Axonius

Axonius for *Healthcare*

Complete Protection for the Connected Hospital Overview

Hospitals today operate as digital ecosystems. From bedside monitors to MRI machines, from HVAC systems to pharmacy automation, every component is connected, and every connection introduces risk. Traditional security tools weren't designed for this reality.

Axonius for Healthcare delivers complete protection for the connected hospital. Purpose-built for clinical networks, it provides full visibility, continuous monitoring, and real-time threat detection across all connected devices, without disrupting patient care.

By unifying visibility, context, and control, Axonius helps healthcare organizations safeguard patients, maintain compliance, and prevent operational disruption from inside the network.

A Perfect Storm of Complexity, Connectivity, and Risk

Healthcare networks are expanding faster than teams can secure them.

Unmanaged devices everywhere

Thousands of IoMT, IoT, and OT systems connect daily, often with outdated firmware or default credentials.

Siloed operations

Biomed, IT, and Security teams each manage separate tools and datasets, creating visibility and response gaps.

Flat networks, high impact

Once an attacker gains access, lateral movement can quickly compromise critical care systems.

Regulatory and patient safety pressure

HIPAA, HICP, NIS2, and Joint Commission requirements demand verifiable proof of protection and continuity.

Traditional IoT inventory tools stop at visibility. Hospitals need actionable intelligence and control, a solution that protects connected devices as dynamically as modern threats evolve.

The Axonius for Healthcare *Advantage*

1 Total Clinical Network Visibility

See everything in your hospital environment, from infusion pumps and imaging machines to workstations and smart infrastructure.

- Automatically discover and classify every connected device using passive traffic analysis.
- Assign contextual risk scores based on vulnerabilities, exposure, and care criticality.
- Maintain a live, continuously updated asset inventory without agents or active scans.

2 AI-Powered Threat Detection

Identify and respond to threats other solutions miss.

- Detect lateral movement, unauthorized scans, protocol misuse, and anomalous behavior.
- Leverage healthcare-trained AI that translates raw network activity into plain-English narratives.
- Generate high-fidelity, SOC-ready alerts that drive faster, more confident response.

3 Intelligent Response and Enforcement

Contain threats before they impact care delivery.

- Segment, quarantine, or isolate compromised devices using device-aware playbooks.
- Integrate seamlessly with SIEM, SOAR, NAC, and firewalls for coordinated enforcement.
- Apply enforcement methods that protect operations without disrupting patient safety.

4 Built-In Compliance and Audit Readiness

Simplify proof of security across every device class.

- Validate continuous compliance with HIPAA, HICP, and NIS2 standards.
- Generate audit-ready reports with contextual device data and risk posture.
- Demonstrate control coverage across both IT and clinical networks in minutes, not months.

The Results: Stronger Security, Simpler Operations, Safer Care

Improved Efficiency
Unite IT, Security, and Biomed with a single view of every asset.

Accelerated Response
Act immediately on high-fidelity alerts with automated playbooks.

Reduced Complexity
Consolidate tools and eliminate manual device management.

Patient Safety First
Maintain uninterrupted care while strengthening cyber resilience.

Proven Compliance
Automatically align and report against regulatory frameworks.

Capabilities That Turn Insight *Into Action*

Capability	Description
Passive Discovery	Continuously identifies every connected device, medical, IoT, and OT; without deploying agents or active scans.
AI-Based Threat Detection	Detects anomalous activity and translates it into plain-English attack narratives for faster response.
Device-Aware Playbooks	Provides model-specific response guidance for isolating or segmenting compromised assets.
Integration with Enforcement Tools	Works with SIEM, SOAR, NAC, and firewalls to trigger coordinated containment.
Real-Time Risk Scoring	Automatically ranks device risk based on vulnerabilities, exposure, and clinical impact.
Contextual Enrichment	Correlates each device with firmware, utilization, and care function for prioritization.
Compliance Reporting	Aligns with HIPAA, HICP, and NIS2, generating evidence for audits automatically.
Agentless Deployment	Deploys passively through a network appliance, ensuring zero impact on patient care.

Why Axonius for Healthcare

Purpose-built for complex, regulated healthcare environments.

Extends the Axonius Asset Cloud to cover medical, IoT, and OT systems.

Designed to unify IT, Security, and Clinical Engineering workflows in one platform.

Scales seamlessly from single hospitals to multi-facility health systems.

Axonius for Healthcare helps hospitals strengthen security, maintain compliance, and deliver safer care, all through a single platform built to secure what matters most: the connected network behind every patient experience.

Visit www.axonius.com

Learn more

Axonius