# Protect Patient Safety: See, Know, Secure Every Connected Device in Healthcare

Connected devices are now a significant part of the healthcare environment and play a role in the patient care experience. These IP-enabled devices can range widely, from medical devices such as infusion pumps, imaging systems, and EKG machines to building management systems, IP cameras, smart lighting and HVAC systems.

While these devices are critical to digital transformation and enhancing healthcare efficiencies, they also increase the attack surface. Many of these devices are not designed with security in mind, cannot be easily patched and run obsolete operating systems. In addition, because these devices are being procured and managed by teams outside of security, true and accurate real-time inventory is missing.

Healthcare organizations need to discover these devices, understand what they are doing, and secure them at scale in order to deliver higher quality care without compromising patient safety or sensitive medical information.

## Introducing Ordr Connected Device Security

Ordr was founded in 2015 by industry veterans from Cisco and Aruba Networks to address the visibility and security of all connected devices. **Ordr is the leader in Medical Device Security and has been designated the market share leader for Healthcare IoT Security by KLAS Research for three years in a row.** The company is funded by Battery Ventures, Wing Venture Capital and Ten Eleven Ventures; and as a testament to its leadership in healthcare Mayo Clinic and Kaiser Permanente Ventures also invested in the company.

Ordr is the only purpose-built platform to discover and secure every connected device - from traditional servers, workstations, and PCs to Internet of Things (IoT), Internet of Medical Things (IoMT) and Operational Technology (OT). Ordr's ability to deliver comprehensive visibility and security for all devices in an organization — its “whole hospital” approach — is critical to protecting every device and delivering one platform of choice for multiple stakeholders.

## Ordr Delivers Many Benefits for Healthcare Organizations

### Patient Care & Safety

1. Automated Clinical Risk Assessment
2. Business Continuity (Ransomware and Malware)
3. Proactive Vulnerability Management.
4. Improved HTM Visibility to IoMT Security Issues

### Data Security & Privacy

1. Improved PHI Visibility and Prevention of Exfiltration
2. Compliance & Audit Preparation (with Safe Harbor)
3. Identify Unauthorized Access
4. Prevent Unauthorized Usage
5. Enhanced Governance

### Financial Stewardship

1. Automated "Whole Hospital" Asset Discovery and Inventory
2. Medical Device Utilization
3. Asset Reconciliation and Improved Capital Efficiency
4. Capital Equipment Lifecycle Management.

## Key capabilities:

- ✓ **Real-time Asset Inventory** – Automatically discover and classify all devices including medical, IoT and OT devices in a healthcare organization. Integrate with CMDB and ITSM systems.
- ✓ **Vulnerability and Risk Management** – Find devices and vulnerabilities that are missed by traditional vulnerability scans, or devices with unnecessary exposure to the Internet.
- ✓ **Behavioral Baselining** – Understand device connectivity and communication patterns. Surface suspicious behaviors such as communications to malicious domains, or identify any other anomalous activity.
- ✓ **Threat Detection** – Find devices with exploits or those that are exhibiting signs of compromise.
- ✓ **Device Utilization** – Identify how devices are being used for maintenance reasons and to support capital spending decisions.
- ✓ **Regulatory Compliance** – Accelerate regulatory reporting with complete visibility over every device and its security posture.
- ✓ **Automated Response** – Automatically or manually segment and microsegment devices based on least privilege, Zero Trust, or CARTA frameworks. Implement proactive, reactive and retrospective policies.

## One Unified Platform for HTM, Security and IT Teams:

### HTM/BIOMED BENEFITS

- Identify, inventory, and monitor all IoMT devices
- Identify non-compliant devices such as devices running outdated O/S
- CMDB/CMMS lifecycle mgmt automation and accuracy
- Optimize IoMT utilization & procurement spend

### SECURITY BENEFITS

- Discover all connected devices
- Detect devices with vulnerabilities and threats
- Baseline and monitor device behavior
- Streamline incident response based on risk
- SOC events enrichment with rich device context

### IT/NETWORKING BENEFITS

- Discover all connected devices
- Accurately monitor and track all connected devices
- Map all device communications patterns
- Accelerate segmentation & NAC initiatives

## How it works:

Within hours of deployment, Ordr will discover and provide high-fidelity context on every connected device, including make, model, operating system, location, and application/port usage. This device context is then enriched with threat intelligence, vulnerability data, FDA and manufacturer databases to build the most complete profile on every device.

Ordr then maps and baselines device communications patterns, ensuring that organizations can identify anomalous behaviors, suspicious network communications and quickly visualize devices in the wrong network (subnet/VLAN) location.

Finally, with the complete understanding of what devices are in the network and what they are doing, Ordr can automate response.

- ✓ **Proactive Zero Trust policies** — Embracing a positive security model, Ordr generates policies to allow devices only appropriate "sanctioned communications", thus limiting exposure. Ordr automatically generates these Zero Trust policies for enforcement on next-generation firewalls, NAC or switching infrastructure.
- ✓ **Reactive policies** — In the event of a security incident, or if devices have triggered an alert such as a high-severity vulnerability, weak cipher, weak certificate, active threat, or suspicious behaviors, Ordr can push alerts to a SIEM, or generate policies to block traffic, terminate a session or automatically segment or quarantine the impacted device. Policies are enforced on existing networking and security infrastructure.
- ✓ **Retrospective policies** — When new indicators of compromise (IoC) are announced, Ordr is the only connected device security vendor that offers a "time-machine" to analyze historical communications from devices to these new IoCs.
- ✓ **Operational workflows** — When a new or unknown device is discovered, Ordr can trigger a centralized workflow with a CMMS or CMDB to ensure proper inventory, authentication, and routing to the right device owners. Ordr can also open an ITSM ticket.

## Key Ordr Healthcare Use Cases

**Real-Time Asset Inventory** — You can't protect what you don't know about. Ordr discovers and classifies every connected device in healthcare, and can correlate this with existing CMMS/CMDB solutions for real-time asset inventory and management. Granular details are provided for every device, and alerts can be triggered for new devices that show up on the network in the last 24 hours, or devices that have not connected in the past 30 days.

**Protect Against Attacks** — Threat actors continue to target healthcare organizations, particularly with attacks like ransomware. Ordr's "whole hospital approach", device insights and integrated IDS engine can be enriched with threat intelligence feeds to quickly identify any device at risk. Ordr can monitor supervisory protocols like FTP, Telnet and more. Ordr also baselines device communications patterns using advanced machine learning to surface suspicious behaviors (including east/west traffic) or communications to a malicious domain.

**Cost Avoidance for Devices with Obsolete Operating System** — Because medical devices are in operations for years (compared to the typical endpoint), a significant number run obsolete operating systems. The cost to replace them can be exorbitant and new manufacturers may not offer similar features. Ordr automates Zero Trust policies allowing devices appropriate access while limiting exposure. This allows devices with obsolete operating systems to be properly segmented so they can continue to provide care.

**Bring Devices into Compliance** — Ordr discovers all connected devices and automatically classifies them. Ordr validates the vulnerability, threat, and risk level of each device through an extensive series of security checks. Connected devices are compared against a suite of 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. Ordr also detects the use of weak ciphers, default passwords and non-trustworthy certificates to bring devices into compliance. Reports are available for auditors.

**Utilization Insights** — Ordr provides deep insight into device utilization. This allows teams to identify areas of over or under use, to ensure data-driven optimization of devices as teams scale their capacity. Organizations can also use device utilization insights to manage maintenance schedules and optimize capital spend.

**Identify Anomalous Behaviors** — Using machine learning, every device communication pattern is profiled via the Ordr Flow Genome. Communications to other IP/VLAN segments within the organization are easily visualized, as well as communications to external networks. Ordr identifies anomalous communications, for example traffic going to known malicious sites or command and control.

**Accelerate Zero Trust initiatives** — Ordr enables practical segmentation that actually works, is scalable and leverages existing infrastructure. Ordr takes the tedious work out of creating and implementing policies for micro-segmentation by generating them dynamically for any device. These policies can then be pushed to and enforced on firewalls, network access control solutions, switches, and wireless LAN controllers.

## Case Studies:

### Top Healthcare System in Minnesota Embraces Healthcare IT Security

One of the top healthcare systems in the world, based in Minnesota, has been deploying Ordr for several years. The healthcare system began their cybersecurity journey by assessing risks associated with hundreds of thousands of medical devices, mitigating these risks and proactively segmenting devices that needed to stay in operations. The healthcare system eventually expanded their strategy to secure all connected devices that had the potential to impact patient care. This healthcare system also used Ordr to address additional use cases such as Zero Trust segmentation, behavioral detection of anomalies such as traffic to external malicious sites, and device utilization insights to identify devices of under and over use.

### Children's Hospital in Texas Identifies Rogue Connected Device with Malware

A Texas Children's Hospital embraces an inspiring promise — to improve the health of every child in its region through the prevention and treatment of illness, disease and injury. During the Ordr Proof-of-Value, Ordr discovered a parking lot gate controller systems was unknowingly hosting malware and connected to the network. The security team was able to quickly address the issue using the device insights and location that Ordr provided. This hospital went on to become an Ordr customer, embracing the "whole hospital" approach by securing not only medical devices but devices deployed by other parts of the organization such as the facilities team.

## About Ordr

Ordr makes it easy to secure every connected device, from traditional IT devices to newer and more vulnerable IoT, IoMT, and OT. Ordr Systems Control Engine uses deep packet inspection and advanced machine learning to discover every device, profile its risk and behavior, map all communications and protect it with automated policies. Organizations worldwide trust Ordr to provide real-time asset inventory, address risk and compliance and accelerate IT initiatives. Ordr is backed by top investors including Battery Ventures, Wing, and TenEleven Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.