ORDR

DATASHEET

ORDR Software Inventory Collector

Closing Visibility Gaps in Complex Device Ecosystems

Modern networks are more complex than ever, with a vast array of connected devices — from printers and cameras to payment systems, medical devices, and HVAC systems. These devices often operate on lightweight or proprietary operating systems, making them incompatible with traditional security measures like fingerprinting, vulnerability scanning, or endpoint agents.

Compounding the challenge, these devices frequently connect and disconnect or change physical locations, creating critical visibility gaps across IT, business, and security operations. Without a comprehensive approach to visibility, organizations face increased operational and cybersecurity risks.

Supported Devices and Operating Systems:

- Operating Systems: Windows, macOS, Linux
- IoT (Internet of Things)
- IoMT (Internet of Medical Things)
- Operational Technology (OT), including HVAC systems, cameras, and payment systems
- Peripheral Devices: Printers and other connected assets

The ORDR Solution

Reliable, Non-Disruptive Visibility ORDR Software Inventory Collector (OSIC) bridges these gaps by providing continuous, detailed device visibility using lightweight, read-only permissions. OSIC gathers rich device data without disrupting network or device performance, ensuring safe and reliable operation across all device types, including those that cannot support agents.

Key Benefits of OSIC

Lightweight, Non Intrusive Collection

OSIC uses a lightweight, OS-driven script to collect device information and send it to your Ordr instance. Unlike traditional agents, OSIC avoids consuming device resources like CPU cycles, ensuring no impact on device performance or operations.

Extend Visibility to Remote Devices

Keep track of all devices, even those that connect via VPN or are offline intermittently. OSIC ensures up-to-date tracking of IP-MAC changes, enabling seamless network traffic correlation.

Simplify Compliance and Audit Readiness

Easily identify devices running outdated operating systems or software versions to meet compliance requirements. Generate detailed reports on connected devices, installed applications, running processes, and unauthorized software.

Streamlined Patch Management

Identify missing patches and unpatched vulnerabilities with ease. Generate vulnerability reports in a single click and integrate with patch management systems to track and remediate issues for every device.

Responsive Security Posture Management

Leverage OSICs data for on-demand policy creation to segment vulnerable devices, respond to threats, and enforce security configurations like disk encryption or local firewall policies.

In-Depth Data Collection Capabilities

OSIC gathers detailed insights to help security teams monitor and secure their networked devices. This includes critical details such as IP-MAC binding, which is especially crucial for devices connected via VPN. These devices often change their IP addresses.

Enhanced Context for Holistic Visibility

Ordr combines OSIC and other data sources to deliver enhanced device visibility, including:

- Network Data Analysis: SPAN/TAP, NetFlow, or APIs for analyzing network traffic.
- Device Queries: Specialized protocols such as SNMP, UPnP, and mDNS for direct device interrogation.
- Ecosystem Integrations: Seamless API integrations with tools like Active Directory, DNS, and IP Address Management systems.

Category	Details Covered
Network Information	IP-MAC Binding, DHCP, Hostname, NIC, Subnet, First/Last Seen
System Information	Device Model, Serial Number, BIOS, Manufacturer, Uptime, Memory
Software Details	OS Type, Third-Party Software, Version, End-of-Life Status
Security Posture	Disk Encryption, Cryptography Type, Local Firewall, User Policies
Patching and Updates	OS Patch Details (e.g., Hotfix IDs, Install Dates)
Antivirus Status	Software, Vendor, Version, Update Details, Active Status
Running Processes	Protocols, Ports, Authorized/Unauthorized Software, Memory Usage
Vulnerabilities	CVEs, PHI Exposure, Compliance Gaps

MRI Device

GE-Optima MR450w-MRI
In group Medical Devices

Before ORDR

MAC

00:0A:F7:50:14:08

IP

10.58.124.217

With ORDR

MAC: 00:0A:F7:50:14:08
Device Description: MRI
Manufacturer: GE
Model Name: Optima MR450w
Serial No.: SN34632684
OS Type: Linux
DHCP Hostname: optimamr450w-403
PHI: YES
SCE Sensor: Datacenter Santa Clara

IP: 10.58.124.217
Subnet: 10.58.124.0/22
VLAN: Vlan1082
Access Type: WIRED
Network Device: 10.100.16.10 (HP J957)
Access Interface: GigabitEthernet1/0/41
First Seen: 1/10/2022 1:21:29 AM
Last Seen: 2/8/2022 7:17:00 PM

Enhancing Security Posture with OSIC

As part of the ORDR AI Protect Platform, OSIC provides the timely, actionable insights needed to strengthen organizational security. With OSIC, teams can:

- Dynamically create policies to stop active attacks or segment vulnerable devices.
- Perform retrospective analysis using new indicators of compromise (IOCs)
- Prioritize remediation efforts for devices with known vulnerabilities.

About Us

ORDR is the leader in AI-powered asset risk and exposure management, trusted by top organizations across healthcare, pharmaceuticals, manufacturing, and financial services. With insights from over 100 million asset types, ORDR's platform empowers security teams to identify their biggest risks and take swift, effective action. From maintaining security hygiene to real-time threat detection and protection using microsegmentation, ORDR makes action not just possible but automated and simple — bringing ORDR to chaos.

ORDR is backed by top investors including Wing Venture Capital, Ten Eleven Ventures, Battery Ventures, Mayo Clinic Ventures, and Kaiser Permanente Ventures. For more information, visit www.ordr.net and follow ORDR on X and LinkedIn.

For more information, visit **ordr.net**

Follow Ordr on

Ready to bring ORDR to your chaos?

REQUEST A DEMO