SOLUTION BRIEF

Integrated Cybersecurity Technology from Dragos and AWS

Secure and Manage Industrial Control Systems (ICS) Cyber Risk in the Cloud

HIGHLIGHTS

- Protect your industrial assets and simplify regulatory compliance to help secure your business transformation.
- Remotely monitor and manage your Dragos Platform deployment with AWS Cloud-hosted CentralStore and SiteStore.
- Provide comprehensive visibility of ICS/OT assets and threats, threat behavior analytics, and investigation playbooks with best-practice guidance.
- Rapidly pinpoint malicious behavior on ICS/OT networks, providing in-depth context of alerts and reducing false positives for unparalleled threat detection.
- Leverage comprehensive ICS/OT vulnerability management with corrected, enriched, and prioritized guidance.
- Enable collective defense and community-wide visibility solution through Neighborhood Keeper, allowing you to share threat intelligence and collaborate at machine-speed.

With the increase in connectivity and accessibility required to improve operational efficiency, industrial organizations must manage cybersecurity risks to their industrial control systems (ICS) and operational technology (OT). Together, Dragos and AWS strengthen your organization's defensive capabilities by offering comprehensive ICS/OT cybersecurity technology to detect threats to your core business and securely accelerate digital transformation.

THE CHALLENGE

As organizations move to modernize and digitally transform their OT environments, cybersecurity is key to ensure these environments are protected from growing cyber threats and in compliance with

industry regulations. Security teams at industrial organizations across the electric utility, oil and gas, and manufacturing industries are being tasked with assessing cyber risks to their environments and adhering to audit and compliance programs.

With an increase in ICS/OT connectivity and accessibility to improve operational efficiency, organizations must manage the cybersecurity risks to their ICS and OT environments, amidst an expanding attack surface, to ensure secure and reliable operations, stakeholder alignment, and effective cyber risk management.

THE SOLUTION

To address these challenges and secure OT environments, stakeholders from both IT and OT teams must work together to architect layered cybersecurity measures that provide defense-in-depth, including asset visibility, threat detection, and prevention technologies – ultimately enabling IT and OT professionals to improve facility operations while maintaining the availability of the network and protecting plant processes.

The Dragos Platform, powered by AWS, is the most trusted industrial control systems (ICS) cybersecurity technology, and provides comprehensive visibility of your ICS/OT assets, built to analyze multiple data sources including protocols, network traffic, data historians, host logs, asset characterizations, and anomalies. Establishing comprehensive ICS/OT vulnerability management with corrected and enriched risk scores, and prioritized guidance that enables customers to manage the full lifecycle of specific vulnerabilities in their environment. The Dragos Platform provides the industry's most accurate threat detection to rapidly pinpoint malicious behavior on your ICS/OT network, with in-depth context of alerts, while reducing false positives for unparalleled threat detection.

Dragos Neighborhood Keeper, powered by AWS, strengthens your cybersecurity posture by providing insight into the prevalence of real-world threats. Companies benefit from a collective defense and community-wide visibility solution that provides a more effective industrial cyber defense by sharing threat intelligence at machine-speed across industries and geographic regions. This collective defense solution servicing the ICS community allows participants to request and offer assistance and collaborate with trusted program partners.

HOW IT WORKS

Together, Dragos and AWS provide users the flexibility and scalability of a cloud option to defend OT environments combining on-prem Dragos Sensors with cloud-hosted Dragos Platform components for remote management and monitoring.

Figure 1 shows a high-level deployment of the Dragos Platform, based on the Purdue Model architecture. In this scenario, the Dragos Platform cloud-hosted SiteStore, CentralStore, and Neighborhood Keeper provides defenders with unprecedented knowledge and understanding of their industrial assets and activity, potential threats, and provides the information and tools to respond.

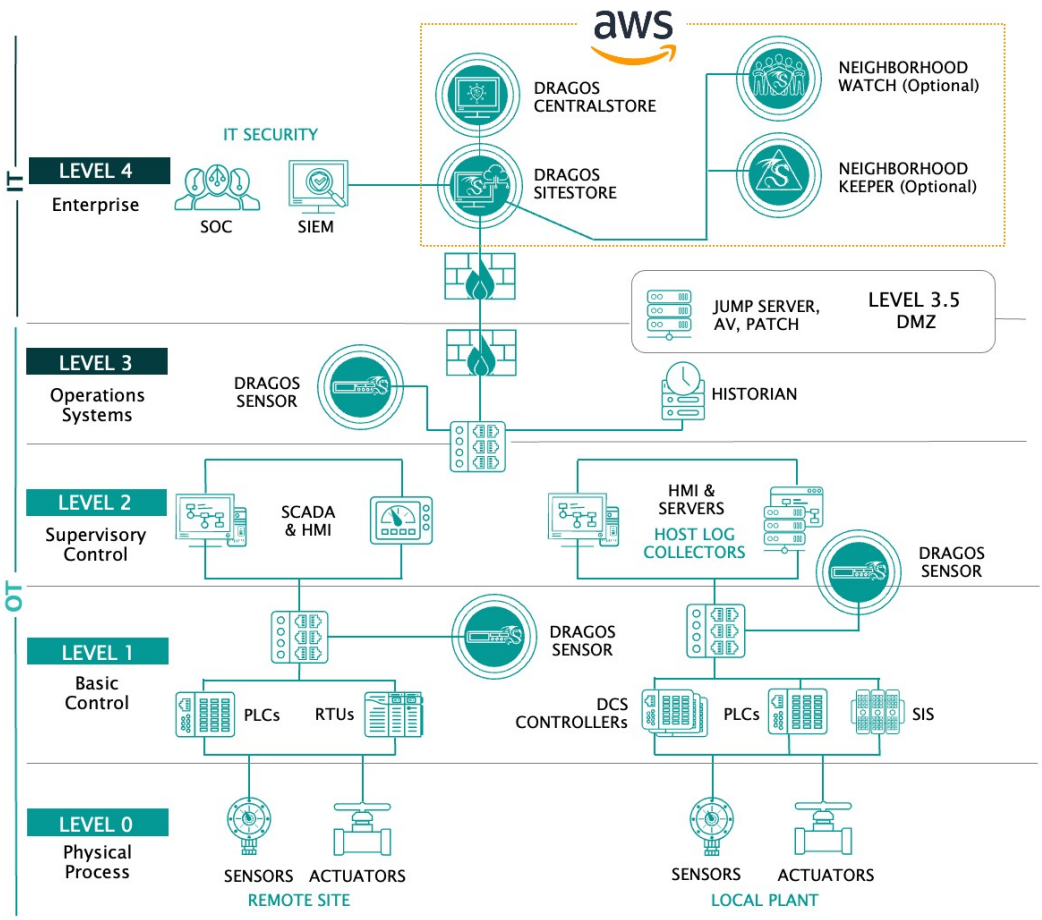


Figure 1. The Dragos Platform, powered by AWS, deployment architecture representation based on the Purdue Model

USE CASE: Improved Asset Visibility with Remote Central Management

One of the fundamental challenges industrial asset owners face is having a complete and accurate inventory of their connected devices. Industrial companies inherently understand that the equipment operating in their environments is critical to the success of their business. Unfortunately, over time the complexity of these environments increases, inventories change, technology ages, systems drift out of compliance with configuration standards, new vulnerabilities are discovered, and the simple challenge of having full visibility into your environment so it can be properly secured becomes imperative.

With increased visibility, cybersecurity analysts can also encounter alert fatigue. Many anomaly-based threat detection methods are known to create high numbers of notifications with false positives on alert notifications, with little transparency and context into why the alerts occur. This additional time researching alerts burns cybersecurity resources, taking attention away from mitigating risk and minimizing downtime, which are priorities.

The Dragos Platform addresses this by building a continuously updated asset list by analyzing network traffic and capturing detailed asset information and communications. These assets can be grouped and managed by various properties based on asset attributes like “hardware vendor” or “firmware version” or configurable parameters like which zone the asset is associated with.

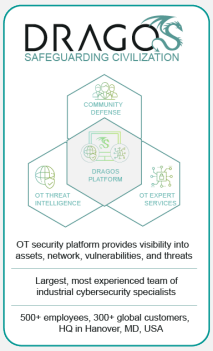
The Dragos Platform rapidly pinpoints malicious behavior on your ICS/OT network, providing in-depth alert context, and reducing false positives for unparalleled threat detection. In addition to threat detection, users are presented with prioritized vulnerability guidance with “Now, Next, Never,” giving defenders the information needed to focus on the highest priority issues requiring further investigation. These notifications trigger based on certain configurable conditions created in the Dragos rules engine, allowing administrators and analysts proper guidance for response actions.

The Dragos Platform, AWS Cloud-hosted CentralStore and SiteStore, provide remote central management and reporting console for distributed Dragos sensors.

ADVANTAGES OF THE INTEGRATED AWS AND DRAGOS SOLUTIONS INCLUDE:

- Securely accelerate digital transformation and take full advantage of the cloud with Dragos and AWS.
- Receive continuously updated detection and response content through the Dragos Platform’s intelligence-driven Knowledge Packs.
- Span the needs of analysts for both IT and OT networks for improved complete situational awareness and decision-making.
- Contribute to meeting a variety of industrial standards, regulations, and guidelines such as NERC CIP, ISA/IEC 62443, CFATS, ANSI/AWWA G430, GxP, IT-SIG 2.0, NIST2 Directive and others.

For more information, please visit dragos.com/partner/aws/ or contact us at info@dragos.com



About Dragos, Inc

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit dragos.com or connect with us at sales@dragos.com.

aws PARTNER Manufacturing and Industrial Competency