Ordr and CrowdStrike Integration

See, Know, and Secure Every Managed and Unmanaged Connected Device.
Eliminate blind spots across IT, IoT, IoMT, and OT infrastructure.

Challenges

Connected devices are now a significant part of the IT ecosystem and provide critical business services across all industries. These IP-enabled devices range widely from surveillance cameras and payment card systems to infusion pumps in healthcare and programmable logic controllers in manufacturing environments.

Connected devices can create business, IT, and cybersecurity blind spots since they can be difficult to discover via traditional asset inventory solutions and at present, cannot be scanned via vulnerability management systems or support corporate endpoint security agents.

Solution

Integration between OrdrAI Asset Intelligence Platform and CrowdStrike Falcon's Endpoint Detection and Response (EDR) and Next-Gen SIEM solutions ensures security across all managed and unmanaged devices with comprehensive device visibility, detailed vulnerability insights, an understanding of risk, and the ability to enforce policy to mitigate active threats and improve security across all connected devices.

Key Solution Benefits

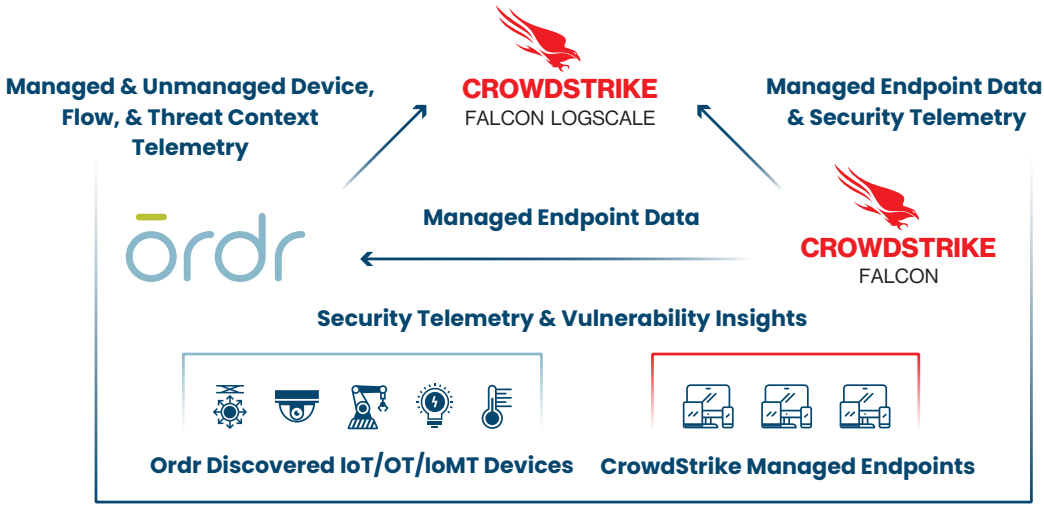
Gain complete visibility into all agentless and agent-based devices: See every connected device from traditional IT to new IoT, IoMT, and OT devices by combining CrowdStrike managed devices with Ordr Discovery Engine built to automate and centralize discovery for all managed, unmanaged, and newly connected devices.

Minimize risk with threat detection for all devices: Identify vulnerabilities and devices exhibiting risky or malicious behavior by combining CrowdStrike device and risk context with granular insights from Ordr including network activity for each device.

Meet compliance requirements: Identify all agentable devices missing CrowdStrike agents to ensure compliance with corporate policy.

Remediate faster: Identify high-risk agentless devices and block, quarantine, or segment managed devices in Ordr for rapid remediation via the network.

Stay ahead of threats: Simplify investigating and debugging issues quickly by combining Ordr device insights with CrowdStrike security data for unified security operations via CrowdStrike's Next-Gen SIEM.



How Ordr and CrowdStrike Integrations Work

Endpoint Detection and Response (EDR)

- OrdrAI Asset Intelligence Platform automatically discovers and classifies every connected device, profiles behavior, and identifies active threats.
- Security telemetry from the CrowdStrike Falcon platform, powered by the CrowdStrike Security Cloud and world class AI, is shared with Ordr to enhance device insights, and provide a centralized, deep understanding of each device and its associated risk.
- Ordr uses multiple factors to calculate risk for each device based on business context, asset criticality, vulnerabilities, and overall threat details. With additional device data from the Falcon platform, Ordr provides a highly accurate risk score for each device.
- By continuously synchronizing device risk scores with CrowdStrike's enriched security data, Ordr enables teams with an up-to-date view of risk to help them focus on the most critical devices.
- Ordr aids security and compliance efforts by providing organizations with a single source of truth for all managed and unmanaged devices and can help easily identify devices missing a Falcon Sensor (endpoint agent).

Next-Gen SIEM

- Ordr sends all connected device data including comprehensive risk levels, network connectivity insights, vulnerabilities and incidents to CrowdStrike Falcon Logscale.
- Logscale aggregates and correlates telemetry from OrdrAI Platform and CrowdStrike Falcon enabling Security, IT, and DevOps teams to run advanced device and risk analyses and create custom dashboards for more efficient SIEM and log management.

About Ordr

Learn more at **ordr.net** and follow Ordr on **LinkedIn** | **X**

About CrowdStrike

Learn more at **crowdstrike.com** and follow CrowdStrike on **Blog** | **X** | **LinkedIn** | **Facebook** | **Instagram**

ordr