PARTNER BRIEF

Dragos + ORDR: Unified OT Visibility and Intelligent Network Segmentation

The Challenges

As OT environments become more connected to the outside world, security teams struggle to maintain visibility and control. IT tools lack OT context for prioritizing risks and changing policy, and OT environments can be highly complex and make it challenging to implement new controls. The result is increased exposure to ransomware, supply chain attacks, downtime, and other OT-related attacks.

Network segmentation—vital for defensible architecture—is difficult without real-time visibility. Without coordination between security and operations, policies can break uptime or miss lateral threats. Effective segmentation requires trusted insight into device communications, knowledge of the OT environment, and policies that can be reviewed before implementation.

The Solution

Dragos and ORDR combine OT visibility and intelligent policy enforcement to simplify network segmentation. The Dragos Platform identifies assets, vulnerabilities, and communication flows, while ORDR's Systems Control Engine translates this context into enforceable policies. Together, they enable secure segmentation grounded in real OT requirements.

This integration converts Dragos's asset intelligence (device types, firmware, and communication baselines) and OT-contextualized risk-analysis into actionable policies managed through ORDR's platform. The result: stronger protection, faster enforcement, and sustained uptime.

Examples include:

- Isolating legacy PLCs from external connections.
- Restricting engineering workstations to approved HMIs.
- Blocking high-risk protocols like SMB or RDP.
- Moving vulnerable or rogue devices into restricted zones until remediation occurs.

How It Works

The Dragos Platform integrates with ORDR through an API-based connection, enabling automated sharing of enriched OT asset data. This integration helps organizations translate visibility into actionable network controls:

- Deploy Dragos sensors across OT networks to identify assets, vulnerabilities, and communication patterns.
- Configure the Dragos–ORDR API integration for continuous data synchronization and enrichment.
- Use ORDR's platform to generate segmentation policies based on Dragos-enriched OT data and contextual risk scores.
- Enforce policies through existing network infrastructure while maintaining process integrity.
- Monitor ongoing performance and policy adherence through shared dashboards and automated reporting.

Benefits

- Unified visibility across IT, OT, and IoT environments
- OT-specific threat detection and contextual risk scoring
- Automated, enforceable network segmentation policies
- Reduced downtime and improved operational resilience
- Support for IEC 62443, NIST 800-82, and SANS ICS 5 Critical Controls
- Joint Dragos–ORDR support and rapid deployment

Tech Specs / Integration Details

Integration Type	API-based connector
Deployment Model	On-premises, hybrid, or cloud
Supported Data	Asset lists, asset profile, alerts, and vulnerability data
Licensing	Included with Dragos Platform and ORDR SaaS subscription
Support	Joint Dragos & ORDR TAC Support

About Dragos, Inc.

Dragos safeguards civilization from those trying to disrupt the industrial infrastructure we depend on every day. Headquartered in the Washington, DC area with global operations across North America, Europe, the Middle East, and Asia-Pacific. Learn more about our technology, services, and threat intelligence offerings: **request a demo** or **contact us**.

About ORDR

By filtering out noise and pinpointing critical risks, ORDR empowers you to safeguard every asset—in the cloud, on-premises, or in SaaS environments—and enable cyber resilience.