aruba
a Hewlett Packard Enterprise company

AT A GLANCE

MODERNIZING CYBERSECURITY IN HEALTHCARE

Healthcare is one of the most targeted and breached industries by cybercriminals. Stolen electronic medical health records are highly lucrative as they give a comprehensive and multi-faceted profile of an individual from which to launch personal identity theft scams as well as phishing and a variety of other cyberattacks to gain access to company networks.

BROAD ATTACK SURFACE

Healthcare network infrastructures are complex. The physical facility is open to a constantly changing array of new visitors who access guest networks with personal devices or can even connect into unsecured wired ports. The network supports many different types of Internet connected IoT devices and sensors in addition to staff computers, tablets and handhelds - both company owned and BYOD. And with the expected useful life of biomedical devices at 10+ years, IT and security teams also have to deal with older, outdated connectivity and security standards. All this widens the attack surface and makes the infrastructure more difficult to secure.

CLOSING THE GAPS

Although healthcare organizations are investing in cybersecurity, recent breach statics suggest there are opportunities for improvement to stay ahead of threats.

Let's investigate how modern security solutions from Aruba can help healthcare organizations better:

- Gain visibility into everything connected to both wired and wireless networks
- Ensure that the appropriate IT access policies are applied to users and devices

There has been an upward trend in data breaches over the past 9 years. Healthcare data breaches are now being reported at a rate of more than 1 per day.[1]

Healthcare breaches of 500+ records during 2009-2017[1]:

- 2,181 breaches
- Theft/exposure of 176.7M patient records
- 54% of US population

- HIPAA Journal

On the black market, the going rate for your social security number is 10 cents. Your credit card number is worth 25 cents. But your electronic medical health record (EHR) could be worth hundreds or even thousands of dollars[2]

- Forbes

Reference Sources:

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/

[2] https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#4257843850cf

SECURE INFRASTRUCTURE

For over 15 years, Aruba has delivered high performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.
- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall (PEF) enables user/application visibility and policy enforcement based on user role, application, device and location.

ACCESS CONTROLS

Security starts with visibility of who and what is connected to your network and what they are doing on the network at all times.

- **Know What is on the Network**
  Today, many IoT devices are built on standard hardware platforms. That can make it extremely difficult to know exactly what is on your network. For example, a security camera and smart thermostat could both be built on the same Linux platform. ClearPass Device Insight uses machine learning to identify devices based on multiple attributes, traffic destination, and communication frequency. Knowing what is on the network is the first step in protecting it.
- **"Zero Trust" Access to the Network**
  Aruba ClearPass NAC (Network Access Control) delivers discovery, profiling, authentication and authorization of users, and devices, including IoT, before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network.
- **Precise Control of Access to IT Resources and Assets**
  ClearPass provides adaptive, granular policy-based access controls by user, device, role and location. These controls ensure that each user, device, or IoT has access only to the network, application, or IT resources and assets they are approved for.
- **Intelligent Segmentation**
  Aruba Dynamic Segmentation leverages the Aruba secure infrastructure, PEF and ClearPass Policy Manager to deliver a network edge that securely isolates and separates user and device traffic across wired and wireless networks.

NEXT STEPS FOR A HEALTHIER SECURITY POSTURE

With advanced access controls and interoperability with over 140 multi-vendor network and security solutions, you can rest assured that Aruba will give you the visibility you need and the confidence that your security policies are dynamically enforced. With Aruba, your security posture is in a much healthier state.

TO LEARN MORE

- https://www.arubanetworks.com/solutions/healthcare/
- https://www.arubanetworks.com/solutions/security/

aruba
a Hewlett Packard Enterprise company

AAG_SecurityInHealthcare_SK_020420 a00065994enw