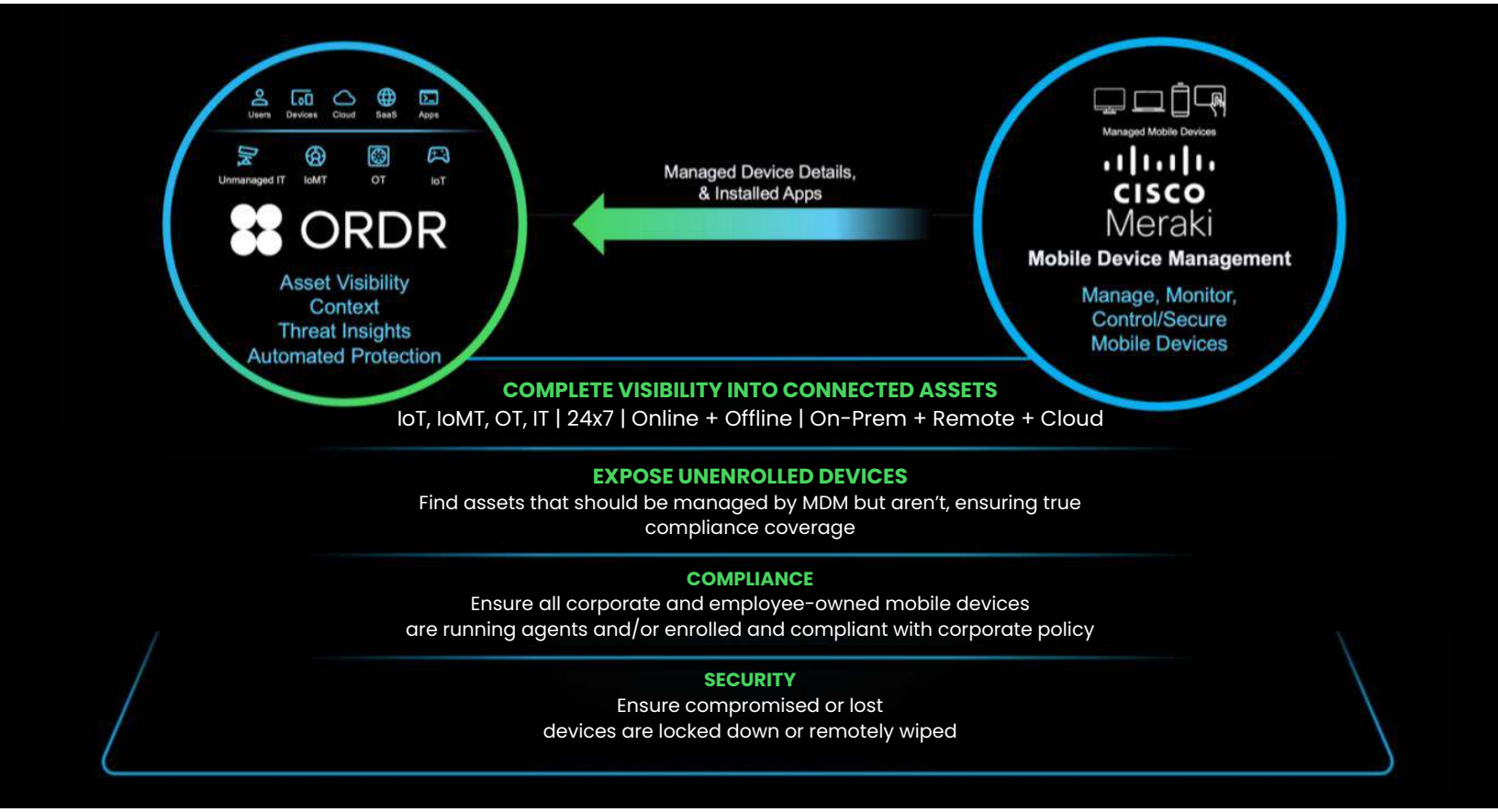
ORDR

INTEGRATION BRIEF

ORDR + Cisco Meraki MDM

Secure Every Device, Everywhere



Imagine a world where every connected device in your organization is not just discovered, but understood. Where security isn't just a checkbox, but an intelligent, automated response to risk. That's what ORDR delivers – asset intelligence that spans every device, offering in-depth insights into its profile and context. And with the power of Cisco Meraki, it's even easier to track and secure every device, across your entire network.

ORDR AI Protect takes security automation to the next level, seamlessly integrating with Cisco Meraki to discover and classify every device, identify risks, map communications, establish baseline behavior, and automatically enforce protection with smart policies. The result? Your organization is empowered to uncover security gaps, prioritize vulnerabilities, and respond to threats faster and more efficiently than ever before.

How It Works

Once configured to collect managed device details, installed apps, and user data from Cisco Meraki MDM, ORDR gets to work. It deduplicates, correlates, and analyzes all this data to fill in the gaps, enhance the context, and deliver a full picture of your asset landscape. No device is left behind.

ORDR's power lies in its sophisticated deduplication engine, ensuring that asset data is always accurate—whether it's discovered by ORDR or pulled from Cisco Meraki or other ecosystem tools. And with ORDR's correlation engine, all data from different sources is transformed into meaningful, actionable insights. For even greater flexibility, the Device Data eXchange (DDX) engine lets you customize how device attributes are applied, giving you control over how Meraki data is integrated with ORDR's insights.

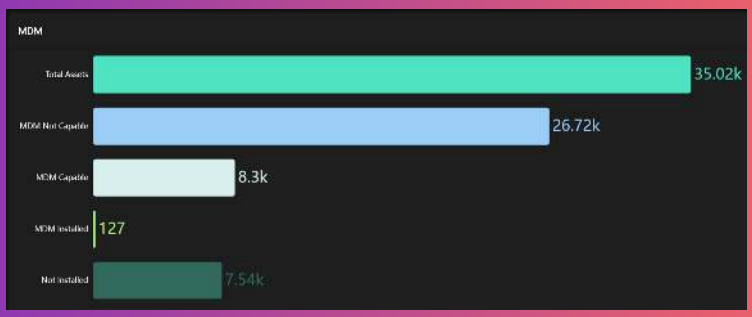
Why This Matters

ORDR and Cisco Meraki give organizations a complete, trusted view of every asset—managed and unmanaged, on-prem and remote—all in one place. Security gaps are exposed early, risk is prioritized based on real business impact, and compliance is easier to maintain.

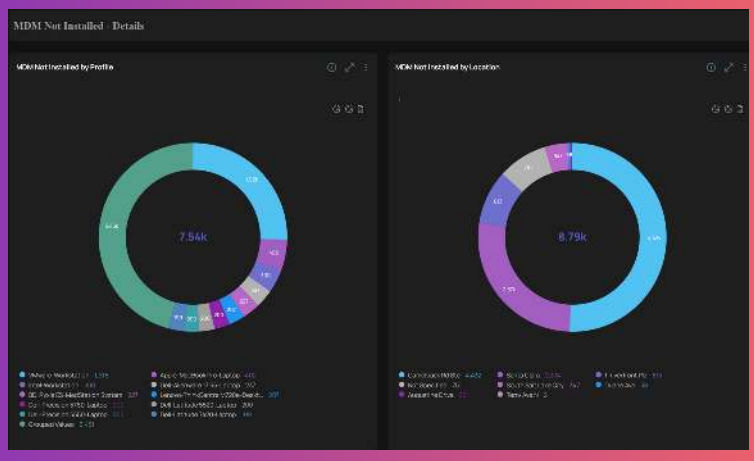
When vulnerabilities can't be patched, ORDR automates protection to reduce exposure without slowing operations. And when incidents occur, rich asset and user context accelerates investigation and containment.

The result: faster decisions, stronger security, and a simpler path from insight to action.

MDM Dashoard Examples



MDM Overview



MDM "Not Installed" by Profile & Location