



CASE STUDY

Middle Eastern Oil & Gas Company

OT Cyber Asset and Security
Event Management



INDUSTRIALDEFENDER.COM



COMPANY PROFILE

This Industrial Defender customer delivers 2 billion standard cubic feet of natural gas every single day, providing a source of clean energy. They manage the production and processing of natural gas, as well as the transportation of the gas by pipeline. The company's OT/ICS and IT infrastructure is complex, with many systems, sub-systems, and components supplied by multiple vendors, and has evolved substantially since its inception over 20 years ago. With an initial investment of \$7 billion, the company has continued to modernize and expand their cybersecurity program.

THE SITUATION

Increased global connectivity and the significant increase in the number of sophisticated cyberthreats targeting industrial control systems (ICS) drove the company's leadership to identify new risks and develop solutions to enhance cyber resilience and reduce risk to their ICS environments.

CUSTOMER REQUIREMENTS

- ◆ Hybrid asset data collection (agent, agentless, and network traffic analysis)
- ◆ Asset baselining and snapshot of the current security state (patches, signatures, compliance, etc.)
- ◆ Comprehensive asset management (auto-discovery, device inventory, software inventory, topology view, logical ports, and approved services)
- ◆ Configuration change management (baseline management and change detection)
- ◆ Events and alerts (centralized collection and consolidation, logical and correlation rules)
- ◆ Compliance with best practice standards and regulatory guidelines
- ◆ Integration with SIEMs and log managers
- ◆ Monitor all aspects of endpoints at all Purdue levels (from 4 to 1)
- ◆ Patch management
- ◆ Vendor-agnostic
- ◆ Zero downtime during deployment

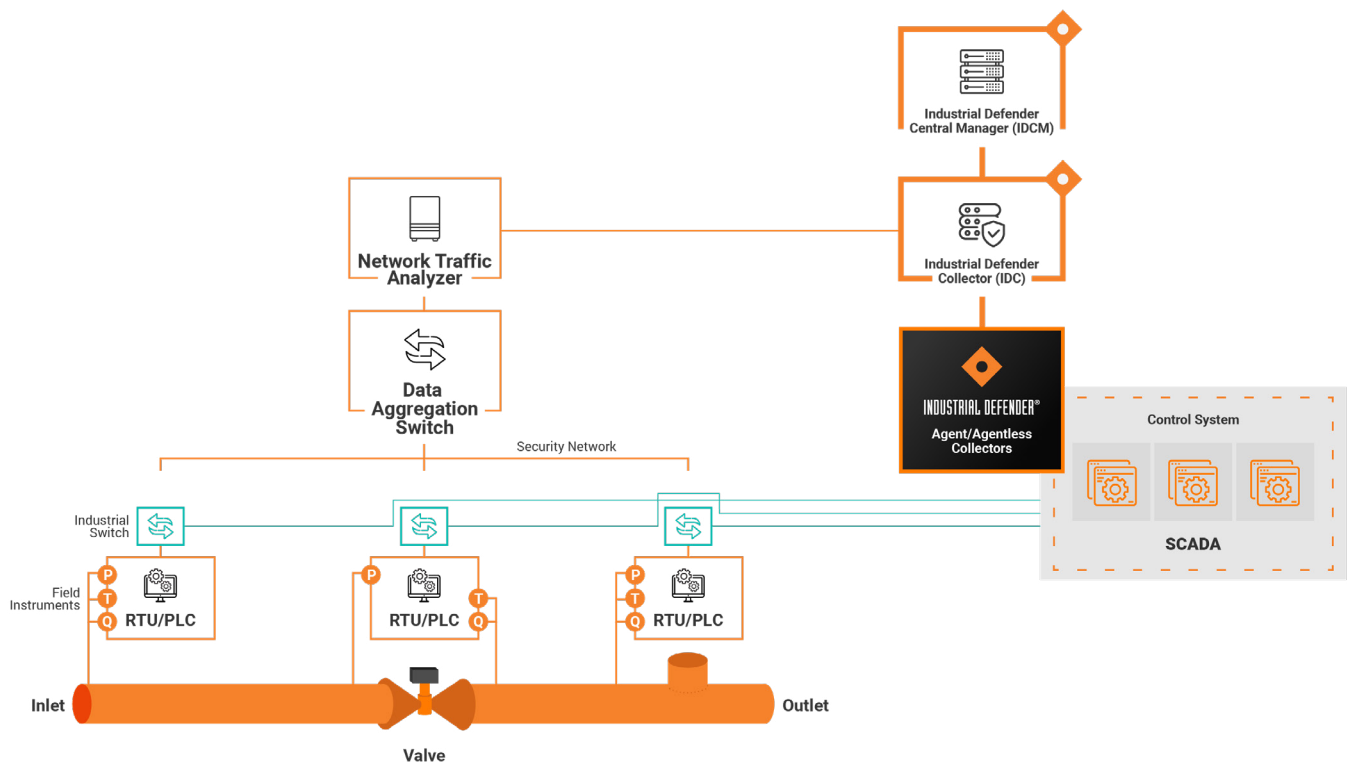
“The company's OT/ICS and IT infrastructure is complex, with many systems, sub-systems, and components supplied by multiple vendors.”

THE SOLUTION: INDUSTRIAL DEFENDER

The company implemented the Industrial Defender platform which provides them with a single comprehensive solution to meet their needs for cyber resilience. The ID system collects data from the endpoint devices as well as from the process control network traffic. This data is then processed to provide the company with events, alerts and reports that provide actionable intelligence for threat detection and protective cybersecurity measures.

The Industrial Defender system manages and monitors:

- Endpoints (servers, workstations, and network equipment)
- IT/OT networks
- Control system data centers for the upstream, midstream, and downstream processes
- Safety information systems
- Physical security systems



THE RESULTS

◆ Asset Management

- A detailed hardware and software inventory is maintained, including versions, vulnerabilities and patches from each endpoint.
- The configuration information collected from endpoints includes ports and services, interfaces, software installed, audit settings, and firewall rules, which is used to harden the environment and apply the concept of least functionality.
- Changes to configuration states are identified for use in configuration change control/management.
- The NetFlow feature visualizes communication patterns to help identify abnormalities.

◆ Access Control and Personnel Security

- The firewalls that segregate the process control networks are monitored for rule changes.
- Firewall rules on all endpoint devices are monitored for changes.
- User accounts are extracted into an easy-to-audit list from all endpoints, with privilege levels and credentials available for examination.
- Use of removable media is monitored.

◆ Cybersecurity Controls, Monitoring, Response, and Reporting

- Security-related and device performance data from all endpoints are captured and normalized.
- Malware detection events are captured from Anti-Virus application logs.
- Network traffic is analyzed using deep-packet inspection and signature-based patterns.
- Event streams are processed with logic and correlation rules, applying thresholds, volume counts, etc. to identify issues and assign priorities of significance.
- Specific events of significance trigger email notifications to process control engineers and cybersecurity analysts.
- Periodic reports are automatically delivered as subscriptions.

“Industrial Defender’s detailed compliance reports are absolutely music to my ears and make my day.”

-CISO

◆ Compliance

- Categorical summary reports are available out-of-the box that align with best practice standards and regulatory guidelines.
- The ID policy functionality is used to find settings, software inventory, configuration data, firewall rules, and/or user accounts that are not in compliance with corporate policies.

◆ Professional Services

- Industrial Defender continues to provide professional services and external consultation onsite and remotely to maintain, upgrade, tune and optimize the ID system, as well as consult on security best practices.

THE INDUSTRIAL DEFENDER DIFFERENCE

Since 2006, Industrial Defender has been solving the challenge of safely collecting, monitoring, and managing OT asset data at scale, while providing cross-functional teams with a unified view of security. Their specialized solution is tailored to complex industrial control system environments by engineers with decades of hands-on OT experience. Easy integrations into the broader security and enterprise ecosystem empower IT teams with the same visibility, access, and situational awareness that they're accustomed to on corporate networks. Learn more at www.industrialdefender.com.

Planning an OT Security Project?

[SCHEDULE A DEMO](#)

FOR MORE INFORMATION

1 (877) 943-3363 • (617) 675-4206 • info@industrialdefender.com

225 Foxborough Blvd, Foxborough, MA 02035

industrialdefender.com