ORDR

Solution Brief

ORDR + Kandji

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) solutions like Kandji 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 Kandji

ORDR delivers asset intelligence that spans every asset, with in-depth insights into its profile and context. The ORDR AI Protect platform automatically discovers and classifies every device, identifies risk, maps communications, establishes baseline behavior, and provides protection with automated policies. These capabilities, integrated with the Kandji platform, enable organizations to easily identify all connected devices, uncover security gaps, prioritize vulnerabilities, and respond to threats quickly.

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 seamlessly combines and correlates managed Apple devices details and installed applications collected from Kandji alongside ORDR's own data sources to build true asset intelligence that can easily be turned into risk insights and remediation workflows.

Benefits of Integration with Kandji

ORDR's comprehensive asset intelligence combined with managed device details from Kandji empowers organizations to:

- **Gain insights into all assets, agentless and agent-based, on premises and remote:** Get centralized intelligence across all connected assets and operating systems – whether or not they can run an agent — including vulnerable IoT, OT, IoMT, and traditional IT devices, as well as users, applications, SaaS, and cloud -- all on a single platform.
- **Detect security gaps**: Uncover coverage and enrollment gaps including Apple devices that are unenrolled, misidentified, missing agents, associated with expired agents, or that are not reporting into Kandji.
- **Prioritize vulnerability management:** Leverage risk-based vulnerability insights to track and prioritize remediation for devices based on criticality and impact to organization.

- **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.

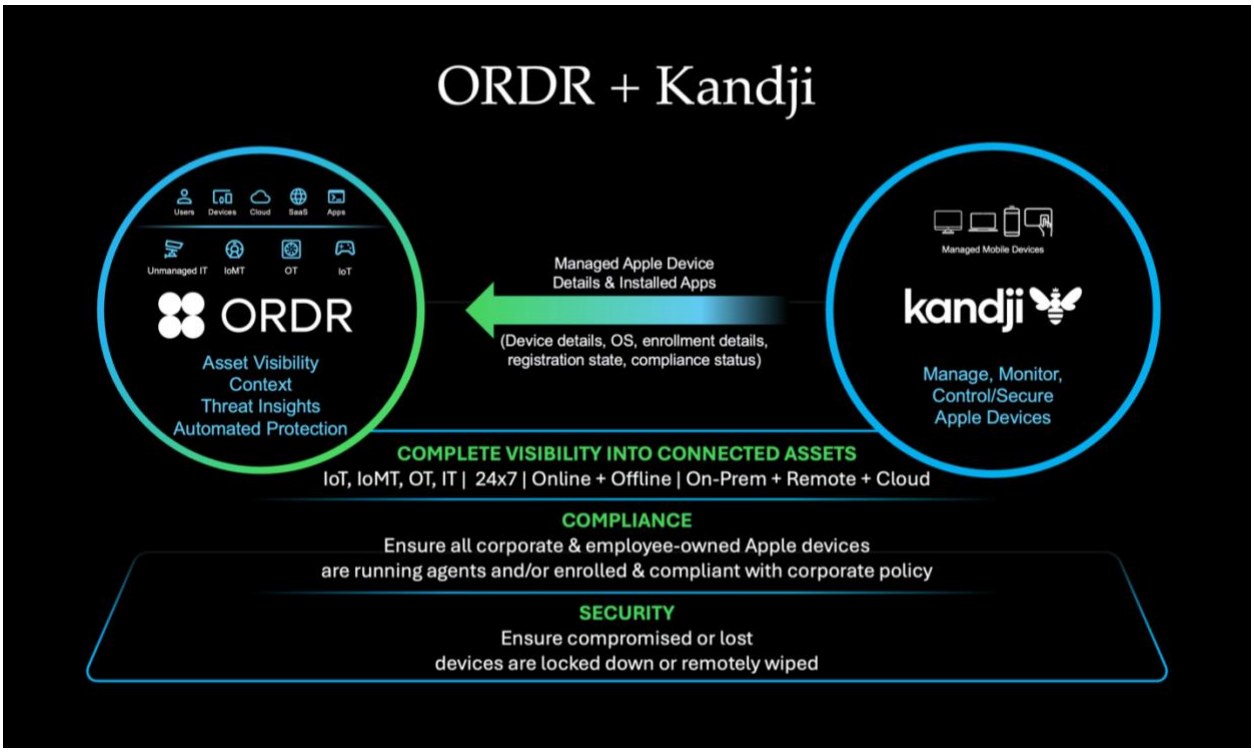
- **Automate risk remediation and mitigation:** Automate workflows and segmentation policies for vulnerable assets that cannot be patched, or until patches and resources are available.

- **Accelerate incident response time**: Speed up investigation and analysis with rich, 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 Apple device details and installed application from Kandji, ORDR deduplicates, correlates, and analyzes all the data. It uses the additional data from Kandji to enhance context for previously discovered devices, add details for any new devices, and identifies gaps in visibility and security.



ORDR's deduplication engine ensures all asset data is accurate, whether discovered by ORDR or collected from Kandji or other ecosystem tools. Additionally, the ORDR correlation engine ensures data from all the different sources delivers complete, meaningful, and actionable insights.

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 information collected from Kandji.

ORDR

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 technology 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, making security teams more efficient, and cyber defenses stronger.

About Us

ORDR is the leader in AI-powered asset risk and exposure management, trusted by top organizations across healthcare, pharmaceuticals, manufacturing, and financial services. With insights from over 100 million asset types, ORDR's platform empowers security teams to identify their biggest risks and take swift, effective action. From maintaining security hygiene to real-time threat detection and protection using microsegmentation, ORDR makes action not just possible but automated and simple — 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