INDUSTRIAL DEFENDER®



CASE STUDY

US Plastics Manufacturer

Improved Cybersecurity Defenses & Corporate Compliance Monitoring

INDUSTRIALDEFENDER.COM

COMPANY PROFILE

This Industrial Defender customer is a manufacturer and supplier of petrochemicals, polymers and fabricated building products, which are fundamental to various consumer and industrial markets. This company is integrated through the value chain of plastics, with an annual revenue exceeding $7 billion and over 10,000 employees operating around the world.

THE SITUATION

Because the company's operations are subject to significant hazards and risks inherent in ethylene production operations, a successful cybersecurity attack could have grave consequences. The company's leadership was tasked with securing their systems against cyberthreats to protect the health and safety of workers and the environment around them, while also avoiding business disruptions.

The OT infrastructure inside their manufacturing facilities is large-scale and complex environment, so they were facing a substantial challenge. Their process control systems consist of many sub-systems and devices from various vendors including:

- ABB
- Honeywell
- Emerson
- Schneider Electric
- OSIsoft

"Because the company's operations are subject to significant hazards and risks inherent in ethylene production operations, a successful cybersecurity attack could have grave consequences."

CUSTOMER REQUIREMENTS

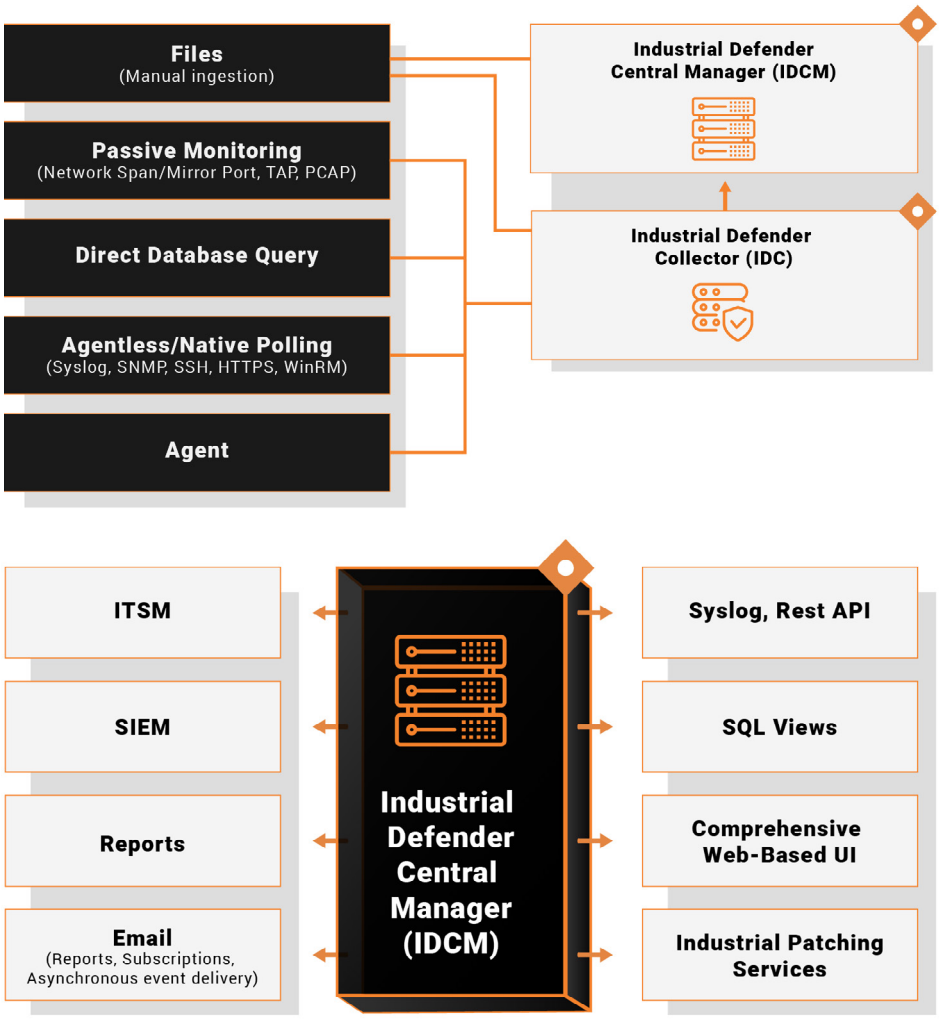
The company needed a comprehensive, straightforward solution that would:

- Manage asset inventory, monitor network and endpoint security, administer firewall configurations, detect intrusions, and implement access control
- Deliver data on attempted security breaches, then mitigate security weaknesses and vulnerabilities
- Facilitate internal security audits, risk assessments and in-depth root cause analysis
- Couple system performance monitoring for maintenance cost avoidance, along with enhanced cybersecurity resilience
- Enable the use of best practice industry guidelines, including the NIST CSF and CFATS guidelines
- Deliver an efficient solution to achieve a low cost of ownership

THE SOLUTION: INDUSTRIAL DEFENDER

The company has successfully used the Industrial Defender platform for 10+ years. This single, robust solution meets their needs for both OT/ICS cyber resilience and monitoring their process control system computing resources. By collecting and normalizing data from endpoint devices, as well as process control network traffic, the platform provides the company with actionable events and alerts that support their OT cyber resilience goals.

The leadership team did not need to hire dedicated cybersecurity personnel to manage the ID platform and are using process control engineers and specialists to monitor their OT/ICS infrastructure for both cybersecurity and performance issues.



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.

Examples of Issues Detected by Industrial Defender	
☑	**Excessive or abnormal authentication/login attempts**
☑	**“Guest” user ID (pass-through) enabled on firewalls**
☑	**Excessive and abnormal deny/drop traffic from firewalls**
☑	**Vital systems not backed up**
☑	**Performance and stability problems**

Audit

- 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

© 2022 iDefender, LLC

INDUSTRIAL DEFENDER®