better, more personalized control over their environments with entertainment systems, HVAC, or lighting (Memoori).[5]

Historically, IT was dependent on an operator to stay on top of alarms and events in order to know what's going on and take responsive action. Data management, data modeling, and visualization enables the ability to bring together a higher level of situational awareness, offering IT full visibility into what's going on in the building using a location system. Not only is it possible to receive alerts when there's an alarm or an event, but it's also possible to know that it took place at a certain part of the building. Analysts can tie a response procedure to any given event, orchestrate a response with the right people who are certified to do what they need to do, and incur an audit trail as the process unfolds.

Today, hospital buildings are becoming hubs for comprehensive awareness. Operators are gaining the power to ensure continuity of standard procedures and identify performance and improvement opportunities, which leads to significant returns. For example, running Operations Performance Management, a solution from IoT firm, ThoughtWire, resulted in an annual ROI of 900% for one hospital, ultimately saving the facility $2.7 million per year. ThoughtWire's Smart Hospital Suite includes synchronized operations, an early warning system, and a rapid response mode.5

> *"The convergence of HVAC systems and the wireless network is an interesting smart hospital trend. It will help to get the data out and ensure safety, security and comfort at the same time."*
>
> **Himanshu Khurana, VP and CTO, Honeywell Building Solutions**

How Connected HVAC and Building Sensors are Changing Hospital Operations

HVAC is a fundamental aspect of building systems traditionally associated with temperature and comfort. However, in hospital and healthcare environments, comfort ties to parameters of temperature, humidity, air pressure, and air flow, and it's used in very precise, defined ways to manage environmental conditions. Today, the industry is seeking to take HVAC systems to the next level by leveraging network infrastructure to add sensors for real location systems, or feeding HVAC-generated data into an analytics framework for predictive insight and behavioral monitoring.

For instance, instead of communicating back and forth via phone to determine whether a system is down and where, how can operators predict system failures and shift the treatment of service cases to a proactive approach? Through connected HVAC and building sensors, there are many different parameters that can be monitored over time in order to power predictive operations and a proactive environment.

Keep in mind: smart HVAC systems are connected to the network in the hospital. From there, it may go to a secure private cloud, or a secure public cloud. Today, there are well-defined practices for secure ways to define endpoints and gateways, as well as extracting the data. Those gateways then become the means to control data flow and take advantage of analytics tools.

Combatting Increasing Attacks and Reigning in Rogue BYOD Devices

IoT devices are a fundamental component of the smart hospital; they're what make intelligence possible. Rogue BYOD devices (unauthorized devices connected to the network that create security risks), are often brought into the hospital environment, so how do you reign them in and achieve continuous security?

Combatting rogue devices requires network segmentation via guest access, which prevents end users from jumping to other devices or access points within the network. Similarly, BYOD devices should be disabled from talking with one another or detecting other devices. Network and access control are also critical; guests need to be required to acknowledge terms of use and monitoring via a click through. All of these components add up to defense in depth: monitoring, access control, and segmentation.

Consider Extreme Defender for IoT: a key element to achieving full defense in depth. Both users and devices operate on the edge of the network, which is why layers of security are so critical. Network access control, authentication, and authorization are all parts of reigning in rogue devices. What users are allowed to do can change depending on which part of the campus they're on, or where they're located. It's all about strong emphasis on security at the access layer or around the perimeter of the network.

Simplicity in network products is also important. Any organization can do a moderate amount of security, but with the amount of threats and attacks that are growing, progress needs to quicken. Old user interfaces and command lines keep IT analysts on their toes in terms of the administration and effort that's required to prevent attacks in hospital environments. Defender for IoT addresses these problems with a simple user interface that even non-technical people can apply to devices to protect them, ultimately lessening the complications that accompany the ever-growing number of BYOD devices in hospitals.

Managing and Analyzing a Growing Legion of IoT Data

Using Data to Reveal Relevant Business Insights

A key component of the intelligent hospital is effectively managing and filtering data. Modern hospitals have to move beyond the network foundation to integrate intelligence capabilities for analyzing data and delivering actionable insights.

Healthcare is an equipment-reliant industry, especially when it comes to mobile devices, thus availability is key. Gathering data from the network via a consolidated platform enables hospitals to make informed decisions about the equipment that's needed and where it should be deployed as they move toward becoming a fully intelligent facility.

Resolving the Challenges of Acquiring and Securing Hospital Data

Another challenge impacting hospitals seeking to adopt intelligent capabilities is finding a way to successfully manage IoT in consideration of how it joins the network, data it creates, and the opportunity that the data presents, whether it's digital transformation or network management-driven. Finding the right solution to make it as easy and automated as possible, rather than task-driven, will help to reduce overall complexity, such as Extreme Management Center.

Traditional, event-driven networks and management tools don't work in the intelligent hospital. Rather, management tools must be predictive and proactive in nature across the campus-wide continuum of data, workflow, and business outcomes. Two major components of the intelligent hospital's wireless network are proactivity and understanding.

The discovery portion of determining what's on the network is also crucial to resolving the challenges of acquiring and securing hospital data. There must be policies around devices and data they have access to; security governance, ultimately. Healthcare is a highly regulated environment, so having a platform around management that gives insight into all of those things is necessary.

> *"With the network platform we have and data we're gathering, we can get contextual information. What room was someone in? Where was the device? It's possible to take a look at device utilization based on timeframes, or whether the device is being used. Is there an anomaly, and is that anomaly because the device was being used for its intended purpose at that point in time, or was there something else going on?"*
>
> **Eric Miller, Senior IT Director, Ascension Technologies**

Dealing with Healthcare Regulations and the Framework for Compliance

Compliance will remain a priority in healthcare. As a result, hospitals and healthcare organizations at large must have visibility into what's on the network, how it's acting, and whether events are suspicious. Newer technologies are allowing for a simple network that can be segmented, isolated, and protected. This is timely because cybersecurity frameworks in the U.S. are frequently mapped to regulations.

If you're not currently adhering to a formal cybersecurity framework, the NIST cybersecurity framework for critical infrastructure is recommended. It encompasses five simple steps:

1. Identify
2. Defend
3. Protect
4. Respond
5. Recover

When it comes to global data protection requirements, such as GDPR, it's never been more important to keep emerging needs and best practices for meeting compliance regionally at the forefront of your initiatives.

Conclusion: Becoming a True Intelligent Hospital

Bracing for New Technologies and New Challenges

In pursuit of evolving into the intelligent hospital, what sorts of technologies and challenges are on the horizon that healthcare organizations should be aware of?

When it comes to the IoT, edge computing is a critical advancement in technology. Once again, the network should be leveraged as a platform, such that it's possible to operate in disparate locations for edge functionality while running analytics. It's predicted that major networking manufacturers will soon release solutions that enable network gear to run software like Docker on the edge, which holds a lot of promise for innovation. Additionally, there's the potential for machine learning and artificial intelligence to run at the edge versus up to a cloud platform.

As edge devices get smarter and gain more capabilities, they're becoming points of control, management, and risk. From a network and systems perspective, the evolution requires taking a new approach to thinking about how you would design systems where everything is IP, and smart to a certain extent. The edge is becoming full stack, and a much richer system that can be easily managed. While this is a complication, it's also a benefit. The edge will generate the data needed for value. In healthcare, there's still a fair amount of inefficiency out there, but this is a new generation of opportunity well poised to reduce it.

"It seems like the industry is on a pendulum swing. We were centralized with mainframes, then we decentralized with PCs, and then we've centralized again with the cloud. It also seems IoT went through a period of decentralization again. When I look at that from a network perspective and the stresses that are going to be put on the network, the traffic flows are not necessarily going straight to the cloud. You may not want to send all that sensor data straight to the cloud."

Dave Raftery, Chief Customer Officer and General Manager of the Healthcare Practice, Integration Partners

When you look at real-time location systems that are better built and deployed, it's possible to track assets and people, as well as generate information. This sort of capability transcends building management systems in the intelligent hospital and extends into IT networks, wireless networks, patient workflow, and patient care. As real-time location systems evolve, they're proving to be a technology that's transcending boundaries to create full value outcome, plus a whole lot of data. There's also the potential to add AI and machine learning on top of real-time location systems to predict what's going to happen in the near term in addition to long-term performance

There is a reevaluation that has to be made when it comes to the way experts, end users, and healthcare decision makers view networking. It cannot be a platform that equals complexity—the enemy of efficiency and management. Complexity increases costs, administration, and time to troubleshoot. Becoming the intelligent hospital and keeping pace with changes in technology as best as possible in healthcare calls for simplicity in networking.

Autonomizing the Healthcare Industry: Becoming the Intelligent Hospital

To truly become an intelligent hospital, healthcare organizations would do well to take steps to center the wireless network on its ultimate beneficiaries: clinicians, patients, and visitors. This process can be accelerated by autonomizing the network infrastructure.

As the evolution of the smart hospital continues and new technologies are introduced, healthcare has to put simplicity, quality of experience, and design at the forefront of the wireless network. IT teams need to be able to reduce their workload and easily add additional devices and applications at the edge. Finally, hospitals need to strive to forge relationships between IT and clinicians.

With Extreme Elements, healthcare organizations can achieve an Autonomous Network that is capable of self-driving and self-healing. This empowers them to deliver a heightened patient and clinician experience for better healthcare outcomes. An autonomous network has four major attributes:

1. Software-driven infrastructure
2. Insights and analytics
3. Automation
4. Open ecosystem

In the healthcare space, an Autonomous Network can alleviate much of the network complexity that comes with managing thousands of users and IoT. The pursuit of becoming a true smart hospital becomes feasible and attainable. Connecting a life flight to the doctors on the helipad, monitoring IV pumps keeping a patient alive, and metering pill distribution and tracking volumetrics are all possible use cases.

Healthcare facilities need to find a way to better prepare themselves to be there for patients and clinicians while making room to safely adopt new technology; all of these results add up to an Autonomous IT Enterprise, the key enabler of the intelligent hospital.

> *"The networking space has really caught up to the ability to deliver these technologies. My perspective is we do need to do all these things, but at the same time we still have to reduce complexity. Complexity equals downtime and probably failure. Projects that don't deliver these outcomes never get achieved. The lift gets too heavy, too big, and too hard. When you're on year three of something that should've been done in six months, the plug gets pulled. Healthcare has to come to the networking space with a different plan. We can't build networks like we've built them in the past."*
>
> **Scott Fincher, Senior Outbound Product Manager and Architect, Extreme Networks**

References

1. Shah, S. (2017, October 23). Understanding smart hospitals and why most aren't there yet. Retrieved March 25, 2019, from https://www.healthcareitnews.com/blog/understanding-smart-hospitals-and-why-most-arent-there-yet.
2. Industry report: Internet of Things IoT Healthcare Market. Allied Market Research. February, 2016. Retrieved April 11, 2019 from https://www.alliedmarketresearch.com/iot-healthcare-market.
3. White paper: Medical Device and Network Security – Coming to Terms with the Internet of Medical Things. Frost and Sullivan. 2019. Retriever April 11, 2019 from https://www.extremenetworks.com/resources/white-paper/medical-device-and-network-security-coming-to-terms-with-the-internet-of-medical-things/.
4. Memoori. (2016, Fall). Growth in Smart Building Connected Devices over time [Digital image]. Retrieved April 11, 2019, from https://www.memoori.com/portfolio/internet-things-smart-commercial-buildings-2016-2021/.
5. (2018, July 27). Smart Buildings at the Center of a Fundamental Shift in Healthcare. Retrieved April 11, 2019, from https://www.memoori.com/smart-buildings-at-the-center-of-a-fundamental-shift-in-healthcare/.

Extreme™
Customer-Driven Networking

http://www.extremenetworks.com/contact