

ENHANCED SECURITY AND VISIBILITY AGAINST ICS/OT THREATS

Keysight Technology and Dragos Platform combine for ICS & OT cybersecurity

HIGHLIGHTS

- The utilization of Dragos and Keysight Technology provides enhanced visibility and security throughout your environment, regardless of network complexity.
- Minimizes risk due to unmanaged or legacy switches that would otherwise result in a lack of network visibility.
- Improved versatility of Dragos Platform deployments, regardless of environment limitations.
- Ability to consolidate desired traffic if managed switches are available, regardless of limited site or rack space.
- Easy utilization during Proof of Concepts, Pilot environments and training simulators, thus reducing risk.

OVERVIEW

Millions of industrial devices operate at energy, manufacturing, transportation, mining and other industrial sites. Comprehensive cybersecurity that focuses on asset visibility proves essential in reducing risk and improving the resiliency of industrial operations. Dragos and Keysight are working together to improve cybersecurity and operational reliability, while reducing integration efforts and costs.

THE CHALLENGE

Traditionally, operational technology (OT) networks were architected almost wholly separated from information technology (IT) networks. However, as industrial environments support digital transformation, they shift to a more interconnected architecture, enabling cyber threats to reach beyond the traditional IT assets. Thus, Cybersecurity teams are being challenged to secure and then manage networks that traverse their entire organization, requiring operational visibility to include the wide variety of OT and IT devices on their networks.

THE SOLUTION

The need for passive, real-time monitoring is more vital than ever in an ICS/OT environment saddled with legacy equipment. Having comprehensive visibility of the ICS/OT environment is both the tactical and strategic foundation of an effective cybersecurity

program. Organizations can leverage Keysight’s visibility solutions to feed data to the Dragos Platform to help streamline the security of the ICS/OT network infrastructures, while helping to avoid operational impacts in legacy systems. Keysight network TAP’s and Packet Brokers can be used to provide visibility into network segments that enables the Dragos Platform to passively observe network activity for the purposes of asset discovery and threat detection. The passive network TAPs are available in fiber and 10/100M/1000M copper models to support all legacy and modern architectures, yet will not add any latency or security risk to the environment. By tapping points of interest throughout the ICS/OT network, security and other monitoring solutions can receive 100% of the traffic to enhance their defense capabilities without introducing new or manipulated traffic to the production network streams. Organizations can centrally visualize the systems, devices, and interactive communications between them by utilizing the joint Keysight and Dragos solution. Additionally, they can continuously monitor and detect threats as they occur and use prescriptive workbench tools for more efficient investigations and responses. With this enhanced deep packet level of visibility across

critical infrastructures, defenders can more competently protect their operations from potential disruption caused by threats and anomalies while improving their safety, reliability, and cyber resilience across their unique network infrastructures.

HOW IT WORKS

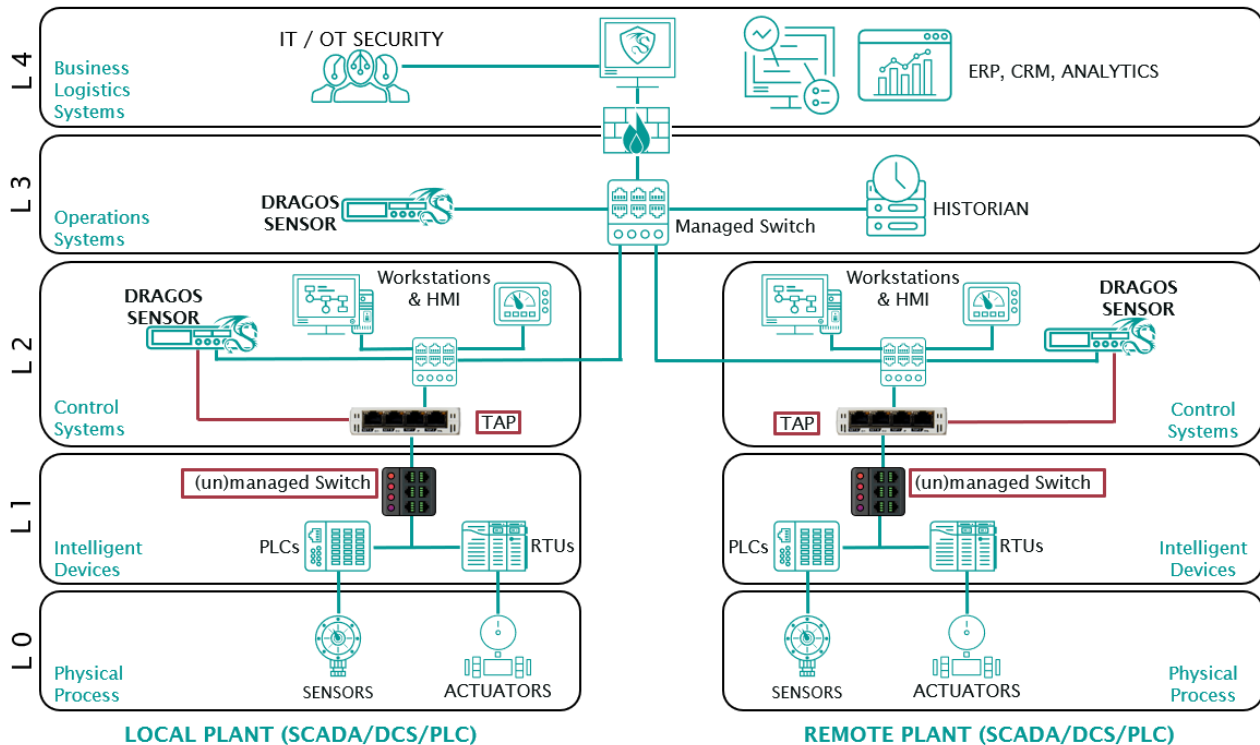
Keysight Technology copies packet data from OT networks, such that it can be made visible to monitoring technologies, which minimizes blindspots. Their network visibility solutions distribute multiple links from various locations into Dragos platform, such that Dragos Platform can accurately map out OT assets and vulnerabilities. The Dragos Platform then analyzes the traffic to create a network map and identify vulnerable devices, cyber threats, and operational anomalies on your network.

USE CASES

Network TAPs (test access points) and SPAN (switch port analyzer or port mirroring) are the two most common methods for network traffic access used for data monitoring and security analysis. There are significant differences that can affect the integrity of the network device, the traffic being analyzed, and the performance of network tools leveraging the data. The following discusses three different use cases where TAP versus SPAN options would be best leveraged in regard to monitoring the ICS/OT network.

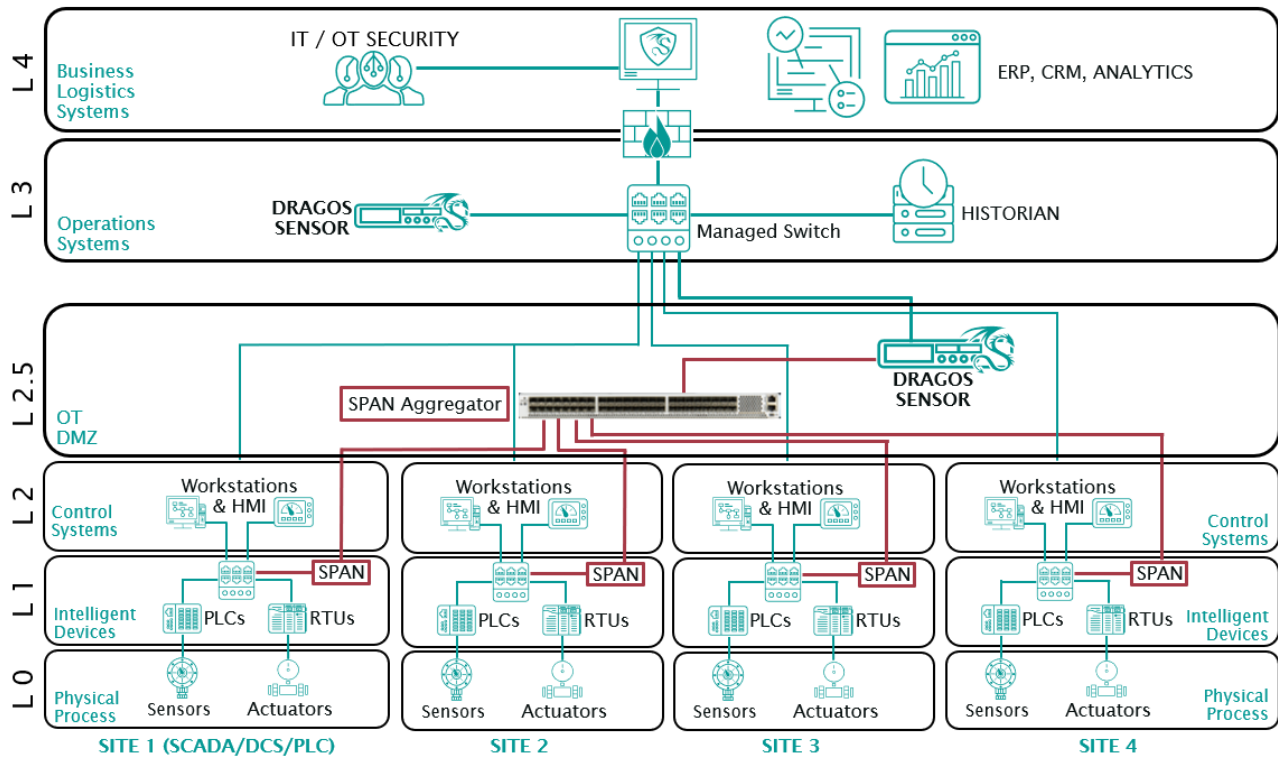
Use case - Legacy Architectures

Legacy ICS/OT networks were designed primarily with reliability and safety in mind, evolving business objectives have caused the underlying OT systems to keep pace over the past decade to support newer business requirements. When you start to push legacy equipment to transfer data outside of these proprietary systems, you open the industrial network to security vulnerabilities. The basic architecture below depicts a scenario where legacy networking devices are unmanaged switches (no SPAN option) or managed switches that lack the resources to support SPAN capabilities. Deploying Keysight TAPs designed to support 10M/100M/1G between the two network segments will provide the Dragos Platform with at least a baseline amount of data to provide asset inventory, vulnerability management, and threat detection in a single application, making your cybersecurity teams more effective.



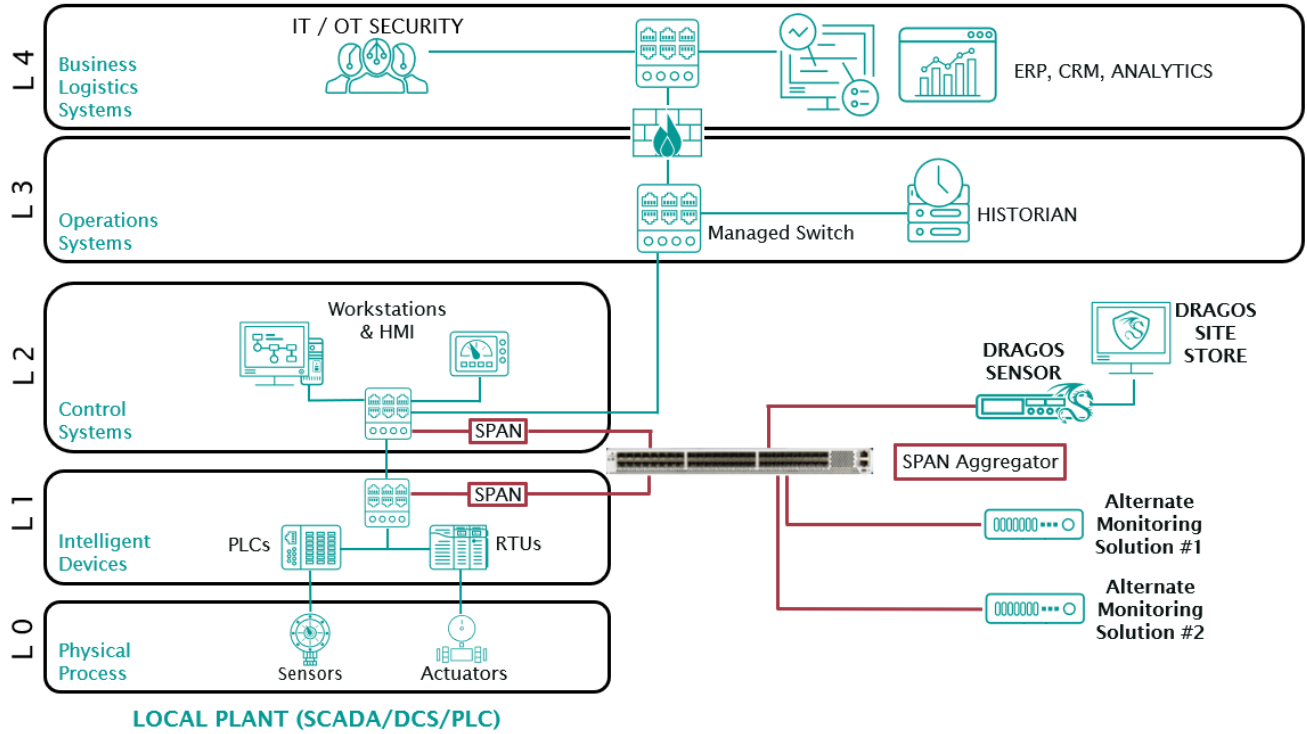
Use case – Distributed Networks

As ICS/OT environments get upgraded and modernized, the network switches include features that help support monitoring requirements. For example, port mirroring, also known as SPAN (Switch Port Analyzer), are designated ports on a switch programmed to send a copy of network packets seen on one or more ports to another port, where a monitoring solution can analyze the packets. The basic architecture below depicts a scenario where several site locations have SPAN capabilities, however the physical location cannot support additional hardware due to space, power, environmental, or budget constraints. Deploying Keysight's High-Density Aggregator Network TAPs will overcome these challenges while allowing multiple sites to consolidate their SPAN traffic to a single aggregator that will send the data to the Dragos Platform for a comprehensive asset inventory, vulnerability management, and threat detection view making your cybersecurity teams more effective.



Use case – Proof of Concept

With the changing cyber-threat landscape impacting how the management of ICS/OT environments occurs, the need for passive, real-time monitoring is more vital than ever, especially for infrastructures with an abundance of legacy equipment. As with any solution selection process, organizations must traverse through a series of requirements before making a final decision. To ensure that the comparison process for each solution is equal and addresses the essential goals, the basic architecture below depicts a scenario where a proof-of-concept, staging, pilot, or training simulator environment is set up. This environment provides managed switches that support SPAN and a replica of a production environment that mimics where the solution will ultimately monitor and protect. Deploying Keysight's High-Density Aggregator Network TAPs allows consolidation of the traffic on the two networks, then sending that data to the Dragos Platform and another monitoring solution simultaneously. This configuration provides a side-by-side comparison of how each solution handles asset inventory, vulnerability management, and threat detection with the same data.



ADVANTAGES OF THE JOINT KEYSIGHT AND DRAGOS SOLUTION INCLUDE:

- Minimized operational risk for legacy ICS/OT environments while supporting cybersecurity requirements.
- Enhanced visibility and security throughout your environment, regardless of network complexity.
- Maximized performance powered by packet-level visibility for ICS/OT communications.

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