Industry: Healthcare

Use Case: Hospital Network in Germany

The hospital is a leading healthcare provider in North-West Germany, employing 3,500 staff members and serving over 500,000 patients annually. Its IT infrastructure spans 18 locations, integrating innovative medical technologies as well as legacy systems.
The hospital handles vast amounts of sensitive patient data, making robust cybersecurity measures essential to protect operations and comply with data protection regulations like GDPR, **NIS2**, KRITIS, B3S and other healthcare-related **cybersecurity and data protection obligations.**

Alignment with Broader Trends in Healthcare Cybersecurity

In healthcare, digital transformation has introduced expanded attack surfaces, mainly through the adoption of telemedicine and electronic health records (EHRs), necessitating robust security measures to maintain compliance with healthcare regulations. Ensuring operational resilience is critical, as cybersecurity incidents can disrupt service delivery, posing risks to patient safety and continuity of care. Furthermore, achieving regulatory compliance requires a comprehensive approach that provides visibility across digital assets while aligning with strict healthcare security standards.

Searching for an On-Premises Solution with Centralized Visibility and Monitoring

The solution should provide complete oversight of hybrid IT environments, including data centers, IoT devices, and remote systems. It should detect anomalies through a centralized interface, safeguarding critical medical data.

The Challenges in Detail

1. Data Privacy and GDPR Compliance

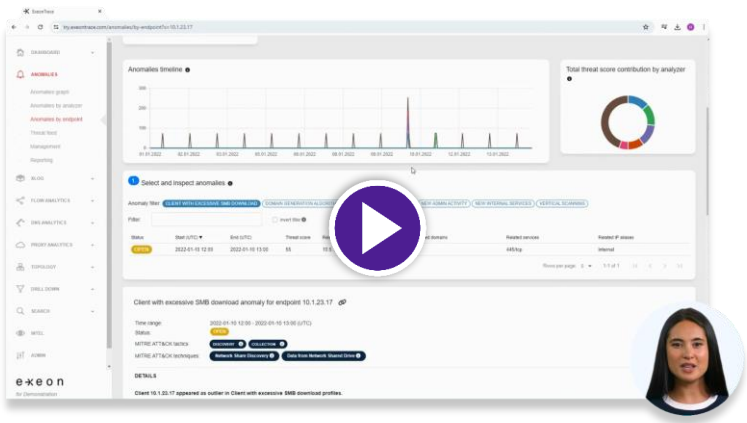
Deployment on-premises was mandatory to ensure sensitive data remains within the hospital's secure network. The platform processes pseudonymized data, fully meeting GDPR and Swiss regulatory standards.

2. Medical Device and Network Segmentation Protection

There is a need to monitor activity even within segmented networks to identify unusual activities like unauthorized data access and to ensure the security of critical systems such as IoT medical devices.

Detecting new, complex threats in OT

Watch the demo video



exeon
Smart Cyber Security.

3. Advanced Persistent Threat (APT) and Ransomware Protection

Ransomware, zero-day and supply chain exploits, and insider threats should be detected early to enable proactive mitigation before operations are affected.

4. Legacy Systems Security

Older diagnostic devices are to be secured with customized monitoring rules. The solution should also detect anomalies in communication patterns or unauthorized access attempts in legacy systems.

5. Non-Disruptive Implementation

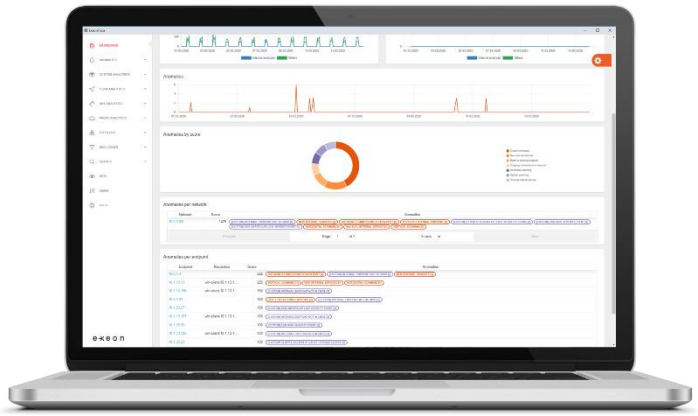
It should be possible to implement a software-only solution very quickly, ideally without additional hardware, as critical hospital operations must continue without interruption during the implementation phase.

6. Support for Zero Trust Strategies

Continuous authentication and monitoring of all users and devices, granular access controls should support integration into future Zero Trust architectures.

Results and Benefits

- **Comprehensive, centralized network visibility:** Using NetFlow data, the hospital monitors all network traffic and efficiently identifies anomalies via a central user interface. This enables end-to-end visibility across medical devices, patient systems and administrative networks.
- **Protects sensitive data:** On-premises, pseudonymized data processing ensures GDPR compliance while protecting sensitive patient data.
- **Protects IoT and medical cyber-physical devices:** Secures IoT devices and medical devices through behavioral analysis and metadata monitoring.



- **Integration of legacy systems:** Specialized monitoring rules secure legacy systems that are critical to patient care.
- **Agentless detection:** AI-driven metadata analysis secures devices without the need to install agents on medical devices.
- **Real-time threat detection:** Detects and reports anomalies quickly to prevent disruption to patient care.
- **Compliance support:** Advanced reporting and event management meet stringent healthcare regulatory requirements.
- **Insider threat detection:** Identifies unusual access patterns to protect sensitive information from internal threats as well.
- **Seamless integration:** Easy integration into existing IT infrastructure to minimize business disruption.
- **Scalability:** The system adapts to growing and complex hospital networks and ensures flexible deployment.
- **Enhanced SOC support:** Complements tools such as SIEM, SOAR and EDR and improves security operations and response times.
- **Minimal disruption:** Non-intrusive integration eliminates downtime and ensures continuous hospital operations.

exeon
Smart Cyber Security.

Other critical infrastructures who trust in ExeonTrace:

solothurner spitäler soH

Bonn Netz

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

ExeonTrace: Secure Hospitals, Seamless Care

ExeonTrace provides its customer a comprehensive, scalable and DSGO-compliant cyber security solution tailored to the unique challenges of hospitals.

ExeonTrace's ability to secure distributed networks, protect legacy systems and detect advanced threats ensures the continued safety of critical medical operations. By adopting ExeonTrace, hospitals can approach digital transformation without compromising security or compliance.

Why Hospitals Choose Us

In this testimonial video, Patrick Käppeli, Network Engineer at our valued customer Solothurner Spitäler, explains how ExeonTrace safeguards their operations.

Allianz für Cyber-Sicherheit

CYBERSECURITY MADE IN EUROPE

ATTESTA ISO 27001 CERTIFIED

Exeon Analytics AG
contact@exeon.com
exeon.com

Grubenstrasse 12
8045 Zürich
Switzerland

LinkedIn

YouTube