DRAGOS and WATERFALL SECURITY
A More Complete ICS Security Architecture

KEY BENEFITS

- Interoperability of the Dragos Industrial Cybersecurity Platform and Waterfall Unidirectional Security Gateways has been successfully tested and validated.
- Customers can deploy Dragos and Waterfall technologies together to create more secure cybersecurity architectures in ICS networks.
- The joint architecture guarantees safe, continuous monitoring of industrial networks for uninterrupted asset identification and threat detection.
- Dragos and Waterfall Security Solutions have extensive experience in ICS environments, with products, services and on-going research – to assist customers in securing their OT networks.

THE CHALLENGE

With the proliferation of Industrial IoT (IIoT), Industry 4.0, and cloud-based technologies for the purposes of enhanced automation and analysis of large volumes of data, operational technology (OT) managers are faced with the challenge of making industrial networks more accessible for legitimate business drivers without significantly increasing cybersecurity risks. This balance requires an architecture that provides for secure OT network perimeters with controlled data flow, as well as complete network visibility for effective threat detection and response. Some regulated industries are even required to have clearly defined perimeters that use only approved technologies for the transfer of information in/out of the protected network.

As a result, cybersecurity stakeholders are tasked with reducing upstream connections (attack surfaces) – which might compromise OT networks – while maintaining full visibility into those networks for a comprehensive approach to prevent, detect, and respond to threats.

SOLUTION OVERVIEW

Waterfall's Unidirectional Security Gateways provide physical protection of OT networks at OT network perimeters. The gateways enable seamless IT/OT integration, providing safe, enterprise-wide visibility into OT networks, with disciplined control.

The Dragos Industrial Cybersecurity Platform is a passive network monitoring tool that enables complete visibility into industrial control systems (ICS) networks. It allows users to visualize industrial assets and their communications, detect threats as they occur, and utilize prescriptive workbench tools for more efficient investigations and response, while avoiding operational impacts to existing security team's operations.

The combination of Waterfall Unidirectional Security Gateways and the Dragos Industrial Cybersecurity Platform enables safe monitoring of ICS / OT networks – providing a secure and effective approach to improved threat prevention, detection and response.

TECHNOLOGY

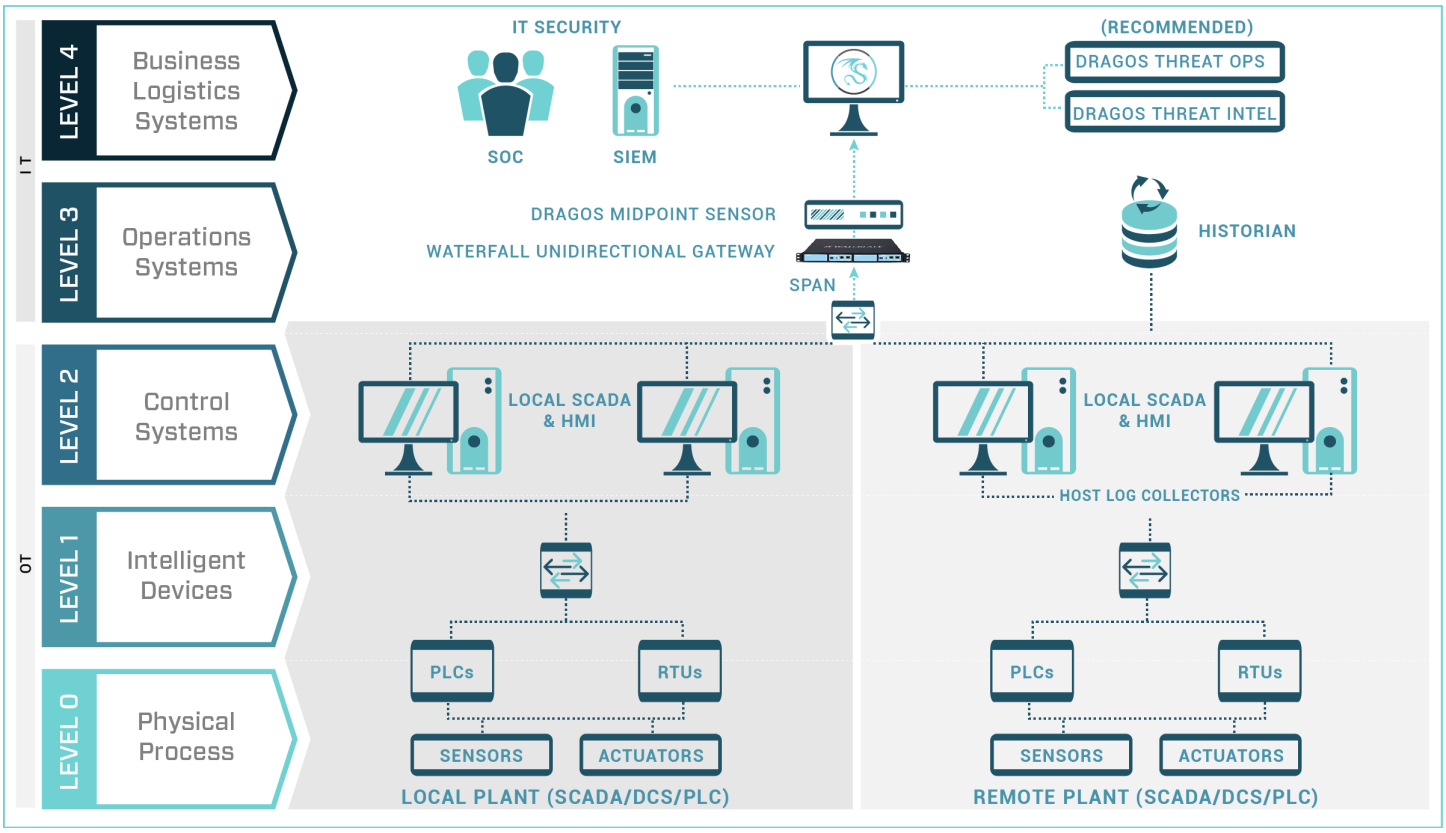
The Dragos Industrial Cybersecurity Platform consists of network appliances referred to as Sensors and a centralized server known as the SiteStore, which can be deployed on-premise or in an AWS cloud. The Dragos platform provides passive network monitoring with threat detection and response capabilities:

- **Asset Identification** – industrial assets communicating on the network are identified and characterized so analysts can visualize the complete operations environment.
- **Threat Detection** – by leveraging threat intelligence of known malicious activity, Dragos utilizes Threat Behavior Analytics to automatically provide notifications when known malicious behavior has been detected in the ICS network with appropriate context as to what the behavior means and what should be done.
- **Response** - Investigation Playbooks and query-able datasets guide analysts on the appropriate response path, leveraging all the network, host, and system data available, to help scale industrial-specific security knowledge across teams of diverse backgrounds.

Waterfall Unidirectional Security Gateways are a combination of hardware and software. Unidirectional Gateway hardware is physically able to send in only one direction, while the gateway software replicates servers and emulates devices. Unidirectional Gateways are routinely deployed to gather network packet captures, system logs, SNMP traps, historian data, OPC data and other security monitoring and operations intelligence from an industrial network. A Unidirectional Gateway transmits this information safely to a corporate network, where the information is used to populate replica industrial servers and emulate industrial devices such as ICS SPAN and mirror ports. Since the gateway is physically able to send information in only one direction, there is no possibility of IT-based or Internet-based attacks pivoting through IT-hosted equipment to put OT networks at risk. The gateway's replica servers and emulated devices make IT/OT integration straightforward – IT-resident equipment works normally and bi-directionally with the replicas.

The Dragos platform and Waterfall Unidirectional Security Gateways have been tested and validated for compatibility. This demonstrated unidirectional interoperability enables safe and continuous monitoring of industrial assets.

ARCHITECTURE



In the example architecture above, the core switch at the boundary of level 2 and 3 networks is configured to produce SPAN / Mirror traffic from the OT network for the purposes of security monitoring. A Waterfall Unidirectional Gateway is configured to gather packet captures from that port and transmit those captures unidirectionally to the IT network, where the gateway emulates the OT SPAN port to the Dragos sensor beyond the gateway perimeter. Spanning mode allows the Dragos sensor to monitor traffic from a protected OT network without the sensor being installed within the protected network – which is both more secure and generally a simple change to OT networks.

Please refer to the Interoperability Guide for more information.

BENEFITS and IMPACT

Benefits	Impact
Validated Interoperability	Industrial enterprises are assured that the Dragos Industrial Cybersecurity Platform will function properly in environments using Waterfall Unidirectional Security Gateway technology.
Secure Architecture	Industrial enterprises enjoy both in-depth security monitoring and strong OT perimeter protection to enable safe visibility into OT networks.
Complementary Technologies	Industrial enterprises can continuously monitor OT networks and production operations, while maintaining a layer of physical protection to prevent cyberattacks against OT networks.
Extensive Experience	The combined experience of Dragos and Waterfall Security in many different industrial environments across multiple industry verticals provides greater confidence to industrial security professionals focused on securing OT infrastructure.
Convenient Management	Dragos Sensors can be managed, updated and adjusted safely and easily beyond the perimeter on IT networks, without needing to be installed on OT networks.

For more information, please visit www.dragos.com or contact support at info@dragos.com