



Solution Brief

Gaining Visibility into Private Networks with ORDR Software Inventory Collector

Expose what's hidden behind private IPs with ORDR's lightweight discovery tool.

Closing Visibility Gaps in Non-Routable/Private Networks

Most enterprises and vendors are recommending building networks with security requirements in mind. It is excellent that vendors and customers are prioritizing security. Still, the model of creating airgap networks using security controls is creating multiple private networks, often using overlapping IP ranges. Most teams are relying on asset management tools to get visibility into devices along with context for maintenance and support and to get visibility into security issues.

The ORDR Solution – Complete Visibility into Every Device

ORDR Software Inventory Collector (OSIC) bridges these gaps by providing visibility into these networks by detecting all the neighborhood devices connected to the device that is acting like a bridge between the private network and the routable network.

Key Benefits of OSIC

- **Complete visibility into private network:** OSIC uses a lightweight, OS-driven script not only collects deep device context but also provides deep visibility into all devices connected behind the in a private network using simple to deploy discovery tool.
- **Deep visibility into neighborhood devices:** OSIC can initiate active scans such as Winrm to collect deep context from remote devices including applications and vulnerabilities. The info includes make, model, serial no, and OS which is very important to understand support and security issues.
- **Manages overlapping networks:** Most private networks use the same IP range, and it will be difficult to track and assign the right IP addresses. OSIC auto assigns the network ID based on the base host where it is deployed and tags every neighborhood device with the same id and tracks all changes to IP based on the network id.

ordr AI-PROTECT Dashboard Device Security Network Integrations Reports Profiles Settings

External Services and Tools Integration

Ordr Software Inventory Collector (Service Detail)

API Portal Advanced Imported Data

Total 86 Data Records

Search currently visible fields Filter Saved Queries Actions

No.	UUID	MAC(s) with traffic	Info	OSIC Data Source	OSIC Data Source Version	OSIC Installed Apps Count	OSIC OS Patches Count	OSIC AV Present	OSIC Uptime (in seconds)	OSIC Number Of Processors	OSIC Total Physical Memory	OSIC Last Boot Time
10	C			OSIC Cloud	R4.2.19	117	20	yes	52363	1	32.00 GB	1/15/2025 7:58:12 AM
11	C			OSIC Cloud	R4.2.19	115	21	yes	131464	1	32.00 GB	1/14/2025 9:44:36 AM
12	C			OSIC Cloud	R4.2.19	115	21	yes	131464	1	32.00 GB	1/14/2025 9:44:36 AM
13	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
14	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
15	C			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
16	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
17	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
18	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
19	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
20	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
21	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
22	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
23	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
24	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	
25	E			OSIC Cloud Proxy	R4.2.19	0	0	no		1	0 Bytes	

External Services and Tools Integration

ordr AI-PROTECT Dashboard Device Security Network Integrations Reports Profiles Settings

Devices Device Users Limited Visibility

Device - [REDACTED]

MAC 00:19:17:61:51:75

Details Assets 1 Network History Change Log OSIC Comments Actions

DEVICE INFORMATION

MAG Address : [REDACTED]

Device Description : POS Terminal

Manufacturer : Posiflex

NIC Vendor : Posiflex Inc.

Model Name/No. : [REDACTED]

Serial No. : [REDACTED]

OS Type : Windows 10

FQDN : [REDACTED]

IP Binding Source : AD

DHCP : [REDACTED]

DHCP Hostname : [REDACTED]

CONFIDENCE SCORES

Classification Confidence : 95

OS Confidence : 95

Installed Software Confidence : 0

CLASSIFICATION

Classification State : Classified

Classification Source : PROFILE_LIB

Device Category : POS Terminal

Group : [Retail Devices](#)

Profile : [Posiflex POS Terminal](#)

Profile Lock : false

RISK

Criticality : LEVEL_3

Incident Count : 0

IntComm Risk Score : 0

ExtComm Risk Score : 0

Incident Score : 0

Incident Level : normal

Vulnerability Score : 0

Vulnerability : normal

Agg Risk Score : 0

Risk : normal

AI/ML TRAINING

CONNECTIVITY

SCE Sensor : [REDACTED]

IP Address : [REDACTED] (DHCP)

Subnet : <1> [REDACTED]

VLAN : 000

Access Type : WIRED

Port Status : ACTIVE

Network Device : [REDACTED]

Access Interface : [REDACTED]

Connected Devices : 1

First Seen : 11/25/2024 2:37:43 AM

Last Seen : 4/13/2025 10:41:44 PM

BUSINESS FUNCTIONS

T [REDACTED]

B [REDACTED]

B [REDACTED]

LOCATION

Region/Location : [REDACTED]

Sensor Location : [REDACTED]

NW Device Location : [REDACTED]

Building : [REDACTED]

Floor : [REDACTED]

Zone : [REDACTED]

NW SNMP Location : [REDACTED]

Click to provide classification feedback

SAVE CHANGES

Device Name: [REDACTED]

Tags: RDR EDR Not Installed MDM Not Installed Not Scanned for Vulnerability

Select a Tag

In-Depth Data Collection Capabilities

OSIC gathers the below provided data insights into every device 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.

Category	Details Collected
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



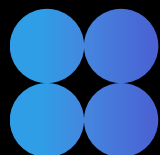
About Us

ORDR is the leader in AI-powered segmentation, securing some of the largest organizations in healthcare, transportation, manufacturing, and financial services. Having analyzed more than 100 million unique device types, the platform is purpose-built to solve the toughest security challenge: unmanaged and IoT assets that put business uptime on the line. By turning intelligence into swift, automated protection, ORDR helps teams contain threats, reduce exposure, and keep operations resilient — 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 Twitter and LinkedIn.

*For more information,
visit ordr.net*

Follow ORDR on



Ready to bring ORDR to your chaos?

[Request a demo](#)