Ordr + Mobile Device Management Integration

Securely supporting a hybrid and remote workforce has become a fundamental component of an organization's cybersecurity strategy. As a result, mobile device management (MDM) tools play a critical role in managing all devices that access essential enterprise resources.

However, these managed devices cover only a small portion of all assets interacting with an enterprise network. With a rapid rise in the variety and volume of devices, every enterprise's attack surface continues to expand. To effectively manage and secure all devices, security and IT teams need a centralized view of all devices and threats across their entire environment.

Ordr and MDM Solution Integrations

Ordr's value is in the asset intelligence it provides, which spans across every asset, with in-depth insight into its profile and context. The OrdrAI platform automatically discovers and classifies every device, identifies risk, maps communications, establishes baseline behavior, and provides protection with automated policies.

Security and IT teams can easily discover and secure every managed and unmanaged asset — from traditional IT to vulnerable IOT, OT, IOMT devices, along with users, applications, SaaS, and cloud on a single platform.

Ordr integrates with MDM solutions to enable organizations to easily identify all devices, uncover security gaps, prioritize vulnerabilities, and respond to threats quickly. Ordr seamlessly combines and correlates device, installed applications, and user information collected from MDM solutions alongside Ordr's own data sources to build true asset intelligence that can easily be turned into remediation workflows and policies.

Benefits of Ordr Integration with MDM Solutions

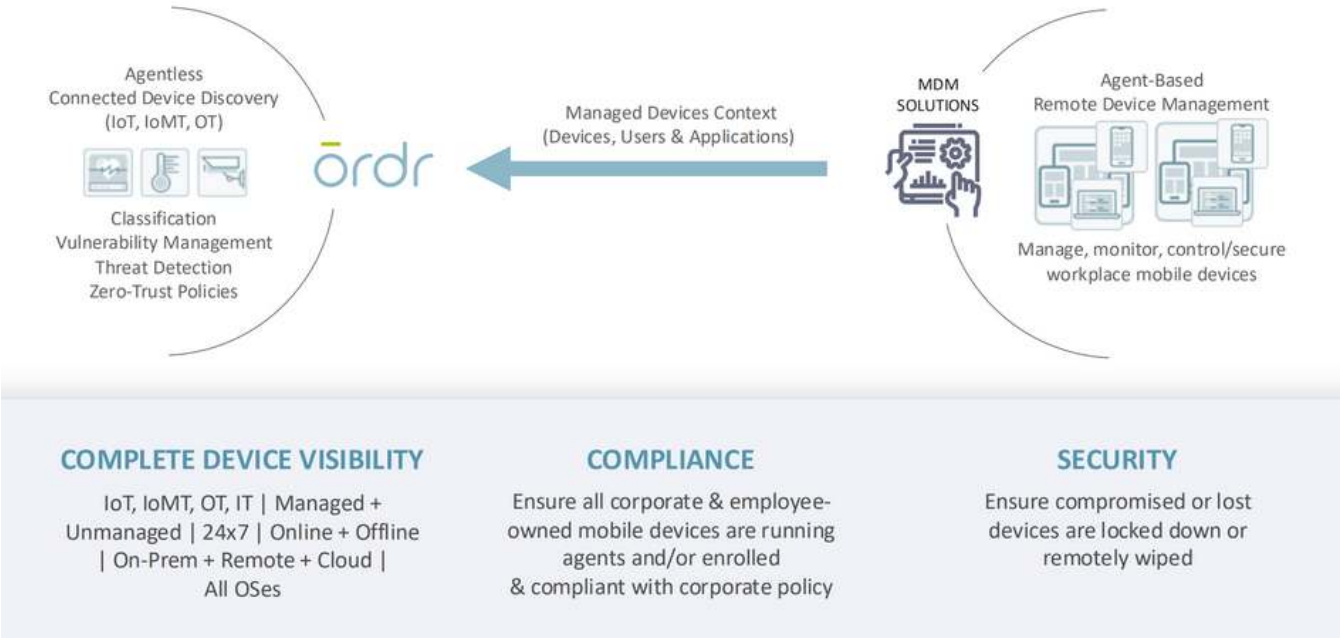
Combining the Ordr asset intelligence with managed device details from MDM solutions empowers organizations to:

- **Gain real-time visibility into all connected devices:** Centralized intelligence into devices across all operating systems, whether they're on premises, remote, managed, or unmanaged.
- **Prioritize vulnerability management:** Leverage risk-based vulnerability insights to track and prioritize remediation for devices based on criticality and impact to organization.
- **Detect security gaps:** Uncover coverage and enrollment gaps including devices missing an agent or not reporting into MDM solutions.
- **Ensure corporate compliance:** Get up-to-date device details to meet compliance and cyber insurance requirements, including device encryption status and the ability to lock down or remotely wipe compromised devices.
- **Automate risk remediation and mitigation:** Automate workflows and segmentation policies for vulnerable assets that cannot be patched, or until patches and resources are available.
- **Accelerate incident response time:** Speed up investigations and analyses with rich and accurate context necessary to contain suspicious activity quickly, including asset classification, device users, mapped events, and more.

How it Works

Ordr's self-service ecosystem integrations are designed to be turnkey with minimal configuration and setup time, while enabling quick customizations to meet business needs.

Once configured to collect managed device, installed application and user information from MDM solutions, Ordr deduplicates, correlates and analyzes all the data. Ordr leverages additional data from the MDM solutions to enhance context for devices previously discovered by Ordr, add any new devices and their details, and identify gaps in visibility and security.



The Ordr deduplication engine ensures all the asset data is accurate, whether discovered by Ordr, collected from the MDM solutions or other ecosystem tools. And the correlation ensures data from the different data sources deliver complete, meaningful and actionable insights.

Additionally, Ordr's Device Data eXchange (DDX) engine offers the flexibility to determine whether to apply Ordr detected device attributes by default, or prioritize and customize mapping rules based on the information collected from MDM solutions.

Ordr Ecosystem Integrations

Ordr integrates with industry-leading security, networking, infrastructure, IT, and clinical solutions to unify device details, enrich device context, and extend the value of your existing investments. Data from integrations is combined in the Ordr Data Lake to create the most complete and accurate view of every connected device across your whole organization. Ordr also enriches these solutions with accurate insights, makes teams more efficient, and security stronger.

About Ordr

Ordr addresses the entire asset and attack surface management journey—visibility, risk-based vulnerability management, advanced threat detection and Zero Trust segmentation. By utilizing unified data discovery methods, combined with AI/ML analytics, Ordr effectively eliminates asset noise, prioritizes the top exposure to the organization, and delivers rapid threat containment using automated actions. Trusted by global enterprises, Ordr improves security hygiene, accelerates incident response, and facilitates Zero Trust initiatives. Ordr is backed by top investors including Battery Ventures, Wing Venture Capital, Ten Eleven Ventures, and Kaiser Permanente Ventures. For more information, visit www.ordr.net and follow Ordr on Twitter and LinkedIn.

ordr

© 2024 ORDR. ALL RIGHTS RESERVED. | ORDR_SB_MDM