

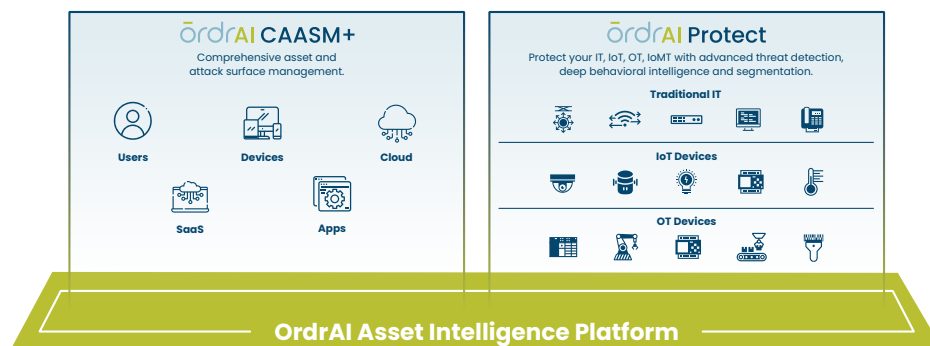


OrdrAI Software Features and Packaging

See. Know. Secure. Every Connected Asset, Everywhere.

OrdrAI Asset Intelligence Platform

OrdrAI Asset Intelligence Platform provides complete, real-time visibility and insights for every network-connected asset, including devices, users, installed software, SaaS applications, and cloud workloads, all enhanced by AI-driven analytics. Ordr addresses these challenges with a cybersecurity framework that can support your organization's asset management journey, from visibility and risk mitigation, threat detection and response, to Zero Trust segmentation.



OrdrAI Products

The OrdrAI Asset Intelligence Platform has been designed to be modular, and enable a building block approach to address your cybersecurity maturity — from asset visibility all the way to Zero Trust.

OrdrAI CAASM+

Complete visibility and attack surface management for all cyber assets.

- Get real-time, asset inventory
- See granular asset details beyond IP and MAC addresses
- Understand device ownership, access, connectivity status and activity
- Establish end-to-end vulnerability management and prioritize remediation based on customizable risk scores
- Continuously monitor for security controls gaps and compliance issues
- Use automated workflows for remediation

OrdrAI Protect

Protect your IT, IoT, OT, IoMT with advanced threat detection, deep behavioral intelligence and segmentation.

- Assess your attack surface with customizable risk scoring
- Identify vulnerable devices based on passive and active data analysis
- Eliminate blind spots with complete N/S and E/W traffic visibility
- Uncover real-time threats with traffic analysis and threat insights
- Meet compliance with device communication and activity tracking
- Understand the retrospective impact of every new IoC detected

Protect Add-Ons:

Zero Trust Segmentation: Confidently create Zero Trust segmentation policies based on business risks

- Ensure only trusted devices are allowed on the network while letting devices perform core functions
- Define and apply flexible policies that align segmentation to business requirements
- Transform visibility into protection with one-click policy automation and scale across multiple layers, zones and locations
- Enforce policies on existing switches, NAC infrastructure, and firewalls
- Integrate with existing security infrastructure including EDR, firewall, NAC, and vulnerability solutions

BI Analytics: Customizable dashboards for personalized insights, reports, and streamlined communications across teams.

- Personalized dashboards tailored to specific user preferences and needs, offering customizable insights covering risk assessment, user behavior analysis, and security control monitoring
- A variety of predefined reports including device summaries, executive overviews, and detailed security analyses
- HTM dashboards and reports

Note: The Ordral CAASM+ and Protect products work independently as described but also complement each other to provide a comprehensive asset visibility solution that allows you to fully understand, collaborate on, and manage risk in an efficient and effective way.

Platform Capabilities	Ordral CAASM+	Ordral Protect	Ordral Protect Add-On: Segmentation	Ordral Protect Add-On: BI Analytics
Asset Visibility: See What Is On Your Network				
Ordral Device Discovery From Multiple Sources: SPAN, API, Network Infra	API/Network Infra	SPAN/TAP/API/Network Infra		
Visibility: On-Prem & Remote Devices (IT, IoT, IoMT, OT)	◆	◆		
Visibility: Cloud Assets	◆			
Visibility: Installed Applications	◆	◆		
Visibility: SaaS Applications	◆			
Visibility: Asset Users From AD	◆	◆		
Visibility: Asset Users From SSO Applications	◆			
Deduplication of Devices	◆ (Also in UI)	◆		
Asset Context: Understand & Accurately Identify Assets				
Asset Location	◆	◆		
Visual Location Mapping	◆	◆		
Connectivity Status	◆	◆		
Parsing Of SNMP Info To Build Location Context	◆	◆		
Medical Device: Clinical Details		◆		
Medical Device: MDS2 Association		◆		
Medical Device: Utilization		◆		
Device Level Flow Visibility		◆		

Platform Capabilities	OrdrAI CAASM+	OrdrAI Protect	OrdrAI Protect Add-On: Segmentation	OrdrAI Protect Add-On: BI Analytics
Device Risk And Cyber Threats: Know Your Potential Threats & Business Risk				
Device Risk Scoring	◆	◆		
Device Recalls And Advisories	◆	◆		
OS And Firmware Vulnerabilities	◆	◆		
Behavioral Analysis		◆		
Traffic Analytics		◆		
Application Destination (URL Visibility)		◆		
Threat Intelligence Feeds	◆	◆		
User To Device Tracking		◆		
Ransomware Detection		◆		
Lateral Movement Detection		◆		
Retrospective Security		◆		
Active Scanning	◆	◆		
Vulnerability Prioritization And Management	◆	◆		
Clinical Risk Assessment Scoring: Vulnerabilities		◆		
Clinical Risk Assessment Scoring: Cyber		◆		
Dashboards & Reporting: Automate Reporting And Improve Collaboration Across Teams				
Customizable Dashboards	◆			◆
Customizable Insights (Risk, User, Security Controls...)	◆			◆
Predefined Reports (Device, Exec Summary, Security...)	◆	◆		◆
HTM Dashboard & Reports		◆		◆
Network Neighbors/Peers For Devices				◆
"All Persona " Dashboard: Executive View And Sections				◆
Data Exploration				
Search And Filters (Quick Query & Query Builder)	◆	◆		◆
Advanced Data Shaping (7/30/60/90 Days)		◆		
OrdrAI Natural Language Query	◆			
Visual Hierarchical Navigation	◆			
Actions: Secure Your Environment				
Device Actions	◆	◆		
Vulnerability Actions	◆	◆		
Location Actions	◆	◆		

Platform Capabilities	OrdrAI CAASM+	OrdrAI Protect	OrdrAI Protect Add-On: Segmentation	OrdrAI Protect Add-On: BI Analytics
Actions: Secure Your Environment (continued)				
Business Function Actions	◆	◆		
Common Actions	◆			
Enforcement: Threat Containment	◆		◆	
Enforcement: Enhanced Policy Grouping			◆	
Segmentation Policy Creation & Enforcement			◆	
Enforcement: Policy Optimization			◆	
Enforcement: Ability To Add "Deny ACLs"			◆	
Enforcement: Customization of Policy Fields			◆	
Enforcement: Import ACL/Policies			◆	
Enforcement: Multiple Firewall Support				
Administration/Management				
Dynamic Data Exchange (DDX)	◆	◆		
User Management	◆	◆		
Role Based User Access				
User: Mode Toggle (Between Basic & Advanced)		◆		
Alert Management	◆	◆		
Integrations: Integrate With Existing Security Tools & Infrastructure				
Syslog, SNMP, SMS, SMTP	◆	◆		
Ordr Software Inventory Collector	◆	◆		
Microsoft Active Directory	◆	◆		
Application Security	◆			
Discovery Tools	◆			
Cloud Infrastructure	◆	◆		
Cloud Security				
CMDB (Configuration Management Database)	◆	◆		
CMMS (Computerized Maintenance Management System)	◆	◆		
Collaboration & Business Tools	◆			
Data Center	◆	◆		
Endpoint Detection & Response (EDR)	◆	◆		
Endpoint & Patch Management	◆	◆		
Extended Detection & Response (XDR)	◆	◆		
External Attack Surface Management	◆			

Platform Capabilities	OrdrAI CAASM+	OrdrAI Protect	OrdrAI Protect Add-On: Segmentation	OrdrAI Protect Add-On: BI Analytics
Integrations: Integrate With Existing Security Tools & Infrastructure (continued)				
Firewalls (Visibility)	◆	◆		
Firewall Policy (Enforcement)	◆		◆	
Identity & Access Management (IAM) (SSO)	◆	◆		
IP Address Management (IPAM)	◆	◆		
IT Asset Management (ITAM)	◆	◆		
IT Service Management (ITSM)/Ticketing Systems	◆	◆		
Location Services	◆	◆		
Log Management		◆		
Clinical Systems	◆	◆		
Mobile Device Management	◆	◆		
Mobile Threat Defense	◆	◆		
Network Access Control (NAC): Profile		◆		
Network Access Control (NAC): Segmentation			◆	
Network Infrastructure	◆	◆		
Network Management	◆	◆		
Security Information Event Management (SIEM): Device Insights	◆	◆		
Security Information Event Management (SIEM): Security Alerts	◆	◆		
Threat Feed	◆	◆		
Vulnerability Scanners & Management Platforms	◆	◆		

For assistance with your asset visibility and security needs, visit ordr.net for more information or contact us at info@ordr.net.