OrdrAI CAASM+

Complete Visibility and Attack Surface Management for All Cyber Assets

Security and IT teams grapple with fragmented views of their assets, manually stitching together insights from disparate sources. This challenge is further complicated by shadow IoT devices and assets that dynamically shift IP addresses. Security professionals often question which actions will yield the most significant risk reduction for their business and struggle to identify device owners for remediation.

OrdrAI CAASM+ provides teams with a comprehensive asset view and actionable business insights for confident, straightforward decision-making. Ordr's multifaceted approach goes beyond API-only solutions combining 100+ security and IT ecosystem integrations with Ordr's Discovery Engine and AI/ML classification. This offers teams an easy-to-deploy solution that delivers complete asset intelligence and business-relevant insights.

Introducing OrdrAI CAASM+

Key Benefits

Real-time, accurate asset data and insights: Ordr provides a single, accurate source of asset data, eliminating noise from duplicates. Visualize relationships and dependencies with an intuitive UI, customizable dashboards, and advanced RBAC capabilities. Ordr combines API collection and proprietary discovery methods with AI/ML classification, eliminating manual processes to correlate data and filtering out noise from duplicates.

Eliminate blind spots: The Ordr Discovery Engine, a proprietary discovery methodology, enables teams to continuously identify and classify unmanaged IoT and OT devices, providing a real-time view across the entire cyber asset attack surface.

Reduce time to respond and improve security hygiene: Ordr's powerful mapping and correlation engine align technical and business priorities, reducing alert fatigue, identifying security gaps, delivering a prioritized list of top risks. This ensures teams know when assets are missing critical security controls, have out of date software, when misconfigurations create security gaps, and when known vulnerabilities exist.

Automate remediation and improve collaboration: Automate remediation workflows using ITSM, SIEM, and SOC integrations, empowering teams with asset and business data to accelerate incident response. Enrich CMDB and other IT tools with the most comprehensive, accurate, and trusted insights for all assets.

Ordr's CAASM Data Collection & Classification Methodology

OrdrAI CAASM+

Users | **Devices** | **Cloud** | **SaaS** | **Apps**

Use Cases

- Automated asset inventory
- CMDB asset reconciliation
- Issue prioritization
- SBOM reporting
- Security control reporting
- User access and status (service accounts with admin rights or inactive admin users)
- Security coverage gap analysis
- Audit and compliance reporting
- Incident response

Ordr CAASM+ goes beyond API-only solutions, utilizing API data collection and proprietary discovery methods with AI/ML classification to give customers accurate, complete asset visibility, business context, and insights to concentrate on the most critical risks.

Deploy in Minutes, Results and Visibility in Hours: How Ordr CAASM+ Works

1. **Connect:** Connect Ordr with existing data sources leveraging 100+ out-of-box integrations for real-time view across the entire cyber asset attack surface.
2. **Discover:** Surface risks relevant to your business with reports, customized dashboards, and queries using natural language.
3. **Enable fast, data-driven decision-making, priority setting, and action:** Use reports, dashboards, and natural language queries to uncover risk across all assets and trigger customizable, automated action.

Asset discovery is extremely important but understanding what risks are around those assets is critical. Not all assets should be treated the same. If you don't have an individual profile for each asset, your system treats them the same. Our core payment system is not going to be treated the same as another system that doesn't contain the same type of data, or the value data from a regulatory perspective. Understanding assets and their risks is how CSOs should approach security."

// CISO, Financial Services Organization (788 Branches Across 17 States)

With automated inventory, vulnerability prioritization, and compliance reporting at their fingertips, Ordr enables teams to improve their security posture and accelerate incident response. Organizations can secure their connected world with confidence, knowing that every cyber asset, whether in the cloud, on-premises, or in hybrid environments, is within their command.

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

ordr