# CLAROTY
# CASE STUDY

# OFFSHORE
# GAS FIELD

**Customer**
Fortune 1000 Oil and Gas company operating multitude of onshore and offshore production sites across the globe. The gas production holds a significant portion of the country's natural gas supply. The customer is the production and process sites are viable attack targets for hostile nation states and terrorist groups threat actors, and thus invests heavily in securing them from both physical and cyberattacks. Any halt in production would entail significant monetary losses due to various contractual and regulative obligation

**Problem statement**

**Security**: the customer's SOC team at the onshore HQ lack visibility into the production and process sites' network asset and traffic. This prevents both the ability to respond in real time to an ongoing attack, as well as reducing the attack surface by conducting an efficient network segmentation. The production rigs and onshore process terminal are connected through microwave link, raising concerns that compromise of one site would enable attackers to propagate into other sites.

**Operational**: the head of OT team onshore lacks real time visibility and backwards auditing into logic changes performed by the site's teams. Getting both network and logic changes data requires manual arrival to the offshore rigs which consumes both man-hours and money. Local regulations require periodic asset inventory reports on the site's activity that cannot prior to installation of the Claroty Platform cannot be easily met.

**Site**

- Two producing offshore gas fields (rig per site) with joint proven reserves of 7.9tr cubic feet.
- Onshore terminal for processing the raw gas before streaming to the gas distribution company.

. **Product**

- Claroty Continuous Threat Detection
- Enterprise Management Console
    - Core (onshore gas process terminal)
    - Replication over data diode to the customer's HQ

**Assets (per site)**

- HMI\EWS (each physical machine occupies both) – 2~4
- Controllers (Rockwell) – 20

- Remote I\O - ~200
- Other endpoints (servers, Historian etc.) – 30

**Networking**

- All of the site's traffic flows through 2 main switches. These switches were connected to an aggregation switch which sends the traffic to Continuous Threat Detection.

**Process**

- **POC**
    - 3 days of a POC on one of the rigs.

- **Full Deployment**
    - CTD – configuring all switches to SPAN + connect to aggregation switch + mounting the physical server for CTD – 1 day per site
    - Enterprise Management Console
        - Core (onshore gas process terminal) – 1 day
        - Replication over data diode to the customer's HQ – 1 day
    - CTD training mode – 2 weeks
    - Shift to operational mode + connection to the Enterprise Management Console + connect Enterprise management console to SIEM – 1 day

**End Result**

Full visibility to all assets and connections. The customer proactively uses CTD to discover networking misconfigurations and other security issues both on OT and IT networks, as well as generate full network map for further segmentation project. A timeline has been set to globally expand deployment to additional rigs (land and offshore