Patient Safety, Security, and Privacy

Extreme Networks for Healthcare

Introduction

The risks of an insecure network and connected medical devices goes far beyond stolen medical records; it's about people's lives. Insulin and infusion pumps, for instance, can be hijacked to deliver a different dose than prescribed. To make matters worse, hospitals may use infusion pumps over a long lifetime, and legacy devices can be extremely vulnerable to cyber-attacks. In an environment flooded with life critical devices, patient safety is of the utmost importance. All devices require a secure connection to reliably and flawlessly communicate via the network and deliver vital patient information, so the networks must maintain severe protection against potential threats and remain uninterrupted.

The reality is, however, that healthcare organizations have not invested in their infrastructure to address these growing threats. With the introduction of new technology, and the continued use of legacy devices, IT requires a network that is simple, agile, and resilient, all while maintaining compliance with strict regulations like HIPAA and GDPR. With Extreme Networks, healthcare organizations can achieve the policy-based network access control and automation needed to remove the risk of human error, validate and protect clinical devices in real-time, and ensure patient safety, security, and privacy. What's more, Extreme Networks is the first major cloud-managed networking vendor to attain ISO/IEC 27001 certification for its Information Security Management Systems (ISMS).

Critical Technology Issues

Maintain Compliance with Strict Regulations

A constant risk to hospitals and their patients are unapproved applications and rogue devices that may appear on the network, and either permit unauthorized access or interfere with other devices. Having a means to monitor all devices and applications that operate across the network is vital for healthcare organizations. Just as important are the audit capabilities necessary to report on who, what, where, when, and how patient data is accessed. With a robust infrastructure and comprehensive network management solution, it's possible to simplify and automate compliance with strict regulations.

Extreme Networks create a secure healthcare network without compromising simplicity through policy-based, end-to-end hyper-segmentation. While traditional network segmentation approaches are complex with multiple levels of protocols, route policies, and access control lists, Extreme's approach based on policy and fabric delivers a simpler, more automated alternative.

Ensure Medical Device and Network Security

Healthcare organizations are going through a fundamental transformation to provide the best patient care, with technology playing a vital role in patient safety, engagement, and treatment. As new, innovative devices and applications are added on to the network, safeguarding

critical patient information and meeting regulatory compliance is essential to protect patients, facilities, and devices from the ever-present threat of breaches. What's more, it is not uncommon for a single medical device system to incorrectly be configured and compromise the entire network.

Extreme Networks provides hospitals with a resilient wired and wireless network infrastructure that efficiently on-boards and manages devices used by patients and clinicians with the necessary security capabilities for data compliance. From a single window, IT can set policy controls to determine device access rights based on user, device type, location, and time of day. This unique capability provides automated, secure, and fast provisioning and control of devices on the network.

Secure IoT and Legacy Devices for Peace of Mind

IoT is having a profound impact in every industry and healthcare is no exception. From remote monitoring systems to smart sensors and medical device integration, connected technologies have become more pervasive in healthcare; and for good reason. IoT has the potential to deliver better patient care, improve operational efficiency, and drive down healthcare costs. However, IoT poses new requirements and challenges to ensure cybersecurity and patient data privacy. In addition, legacy medical devices without inherent internet accessibility are also being connected and significantly increasing security risks.

Extreme Defender for IoT is a unique, award-winning solution that delivers security for end points with limited or no embedded security capabilities. It is especially targeted to aging, wired medical devices that need to roam around a room, building, or campus. It complements a hospital's existing security infrastructure by adding additional defense directly to the device. It can be deployed over any network infrastructure to enable secure IoT management without significant network changes, giving healthcare organizations simple and fast peace of mind.

Hyper-Segmentation and Stealth Simplifies Security

While a healthcare network must be capable of connecting all medical devices, it must also be very selective in doing so. Authorized devices should be expeditiously on-boarded, while unauthorized devices must be prevented from gaining access to the network or moved to a patient/visitor network. Deploying a network that can isolate medical devices from the rest of the network through hyper-segmentation helps ensure healthcare network security. Access control capabilities allow network administrators to authorize device access based on location, time of day, and function. By keeping medical devices virtually separated from all the known and unknown devices, an attack on one device won't lead to a hack on another.

Extreme Networks ensure network security with necessary segmentation and partitioning. Secure network segments can be created quickly and easily, end-to-end, without requiring any additional overlay protocols. The network can be designed to fit the needs of different departments in a traditional multitenant environment, like a clinic or patient records department, and seperate different types of devices and users, such as smart phones or IoT devices worn by patients, and even isolate traffic types for security or regulatory compliance, including medical imaging devices to comply with HIPAA. What's more, through the avoidance of complex configuration issues, network isolation is deployed quickly and easily via simple edge-only configuration.

Comprehensive Service and Support

Hospitals never close and neither does Extreme's 100% insourced 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 Networks 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 by a single network screen for easy management by constrained healthcare IT teams.

Summary

Healthcare organizations today are balancing the complexities of digital transformation with innovative technology, maintaining safety and compliance, and dealing with age-old challenges like streamlining processes and maintaining connectivity – all to drive better patient outcomes. Safeguarding critical patient information and meeting regulatory compliance is essential to protect people, places, and assets from the ever-present threat of breaches. Extreme Networks delivers the end-to-end clinical-grade infrastructure solutions healthcare organizations need to meet the reliability, scalability, security, and intelligence required for life, patient, and mission critical initiatives.

Resources

To learn more, visit the Extreme Networks Healthcare Solution Center.

Solution Guide: Clinical Efficiency and Staff Satisfaction

Solution Guide: Enhanced Patient Care and Experience

©2021 Extreme Networks, Inc. All rights reserved. 24351-0221-19