Seliton®

Solving the problem of IT Security in Hospitals

One of the biggest unsolved puzzles in healthcare technology - particularly around online security and patient data protection - is how to construct, staff, equip and secure a “hospital without walls”. Essentially a healthcare system that isn’t restricted by location when it comes to technology and communication, but which relies on equipment that’s highly vulnerable to cyberattacks, and where threats are faced by weak security.

You want a solid network security system build to your needs

You can’t avoid security risks completely. But you can be in control of them while opening up essential resources to users and creating a non-intrusive workplace. You can prioritise security and reduce the burden on your IT department, employees, patients and visitors.

Network Access Control (NAC): a sensible approach

Most data breaches occur behind firewalls, so NAC is a critical component of multi-layered security. It’s not a silver bullet against every threat, but NAC helps build a safe, productive work environment, delivering an immersive, seamless user experience.

Dangers of wired access

In the face of wireless networks and devices, we often forget about protecting wired ports readily available in public areas like waiting rooms. These can be big security holes, and the devices plugged into these ports may lack the enterprise security you need, allowing third parties to piggyback into your network.

NAC prevents this. That’s because access must be given before any device can access a network through a wired port, and the access request is logged.

NAC also helps comply with NEN7510 standards, which govern healthcare information security.

Hospital Internet & WiFi: a black hole for cybercriminals

Hospital networks are particularly challenging to secure because of the number of people and devices needing (or wanting) to connect:

Doctors and medical staff carry devices to log real time patient information

There is a growing fleet of wireless medical devices

Plus, the personal devices of patients and visitors

NAC gives greater control over devices accessing the network and what they can access within it. When users request access to the hospital Internet or WiFi, the system immediately checks their credentials by, in most cases, checking if a certificate exists. Patient databases and other sensitive areas can be placed in restricted networks. Malicious actors will struggle to move laterally throughout networks, limiting the dangers posed by malware attacks.

While healthcare is blending to provide the best solution for every patient it also means that those who need to access information aren't always sitting at their desk – they are often working remotely from different devices.

Connecting to a network remotely from unknown devices is risky, as not all devices will be secure. Additionally, healthcare staff are often unfamiliar with even the most basic cyber security best practices. Compromised devices must never gain access to the network, as just one hacked device can leave a whole organization wide open.

Breaking up with hackers

Medical devices don't contain patient data; they fulfil other functions like monitoring heart rates and dispensing drugs. But they can provide a bridge to other systems in the network that does hold sensitive information. And many lack the necessary security. Attackers can use these vulnerable devices to attack a server to access sensitive information or install ransomware.

Network segmentation solves this challenge, improving security and control over large-scale networks. Network segmentation divides a large network into smaller - isolated - segments.

By breaking connections between medical devices, cybercriminals can't jump from one to the other, stopping them from gaining access to more sensitive information.

Network administrators can assign different monitoring policies to different segments and put access controls on the traffic between segments. If the hospital network is segmented wisely, most traffic stays between devices and applications within each segment, with much less traffic crossing segment boundaries. Segmentation therfore improves network monitoring, performance and security. Network segmentation prevents unauthorised user access and malicious attacks on medical devices by containing attacker activity to disparate parts of the network.

NAC only gets better as more and more devices are added

The average hospital room contains 15 to 20 connected medical devices. While each device plays a role in delivering care and operational efficiency, hospitals rely on many legacy devices that were never built with security in mind. It's also cumbersome to update devices or carry out security patches.

NAC provides access management and network visibility using policy enforcement on devices and users. Administrators can dynamically assign switch ports to VLANs, separating and isolating devices into different network segments, based on the device or user authorisation and characteristics.

VLANs let network administrators keep devices and network resources separated from each other, while still connecting to the same physical network port. Once VLANs are defined, you can create Access Control Lists to restrict specific communication to and from the VLAN and the devices within it.

NAC won't disrupt the convenient working practices of your medical staff

Healthcare staff are busy enough - working long hours with tight deadlines - without the hassle of adding online security processes to their work. They need minimal distractions. NAC is a secure and user-friendly certificate based authentication. It constantly runs in the background, without the need for user input. Authentication happens without them noticing, so they won't have to continually authenticate themselves. These digital certificates provide the best workflow for users, with the highest level of security.

Users can access the network areas they need every time, reducing IT queries. And they're scalable, so administrators can simply add or remove users and devices as required.

Better together

Authentication can be seen as a burden. At Soliton, we're changing that perception. We make implementing and maintaining Network Access Control easy and give users a simple solution on any device or operating system.

Soliton works strategically with business partners to build trust and a shared vision. Combining extensive experience and knowledge of highly qualified IT security experts, we help customers manage and mitigate network security risks, in and out of the workplace - without disrupting users.

Partnering with us can be beneficial and profitable to you, your suppliers, and users. We deliver partner expertise and consultants for your NAC projects, ensuring NAC is implemented in phases, aligned to your goals and without burdening users.

At Soliton, we have a straightforward goal: to support our customers in reducing the attack surface and mitigating risk by applying strong authentication, least privilege and isolation to networks and applications. The result for you: greatly improved security posture.

Discover how you can prioritise security and reduce the burden on your IT department, employees, patients and visitors.

Get in touch