Ordr Software Inventory Collector

OVERVIEW

Connected devices are now a significant part of the IT ecosystem across all industries. These IP-enabled devices range widely, from cameras and payment card systems to business-critical devices such as infusion pumps and HVAC control systems. Many of these devices run rudimentary operating systems and cannot be discovered via traditional asset inventory solutions, scanned via vulnerability management systems, or supported by corporate endpoint security agents. These connected device limitations can create business, IT, and cybersecurity blind spots and increase risk.

ORDR SOLUTION

Ordr is the only purpose-built platform to discover and secure every connected device – from IT servers, workstations, and PCs to Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) devices. The solution automatically discovers every connected device, profiles device behaviors, uncovers risks, and automates response. Ordr not only identifies devices with vulnerabilities, weak ciphers, weak certificates, and active threats, but also those that exhibit malicious or suspicious behaviors. With Ordr, networking and security teams quickly respond to threats with dynamically created policies to stop active attacks, segment vulnerable mission-critical devices, and retrospective analysis and policies to identify compromised systems based on new indicators of compromise.

One or more of the following methods are used to gather device context:

- **Network Data Analysis** - Integration with network infrastructure SPAN/TAP, NetFlow, or API capabilities are used to receive network data for analysis.
- **Device Query** - Context can be retrieved directly from connected devices using specialized queries such as SNMP, UPnP, and mDNS.
- **Ecosystem Integrations** - Additional device context can be gathered through integration with enterprise tools such as DNS, IP Address Management, Active Directory, and other third-party tools.

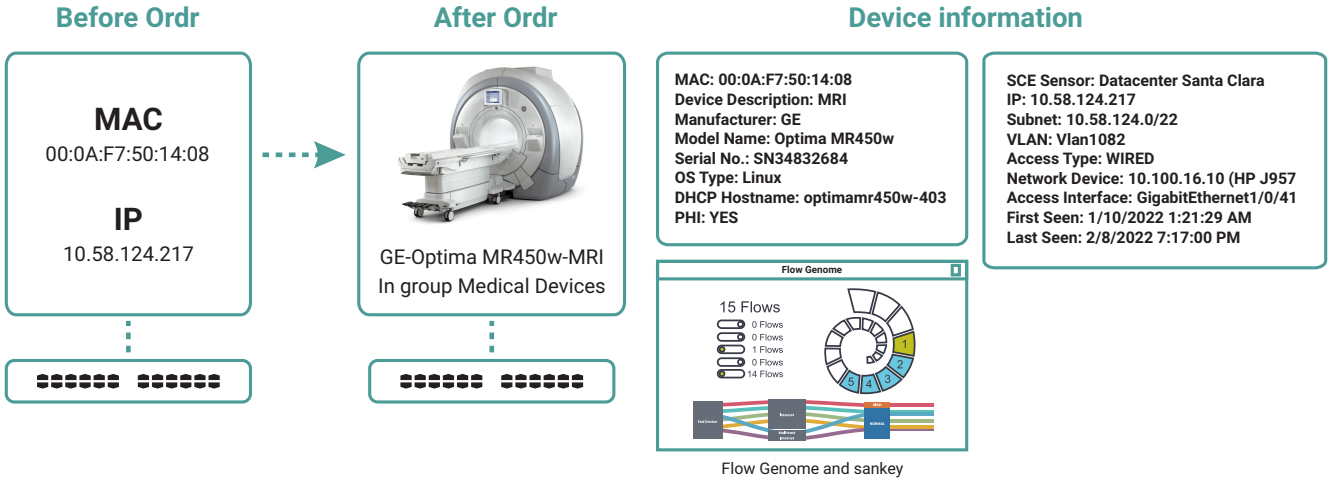

FIGURE 1: Device context gathered by Ordr

INTRODUCING ORDR SOFTWARE INVENTORY COLLECTOR

With a growing remote workforce and new hybrid work models, tracking all devices, 24x7 wherever they connect from is a challenge but necessary to meet end point posture compliance requirements. The Ordr Software Inventory Collector meets these requirements with a simple and flexible approach.

Ordr Software Inventory Collector is a lightweight endpoint device query that automatically gathers software inventory details directly from devices and returns these details to a customer's Ordr instance. This approach simplifies how software stack, patch data, and other device details are gathered for all managed and unmanaged devices. Ordr Software Inventory Collector provides support for connected devices running any leading operating system (Windows, macOS, and all distributions of Linux), no matter where and how the devices and users connect.

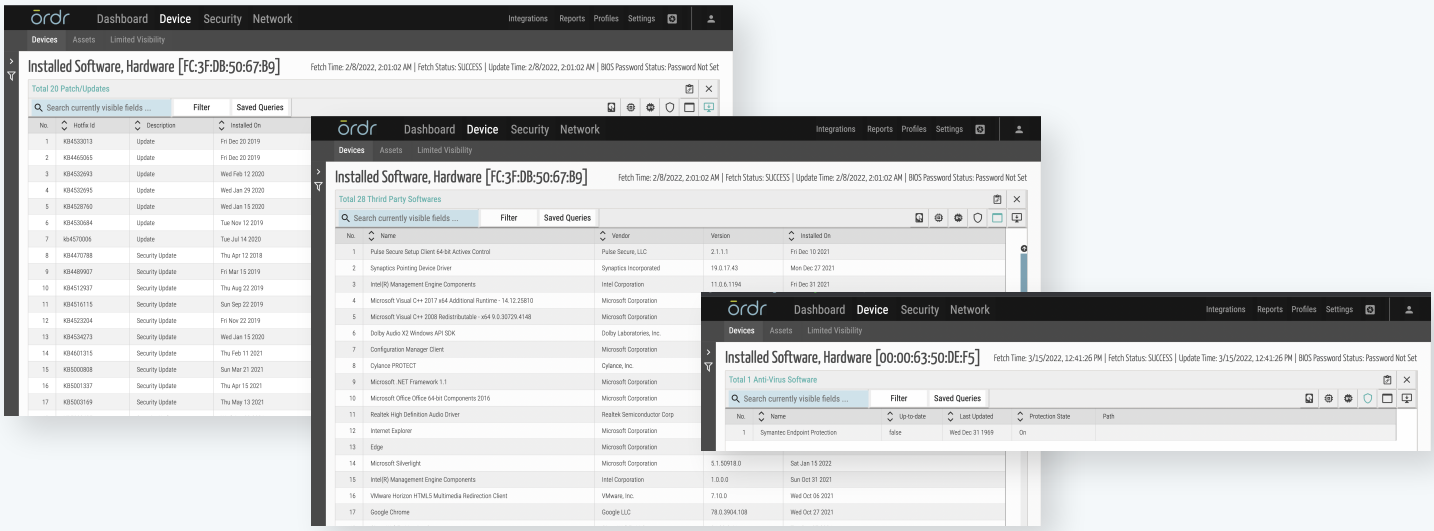

FIGURE 1: Device context gathered by Ordr

Ordr Software Inventory Collector gathers the following detailed device software and system attributes:

- Operating system patches, Windows KB security updates, and hotfixes
- Installed software versions and antivirus status
- Serial number, BIOS, memory, and disk details
- NIC details including IP-MAC binding

NOTE: IP-MAC binding details are even more critical for VPN connected devices as these devices tend to quickly change their IP address.

The details collected by Ordr Software Inventory Collector makes it easy to identify devices with an outdated operating system or known vulnerabilities and enables teams to focus remediation efforts such as patching or implementing compensating controls such as segmentation.

BENEFITS OF ORDR SOFTWARE INVENTORY COLLECTOR

Collect Device Details Without Device Impact

Ordr Software Inventory Collector is a lightweight OS-driven script that collects and sends device information to a customer's Ordr instance without device impact, unlike agents that constantly monitor device activities, consume CPU cycles, and possibly interfere with device operations.

Extend Visibility to Remote Devices

Gain up to date visibility of all remote devices whether they connect via VPN or are occasionally offline and track every IP to MAC change for network traffic correlation.

Ensure Device OS and Software Compliance

Identify devices with old software versions and those running outdated operating systems including any version of Microsoft Windows, macOS, and Linux to meet compliance requirements.

Ensure Corporate Posture Compliance

Generate reports with a comprehensive view of all connected devices including installed applications, processes running, and unauthorized software installations that increase risk.

Streamline Patch Management

Understand device risk such as missing patches and hotfixes, get alerts on new vulnerable devices, generate a list of device vulnerabilities with a single click, and integrate with patch management systems to track patch levels and patching efforts for every device.

FLEXIBLE OPTIONS FOR SOFTWARE INVENTORY COLLECTION

Ordr Software Inventory Collector is the only method that is uniquely comprehensive with the ability to collect attributes from all connected devices across all operating systems, inside and outside your organization. Ordr Software Inventory Collector provides the flexibility to be deployed as a standalone method or integrated with Active Directory to augment software context with user details.

Ordr also supports other device attribute collection methods including WinRM, WMI, Osquery, and PowerShell scripts, depending on organizational requirements and policies.

To learn more, visit https://ordr.net