Protect Patient Safety:
Discover and 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.

NHS & Healthcare organisations 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 and Systems Control Engine

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 two years in a row**. Due to the Ordr strength in healthcare, the company is funded by Battery Ventures, Wing and Ten Eleven as well as Mayo Clinic and Kaiser Permanente Ventures.

Ordr Systems Control Engine (SCE) 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 Technologies (OT) devices. Ordr's ability to deliver comprehensive visibility and security for all devices in an organisation — its “whole hospital” approach — is critical to protecting every device and delivering one platform of choice for multiple stakeholders.

Ordr Delivers Many Benefits for NHS & Healthcare Organisations

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
5. CareCERT integrated for immediate risk assessment

Data Security & Privacy

1. Improved PHI Visibility and Prevention of Exfiltration
2. Compliance & Audit Preparation (with Safe Harbor)
3. Identify Unauthorised Access
4. Prevent Unauthorised Usage
5. Enhanced DSP Toolkit 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 organisation. 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 the connectivity and communication patterns in order to identify suspicious communications to an unknown country or to malicious domain.
- **Threat Detection** – Find devices 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 or Zero Trust framework.

One Platform for HTM, Security and IT Teams:

HTM/BIO-MED BENEFITS

- Identify and monitor all IoMT devices
- CMDB lifecycle mgmt automation and accuracy
- Optimise IoMT utilisation & procurement spend

SECURITY BENEFITS

- Automate IoMT/IoT vuln & threat detection
- Streamline incident response based on risk
- SOC events enrichment with rich device context

IT/NETWORKING BENEFITS

- Accurately monitor and track all IoMT/IoT devices
- Map all device communications patterns
- Accelerate segmentation & NAC initiatives

How it works:

Within hours of deployment, Ordr SCE 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 of every device.

Ordr then maps and baselines device communications patterns, ensuring that organisations can identify anomalous behaviours, suspicious network communications and quickly visualise 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-genereation firewall, NAC or switching infrastructure
- **Operational workflow** — When a new or unknown device is discovered, Ordr can trigger a centralised workflow with a CMMS or CMDB to ensure proper inventory, authentication, and routing to the right device owners. Ordr can also initiate scans or open an ITSM ticket.
- **Security/IT workflows** — 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, block traffic, or automatically segment or quarantine the impacted device.

Ordr can be deployed on-premises and offers a zero-touch, agentless deployment.

Key Ordr Healthcare Use Cases

Protect Against Attacks — Threat actors continue to target healthcare organisations, particularly with attacks like ransomware. Ordr's "whole hospital approach", device insights and its 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 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 very expensive and new manufacturers may not offer similar features. Ordr automates Zero Trust policies to allow devices appropriate access while limiting exposure. This allows devices with obsolete operating systems to be properly segmented so they can continue operating.

Bring Devices into Compliance — The first step to address compliance is real-time continuous asset inventory. 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, as well as detecting the use of weak ciphers and non-trustworthy certificates to bring devices into compliance. Reports are available for auditors. Ordr helps achieve compliance with the DSP Toolkit by ensuring devices with legacy operating systems are secured, mitigating the risk of them being compromised through cyber attack.

Utilisation Insights — Ordr provides deep insight into device utilisation. This allows teams to identify areas of over or under use, to ensure data-driven optimisation of devices as teams scale their capacity. Organisations can also use device utilisation insights to manage maintenance schedules and optimise capital spend.

Identify Anomalous Behaviors — Using machine learning, every device communication pattern is profiled via the Ordr Device Genome. Communications to other IP/VLAN segments within the organisation are easily visualised, as well as communications to external networks. The Ordr SCE 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 Study: Southampton University Hospital NHS Foundation Trust

The team at Southampton embarked on finding a solution that addressed the challenges presented by medical, IoT and other unmanaged and vulnerable devices and subsequently reviewed various NAC and other security solutions before settling on the Ordr Systems Control Engine (SCE).

Using AI to dynamically profile all devices at massive scale to detect vulnerabilities, exploits, weak passwords or even medical device recalls across both wired and wireless networks, Ordr offers UHS an unprecedented level of detail that dynamically, and in real-time, updates with each new device or event to detect and secure rogue or anomalous behaviour instantaneously.

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. Organisations 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**.