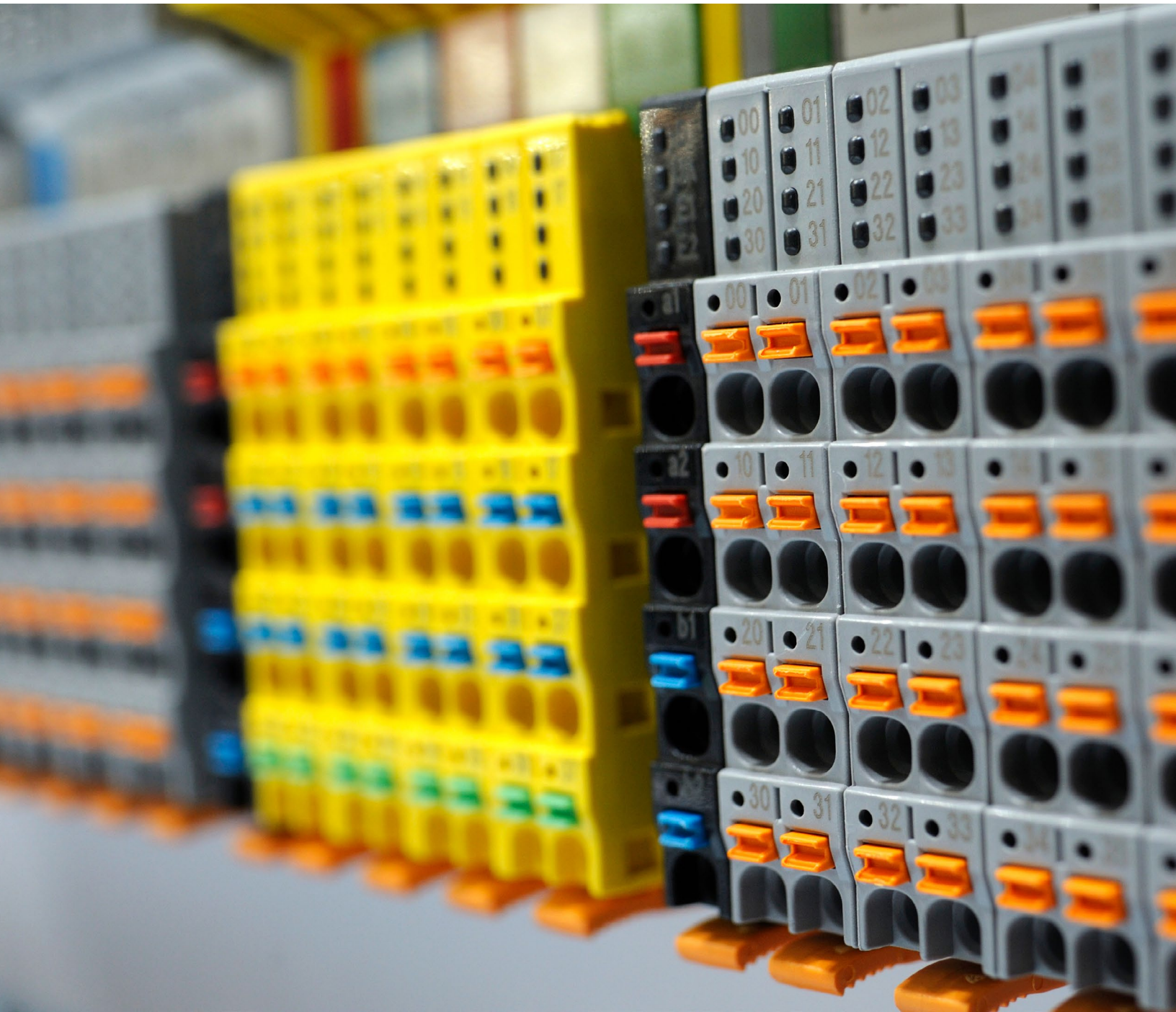


PARTNER BRIEF

OT-Native Cybersecurity Integrated Across the Microsoft Ecosystem



THE CHALLENGE:

As connectivity extends deeper into physical operations, the attack surface grows with it. Organizations need a unified view across IT and OT to modernize confidently.

For most enterprise security teams, the industrial environment—power substations, oil refineries, water treatment facilities, and other critical infrastructure—remains outside the reach of the security tools they rely on every day. Adversaries know this and are actively exploiting the gap.

**ADVERSARIES
ARE TARGETING OT:**



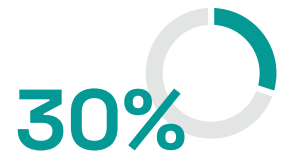
OT-focused threat groups tracked, with 11 active in 2025.*

**VISIBILITY IS
CRITICAL FOR CRITICAL
INFRASTRUCTURE:**



Fewer than 10% of OT networks worldwide have visibility and monitoring in place.*

**YOUR IT SOC HAS
BLIND SPOTS:**



of OT incident response cases started not with a detected intrusion, but with someone saying, “something seems wrong”.*

**Dragos 2026 OT Cybersecurity Year in Review*

Securing operational environments means having OT asset visibility, threat detection, and intelligence informed by how adversaries operate against industrial targets. When these capabilities flow into broader SOC workflows that enterprises already rely on, security teams gain better visibility, make more informed decisions, and respond faster.

THE SOLUTION:**Closing the IT/OT Security Gap at Enterprise Scale**

Dragos and Microsoft deliver OT-native cybersecurity inside the tools your teams rely on, through the procurement channels you are accustomed to, and across the AI workflows your enterprise already runs. The result is unified visibility from the plant floor to the SOC, without disrupting how your teams work, buy, or operate.

Dragos

Named a Leader in the 2026 Gartner Magic Quadrant for CPS Protection Platforms for the second consecutive year, Dragos combines a purpose-built OT monitoring platform with frontline threat intelligence and expert services, including managed detection and incident response retainers. Dragos was built by practitioners who have spent over a decade responding to OT attacks.

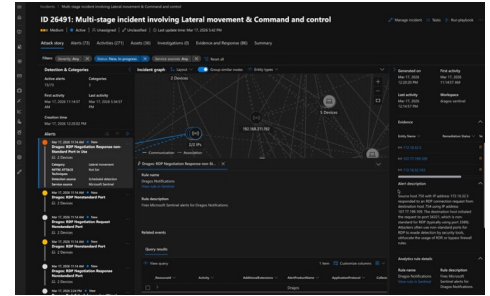
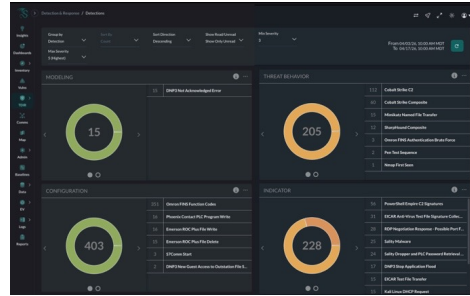
Microsoft

Microsoft sits at the center of enterprise security operations, providing the infrastructure, security operations platform, and AI-assisted workflows organizations trust.

DRAGOS + MICROSOFT

Unified Security Operations

With the Dragos Platform, security teams can monitor deep in OT environments. When detections are triggered, the alerts with OT context flow directly into Microsoft Sentinel giving teams unified visibility across IT and OT in a single workflow. By unifying investigations, your enterprise SOC can monitor for cross-domain threats without switching tools or rebuilding how they operate. Through the Dragos MCP Server, analysts can also query Dragos Platform data in natural language via Copilot, accelerating investigation with the tools your teams use daily.



Deployment and Procurement

The Dragos Platform works within the Microsoft ecosystem, deploys on Azure, and is procured through Marketplace.

Azure SaaS Deployment

The Dragos Platform is available as a fully managed SaaS service on Microsoft Azure, alongside on-premises and hybrid deployment options. Align OT security to any infrastructure strategy. Available in Central US, Germany West Central, and Australia East.

Marketplace Procurement

Available on Azure Marketplace and eligible for Microsoft Azure Consumption Commitments (MACC). Purchases decrement against existing Azure commitments, streamlining how organizations procure and fund OT security.

BETTER TOGETHER

Faster Detection and Response

OT threat detections inside Sentinel reduce mean time to detect and respond across IT and OT environments, giving teams a unified view in a single SOC workflow.

Deployment Flexibility

Run the Dragos Platform as SaaS on Azure, on-premises, or hybrid. Align deployment to your infrastructure strategy and governance requirements.

AI-Assisted OT Investigation

Through the Dragos MCP Server, analysts can query Platform data in natural language via Copilot for Security, accelerating investigation with the tools your teams use daily.

Procure Through Microsoft

MACC-eligible and available on Azure Marketplace. Procure Dragos through the existing Microsoft commercial relationship your organization already has in place.

dragos.com/partners/Microsoft

