comport
HEALTHCARE SOLUTIONS

Explosion of IoT in Healthcare

Secure, Manage and Control Your Healthcare Network

Like many industries, healthcare organizations are undergoing change. The explosion of mobile technology and the proliferation of Internet of Things (IoT) medical devices are taking root. IT managers now face increased challenges to address security while improving patient care and engagement. The increased level of devices added to a healthcare network significantly increase threats to electronic patient data, as well as other potentially damaging threats. These trends are happening and IT managers are seeking solutions to help them address the impacts to their network infrastructure.

Let's look at these trends in a little more detail.

IoT Medical Device Use

The use of IoT in healthcare is exploding. The IoT healthcare market is projected to grow from USD $41.22 Billion in 2017 to USD $158.07 Billion by 2022. These numbers represent a Compound Annual Growth Rate (CAGR) of 30.8% from 2017 to 2022[1]!

While these numbers may seem staggering, the rapid adoption of IoT in healthcare is driven by technology advances with the goals of increasing efficiency of care and improving patient outcomes. Examples of such devices include cardiac heart monitors, intelligent pacemakers, drug infusion pumps, and traditional test equipment such as MRI and X-ray systems. New innovations come out every day. Many of these devices capture patient health information (PHI), which helps in individual patient treatment and monitoring, as well as care and treatment of specific diseases, via applied data from group analytics. In most cases, the number of IoT medical devices in a hospital easily outnumber the laptops and PCs used by caregivers and administrators.

Improving the Patient Experience

Healthcare organizations are also starting to invest in more people and technology to improve the patient experience. From a regulatory level, hospitals are compensated (federally reimbursed) based on patient satisfaction scores. The Hospital Consumer Assessment of Healthcare Providers and Systems (HCACPS) is a survey required by CMS (the Centers for Medicare and Medicaid Services) for all hospitals in the United States. Poor HCACPS survey results can result in lower reimbursements, so hospitals are seeking to improve patient satisfaction through enriching patient experiences.

From a technology perspective, there have been innovations ranging from free guest Wi-Fi access to encourage patients and guests to share their issues and get immediate access to research, etc. when they need it. Additionally, many hospitals have created patient-facing apps based on wayfinding technology to help patients and families easily navigate hospital facilities as well as have food or gifts delivered to their rooms.

BYOD on the Job

Another trend that has become more commonplace as the use of mobile phones continues to rise is "Bring your own device" (BYOD). The healthcare industry is no exception as four out of five doctors regularly use their personal mobile phone at work today. It provides a level of convenience and access for doctors and caregivers to respond to patients quicker as needed information is close at hand. BYOD also (for good or for bad) allows doctors to consolidate their professional and personal life into one device. Having 24-hour connectivity between wireless devices in a healthcare facility can be extremely beneficial.

Mobility and IoT are Today's Biggest Risks

The trends discussed above offer a lot of promise to the healthcare community in terms of increasing efficiency of patient care and improving patient outcomes. However, from an IT perspective, each of these areas offers challenges in terms of security and control.

From an IT perspective, there are many challenges to the BYOD trend. Sensitive data can potentially be disclosed on a BYOD device (either deliberately or accidentally) if the device is lost, stolen, or has compromised integrity (jailbroken or rooted).

Based on sheer numbers and the inherent lack of built-in security, IoT devices present the largest risk. Often, IT managers have no idea when new medical IoT devices are added to the hospital network, how open they are to the outside world, or if they have been compromised. When problems are found, its often too late. In many cases, these devices contain or transmit PHI and, if compromised, theft of confidential health data can occur.

The primary threats of unsecured IoT in healthcare environments are ransomware attacks, Denial of Service (DoS) attacks, or alteration of device functionality. PHI is the most likely target of cyber attackers, who use minimally secure IoT devices to get into a hospital's corporate network and breach other areas where records are kept. There have been a few dozen highly public data breaches of healthcare facilities over the last year and security experts feel it will only get worse as more devices find their way into healthcare facilities.

Ensuring Secure Access for Guests and Patients

In today's digital and mobile world, patients and families live on their smartphones and tablets. They expect the same ability wherever they go; whether it be to work, personal time, or such things as doctors' visits or hospital stays. Technology programs that hospitals put in place to improve the patient experience, such as guest Wi-Fi and/or a patient-facing app, require appropriate network security provisions to be successful while also protecting the healthcare facility's confidential information.

Healthcare Providers Accounted for 78% of all Reported Healthcare Breaches in 2016[2]

Top Reported Healthcare Breaches of 2016

Rank	Covered Entity	Entity Type	Cause of Breach	Records Exposed
1	Banner Health	Healthcare Provider	Hacking/IT Incident	3,620,000
2	Newkirk Products, Inc.	Business Associate	Hacking/IT Incident	3,466,120
3	21st Century Oncology	Healthcare Provider	Hacking/IT Incident	2,213,597
4	Valley Anesthesiology Consultants	Healthcare Provider	Hacking/IT Incident	882,590
5	County of Los Angeles Departments of Health and Mental Health	Healthcare Provider	Hacking/IT Incident	749,017

Bring Control and Security Together

Obviously, IT managers in healthcare facilities are facing a lot of change to their network traffic and need to carefully think about a network policy management approach that offers both control and security. Here are the key things to take into consideration when formulating a sound policy management approach.

- Know what devices (IoT, BYOD, guest, internal personnel) are on the network and how they need to interact with other devices and data systems.
- Identify, inventory, and classify all devices. Only after this step is completed, then proper authorization privileges can be granted.
- Consider a solution that provides as much automation as possible. Given the sheer volume of IoT devices, as well as guests, BYOD devices, etc., administrative efficiency should be maximized, especially in a very dynamic environment.

To meet regulatory compliance, hospital IT organizations need to be able to demonstrate an auditable network access trail, that shows what devices are on the network, what resources they have access to, and access privileges.

When considering a network access policy management solution, it's better to use a cohesive, coordinated network defense from a centralized policy management platform as it's easier to support and use than multiple tools from different vendors. Look for a solution that offers a complete portfolio of network security, management, and mobile engagement to both secure your entire hospital network, but also support the patient experience initiatives you may have planned.

The Ability to See and Manage All

Traditional network access control involves the three "A"s—Authentication, Authorization, and Accountability (AAA). This works well for traditional network devices, but IoT devices provide another level of challenge. Choose a portfolio of policy management solutions that solve today's security challenges across any multi-vendor wired or wireless network by replacing outdated legacy AAA with context-aware policies. By going this route, you get visibility, policy control, and workflow automation in one cohesive solution.

The goal in a healthcare network is to "see all and manage all". When evaluating network policy management solutions, it's important to think about the following:

- Built-in device profiling, a web-based administrative interface, and comprehensive reporting with real-time alerts.
- The ability to collect and leverage all contextual data to ensure that users and devices are granted appropriate access privileges—regardless of access method or device ownership.
- Built-in profiling engine collects real-time data that includes device categories, vendors, OS versions, and more.

There's no longer a reason to guess how many devices are connected to wired and wireless networks. Granular visibility provides the data required to pass audits and determine where performance and security risks could come from.

Key Tips to Identify and Protect Your IoT Network

In healthcare environments, you need a network policy management solution that supports medical grade IoT devices, which are unique as they are often passive devices that do not have CPUs inside. Here are some key tips to think about in a solution feature set:

- Devices are profiled and categorized as new devices are added, so network managers know exactly what they are, what they should look like, and can see possible nuances where rogue devices may signal a potential problem.
- A common policy management platform enables you to manage both wired and wireless devices and dynamically profile and place them in the correct zone.
- In healthcare facilities, protecting confidential patient information is paramount. Hospitals must prove compliance with HIPAA regulations through auditable records. Choose a solution that provides easy access to access logs and reports of device inventory, authentication, authorization, and access trails.

Safe and Secure BYOD Onboarding and Support

Managing the onboarding of personal devices for BYOD deployments can put a strain on IT and help desk resources, and can create security concerns. Choose a network policy management solution that lets users configure devices for use on secure networks, all on their own. Device-specific security certificates even eliminate the need for users to repeatedly enter login credentials throughout the day.

The IT team defines who can onboard devices, the type of devices they can onboard, and how many devices per person. A built-in certificate authority lets IT support personal devices more quickly than an internal public key infrastructure (PKI), and subsequent IT resources are not required.

Get More from Your Investment

We all know that security is expensive and time-consuming to set up, deploy, and manage. But security is a necessity and you need to stay ahead of the hackers, which is tough to do when you're thinking about what's next. When you choose Comport to work with you to solve your network security and policy management challenges with your healthcare network, you will be able to reduce costs. Comport and their technology partners can create solutions that are specifically created to bring together best-of-breed third-party solutions to help provide end-to-end security for your network, as well as patient engagement.

The key to a coordinated network defense is integrating best-of-breed third-party network security IT solutions (such as end-point remediation or app-level policy management at the firewall level) with your network access policy management platform and sharing contextual information back and forth. This is exactly the type of security that is needed in today's mobile enterprise, where more and more Wi-Fi-enabled mobile devices are connecting inside and outside of your network security perimeter. Instead of taking a siloed approach, where your existing systems are blind to each other's actions, select a solution that gives you visibility both ways through the power of integration.

Secure Mobile Engagement

As hospitals look for ways to deliver secure patient engagement through mobile technologies, there are technologies out there that they can leverage. Here are some suggestions to improve patient engagement experiences and maintain security:

- Develop apps on a mobile application development platform that supports electronic beacon technology, which delivers location-based services to their patients, vendors, and other visitors.
- Healthcare facilities can easily create turn-by-turn apps that engage patients and improve their experience with the facility. In today's mobile-driven world, guests will be looking for Wi-Fi access.
- Make sure your network management policy solution provides secure segregated guest access from internal traffic to both maintain access control and deliver a better experience for patients and visitors.
- Use a solution that enables you to define policies that optimize security and access of your healthcare network.

Secure Your Network with Comport

In today's professional services world, your healthcare partner's knowledge and know-how are more than important— they are essential to your IT and clinical success. Comport is well-prepared for the challenge!

Our engineers average 20-25 years of IT experience with industry leaders. We are a Hewlett Packard Enterprise Platinum Partner and a member of their Preferred Healthcare Partner Network, so our expertise in healthcare enables us to be your trusted technology advisor to help you reach your network security goals. Our healthcare network security, policy management, and patient experience solutions include technology from Aruba Networks, an HPE company.

Our actions are guided by what's right for our healthcare clients and their patients. We'll speak up with ideas, and ask questions to understand your full requirements. We owe it to you to be proactive—so your Information Technology reliably supports your institution's clinical excellence and critical business functions.

comport
HEALTHCARE SOLUTIONS

New York Metro Office
78 Orchard Street
Ramsey, NJ 07446
Phone: (201) 236-0505

New England Office
15 New England
Executive Office Park
Burlington, MA 01803
Phone: (781) 270-4784

Mid Atlantic Office
1735 Market Street
Philadelphia, PA 19103
Phone: (267) 223-6673

[1] Web Article: http://www.marketsandmarkets.com/Market-Reports/iot-healthcare-market-160082804.html
[2] Web Article: http://www.hipaajournal.com/largest-healthcare-data-breaches-of-2016-8631/

Hewlett Packard Enterprise
Platinum Partner

Hewlett Packard Enterprise specializations include Platinum: Converged Infrastructure, Networking; Gold: Cloud Builder.

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.