Ordr + SentinelOne Integration

As cyber threats get more sophisticated and enterprise security teams find themselves investing in a variety of security tools, endpoint detection and response (EDR) systems like SentinelOne continue to play a vital role in securing an organization.

However, not every asset in your organization is able to install an agent, which means you cannot rely solely on agent-based solutions to assess your attack surface. Assets connected to your network can range widely from Windows workstations to specialized equipment such as surveillance cameras, payment card systems, infusion pumps or programmable logic controllers.

To effectively manage and secure the entire organization, enterprises need a centralized view of the entire attack surface, whether they can be managed or secured by existing solutions or not.

Ordr and SentinelOne Integration

Ordr delivers asset intelligence that 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.

Ordr's bidirectional integration with SentinelOne Singularity Platform enables organizations to easily identify all connected devices, uncover security gaps, prioritize vulnerabilities, and respond to threats quickly. Ordr seamlessly combines and correlates endpoint data, vulnerabilities, and threat insights collected from SentinelOne alongside Ordr's own discovery and data sources to build true asset intelligence that can easily be turned into remediation workflows and policies. Furthermore, security teams can leverage the insights from Ordr to proactively mitigate agentless device risk via the Singularity Platform.

Benefits of Ordr Integration with SentinelOne

Gain insights into all assets, agentless and agent-based: Get centralized intelligence into every connected asset whether they can or cannot run an agent — from traditional IT to vulnerable IoT, OT, IoMT devices, along with users, applications, SaaS, and cloud on a single platform.

Detect security gaps: Uncover coverage and enrollment gaps including endpoints missing an agent or not reporting into SentinelOne.

Minimize risk with threat detection for all assets: Identify vulnerabilities and assets exhibiting risky or malicious behavior by combining SentinelOne's endpoint and risk context with granular insights from Ordr, including network activity for each device.

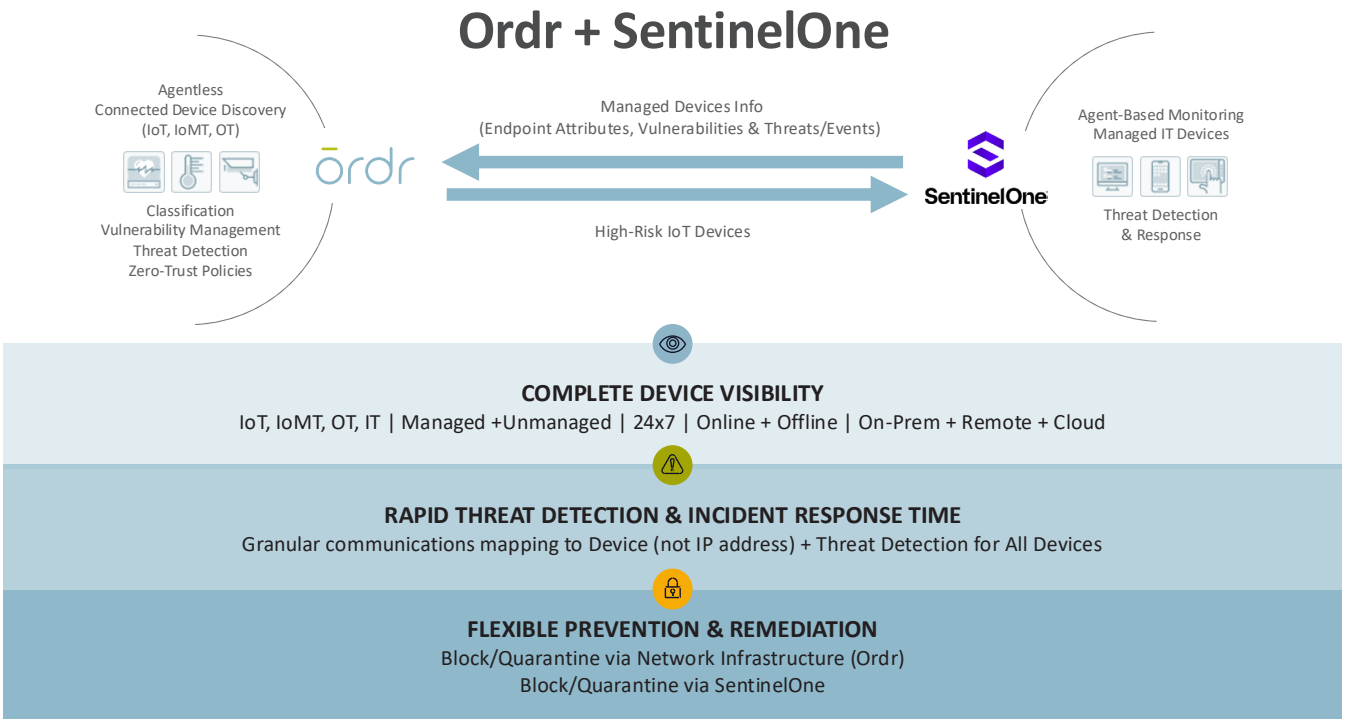
Automate risk remediation and mitigation: Identify high-risk assets — whether umanaged or managed by SentinelOne — so you can block, quarantine, or segment them using SentinelOne, or push enforcement and remediation through Ordr to your network infrastructure.

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.

After configuring the integration to collect data from SentinelOne-managed endpoints — including installed applications, vulnerabilities, and security events — Ordr deduplicates, correlates, and analyzes all the information. It uses the additional data from SentinelOne to enhance context for previously discovered devices, add details for any new devices, and identify gaps in visibility and security.



The Ordr deduplication engine ensures all the asset data is accurate, whether discovered by Ordr, collected from SentinelOne 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 SentinelOne.

During configuration, how and when Ordr sends high-risk agentless device information to SentinelOne can also be easily customized for proactive risk mitigation.

Ordr uses multiple factors to calculate risk for each asset based on business context, asset criticality, vulnerabilities, and overall threat details. With additional data from SentinelOne, Ordr provides a highly accurate risk score for each device.

By continuously synchronizing asset risk scores with SentinelOne's endpoint and threat data, Ordr enables security teams with an up-to-date view of risk to help them focus on the most critical devices.

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