EBOOK

Buyer's Guide for Medical Device Security Solutions

Overview

Healthcare providers rely on a wide range of connected devices to improve clinician productivity and patient care. The volume of devices is increasing every day and medical devices in particular, can range from hundreds of manufacturers, running an enormous volume of varying operating systems. As hospitals merge (or are acquired), the diversity of devices can multiply overnight.

As the care environment becomes more complex, organizations struggle with:

- ⚠ *Manual processes including hours spent manually searching for equipment in need of service action. HTM and clinical engineering professionals typically spend 30-60 minutes per shift looking for devices.*
- ⚠ *Lack of visibility into equipment state (i.e., in use or not) for devices that are in demand 24/7.*
- ⚠ *Lack of accurate device details such as operating system version, patch levels, and vulnerabilities.*
- ⚠ *Large numbers of medical devices critical to patient care that run on legacy or unsupported OS versions and cannot be upgraded or taken out of service. These devices may not be targets of Internet-based attacks but are extremely vulnerable to later stage kill chain threats once the attacker is in the network.*
- ⚠ *Cybersecurity requirements for medical devices that must adhere to standards and regulations that differ from those of IT devices. As an example, hospital IT teams cannot just scan medical devices for vulnerabilities and cannot simply apply a patch from OS providers like Microsoft. Every change in the underlying OS of a medical device needs some level of retesting for recalibration of device performance.*
- ⚠ *Lack of integration with systems such as CMMS (service tickets/history), RTLS, etc. to correlate device data.*
- ⚠ *Hospital funding challenges and workforce turnover – the fewer manual processes HTM teams have the more efficient they can be.*
- ⚠ *HTM Team engagement – more devices with the same or a smaller number of staff equate to a more diverse vendor landscape and higher complexity resulting in the potential for overworked staff.*

A solution that is designed specifically for healthcare and medical device security is needed for healthcare providers to gain needed visibility and security for connected devices.

Seven Things Your Medical Device Security Solution Must Do

The market for healthcare and medical device security solutions is emerging. Healthcare delivery organizations (HDOs) are looking for a comprehensive platform that can deliver a wide range of capabilities - accurate “whole hospital” asset inventory, identification of the attack surface along with corresponding risk mitigation, device utilization, and automated security policies. A medical device security solution can address the challenges referenced earlier for both HTM and security teams.

Here the key requirements for medical device security solutions:

1. “Whole Hospital” Asset Discovery and Inventory

There are a variety of medical and non-medical devices that play a critical role in delivering healthcare services and ensuring patient safety. These devices range from infusion pumps and MRIs to security cameras, HVAC controllers, and elevator control systems. An attack that targets an elevator control system, for example, may impact the ability of an HDO to transport patients; the initial attack may also move laterally to a medical device.

As a result, organizations need a reliable method to discover, classify, and inventory all devices across the whole hospital including those that are managed and unmanaged. This method should also include the ability to gather detailed insight into the type of device that is detected as well as its exact model, capabilities, location, application/port, and operation system. It is essential that the discovery and classification capabilities are continuous and automated as large numbers of unmanaged devices can be hard to track manually, and many devices may be physically moved from one location to another as required.

An aspect of device context that may not always be considered is device “behavior” (i.e., communications patterns). Unlike users, devices have specific functions and therefore can be expected to act in a deterministic manner. An infusion pump for example, regardless of manufacturer, should behave and communicate with other systems the same way every time. Organizations should be able to establish a baseline of behavior for each device in the network as well as known behavior for devices that provide similar functions. Baselining should include the connections with other assets a device needs to communicate with and over which protocols as well as verifying the communications are safe and not destined to bad actors or part of threat activity. (Note: Based on behavioral baselines, security teams can then create very narrowly defined Zero Trust policies that strictly limit devices to communicate to the few resources that are truly needed to operate without service disruption. See “Automated Response” section).

Requirements:

- Automated discovery of every connected device across the whole hospital, using passive, agentless methods that will not impact the function of sensitive medical and IoT devices.
- Methods to gather granular device characteristics such as make, model, current software version, serial number, and operating system.
- Visibility of device network and physical location.
- Details of network connectivity such as wireless or wired, subnet, and VLAN details.
- Automated device insights such as devices that are newly discovered, not in inventory (e.g., CMMS or CMDB), using privileged protocols (e.g., RDP or Telnet), or those using specific access methods (e.g., VPN).
- Establish a “baseline” of device “behaviors”, for example, what other internal or external system is the device communicating with, and how does this behavior compare to those of its peers (e.g., similar devices).
- Asset and data reconciliation with existing data in CMDB/CMMS tools to ensure a centralized and accurate source of truth.
- Integrations with key security and IT tools such as CMDB/CMMS, SIEM, EDR, MDR and XDR, and the ability to enrich those tools with a comprehensive, accurate, single “source of truth” for device details, context, and insights.

2. Vulnerability and Risk Management

Once asset discovery and inventory are in place to establish foundational visibility, organizations should assess the risk profile of devices. This should include device factors such as devices running outdated operating systems, operating with vulnerabilities (CVEs), impacted by recalls, storing or transmitting PHI or other sensitive data, or those using weak passwords or certificates. In addition, exploitability of vulnerable devices and network factors such as VLAN deployment, segmentation, and internal/external device communications should be considered. Organizational factors should also be considered such as device role, criticality, and potential impact to operations and patient safety in the event of a security event.

These factors should be combined to assess a clinical risk score for each device and should be available for security teams to help with the prioritization of vulnerability or threat management efforts, and planning of corrective actions to remediate issues or mitigate risks.

Requirements:

- Visibility into installed applications including minor and major software versions and application status (e.g., AV enabled, latest definitions, etc.) without the need for agents or active scanning.
- Accurate identification of devices with vulnerabilities including vulnerability status and applied hotfixes or mitigations without the need for active vulnerability scans.
- Incorporation of device manufacturer provided MDS2 and SBOM information to help identify potentially vulnerable device components.
- Prioritization of remediation efforts such as vulnerability patching or mitigations such as compensating controls based on clinical risk or a combination of factors such as cyber and environmental risk, device lifesaving capabilities, and PHI exposure.
- Customizable device risk scores based on environmental and device criticality.
- Identification of devices deployed in the wrong VLAN, subnet, or network segment.
- Full-lifecycle vulnerability management capabilities including:
  - Focused views on specific device categories or locations such as a hospital floor, building, branch, or city.
  - Prioritization of vulnerabilities based on device risk scores.
  - Use of workflows integrated across teams and tools.
  - Methods such as tags to associate devices with applications, location, priorities, groups, individuals, or other key attributes, to simplify the coordination of vulnerability management efforts.

3. Threat Detection

Organizations will also naturally want to identify compromised devices including those exhibiting signs of potentially malicious activity as such devices behaving abnormally, contacting malicious domains, or other indicators of compromise. This capability requires a combination of intrusion detection functionality that can detect known exploits as well as machine learning (ML) capabilities to monitor east-west network traffic, baseline device communications, and identify anomalous device behavior.

Requirements:

- Monitoring of north-south and east-west network traffic to detect malicious activity and threats.
- Detection of kill chain stages using the MITRE framework.
- Identification of devices with active exploits.
- Inspection of internal (i.e., behind the firewall) east-west network traffic to identify malware or attacker tools (e.g., Metasploit).
- Inspection of external device communications to identify devices communicating to a malicious domain or other malicious activity.
- Baselining of normal behavior for each device and identification of abnormal behavior (i.e., baseline deviation) as an indicator of potentially malicious activity.
- Retrospective identification of devices impacted by newly defined indicators of compromise (IoC) such as identifying device that have communicated to a known malicious domain.
- Risk scores that can provide input to security teams and aid in the planning and prioritization of mitigation efforts.

Integrate with existing threat monitoring systems such as Security Information and Event Management (SIEM) platforms.

4. Automated Security Policies and Response

Because there may be large volumes of connected devices in an environment, the ability to automate security policies and response is important. A medical device security solution must have ability to respond efficiently during a cybersecurity incident, proactively segment devices to enable devices to communicate to other systems required for its function while limiting exposure, or retrospectively when new IoCs are available.

Requirements:

- Enforcement of security policies through integration with existing security and networking infrastructure such as firewalls, NAC, and switches.
- Simulation of policy enforcement before deployment in a production enforcement state.
- Automation of policy creation to accelerate response during a security incident with actions such as terminating sessions, blocking ports, or quarantining a device.
- Automation of proactive security policy creation based on learned device behavior and open ports derived from an MDS2.
- Automation of segmentation policy creation to proactively reduce the attack surface and mitigate risks based on baseline device communication flows.
- Retrospective analysis of device activity to identify devices that may have previously exhibited activity that aligns with a newly defined IoC.

5. Device Utilization

HDOs face constant budget challenges and are continuously in pursuit of maximizing resources, investments, and efficiencies. But connected medical devices are often:

- Underutilized, with some of the most high-value equipment sitting idle an average of 58% of the time.
- Unaccounted for, with only some assets recorded centrally – and rarely tracked in real-time.
- Lacking insights, with no clear data to aid planning for purchases, renewals, EOL, leases, etc.
- Fragmented, with facilities acting independently instead of considering organization-wide impact when making decisions.

Device utilization insights can provide operational information about the usage of devices over a range of time and deliver clear benefits such as:

- Saving time for clinical administrators by helping teams understand not only how a device is being used but exactly where under-utilized medical equipment is located.
- Helping HTM and Clinical Engineering teams avoid negative impact to hospital services by understanding when to schedule preventative device maintenance.
- Supporting efforts to "right-size" the device inventory including capital equipment purchases, device leasing decisions, or avoidance.
- Providing insights to help teams maximize resources such as ensuring high value medical equipment does not sit idle and is utilized appropriately.

Requirements:

- An understanding of utilization over a range of time for an individual device or fleets of devices.
- Tracking of device utilization based on a scheduled timeframe.
- Comparison of device utilization between facilities.

6. Integrations

IT environments are comprised of a wide variety of tools that serve multiple teams, address a range of capabilities, and provide insights. New solutions that have limited or no integration with exiting tools can result in wasted budget for tools that lack adoption, are not used to their fullest potential, and fail to prove value. Lack of integration can also hinder the progress of efforts to modernize by impacting efficiencies of teams and accuracy of data required to scale operations.

A medical device security solution should integrate with the security, network, and IT tools and workflows that exist in your environment. New solutions that integrate widely will enhance existing tool capabilities and improve connected device management and security. These solutions will also have the best chance for adoption and providing maximum value such as:

- Automating connected device discovery by integrating with network infrastructure and device management tools.
- Maintaining an accurate source of truth by integrating with and reconciling data in existing CMMS, CMDB, or other inventory tools.
- Understanding device location, communications, risk, and active threats by analyzing network data.
- Identifying device vulnerabilities and risk by incorporating external data sources such as threat feeds and recall databases.
- Improving remediation efforts by sending granular device details to vulnerability management and IT Service Management (ITSM) tools.
- Improving incident response by sending alerts with granular device details to SIEM platforms and automating policy enforced with existing security and network infrastructure.
- Accelerating segmentation, NAC, or other Zero Trust efforts by automating policy and enforcing with existing security and network infrastructure.

Requirements:

- Bi-directional integration with existing security, network, and IT tools to enhance device context and improve workflows.
- Defining data from an external tool as a “source of truth”.
- Showing insights from collected data in a clear and concise format.
- Open platform with out of the box integrations and easy to access API.

7. Scalable Management

Connected devices in an average organization can number in the tens to hundreds of thousands. These devices are often owned by multiple teams and deployed across multiple floors, buildings, and sites. No single team in an organization is responsible for managing and securing all connected devices. An increasingly common model is one where the daily operations for a set of devices is managed by the team using the technology while security of those devices is centralized.

A medical device security solution must not only be able to scale to support a large number of devices but must also make data, insights, and capabilities accessible to a wide range of admin requirements. A solution that does not meet these requirements can result in:

- Inability to support the current and future volume of devices deployed in an environment.
- Siloed tools resulting in inconsistent data, insights, and a negative impact to operations.
- Overwhelming amounts of data preventing teams from identifying critical issues and insights.

Requirements:

- Support for hundreds of thousands of devices to meet current and future requirements.
- Centralized view of all connected devices across all locations.
- Admin access based on any combination of criteria such as admin role, location, profile, or business function.
- Role based views to serve the requirements for multiple admins and team members.
- Data shaping and filtering to focus data and views based on criteria such as admin role, admin task, device type, device location, vulnerability status, and other device or environment attributes.
- Access to granular details such as device attributes, network context, and vulnerability insights.
- Support for device management and security capabilities with the ability to coordinate and manage efforts across multiple team members.
- Integration with 3rd party tools with inbound capabilities to enrich the solution’s device insights and outbound capabilities to enrich external tools and workflows.
- Reporting to enable sharing of consolidated insights across teams, with management, and to help with compliance requirements.

ordr
Device - vivide95-523.ordr.net (10.36.101.238)
Flow Genome
Device Risk Summary
2334
Security Incident Summary
361
Vulnerability Summary
2076

How Ordr Addresses Medical Device Security Requirements

Asset discovery and inventory

Ordr Capabilities

Ordr automatically and continuously discovers and accurately classifies every network connected device in the hospital network, including IoMT (medical), IoT, and OT devices, as well as traditional IT endpoints. The solution does this by analyzing network data with the ability to decode more than 80 device and industry-specific protocols.

Ordr gathers granular details for every device including make, model, serial number, operating system, firmware, installed applications, port usage, and network/physical location. Ordr device details provide teams with essential device insights to aid in the full lifecycle of connected device management and security.

Ordr identifies and alerts when a new device is connected to the network and integrates with CMMS, CMDB, and ITSM tools to ensure device inventories and IT tools are always up to date with accurate device details.

Ordr provides robust reporting capabilities with out-of-the-box and customizable reports that can be viewed in the Ordr dashboard or exported to share insights with executives, management, and across operational teams.

Vulnerability and risk management

Ordr Capabilities

Ordr analyzes devices in terms of potential risk to the organization to calculate a clinical risk score for each device. Risk can include a wide range of factors such as devices with vulnerabilities, devices that have been recalled, devices that are using weak TLS passwords, expired certificates, or devices that process sensitive information such as protected health information (PHI). Risk scores are automatically calculated based on environmental factors and device lifesaving capabilities and are easily customized to align with organizational goals.

Ordr offers full lifecycle vulnerability management capabilities including:

- Vulnerability dashboard to help organizations see all clinical device vulnerabilities, across all vulnerability databases, in one place.
- Customizable views to focus on devices under management, within specific patching skillsets, or devices within specific facilities.
- Prioritization of vulnerabilities and remediation efforts based on the Ordr calculated Clinical Risk Score.
- Optimized mitigation efforts via simplified workflows to collaborate across teams and manage the entire vulnerability lifecycle. Custom tags can be used to associate devices with applications, location, priorities, groups, individuals, or other key attributes, to simplify management of vulnerabilities.
- Reports available in the Ordr dashboard or exported to share across teams, with management, or execs with details on vulnerability management status and progress.

Threat detection

Ordr Capabilities

Ordr discovers devices with signs of compromise using both known and behavioral indicators of compromise.

- Known indicators include exploits, attacker tools and communications with known malicious IP addresses or domains.
- Behavioral indicators include device communication anomalies based on deviations from Ordr observed device communication baselines or deviations from norms for a particular device profiled.

When a threat is detected, Ordr sends an alert with detailed information to a SIEM or other mechanism to inform teams. Ordr can also help accelerate response to a threat by dynamically creating policy to stop the attack. See ***Automated response and mitigation for more details.***

Automated response and mitigation

Ordr Capabilities

With device insights such as device context, behavior, and communications, Ordr accelerates response to active attacks and other threats with automated action – from proactive, reactive to retrospective policies. Ordr policies are enforced on a customer's existing network and security infrastructure including switches, firewalls, and NAC.

During a cyber incident, Ordr dynamically mitigates risks such as quarantining compromised devices, blocking ports, or by dynamically creating segmentation policy to restrict device communications or isolate impacted devices.

Ordr also uses device insights to automate the creation of proactive policies to segment vulnerable devices that can't be patched. These "Zero Trust" policies only allow appropriate access required for device functions to limit exposure and can accelerate segmentation and NAC projects.

Finally, when new IoCs are provided, Ordr acts like a "time-machine" to identify devices that have communicated to these newly announced IoCs. This can be invaluable when determining the exposure to a cyberthreat.

Device utilization

Ordr Capabilities

Ordr arms HTM and Clinical Engineers with meaningful insights in real-time to help teams optimize the operational efficiency of their high value equipment and make data-driven decisions for maintenance, capital planning, and cost avoidance. Ordr provides insights such as:

- Underutilized high value equipment to increase the utilization by 25% or more.
- Study count and Image count which could be used to optimize maintenance tasks, parts replacement scheduling, and potentially increase the life span of the medical devices.
- "Body parts examined" metrics to reduce re-setup time.
- Data to compare and contrast device utilization across different facilities to identify and improve operational efficiency of under-utilized equipment.
- Usage patterns along with ordered physician name providing insights to adjust working hours/schedules.

In addition to individual device utilization insights, Ordr can also deliver fleet utilization insights such as:

- Fleet level utilization by auto grouping fleet devices. The utilization is customizable for the working hours of the hospitals/departments in order to provide meaningful data.
- Consistent high usage or bursty usage to inform decisions to buy or rent additional fleet equipment.
- Utilization data compared across facilities to help with planning and aid in optimizing the distribution of demand across existing capacity.
- Identification of offline fleet devices so they can be located and put back in service, and in some instances, to help avoid unnecessary capital purchases.

Integrations

Ordr Capabilities

Ordr supports bi-directional integrations with over 80 security, network, IT, and clinical products and tools to improve visibility, connected device insights, and security. Ordr integrations include:

- CMMS/ CMDB - Ordr collects and consolidates granular details for every asset in an environment and enriches CMMS or CMDB to ensure the asset inventory is always up to date with accurate details.
- Network Access Control (NAC) - Ordr supports NAC projects with automated connected device visibility, classification, and policies created for and enforced with NAC solutions.
- Vulnerability Management - Ordr complements existing vulnerability management solutions with capabilities such as identifying devices that should not be scanned to optimize scanning efforts or by applying Zero Trust policies to protect devices that cannot be patched. Ordr also provides an integrated vulnerability scanner to identify vulnerabilities for any connected device.
- Endpoint Detection and Response (EDR) - Ordr compliments agent-based tools with an agentless approach to discover and automatically classify every connected device. Ordr device profiles can be enriched with EDR data to address critical use cases such as identifying managed devices that do not have an endpoint security agent deployed.
- Firewall - Ordr can dynamically create and send policies to firewalls for enforcement to terminate sessions, block ports, and stop attacks.
- Network Infrastructure - Ordr analyzes network data to automatically discover, classify, and enrich connected device profiles with network details such as physical and network location. Ordr also provides visualization of device communications within and between subnets and VLANs. Ordr can create and enforce policies such as moving devices between VLANs, applying ACLs, and enforcing segmentation.

Integrations

Ordr Capabilities

- Threat Intelligence - Ordr integrates with threat intelligence platforms and correlates data with connected devices to help identify compromised devices such as those communicating to domains used in malicious operations.
- Security Incident and Event Management (SIEM) - Ordr enriches SIEMs with granular details about devices, risks, and events, to support and accelerate incident response.
- IT Service Management (ITSM) - Ordr integrates with ITSM tools to perform actions such as alerting device owners or security teams when a vulnerability, anomaly, or a security incident is detected, and generating a ticket to track further action.
- IP Address Management (IPAM) - Ordr integrates with IPAM tools to collect IP address assignments for connected devices and correlate MAC-to-IP bindings to ensure security alerts and flow data are accurately mapped to the correct device.
- Clinical Systems - Ordr integrates with clinical systems and services to automate device classification, provides physical and network location, accelerate response to vulnerabilities, and deliver utilization insights to improve operational efficiencies and capital spend.
- Cloud –Ordr integrates with cloud environments to provide a centralized view of all data center and cloud assets for complete visibility across the entire attack surface.
- Network Aggregators - Ordr integrates with network aggregators to ensure that high-fidelity connected device network traffic is available for Ordr to analyze.
- Endpoint Management Systems - Ordr integrates with endpoint management systems to collect granular data from all managed devices, across all operating systems for rich context to improve visibility and security.

Scalable Management

Ordr Capabilities

The Ordr platform and dashboard can scale to support hundreds of thousands of devices per customer and provides a single view of all devices deployed in a single site or across multiple sites. The Ordr solution provides:

- A centralized view of all connected devices across all locations.
- Role-based access control to support multiple admins, device owners, and teams.
- Data shaping and filtering to create customized views based on role and use case such as devices in a specific site, building, or floor, devices based on type, owner or service, and devices based on vulnerability status.
- Executive dashboard to understand the vulnerability, risk, and compliance posture for an environment.
- HTM view to focus Ordr insights for clinical engineering teams and tasks.
- Vulnerability dashboard to identify vulnerabilities and manage remediation and mitigation efforts across teams.
- Detailed insights for a granular understanding of the vulnerability, risk, and compliance posture for every device in an environment.
- View of device network connectivity and communications with granular detail down to the flow level per-device.
- Capabilities to automate policy creation based on collected device context and enforce policy with existing security and network products.
- Reporting with a collection of pre-configured and customizable reports that can be viewed in the Ordr dashboard or exported for sharing across teams.

Additional supporting features

Ordr Capabilities

- Platform Security - Ordr is a security focused company committed to the security of the Ordr platform and protection of all customer data. As part of this commitment Ordr has achieved SOC2 Type II certification and maintains certification through regular audits.
- Managed services – Ordr has partnerships with key vendors such as Sodexo, GE Healthcare, HSS, and Accenture Health to enable customers to deploy managed services offering powered by the Ordr platform.

Glossary

ACL – Access control List

CMDB – Configuration Management Database

CMMS – Computerized Maintenance Management System

CVE – Common Vulnerabilities and Exposures

EDR – Endpoint Detection and Response

HDO – Healthcare Delivery Organizations

IoC – Indicator of Compromise

IoT – Internet of Things

IoMT – Internet of Medical Things

IPAM – IP Address Management

ITSM – IT Service Management

MDR – Managed Detection and Response

MDS2 – Manufacturer Disclosure Statement for Medical Device Security

NAC – Network Access Control

NDR – Network Detection and Response

OT – Operational Technologies

RDP – Remote Desktop Protocol

RTLS – Real-Time Location System

SBOM – Software Bill of Materials

SIEM – Security Information and Event Management

TLS – Transport Layer Security

VLAN – Virtual Local Area Network

XDR – Extended Detection and Response

Get Your Devices in Ordr

Request a demo at www.ordr.net

Contact us at info@ordr.net

ordr