Solution Brief

ORDR + Microsoft Defender for Endpoint

Integration

As cyber threats grow more sophisticated, and attack surfaces grow more complex through the adoption of a wide variety of network connected assets, enterprise security teams find themselves investing in a variety of security tools. Endpoint Detection and Response (EDR) systems like Microsoft Defender for Endpoint continue to play a vital role in securing an organization.

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

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

ORDR and Microsoft Defender for Endpoint

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 Microsoft Defender for Endpoint platform, enable organizations to easily identify all connected devices, uncover security gaps, prioritize vulnerabilities, and respond to threats quickly.

ORDR seamlessly combines and correlates endpoint details, including risk and compliance data, collected from Microsoft Defender for Endpoint alongside ORDR’s own discovery and data sources to build true asset intelligence that can easily be turned into risk insights and remediation workflows.

Benefits of ORDR Integration with Microsoft Defender for Endpoint

ORDR’s comprehensive asset intelligence combined with managed endpoint details from Microsoft Defender for Endpoint empowers organizations to:

- **Gain insights into all assets, agentless and agent-based:** Get centralized intelligence across all connected assets – 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 and compliance gaps**: Uncover coverage and enrollment gaps including endpoints that are unenrolled, misidentified, missing agents, associated with expired agents, or that are not reporting into Microsoft Defender for Endpoint.

- **Minimize risk with threat detection for all assets**: Identify vulnerabilities and assets exhibiting risky or malicious behavior by combining Microsoft Defender for Endpoint details with contextual insights from ORDR, including network activity for each asset.

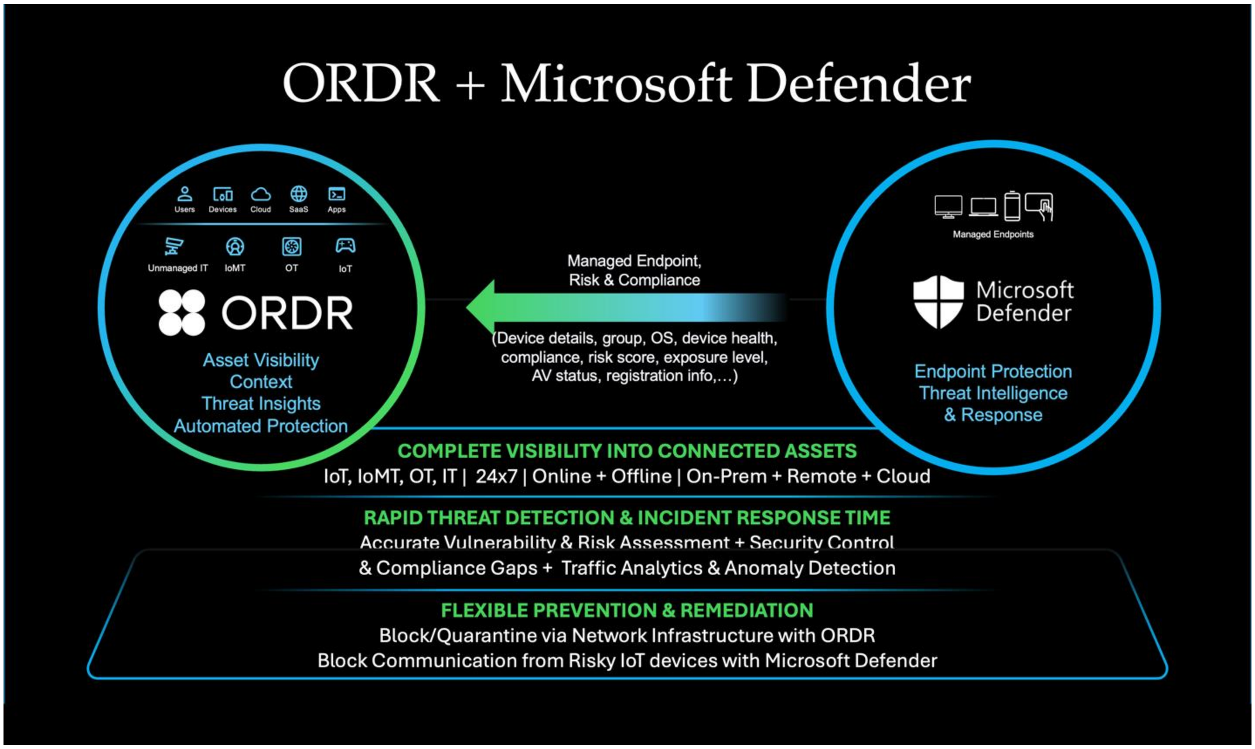
- **Automate risk remediation and mitigation**: Identify high-risk assets, and either contain via Microsoft Defender for Endpoint or push enforcement and remediation via ORDR to your network infrastructure.

- **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 endpoint data from Microsoft Defender for Endpoint, ORDR deduplicates, correlates, and analyzes all the data. It uses the additional data from Microsoft Defender for Endpoint to enhance context for previously discovered devices, add details for any new devices, and identifies gaps in visibility and security.



ORDR + Microsoft Defender

Asset Visibility
Context
Threat Insights
Automated Protection

Managed Endpoint,
Risk & Compliance

(Device details, group, OS, device health,
compliance, risk score, exposure level,
AV status, registration info,…)

Endpoint Protection
Threat Intelligence
& Response

COMPLETE VISIBILITY INTO CONNECTED ASSETS
IoT, IoMT, OT, IT | 24x7 | Online + Offline | On-Prem + Remote + Cloud

RAPID THREAT DETECTION & INCIDENT RESPONSE TIME
Accurate Vulnerability & Risk Assessment + Security Control
& Compliance Gaps + Traffic Analytics & Anomaly Detection

FLEXIBLE PREVENTION & REMEDIATION
Block/Quarantine via Network Infrastructure with ORDR
Block Communication from Risky IoT devices with Microsoft Defender

ORDR's deduplication engine ensures all asset data is accurate, whether discovered by ORDR or collected from Microsoft Defender for Endpoint 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 Microsoft Defender for Endpoint.

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