Cynalytica and Dragos Public Sector Integrate Platforms to Deliver Full-Spectrum OT Visibility

Cynalytica and Dragos Public Sector Integrate Platforms to Deliver Full-Spectrum OT Visibility Across Serial, Analog, and IP Industrial Communications

SAN LUIS OBISPO, CA, UNITED STATES, September 17, 2026 / EINPresswire.com/ -- Cynalytica and Dragos Public Sector Integrate Platforms to Deliver Full-Spectrum OT Visibility Across Serial, Analog, and IP Industrial Communications

Integration combines Cynalytica's non-IP protocol-agnostic monitoring with Dragos's IP-based OT threat detection, enabling correlated visibility from Level 0/1 field devices through the IP network layer.

Cynalytica Inc. today announced its partnership and technical integration between its OTNetGuard®, SerialGuard®, and AnalytICS Engine platforms and the Dragos Public Sector OT threat detection platform, extending unified monitoring across the full spectrum of industrial control system (ICS) communications, from legacy serial and analog field-level signals to modern IP-based OT networks.

> From a technical standpoint, this integration solves a correlation problem the industry has approached in pieces for years."
>
> *Richard Robinson, CEO Cynalytica*

The Technical Landscape

The Dragos Platform delivers asset visibility, vulnerability management, and threat detection across xOT environments through passive network monitoring and active collection, with deep packet inspection across 600+ industrial protocols, behavioral baselining, and detections correlated to known adversary TTPs via the MITRE ATT&CK for ICS

framework.

Water utilities, electric distribution and transmission operators, and other critical infrastructure owners who wish to establish visibility down to the layer where legacy RTUs, protective relays, and field controllers execute the physical commands that operate pumps, breakers, and valves, require additional monitoring of serial or analog field communications.

Integration Architecture
- Cynalytica OTNetGuard® passively monitors IP-based industrial network traffic and correlates it with non-IP communications, feeding normalized asset and communications data into the shared visibility layer and provides out-of-band, non-intrusive monitoring of serial (RS-232/RS-485/RS-422) and analog (current loop, voltage-based) communications at the field device level, extracting protocol-specific telemetry (e.g., Modbus RTU, DNP3 serial, proprietary vendor protocols) without introducing latency or risk to operational control loops.
- Cynalytica AnalytICS Engine applies behavioral analytics and anomaly detection across non-IP data streams, generating a unified asset inventory and communications baseline.
- Dragos Platform ingests correlated Cynalytica telemetry alongside its native IP network monitoring, applying Dragos's OT-specific threat detection, vulnerability management, and playbook-driven response capabilities across the combined dataset.

The result is a single pane of visibility spanning Level 0 through Level 3 of the Purdue Model, correlating serial/analog field-level activity with IP network behavior and enabling detection scenarios that neither platform achieves independently, such as identifying a field-level command injection on a serial RTU link that correlates with anomalous IP-side reconnaissance activity elsewhere on the network.

Deployment Model
Both platforms operate out-of-band, requiring no changes to existing control system configurations, no active polling of field devices, and no introduction of new network paths into operational environments. This preserves the fail-safe operational posture required in water and electric utility environments, where availability and process integrity take precedence over conventional IT security practices.

Technical Benefits:
- Cross-Protocol Correlation — Unified analysis across serial, analog, and IP protocols surfaces attack patterns spanning multiple communication layers
- Level 0/1 Field Device Visibility — Extends monitoring to RTUs, PLCs, IEDs, sensors, and actuators alongside Dragos's native IP-based detection
- Zero Operational Impact — Passive, non-intrusive monitoring architecture introduces no latency, polling, or risk to control processes
- Unified Asset Inventory — Combines IP and non-IP asset data into a single, deduplicated inventory, eliminating the blind spots created by maintaining separate, disconnected monitoring tools

• Extended Detection Coverage — Behavioral baseline and anomaly detection on serial/analog protocols complement Dragos's IP-based threat detection logic, enabling faster identification of cross-layer attack chains
• Protocol-Native Parsing — Native support for Modbus RTU, DNP3 serial, and proprietary field protocols ensures accurate telemetry extraction without relying on IP-centric assumptions
• Standards Alignment — Supports compliance reporting aligned with NERC CIP, AWWA, and other sector-specific frameworks by documenting visibility across the full Purdue Model stack

Executive Perspective
"From a technical standpoint, this integration solves a correlation problem the industry has approached in pieces for years. Dragos correlates threats extremely effectively within the IP domain, our platforms extend that same rigor to the serial and analog layer, so a single anomaly signature can be traced from a field controller all the way up through the network stack," said Richard Robinson, Chief Executive Officer of Cynalytica.

"Government and critical infrastructure operators with complex, multi-generation control system architectures can now bring serial and analog field-level communications into the same detection environment as their IP infrastructure," said Dan Dorchinsky, General Manager of Dragos Public Sector LLC. "The Dragos Platform ingests Cynalytica's telemetry alongside its native OT monitoring, so analysts work from a single, correlated dataset. That extends Dragos threat detection and intelligence across the full communications environment these operators run, including legacy field-level systems alongside modern IP infrastructure."
Availability
The integrated Cynalytica–Dragos solution is available now for deployment by water utilities, electric operators, and government critical infrastructure customers.

About Cynalytica Inc. Cynalytica Inc. delivers cybersecurity and operational intelligence solutions purpose-built for legacy and modern ICS/SCADA environments, providing visibility into serial, analog, and IP industrial communications to protect critical infrastructure.

About Dragos Public Sector LLC Dragos Public Sector LLC is a subsidiary of Dragos Inc., the global technology leader in cybersecurity for industrial and operational technology environments, dedicated to safeguarding civilization from those seeking to disrupt the industrial infrastructure that people rely on every hour of every day.

Media Contact: Jessica Ohnona · Cynalytica Inc.

Jessica Ohnona
Cynalytica Inc.
email us here
Visit us on social media:
LinkedIn
YouTube

This press release can be viewed online at: https://www.einpresswire.com/article/942604557

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.