Microsoft Security

# One of world's largest oilfield services provider secures their OT and ICS with Microsoft Defender for IoT

## Security incident drives the push for greater IT/OT asset visibility

A Fortune 500 company, one of the world's largest field services companies, began hardening their industrial infrastructure while in the midst of a digital transformation initiative and after a previous security incident that resulted in costly downtime. After the incident, the company determined that their lack of visibility into OT assets and vulnerabilities was a major contributing factor. As a result, gaining an understanding of what devices were connected to the network rapidly became a top priority.

The organization discovered their OT and ICS devices were often unpatched, unmanaged and invisible to their security team. The sheer breadth of OT equipment vendors and protocols, plus a variety of existing security technologies and the many regulations placed on the industry made the challenge of gaining complete visibility even more difficult.

From the board all the way down, the company was committed to finding a solution that would secure their intellectual property, including their proprietary refining process, and keep their employees safe. The company also wanted to maintain their focus on safety and environmental protection, increase operational efficiency, and protect their people, production and profits.

## Security incident drives the push for greater IT/OT asset visibility

When the company selected Microsoft Defender for IoT, they were able to rapidly deploy the agentless solution across 150 global facilities. At the same time, by gaining greater visibility into their assets, they also were able to detect, manage and prioritize vulnerabilities, including reporting on Common

Vulnerabilities and Exposures (CVE) disclosures, while balancing the needs of both the operations and security teams.

With so many facilities and devices, simply monitoring logs would not provide the speed, agility or contextual detail needed to detect and respond to threats. Microsoft Defender for IoT's M2M-aware behavioral analytics gave this company superior anomaly detection, providing deep contextual information for rapid incident response, all without any prior knowledge of the company's OT environment and without heavy investments in either human or financial resources.

Microsoft Defender for IoT provided a complete inventory and continuous monitoring of all connected assets, across vendors and protocols, with zero impact on the OT network. The company also utilized Microsoft Defender for IoT's advanced AI capabilities to predict the most likely pathways hackers may use to gain access to crown jewel assets. The IT team was then able to visualize, prioritize and simulate mitigation actions to protect their most critical processes.

Microsoft Defender for IoT is now a critical component of the company's security architecture, bringing the operations and IT teams closer together, and protecting the interests of the organization and key stakeholders. It represented the most mature solution of the vendors evaluated — exhibited both in technology and in the expertise provided by the support team, which ensured that the project was a complete success.

**For more insights on how Microsoft Defender for IoT benefits the oil and gas industry, visit the oil and gas landing page today.**

Microsoft Security