NOZOMI NETWORKS

SOLUTION BRIEF

Unprotected IoT Devices Threaten Hospitals and Healthcare organizations

Healthcare organizations are the second most targeted sector for cyberattacks due their critical and sensitive patient information, which is highly sought after by cybercriminals for ransomware and double extortion schemes. Cyberattacks on hospitals can disrupt patient-critical and operation systems, leading to delays in patient care and potentially putting lives at risk.

Healthcare organizations have embraced automation and digitization for improved patient care, enhanced monitoring and increased efficiency. Whether it's on the medical side – MRI machines, defibrillators or patient monitors – or on the building side – elevators, energy management, HVAC systems or IoT devices such as IP cameras, smart locks or gateways – OT and IoMT technologies have significantly increased healthcare organizations' attack surfaces. A connected device is now an access point to the hospital's network and its sensitive patient information. Hackers can exploit a vulnerable online network, severely disrupting patient care.

Nozomi Networks makes it easy to manage your complex OT and IoMT environments. Our scalable and flexible solution closes OT and IoMT blind spots and security gaps by providing comprehensive visibility and monitoring of networked equipment, medical devices and building systems.

As healthcare organizations connect more IoT devices to their network, their attack surfaces have expanded exponentially.

According to the US Cybersecurity and Infrastructure Security Agency (CISA), 67 percent of medical device manufacturers believe an attack on one or more of their devices is likely.

Benefits of the Nozomi Networks Platform

Eliminate Blind Spots

The Nozomi Networks platform provides accurate and extensive information on smart hospital OT and IoT automation and medical devices for a wide range of vendors and functions. It also supplies data flow diagrams, revealing communications between systems. Our platform eliminates blind spots and improves situational awareness, with 24/7/365 passive monitoring to provide continuous updated risk information for any number of devices. Nozomi Networks also supports DICOM and HL7 standards.

Manage Cyber Risk, While Adding New IoMT Devices

Your vulnerability to cyber risks grows as you add more wireless connected IoMT devices and OT building automation systems to your legacy infrastructure. But how can you gain visibility into the wireless assets in order to secure them? Nozomi Guardian Air detects wireless specific threats that penetrate hospital systems. Through triangulation, it identifies the approximate location of the wireless asset, enabling you to quickly respond and prevent unauthorized control or manipulation of devices that could cause harm to patients.

Mitigate Operational Threats

Nozomi Networks detects cyber risks and deviations from baseline system behavior. It provides alerts and actionable insights to your understaffed security teams so you can mitigate cyber and operational threats before they impact healthcare delivery or harm patients. Suspicious communications and reliability risks are immediately identified and prioritized for action.

Keep Medically Critical Systems Running and Your Patients Safe

Get advance warning of failing OT and IoMT devices and network stability issues as you modernize your systems. The Nozomi Networks platform anticipates issues with your OT/IoMT systems so problems can be fixed before they cause disruptions. It future-proofs your hospitals with continuous threat intelligence to counter tomorrow's malware and provides scalability to handle new smart medical technology and a multitude of vendors.

Let's get started

To see the Nozomi Networks platform for yourself, schedule a demo.

Request a Demo

nozominetworks.com/demo

Nozomi Networks accelerates digital transformation by protecting the world's critical infrastructure, industrial and government organizations from cyber threats. Our solution delivers exceptional network and asset visibility, threat detection, and insights for OT and IoT environments. Customers rely on us to minimize risk and complexity while maximizing operational resilience.

NOZOMI NETWORKS

nozominetworks.com

NN-CSHC-SB-8.5x11-002