Ordr Ecosystem Integrations Overview

OVERVIEW

The number of devices connected to the Internet, including the machines, sensors, and cameras that make up the Internet of Things (IoT) and Internet of Medical Things (IoMT), continues to expand at an accelerated pace. According to the International Data Corporation (IDC), there will be 41.6 billion connected IoT devices, or "things," generating 79.4 zettabytes (ZB) of data in 2025.

Ordr is industry's **most comprehensive platform** to discover and safeguard these devices. With the broadest number of integrations in the market Ordr extends IoT, IoMT, and OT device context, addresses visibility and vulnerability gaps, and automatically generates policies to respond to attacks and help you proactively harden environments to improve security.

Ordr has over 80 integrations across the IT ecosystem that include clinical systems, computerized maintenance management systems (CMMS), configuration management databases (CMDB), network access control (NAC) solutions, vulnerability management tools, endpoint detection and response (EDR), next-generation firewalls, wired and wireless network infrastructure, cloud platforms, threat intelligence feeds, IT services management (ITSM) platforms, security information and event management (SIEM), IP address management (IPAM), network aggregators, endpoint and user management, and authentication solutions.

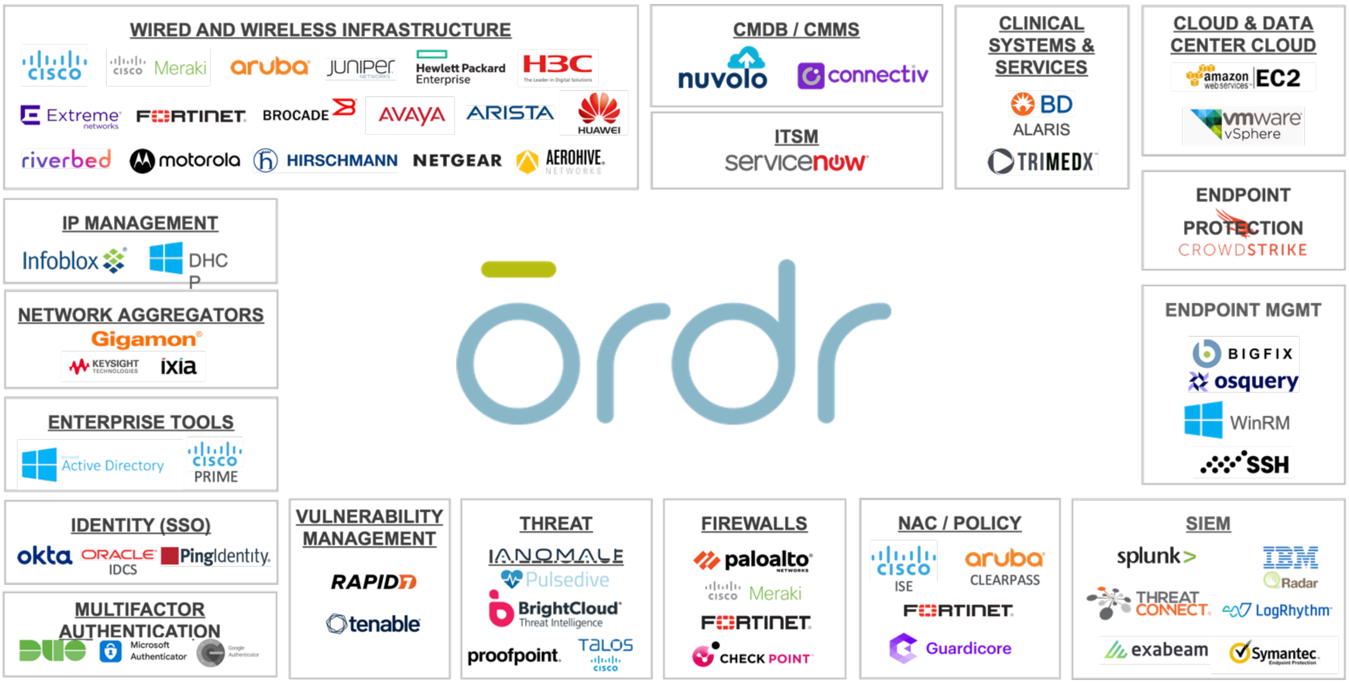

Figure 1: Ordr Ecosystem Integrations

INTEGRATION DETAILS

Ordr categories of integration include the following:

Asset Inventory, CMMS, and CMDB

Ordr collects and consolidates granular details for every single asset in your environment and then enriches your CMMS or CMDB to ensure your asset inventory is always up to date with accurate details.

Network Access Control

Ordr supports NAC projects by providing connected device visibility, automated device classification, also automates policy creation to simplify enforcement and help you reach your goals.

Vulnerability Management

Ordr complements existing vulnerability management solutions by optimizing scanning of specific network environments, excluding devices that should not be scanned, or applying Zero Trust policies to protect devices that cannot be patched. Ordr’s integrated vulnerability scanner can also be used to identify vulnerabilities for any connected device.

Endpoint Detection and Response (EDR)

Ordr uses an agentless approach to discover and automatically classify every connected device, including IT, IoMT, and OT devices. Ordr device profiles can be enriched with EDR data, to address critical use cases. For example, organizations can quickly identify which managed devices discovered by Ordr do not have an endpoint security agent deployed.

Next-Generation Firewalls

Ordr detects exploits and anomalous behavior and can dynamically create policies for firewall enforcement to terminate sessions, block ports, and stop attacks.

Wired and Wireless Network Infrastructure

Ordr offers integrated sensors on network infrastructure such as the Cisco Catalyst 9000 switching family and integrates with Cisco Prime, Cisco Meraki, and Arista devices to simplify deployments. Ordr also enriches connected device context by analyzing network data to include details such as physical and network location to ensure security teams can locate any asset wherever it is. Ordr also provides visualization of device communications within and between subnets and VLANs.

Threat Intelligence

Ordr integrates with threat intelligence platforms and correlates this 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 efforts.

IT Ticketing Systems/IT Service Management (ITSM)

Ordr integrates with IT ticketing systems such as ServiceNow so when a vulnerability, anomaly, or a security incident is detected, we can alert device owners or security teams, and generate a ticket to track further action.

IP Address Management (IPAM)

Ordr integrates with leading IPAM solutions to increase data accuracy for core analytics. We collect IP address assignments for connected devices and accurately correlate MAC-to-IP bindings to ensure security alerts and flow data are always mapped to the correct device.

Ordr Ecosystem Integrations Overview

Clinical Systems

Ordr integration with clinical systems and services automates device classification, provides physical and network location, accelerates response to vulnerabilities, and delivers utilization insights to improve operational efficiencies and capital spend.

Multi-Factor Authentication (MFA)

Ordr integrates with leading MFA providers enabling administrators to seamlessly leverage their organization’s preferred user authentication method for secure access to the Ordr dashboard.

Cloud and Datacenter

Ordr integrates with cloud platforms such as Amazon Web Services (AWS) and VMware to centralize your view of all data center and cloud assets for complete visibility across your entire attack surface.

Network Aggregators

Ordr integrates with network aggregators to simplify deployments and gain access to optimized, high-fidelity connected device network traffic for analysis.

Single Sign-On (SSO)

Ordr supports leading identity providers to provide administrators with frictionless, secure access to the Ordr dashboard with their single set of SSO credentials.

Endpoint and User Management

Ordr integrates with endpoint management systems to collect granular data from all managed devices, across all operating systems, giving organizations rich context to easily see and secure all connected devices.

LEARN MORE

Visit https://ordr.net/platform/integrations/ to learn how Ordr integrates with the tools, solutions, and platforms in your environment to improve security for all your connected devices.