# Securing Oil & Gas at the Edge

## Oil and Gas at the Edge — a Cyber Target

Edge Computing enables OT-level digital transformation for the Oil & Gas industry, eliminating complexity, enhancing automation, and providing meaningful real-time insights for business operations. However, using IoT devices and edge computing has expanded the attack surface, making critical infrastructure vulnerable to cyber threats and giving adversaries more opportunities to breach systems.

## Motivations of Attackers

- Financial Gain
- Sabotage and Disruption
- Espionage and Intellectual Property Theft
- Geopolitical Motivations
- Activism and Hacktivism

# Edge Cyber Risks

## Upstream

- Unauthorized access to edge devices and sensors
- Tampering with real-time data collection and transmission
- Manipulation of edge computing algorithms and analytics
- Breaches compromising edge security and authentication
- Disruption of edge infrastructure, affecting operations

## Midstream

- Cyber attacks targeting edge computing infrastructure
- Compromise of data analytics and predictive maintenance
- Manipulation of real-time monitoring and control systems
- Unauthorized access to edge-to-cloud connectivity
- Breaches affecting data privacy and compliance

## Downstream

- Breaches compromising edge-based customer service systems
- Manipulation of edge computing in fuel distribution
- Cyber attacks on edge-based inventory and supply systems
- Unauthorized access to edge-based payment and POS systems
- Disruption of edge-based IoT devices and smart meters

## Inefficient Traditional Security Solutions

The conventional IT and cloud-based security solutions employed in distributed facilities within the oil and gas industry tend to be inefficient when securing IoT edge environments. They are often resource-intensive, require significant processing power, network bandwidth, and stable connectivity, which may not be available at the edge. As a result, they introduce latency and significant security gaps, struggling to ensure real-time cyber protection during disrupted connectivity or offline mode.

## Advanced Approach to Cybersecurity

**AI EdgeLabs is an AI-powered end-to-end** cybersecurity solution to protect the distributed edge and IoT environments in **real-time**. Leveraging the power of AI and ML, our solution immediately identifies and mitigates threats, even with intermittent connectivity and limited bandwidth.
AI EdgeLabs is purpose-built to operate **inside edge network** with minimum resources. It is optimized for **improved performance, runtime cost, and advanced edge security**.

# What AI EdgeLabs' Customers Value Most

## Business Value

1

### Ensured business continuity

Proactive and immediate protection of cyber threats at the edge to prevent outages

### Enhanced compliance

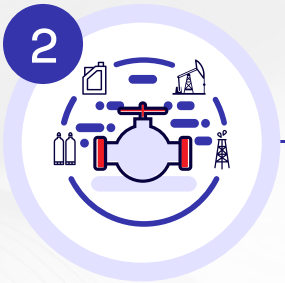
No data transfer – sensitive organizational data kept inside the host's infrastructure

### Reduced costs

No additional hardware and maintenance expenses while eliminating costs associated with bandwidth usage

## Operational Value

2



### Quick deployment

Quick and easy sensor deployment to existing infrastructure through docker/ Kubernetes containerized applications and 3rd-party edge orchestration platforms

### Seamless integration

No disruption to the operations' processes. High compatibility with the existing security tools and broad device support

### High scalability

Software-defined deployment to thousands of distributed edge devices and IoT gateways within hours

### Continuous protection

Continuous 24/7 protection of mission control systems to prevent downtime

### Remote control

A security approach to manage distributed facilities remotely

## Security Value

3

### AI-powered

Precise protection with 99.9% accuracy against unknown AI-driven threats, leveraging ML and AI

### Multi-layered

IDS, IPS, EDR, NDR, firewall, network-based edge asset discovery & monitoring capabilities in one solution

### Stable

Cybersecurity protection, even with intermittent connectivity and limited bandwidth

### Scalable

Effective security operations in the converged OT/IT environments across distributed networks

# AI Edgelabs' Key Features

- Real-time threat detection and prevention
- Autonomous response to network-based threats
- Distributed AI-based firewall
- Container-based edge asset discovery and monitoring
- Lightweight - for resource constrained devices

## AI Edgelabs Security Solution for the Oil and Gas

AI EdgeLabs' security solution is a formidable defense against the diverse and escalating cyber risks plaguing the oil and gas industry across its upstream, midstream, and downstream segments.

### Upstream

Protect real-time data integrity, thwart malicious tampering, and prevent breaches that compromise security and operations downtime.

### Midstream

Thwart cyber attacks aimed at edge infrastructure, prevent the compromise of data analytics and predictive maintenance, secure real-time monitoring, and ensure the security of edge operations even in intermittent connectivity

### Downstream

Protect against refining and distribution downtime, breaches impacting edge-based systems, cyber attacks on edge-based inventory, manipulations in fuel distribution, and disruptions to edge-based IoT devices

## AI EdgeLabs Protects against:

- DDoS
- MITM
- Ransomware
- LLMNR
- Malware
- Botnets
- Brute force
- Reconnaissance

Across every segment, AI EdgeLabs empowers the oil and gas industry to traverse the intricacies of edge environments with the certainty of multi-layered security, unwavering operational continuity, and compliance assurance.