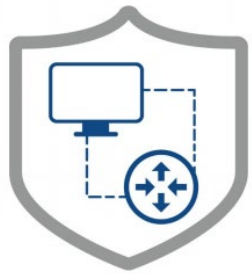
Industrial Control System (ICS) Network Monitoring



Enhanced cyber protection for critical infrastructures based on the Dragos purpose-built platform for the ICS environment

Overview

The cyber world is constantly changing. New threats and vulnerabilities that directly impact both operational technology (OT) and information technology (IT) are regularly emerging at an increasing rate.

Emerson's cybersecurity solutions, including the Power and Water Cybersecurity Suite with a broad portfolio of cybersecurity services, are designed to keep pace with this ever-changing environment. Our forward-looking and adaptable cybersecurity programs bridge the gap between OT and IT to mitigate risk and maintain reliable operation by proactively addressing threats, enhancing protection and streamlining security program management.

In 2019, Emerson and Dragos, Inc., developer of the Dragos Platform for industrial cybersecurity assets signed a global agreement to collaborate on cybersecurity solutions for the power and water industries. The agreement leverages the respective strengths of both companies to help customers more effectively detect and respond to cybersecurity threats. One result of the collaboration is integration of Dragos' threat detection technology into the Ovation™ automation platform and Power and Water Cybersecurity Suite.

This paper focuses specifically on passive monitoring of industrial control system (ICS) networks using a solution that delivers detailed information on the control network and pairs it with comprehensive tools that assist with threat detection and response.

Introduction

Emerson's cybersecurity solutions follow a defense-in-depth approach that helps safeguard people, assets and data from cyber threats. Incorporating data collected by the Dragos Platform into the Power and Water Cybersecurity Suite provides an additional layer of protection that complements Emerson's robust portfolio of security offerings for industrial control systems in the power and water industries.

The Dragos Platform is a flexible tool that can be deployed as a component of the Power and Water Cybersecurity Suite or as a standalone solution and can also be applied to both to Ovation and non-Ovation systems. The platform is comprised of three key components:

- **Dragos SiteStore** - Deployed on a server class machine or in the cloud, the SiteStore collects, stores and correlates ICS information provided by Dragos Sensors. A web-based interface visually presents identified assets and detected threats or malicious activity. Response playbooks are also included with the interface, providing step-by-step guidance on how to investigate incidents and respond accordingly.

- **Dragos Sensor -** Dragos Sensors collect data from the electronic security perimeter of the control system network and at other strategic locations within the ICS using mirrored switch ports. Network taps can be deployed if needed. The collected ICS data is sent to a centralized SiteStore for aggregation and correlation.
- **Data Accumulation Switch -** The data accumulation switch is a central point of connection for all passive monitor sessions. A switch is used when the number of monitoring sessions exceeds sensor limits.

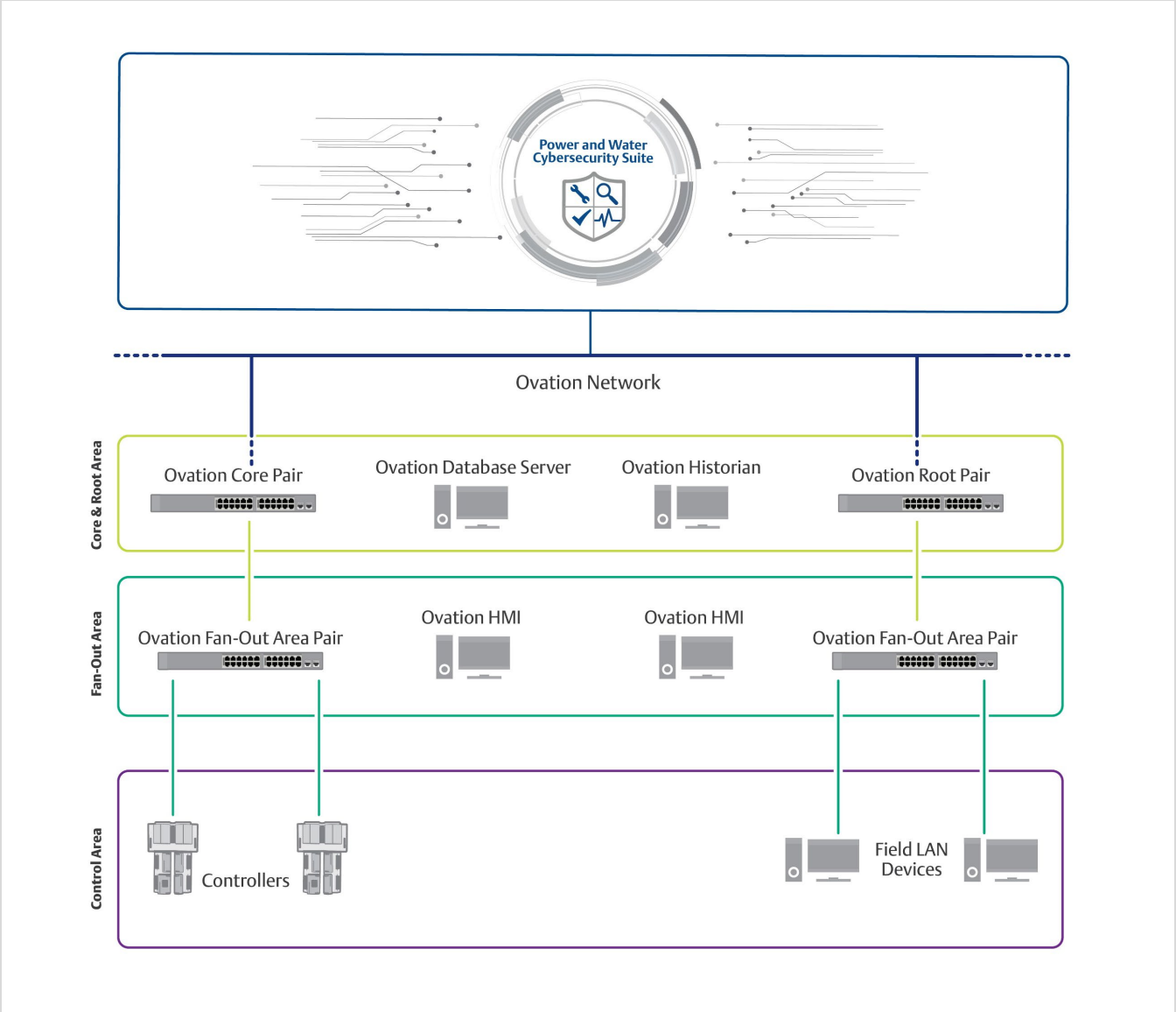
The cybersecurity philosophies of both Emerson and Dragos closely align with industry best practices and frameworks, such as the core functions identified in the National Institute of Standards and Technology (NIST) cybersecurity framework.

NIST Cybersecurity Framework Core Functions	Emerson Network Monitoring Solution using the Dragos Platform
Function & Purpose	**Feature & Benefit**
Identify - Develops an organizational understanding of managing cybersecurity risk to systems, people, assets, data and capabilities	Continuously **identifies and inventories network-connected devices** using asset-mapping for detecting changes, such as new or dropped assets, in real-time.
Protect - Outlines safeguards that supports the ability to limit or contain the impact of a potential cybersecurity event.	Uses behavioral analytics and threat hunting guidance to **help protect identified assets**. Our solution is tailored to the ICS network environment and is frequently updated as the threat landscape changes. The solution starts working immediately upon deployment without the need for tuning.
Detect - Defines activities for timely discovery of a cybersecurity event	Establishes a baseline for known network-connected devices and **performs protocol detection** to assist in anomalous device and communication detection.
Respond - Contains the impact of a potential cybersecurity incident by taking appropriate action	Provides a codified playbook that **guides users on incident response** using best practices and case management software that facilitates incident tracking and reporting.
Recover - Supports timely recovery to normal operations via plans that restore capabilities or services impaired by a cybersecurity incident	Tracks device, protocol and communication patterns that **assist with determining recovery priorities**. A dashboard provides a high-level visual identification of system-level health and status.

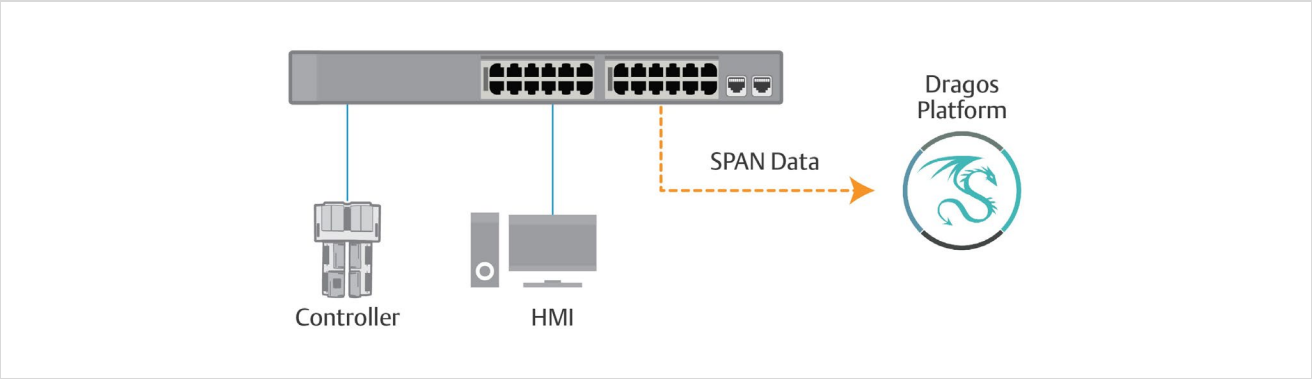
Deployment Method

Data Collection

The ICS network infrastructure is segregated into explicit layers. All Ovation networks, whether a small Local Area Network (LAN) or a larger Wide Area Network (WAN), follow a similar structure. The figure below details the types of devices located in each area. For maximum visibility into asset inventory and comprehensive data analysis, Emerson recommends deploying the Dragos Platform at all network layers.

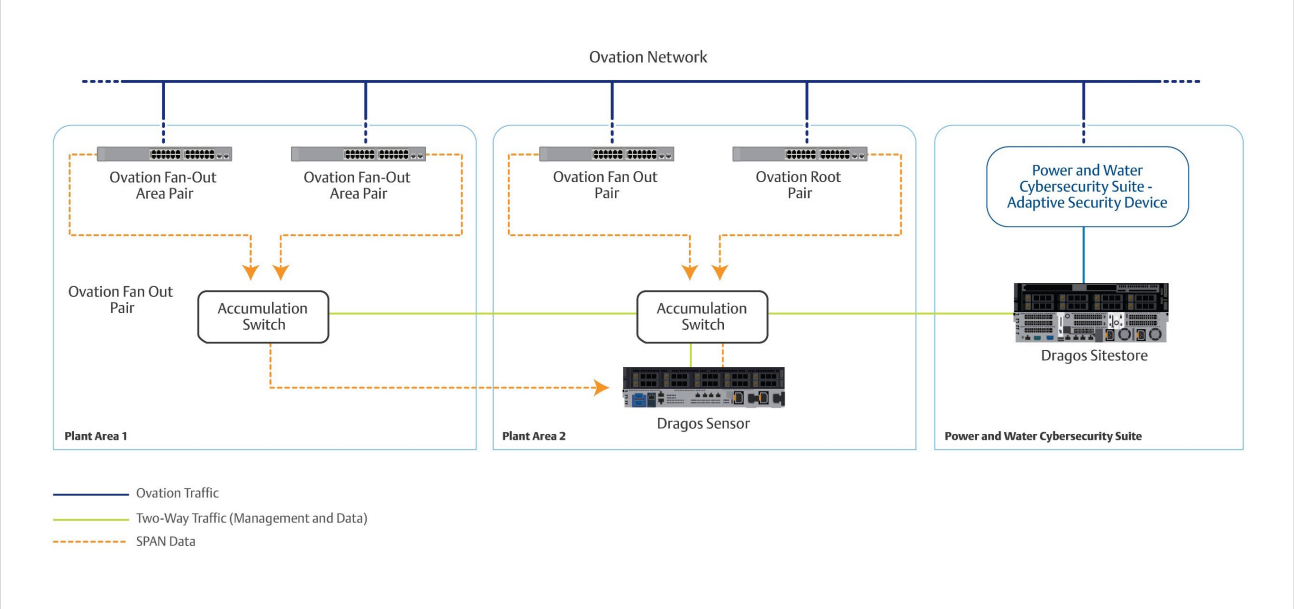


Emerson uses Cisco Switch Port Analyzer (SPAN) unidirectional port mirroring technology for collecting and storing network traffic data on the Dragos Platform. Each network switch is configured with one SPAN port that forwards all communication transmitted and received by the assets connected to that switch to the Dragos Sensor.



Network Architecture

The Dragos Platform passively monitors all Ovation and non-Ovation ICS network traffic with minimal impact. One or more Dragos Sensors and data accumulation switches are strategically placed within the ICS environment to maximize data collection.

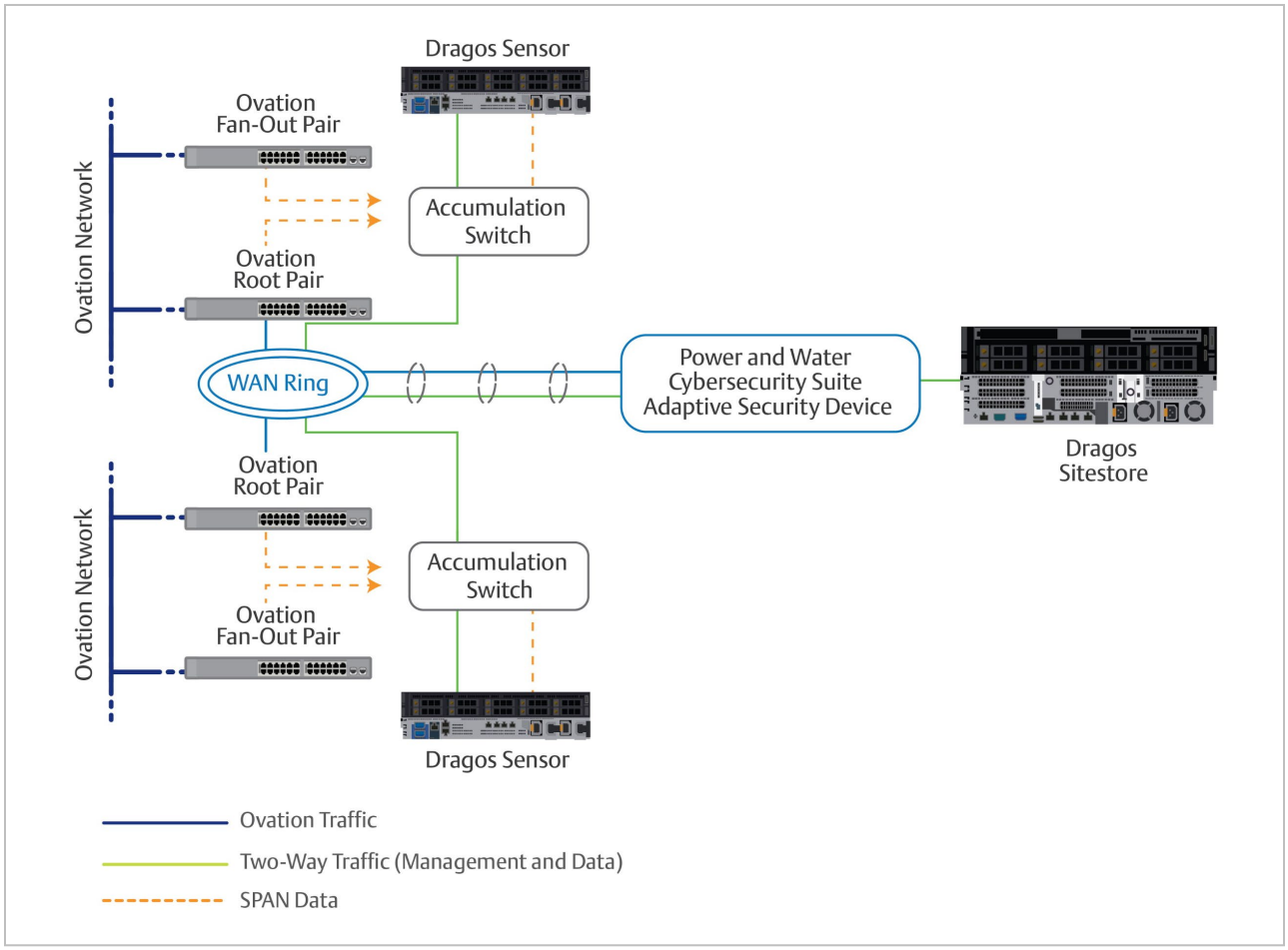


All collected SPAN data is sent to the Dragos Sensor with direct connections from either an ICS network switch or a data accumulation switch. The current Emerson offering for the Dragos Sensor has four collection interfaces for SPAN traffic[1], which can accommodate connections from up to four data accumulation switches or four SPAN connections from ICS network switches.

At a minimum, Emerson recommends following a few best practice guidelines when choosing monitoring points:

- Monitor all points of ICS network ingress (traffic entering the network from a remote server or over the Internet) and egress (traffic originated inside the network that is sent to an external network)
- Monitor both devices in a redundant pair
- Monitor at remote fan-out areas

Emerson's network monitoring architecture can be adapted based on network sizes and can easily accommodate network expansion. For large WAN networks, each WAN area uses the same basic architecture and existing network infrastructure to route data collected by Dragos Sensors to the SiteStore.



[1] Only applies to the Dragos enterprise sensor

Specifications

Hardware Specifications

The following Dragos components are required to implement a validated Emerson network monitoring solution:

Dragos SiteStore

- Option 1 – Deployed as part of the Power and Water Cybersecurity Suite virtual host
- Option 2 – Deployed as a standalone solution
  - 48 CPU / 126 GB RAM
  - 6x 4TB SSD HD
  - 4 - 1Gbps management ports

Dragos Midpoint Sensors

- Rack-mount, 1U server
- 4 – 1Gbps SPAN data ports

Data Accumulation Switches

- Cisco 2960x
- 24 – 1Gbps Ethernet ports
- 2 – SFP compatible ports

If deploying in a non-Ovation network, the non-Ovation system switches should be SPAN capable.

Note: Additional hardware options are available on an as needed basis to fit specific deployment scenarios.