ORDR | Microsoft Intune

SOLUTION BRIEF

ORDR Integrations with Microsoft Intune

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

However, these managed endpoints 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 Microsoft Intune Integration

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.

BENEFITS OF ORDR INTEGRATION WITH MICROSOFT INTUNE

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 endpoints missing an agent or not reporting into Intune.

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.

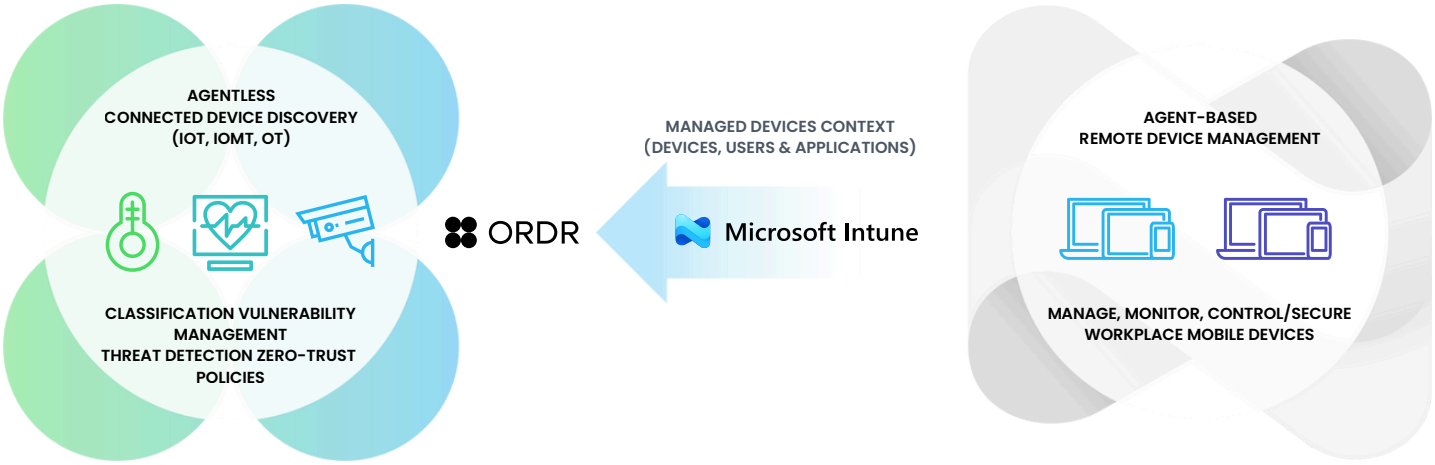
Accelerate incident response time

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 Microsoft Intune's managed device, installed application and user information, ORDR deduplicates, correlates and analyzes all the data. ORDR leverages the additional data from Intune to enhance context for devices previously discovered by ORDR, add any new devices and their details, and identify gaps in visibility and security.



VISIBILITY

- Software Apps Installed
- Patches with Dates
- HW Encryption Status
- BIOS Password Checks
- Devices without an Agent

COMPLIANCE

- Non-Compliant Devices per Corporate Policy
- Agents Present
- Endpoint Firewall Enabled
- Agents Disabled from Updates

SECURITY

- Ensure compromised or lost devices are locked down or remotely wiped
- Ensure IP data is protected during employee turnover

The ORDR deduplication engine ensures all the asset data is accurate, whether discovered by ORDR, collected from Microsoft Intune or other ecosystem tools. And the correlation ensures data from the different data sources delivercomplete, meaningful and actionable insights. Additionally, ORDR's DeviceData 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 Microsoft Intune.

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 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 **X** and **LinkedIn**.

For more information, visit **ordr.net**

Follow ORDR on

Ready to bring ORDR to your chaos?

Request a demo