OrdrAI Protect for Healthcare

Protect Every Connected Asset — IoMT, IoT, OT, IT — With Advanced Threat Detection, Deep Behavioral Intelligence and Segmentation

The modern healthcare cybersecurity landscape is evolving and expanding rapidly, with connected assets ranging from medical devices such as infusion pumps,imaging systems, and EKG machines to building management systems, IP cameras, smart lighting, and HVAC systems. Security teams struggle to gain visibility into all connected assets, including the 40% of devices that are unmanaged and go undetected creating security blind spots. Recognizing unauthorized data flows or Internet communications poses another challenge, as does identifying and mitigating against threats to mission-critical medical devices without compromising patient safety or confidential medical information.

Introducing OrdrAI Protect for Healthcare

OrdrAI Protect empowers Healthcare organizations with unparalleled granular insights into every connected asset including make, model, serial number, device owner, connectivity. Security teams can identify and prioritize vulnerabilities based on business relevance and detect advanced threats, anomalous behavior, and risky communications. OrdrAI Protect automatically generates policies — from reactive to proactive — to secure all assets, ensure compliance, and maintain operational integrity.

Key Benefits for Healthcare Organizations:

Eliminate blind spots: Automated "whole hospital" asset discovery and inventory. Discover high-fidelity asset context with highly accurate AI/ML powered classification of every asset in a healthcare organization including IoMT, IoT, OT and IT.

Reduce risks: Gain comprehensive visibility into vulnerabilities for both managed and unmanaged devices, then translate vulnerabilities into a prioritized action plan with risk scores and automated workflows. Ordr Flow Genome also profiles the behavior of every device and establishes baseline communications patterns.

Accelerate incident response: Quickly identify both known and unknown threats through an integrated intrusion detection engine and AI/ML-based anomaly detection. Generate policies to quarantine a device, block ports or terminate sessions on existing networking and security infrastructure. Share deep asset context with SIEM/SOC, create ITSM tickets, facilitating faster incident response.

Maintain operational integrity and deliver high quality patient care: Confidently create segmentation policies based on Zero Trust, least privilege, or CARTA frameworks to prevent lateral movement or isolate vulnerable medical devices based on baseline communications.

OrdrAI Protect Healthcare Use Cases:

- **Asset inventory & management:** Automate hardware and software asset inventory for every connected asset in healthcare across IoT, IoMT, OT, and IT. Visualize asset connections and communications with detailed mapping, providing clarity on network interactions and potential risks.
- **Vulnerability management:** Prioritize vulnerabilities and assess the attack surface with customizable risk scoring aligned with business priorities. Quickly close vulnerabilities for IoT, IoMT, and OT devices with automated workflows assigned to the right owners.
- **Threat/anomaly detection & response:** Stay ahead of threats with real-time monitoring that detects and alerts on active threats, anomalous behaviors and risky communications
- **Security control gaps and medical device compliance gaps:** Compare against multiple industry threat intelligence feeds, network vulnerability databases, CARECERT, ICSA-ICS-CERT advisories, FDA lookups for medical device recalls and alerts, and manufacturer-published vulnerability data. Detect the use of weak ciphers, default passwords, and non-trustworthy certificates to bring assets in compliance. Generate reports with asset details to share with auditors.
- **NAC acceleration:** Accelerate Cisco ISE, Aruba ClearPass, FortiNAC projects with rich device context, and automated policies for connected devices.
- **Zero Trust segmentation:** Automatically generate dynamic policies for Zero Trust segmentation, ensuring that security controls allow only "baseline" device communications.
- **Accelerate incident response:** Share deep asset context with CMMS or CMDB and create automated workflows with ITSM, facilitating faster and more informed incident response.
- **Optimize device utilization and capital spend:** Get deep insights into medical device optimization of devices as teams scale their capacity. Organizations can also manage maintenance schedules and optimize capital spend.

Ordr Healthcare Case Studies

"The power of the Ordr platform has always been its ability to automate device classification and behavioral modeling using AI. This is foundational to our Zero Trust and segmentation strategy."

El Camino Health

// Larry Smith, Deputy Chief Information Security Officer, El Camino Health

"It's eye opening when you put something like Ordr on your network. It has improved our incident response capabilities."

Franciscan ALLIANCE

// Jay Bhatt, CISO, Franciscan Alliance

For assistance with your asset visibility and security needs, visit ordr.net for more information or contact us at info@ordr.net.

ordr