Oil and Gas Company Advances Security at the Edge

Edge-native security helps protect distributed Oil and Gas infrastructure

An oil and gas company with highly distributed edge infrastructure experienced significant increase in cyber risks. As it turned out, the remote oil and gas facilities - production wells, compressor stations, etc, faced regular connectivity issues. That dependency led to security gaps during periods of connectivity loss, and successful cyber attacks as a result. The cyber security audit reported that critical edge networks were inadequately protected by cloud-based security solutions. The oil and gas company required an advanced edge-native security solution to address growing cyber concerns.

Challenges:

- Disrupted connectivity
- Vulnerability of the distributed edge infrastructure
- High latency
- Bandwidth limitations and cost

The need to secure oil and gas revenue generating assets and critical infrastructure was the key driver for AI EdgeLabs deployment

Implementation Overview

The customer successfully implemented the AI EdgeLabs sensor throughout their endpoint locations, including control systems, sensors, and other IoT edge devices. The sensor was seamlessly integrated with existing company's systems within a few hours across several distributed edge locations. The software-defined security solution required no additional investment into the hardware, and significantly saved the overall cybersecurity budget. Besides, by utilizing AI EdgeLabs, the customer achieved reduced bandwidth to operate efficiently even with disrupted connectivity.

"We witnessed an advanced defensive action against sophisticated cyber attacks across edge infrastructure. As a result, our system downtime decreased substantially"

CISO,
Oil & Gas company in US

Leveraging AI-powered security solution, the oil and gas company effectively counters AI-driven cyber threats with its real-time threat prevention and detection, network-based edge asset discovery and monitoring capabilities.

The continuous analysis of traffic and behavior patterns across dispersed edge infrastructure further safeguards revenue generating assets against potential cyber risks.

Moreover, the adoption of AI EdgeLabs' multi-layered solution resulted in strengthened edge security, ensuring continued edge operations without interruptions.

AI EdgeLabs Delivered Results

Cost efficiency - improved by 30%

- Zero hardware footprint — no additional investment
- Reduced bandwidth costs

Advanced cybersecurity

- Improved response time
- Detected and countered advanced AI threats
- Reduced downtime

Improved edge operations

- Protected edge operations even in offline mode
- Decreased latency 10x