

Managed HTM Cybersecurity with Ordr and Sodexo

OVERVIEW

Internet of Medical Things (IoMT) and other connected devices are now commonplace across the healthcare eco-system. Patient care and operational efficiency increasingly rely on these connected devices, but too often, vulnerable devices leave hospitals open to ransomware and other cyber-attacks. At the same time, healthcare organizations struggle with accurate real-time inventory of devices in their CMMS, leading to challenges with locating them for patching and maintenance. Addressing compliance becomes even more complicated with devices often running outdated operating systems and the FDA's stringent requirements on what can be modified on. Healthcare cybersecurity requires a strategy that enables visibility into devices, identifies and mitigates risks, and optimizes efficiencies.

CHALLENGES

- ✓ Maintaining accurate device visibility
- ✓ Understanding unique device characteristics
- ✓ Locating devices for patching and maintenance
- ✓ Identifying and mitigating risks for devices with vulnerabilities
- ✓ Enabling operational efficiencies

PROTECTING AND MITIGATING RISKS FOR CONNECTED HEALTHCARE DEVICES WITH ORDR AND SODEXO

Sodexo Managed HTM Cybersecurity services, built on the Ordr platform, delivers the experience, expertise, and technology that HTM teams need to manage, mitigate risks, and secure all connected healthcare devices.



Ordr is the leader in connected device security, with a proven platform deployed across hundreds of healthcare delivery organizations. The Ordr purpose-built platform can discover and secure everything connected—from traditional servers, workstations, and PCs to IoT, IoMT, and OT devices.



The Ordr platform delivers the following benefits for HTM teams:

- Automate and simplify real-time medical device inventory
- Enable asset reconciliation with CMMS/CMDB
- Identify, prioritize and mitigate clinical and cybersecurity risks
- Gain vital insights into device utilization for operational efficiencies
- Accelerate device management workflows



Sodexo Healthcare Technology Management (HTM) services focus on workflow safety, quality, and efficiency to allow hospitals or healthcare system to deliver the highest levels of patient care and improve outcomes. Sodexo services help optimize medical equipment inventory, advise on equipment replacement and purchases, provide on-site maintenance and repair.

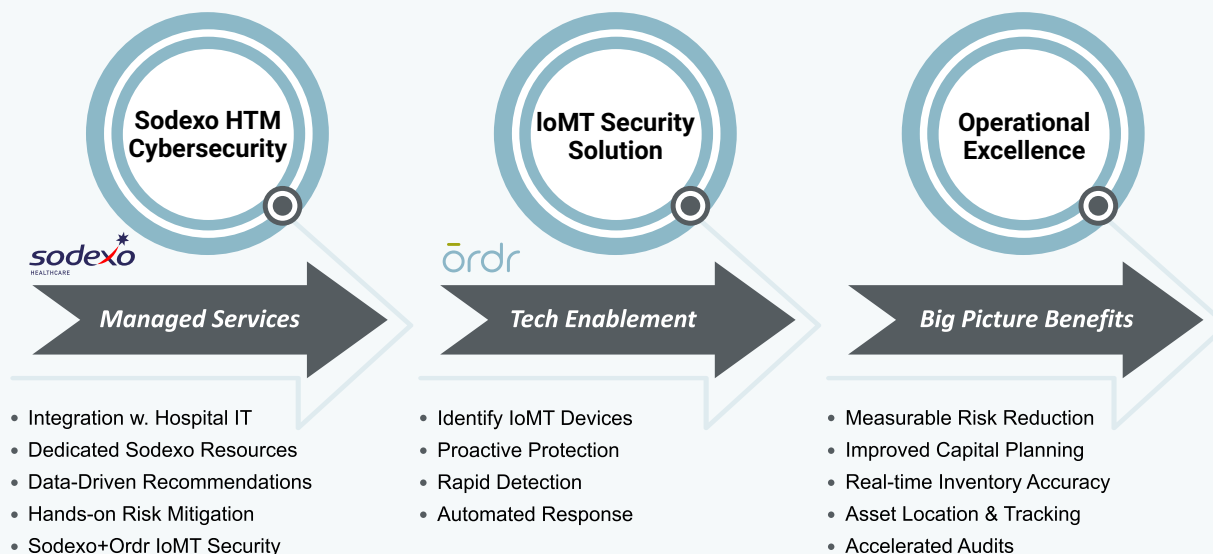


The Sodexo IoMT cybersecurity program adds cybersecurity services for hospital or healthcare systems deploying Ordr platform to manage and mitigate risks such as:

- Analysis of device insights that helps quickly identify security gaps and prioritize mitigations
- Investigation of unknown devices to help support inventory reconciliation
- Contextualization of asset & risk data to support tracking, alerts, and quality assurance

Sodexo + Ordor IoMT Security Solution

MAXIMIZING VALUE THROUGH PEOPLE, PROCESS, AND TECHNOLOGY



HTM DEVICE MANAGEMENT AND SECURITY USE CASES AT A GLANCE:

 Asset Inventory & Management Automate asset discovery and classification to maintain a real-time, accurate inventory of all connected devices synchronized with CMMS tools.	 Vulnerability & Risk Management Prioritize mitigation efforts with risks scores, and identify devices with vulnerabilities, weak passwords, expired certificates, manufacturer and FDA recalls and more.	 Map Device Connectivity & Flows Easily locate devices with connectivity details and actual device pictures. Map communication flows to internal systems and malicious domains.	 Threat Detection & Response Identify high-risk devices and quickly isolate devices with active threats. Baseline device behavior to identify devices behaving abnormally.
 Device Utilization & Capital Planning Gain device utilization insights to optimize efficiencies, schedule device maintenance and maximize the value of the hospital's capital investment.	 Address Compliance Maintain an up-to-date, accurate inventory, identify devices with PHI, and monitor for compliance issues such as medical devices in the guest network.	 Segmentation & Zero Trust Dynamically generate policies to segment devices with outdated operating systems, enabling them to stay in operations while limiting exposure.	 HTM Cybersecurity Strategy Work with Sodexo's experienced teams to create a security strategy, execute plans and optimize security to ensure secure, effective patient care and operations.



Ordor is the leader in connected device security. Organizations worldwide trust Ordor to provide real-time asset inventory, assess connected device risk, address compliance, and accelerate IT initiatives such as zero trust. Ordor is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information about Ordor, visit <https://ordor.net/solutions/healthcare/> and follow Ordor on [LinkedIn](#) and [Twitter](#).



Sodexo Healthcare Technology Management supports care delivery by providing visibility and productivity through scalable technology management. We are a people-focused strategic partner that is invested in your organization's clinical and financial performance across your system of care. To learn more about Sodexo Healthcare Technology Management (HTM) solutions, visit <https://us.sodexo.com/industry/healthcare.html>.