Cybersecurity in Patient Monitoring

Security Framework for Patient Monitors, Control Centers, and Gateways

NIHON KOHDEN

CYBER SECURITY – A GLOBAL CHALLENGE

The realm of operational security is no longer confined to administrative IT systems; instead, it now encompasses critical infrastructures. Networks that incorporate medical devices face significantly higher risks in cases of malfunction compared to conventional IT environments. This vulnerability is particularly pronounced in patient monitoring systems. If compromised or fully dysfunctional, these systems could fail to detect life-threatening patient conditions in a timely manner.

Nihon Kohden adopts a comprehensive approach to safeguarding patients and ensuring the reliability of patient monitoring. This commitment extends beyond mere device safety to include the entire spectrum of networking and communication with hospital systems.

Our approach to monitoring network security considers several distinct elements: device security, network security, and the security of connections to hospital networks. This synergy forms the foundation for warding off threats and malfunctions within the IT domain.

As a manufacturer of medical devices, Nihon Kohden vigilantly monitors the market landscape for emerging vulnerabilities within the systems in use. Prompt actions are taken to ensure the operational safety of devices and thereby patient safety. A dedicated “Cyber Security Task Force” was established to assess inquiries, formulate measures, and devise methods for enhancing the security of our medical solutions, all in response to prevailing threats.

SECURITY BY DESIGN

Shared Responsibilities of Vendor and User

The cybersecurity of medical devices represents a joint responsibility between manufacturers and operators. For Nihon Kohden, as the manufacturer, this responsibility involves not only securing the medical devices themselves but also establishing suitable specifications for deploying these devices within their intended operational and network environment.

Operators, by virtue of their primary responsibility for these environments, must act with a safety-conscious approach and adhere to the manufacturer's recommendations. Nihon Kohden's role is to support operators in deploying purpose-specific products and services, thereby ensuring a high level of operational security.

Device security is achieved through manufacturer-defined tasks that align with the device's intended use, along with instructions for secure integration into a medical network. Healthcare providers must integrate cybersecurity measures during system implementation to establish a protected environment (according to IEC 80001).

Nihon Kohden incorporates processes during the design phase that account for potential attack vectors. As new threats appear, proper countermeasures are swiftly implemented to safeguard devices. Proactive monitoring of the network system detects potential attacks, enabling protective measures to be enacted before threat actors can compromise the system.

Network Security

Commonly exploited threat vectors like phishing, malicious web pages, and pop-ups are irrelevant here, as the system stays disconnected from the internet and the hospital network. The risk of data exfiltration and compromise is nonexistent, with no connection to command-and-control servers.

The monitoring network, including bedside monitors, central nursing stations, and gateway solutions, operates within a physically isolated network as specified by the manufacturer. This segregation offers the advantage of complete separation from the hospital network, mitigating any potential interference even if the hospital network infrastructure experiences disruptions such as management component failures or configuration losses.

Real-time data transmission characterizes the surveillance network. Any communication issues between surveillance monitors and monitoring centers trigger communication error alerts.

Nihon Kohden employs advanced software to monitor network traffic, detecting anomalous activity at an early stage and implementing protective measures. Consequently, network monitoring and control tools are seamlessly integrated into the network care solution.

If the monitoring network is to utilize clinic-operated active components (such as switches), the client must conduct a risk assessment. This assessment comprehensively evaluates all factors influencing communication between surveillance monitors and control centers. It is imperative to prevent data traffic mixing at all costs, even if faults occur in the switch's control components.

Transmission Security and Data Protection

To prevent unauthorized devices from accessing the network, MAC address filtering is employed at network edge components, bolstering endpoint security.

Only approved devices are granted access to the patient monitoring area, effectively blocking all other devices. Additionally, Nihon Kohden ensures data confidentiality by encrypting data between monitoring monitors and control centers.

For telemetry devices or transport monitors operating in the client's WLAN (a planned action requiring a telemetry gateway), the connection between end devices and access points must be secured with at least WPA2. These end devices support various standard security methods, including WPA2 (PSK, Enterprise, 802.1x).

Transition to the Clinic Network – Data Exchange

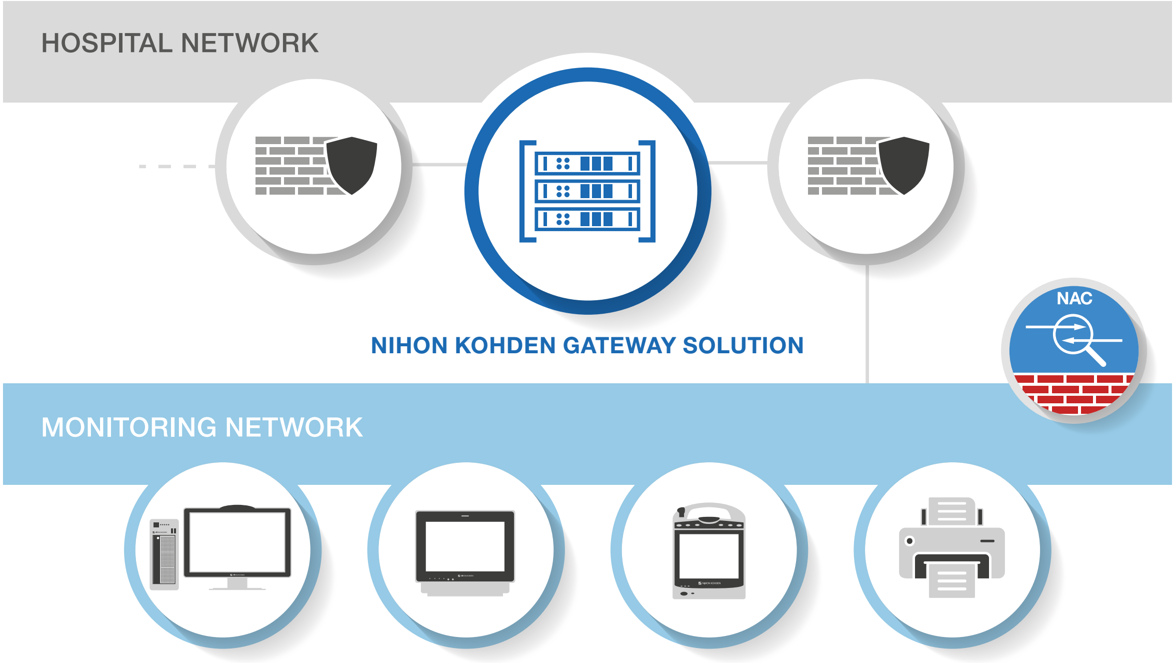
Nihon Kohden's role centers on supporting operators through dedicated products and services to maintain high operational security.

To enable data exchange between the monitoring network and hospital/clinic systems, a gateway is essential. This gateway, equipped with two interfaces, preserves the physical separation of the monitoring network. It retrieves, processes, and exchanges data between the monitoring network and the hospital or clinic network. Centralized data centers enhance service availability and contribute to cybersecurity through segregated systems and controlled access. Nihon Kohden facilitates gateway installation in data centers, supporting all virtualization solutions available in the market.

Servers operate on modern Microsoft Windows platforms. Applications and extensions are exclusively installed as services, minimizing the need for server logins, which are reserved for service purposes. The system accommodates common antivirus scanners, and the internal firewall can be activated if necessary and not already enabled at the network level.

Nihon Kohden provides up-to-date information on Windows updates and patch validation through its website. Timely installation of approved patches ensures the system's secure and protected operation.

Recommendation on Network Security



To ensure data integrity and security within the monitoring network, strict traffic segregation is imperative. Nihon Kohden advises physical separation between the monitoring network and client traffic. Employing a divided network infrastructure offers enhanced protection against attacks originating from the client network.

For comprehensive network protection from the client network, it is recommended to set up firewall zones, with port-level protection for each network card and gateway direction.

Device Safety

All stationary surveillance monitors and telemetry devices feature hardened operating systems that are distinct from Windows or Linux platforms.

Remote services are minimized and exclude critical interventions. Nihon Kohden prioritizes patient safety through a cautious approach. The likelihood of external attacks or data compromise through information extraction is low, given the non-public nature of the data preparation protocol.

Robust data encryption and endpoint-to-endpoint device integrity safeguards prevent data access and the infiltration of third-party data.

Monitoring centers are protected against unauthorized software modifications through whitelisting and the confinement of startup systems within a protected area. The startup system is outsourced to a secure area, preventing malware execution after restarting the control center.

Improving Healthcare with Advanced Technology

Since its foundation back in 1951, Nihon Kohden's mission has been to improve the quality of life with advanced technology. We provide solutions for diagnosis, critical care, clinical information, and in vitro diagnostics – and we are dedicated to collaborate with you to meet the challenges of healthcare today and tomorrow.

Visit **www.nihonkohden.com** to find out more.

NIHON KOHDEN EUROPE GmbH
Raiffeisenstrasse 10, 61191 Rosbach, Germany
Phone: +49 6003 827 0, Fax: +49 6003 827 599
Internet: https://eu.nihonkohden.com, E-mail: info@nke.de

NIHON KOHDEN

This document may be revised or replaced by
Nihon Kohden at any time without notice.