ORDR

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

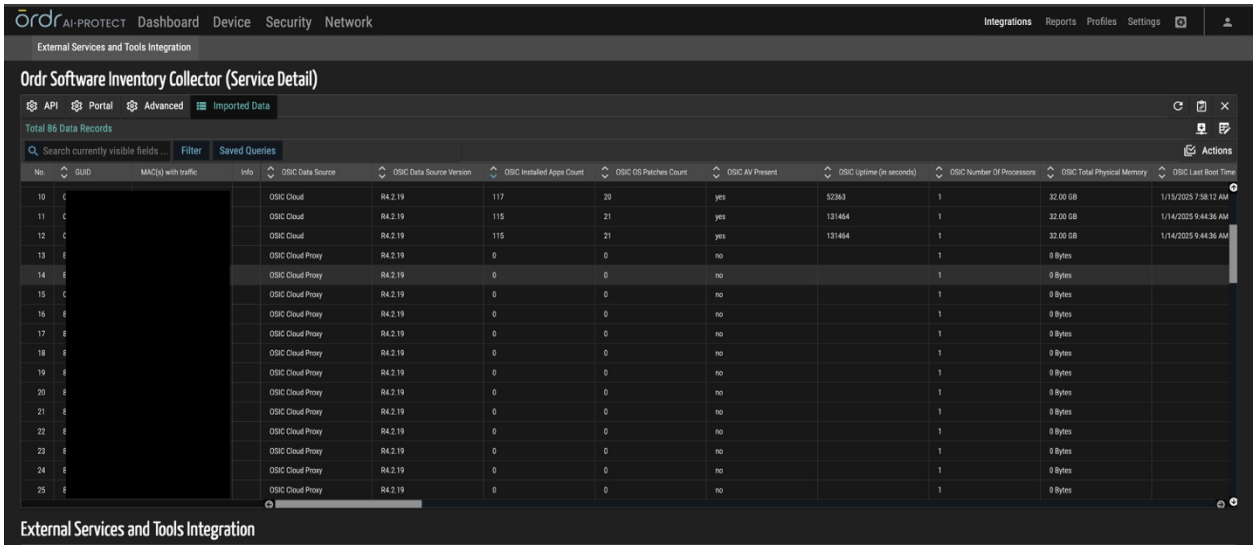
Most enterprises and vendors are recommending building networks with security requirements in mind. It is excellent that vendors and customers are prioritizing security. Still, the model of creating airgap networks using security controls is creating multiple private networks, often using overlapping 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.

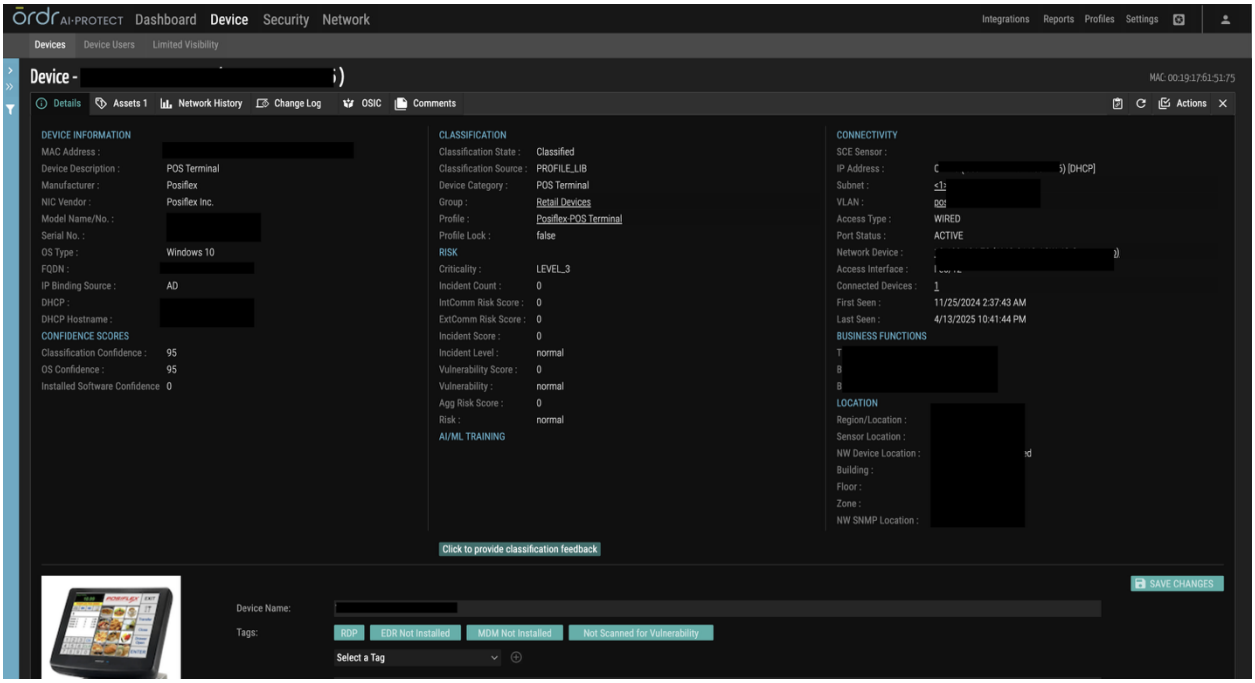
The ORDR Solution – Complete Visibility into Every Device

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

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

ORDR

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