aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

SOLVING TODAY'S HEALTHCARE MOBILITY AND ACCESS HEADACHES

Securing the network amidst BYOD and IoT

EMERGING TRENDS

According to the American Hospital Association, the number of doctors employed by hospitals have grown by a third from 2000 to 2010. The consolidation in the healthcare industry and the acquisition of private practices is accelerating this trend. Many of these doctors have become "free agents," meaning they work as contractors at several hospitals in their local region at any one time. Nurses are just as mobile, as 80% of Healthcare facilities now hire traveling nurses.

The proliferation of free agents, combined with the growth in personal smartphones, laptops, and tablets for work, has created a security dilemma for hospital IT staff.

How can IT protect the hospital, make data accessible, and adhere to HIPAA regulatory compliance? IT groups are now faced with BYOD, poor user behavior by employees and visitors, password loss, and a host of new threats, like ransomware.

UNDERSTANDING TODAY'S CHALLENGES

BYOD created visibility concerns for IT as these devices – owned and managed by their owners – literally walk out the door every day with sensitive data. Now other concerns have also emerged as devices access the network from outside the perimeter and connecting to guest networks has become the commonplace.

Differentiated employee access – In the hospital setting, the roles of users are clearly defined. Whether it be a front desk receptionist, internal administrator, nurse, or physician each user should have clearly defined access to internal resources in the network. Access control to resources must be defined by user/role, device, and what location they are accessing resources from. Policies can then be created using this information to define access privileges.

For example, admittance staff should have access to an admittance server or application, but should not have access to a patient's prescription records. Doctors should have detailed access to patient records, but not access to a hospital's administration services associated with the ordering of medicine or facilities oriented products.

Managed BYOD – Regardless of the mix of users wanting access to the network, IT can configure Aruba ClearPass to differentiate users based on role, device, and location. This contextual information can then be used in predefined policies that can enforce such things as who can onboard their BYOD devices and have full network access, how many devices they can onboard, what type of devices, and from what location they can access certain resources.

ClearPass can issue certificates to onboarded devices so that stronger authentication, easier revocation, and a simpler user experience is possible. Certificate-based authentication relieves the user of manually typing in passwords on small smartphone screens and protects from password loss. And when accessing certain portals, ClearPass can work with third party multi-factor authentication partners for an added level of security.

IOT ACCESS AND POLICY ENFORCEMENT

Imagine the liability from a breach to a drug infusion pump that threatens the health of a patient? On average, it has been estimated that there are up to 15 networked devices per hospital room that are not smartphones or personal devices. This translates into a huge number of non-traditional devices on any given hospital network that can be considered IoT, in addition to the traditional smartphones, tablets, and laptops.

Patient and visitor Internet access – As the healthcare industry consolidates and margins are squeezed, competition for patients has become intense. In fact, patient and visitor customer satisfaction based on their

Wi-Fi experience has become a key component in customer engagement and retention. Unfortunately for IT, they cannot control what it brought into the hospital.

Patients and family members want simple onboarding and reliable access to the Internet. Portals should represent the hospital brand and be simple to use so that staff and IT resources are not involved. Policy management should seamlessly integrate with wireless equipment to enforce bandwidth limits, length of stay contracts, and MAC caching.

Device compliance and assessments – IT should have the ability to ensure all devices on the network adhere to other regulatory compliance policies such as HIPAA for encrypted storage on all devices with patient information, among many other controls. Archiving of information for devices connecting to a network is also important. ClearPass provides the ability to store data locally or send all connection data to a SIEM solution for long-term archiving.

HIPAA, SECURITY BREACHES, AND THE DISCONNECT

Since HIPAA regulations were introduced two decades ago, patient privacy and portability have become a major focus for hospital IT staff. Recently this changed, as network breaches disrupted hospitals and compromised sensitive patient information. These breaches –or hacker takeovers—usually happened when mobile users unwittingly revealed credentials or exposed their unprotected device, which opened up the network to attacks via malware or ransomware.

Over the years HIPAA requirements directed hospital resources to prioritize privacy, where less attention was given to the cyber security threats. But the more hackers get away with monetizing the release of hijacked networks, the more incentive healthcare has for an adaptive defense model for internal users, patients, and visitors.

ARUBA CLEARPASS — CUSTOM BUILT FOR HEALTHCARE

With ClearPass, healthcare IT can allow BYOD users to self-onboard their devices without direct IT staff involvement. Once onboarded, user roles, device, and location information are tied back into pre-defined policies created by IT to ensure appropriate access is available for the appropriate user in the hospital.

Similarly, with the ClearPass OnGuard application, IT can ensure any laptop on the network is HIPAA compliant with encrypted storage or the user will be blocked from the network, and patches and hotfixes, anti-virus, and anti-spyware, updates are enforced, among other features. ClearPass can also prioritize network access.

Headless network connected IoT devices such as infusion pumps or vital signs monitoring equipment are traditionally a challenge to discover with standard fingerprinting tools; ClearPass has the ability to allow IT to custom define fingerprints for headless devices and categories. For example, an infusion pump on the network can be categorized in ClearPass and allowed priority access over any other device type connecting to the network.

With ClearPass Guest, IT can now show value by ensuring reliable, simple guest access to retain customers and enhance the visitor and patient experience. ClearPass can grant either access to any user via social login, usage agreements, or via login where access can be restricted to certain network assets with auditable logs in lieu of simple Internet connectivity. Visitors can be granted access over certain periods of time so that after a one-time login to the guest network, the MAC address can be cached to allow seamless connectivity each time the user connects to the network again.

Most hospitals are multi-vendor environments, not only for point security solutions, but also for networked devices. Unlike other vendors, ClearPass works with any network infrastructure and communicates with any point security solution to bolster your existing network investments for the mobile workforce – all included with ClearPass.

ClearPass is built for the modern and mobile healthcare setting. To learn more about ClearPass Policy Manager and the Onboarding, Guest, and OnGuard applications, click here.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.844.473.2782 | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com