



CASE STUDY

Petrochemical Industry

Ensuring Safety and Uptime
with Secure Process Control
Networks



[INDUSTRIALDEFENDER.COM](https://www.industrialdefender.com)



COMPANY PROFILE

Our customer, a major U.S.-based petrochemical company with more than \$13 billion in revenue, operates more than 30 chemical plants in the United States and around the world and is a major producer of olefins, polyolefins and specialty chemicals from natural gas and other petroleum components. It also serves the oil industry with a variety of oilfield fluids to improve productivity of new wells and restore old ones. It relies heavily on Microsoft products and a heterogeneous mix of distributed control systems (DCS) that manage its global operations.

THE SITUATION

The industrial control systems for production facilities in eight countries from North America to Asia were being managed locally at each site, with no standardized components or corporate view. Reporting on the security status of these systems relied heavily on manual processes and was often unreliable. In the face of increasing cyber risks to industrial control systems, a standardized way to manage these critical systems was needed.

Safety is a core value in the petrochemical industry. Because the essence of safety in industrial processes is stability, cybersecurity is now critical to safety. Coming from the IT side of the business, the ICS security manager understood they needed a solution to address the challenges of both IT security and operational technology (OT) safety.

Customer Requirements

- Provide a standardized view across an existing heterogeneous control environment spanning a variety of DCS vendors, including Yokogawa, ABB, Honeywell, Schneider, Emerson, Rockwell and others.
- Achieve an real-time view of the status and configuration of networks and servers, as well as automate change management, to quickly identify and mitigate threats.
- Enable rapid, coordinated response to security incidents when an issue is identified.
- Protect networks and servers in industrial and process control systems without compromising the stability and uptime critical in OT environments.
- Implement a solution that could address possible future regulations.

“The most important result is that it hasn’t caused any problems within the environment. That is a big deal.”

THE SOLUTION: INDUSTRIAL DEFENDER

Many solutions were evaluated, including Microsoft’s Client Configuration Manager. However, Microsoft’s lack of experience in the OT environment ultimately led them to choose Industrial Defender. Our integrated solution delivers security, compliance and change management across their heterogeneous environment consisting of a broad range of endpoints.

The company began with an installation of Industrial Defender at a single facility that lasted for six months, and brought in both IT and process automation teams to participate in the review. One key result was that the solution was deployed without the need for downtime and without incident in the process environment.

It also provided the visibility needed across tools from multiple vendors. Following the initial success, they decided to roll out Industrial Defender at all U.S. facilities, which took about six months. Implementation began with agentless monitoring, to minimize the manpower needed and the impact on local equipment. Later, agents were used to provide more detailed information and reduce bandwidth needs.

Goals	Results
• Provide a standardized, real-time view across a heterogeneous control environment • Enable rapid response to security incidents • Protect control systems without compromising stability in critical operational networks • Prepare for compliance with emerging oil and gas industry safety regulations	• More effective patch and configuration management while maintaining uptime on critical operational systems • A unified view of network and server configurations. • Flexible reporting dashboards for future compliance requirements

THE RESULT: RAPID DEPLOYMENT, IMMEDIATE VALUE AND VISIBILITY

After full implementation, the company had a unified view of the configuration of networks and servers in the OT environment, both at the site level and centrally. Immediately the customer was able to identify several network and server configuration issues. For the first time, security managers are able to log in to remote locations on a site-by-site basis and get a standardized view of conditions.

As part of a three year project bridging IT and OT asset owners, the implementation of Industrial Defender was swift and efficient. Seven sites were deployed in 9 months on a range of DCS platforms from Yokogawa, ABB, Honeywell, Schneider, Emerson, and Rockwell. The customer also noted that the project helped to advance collaboration between IT and OT staff.

After more than a year with Industrial Defender in operation, the security team is pleased to report that no significant security incident has occurred. The team uses Industrial Defender proactively to ensure that systems are up-to-date and running with the visibility needed to minimize the risk of a security-related disruption. The customer is highly satisfied with the solution and plans to expand to 10 sites.

“The Industrial Defender team had on-site techs who understood OT and IT, enabling rapid deployment at 7 sites.”

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. They secure some of the largest critical control system deployments with vendors such as GE, Honeywell, ABB, Siemens, Schneider Electric, Yokogawa and others to protect the availability and safety of these systems, simplify standards and regulatory requirements, and unite OT and IT teams.

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

© 2020 Industrial Defender. All Rights Reserved.