PROTELION

Use Cases

Highly Secure Communication for Oil and Gas Industry

Oil and Gas companies are an extremely attractive target for cyber criminals, hacktivists and even terrorists. Steps taken toward digitalization and the use of cloud services have exposed vulnerabilities in the operational technology that is used extensively in the Oil and Gas sector. The broad range of diverse business processes and production systems, encompassing Upstream, Mid-Stream, Downstream and trading businesses, create multiple attack targets which can be exploited by threat actors. In addition to the typical impacts of cyber incidents, which include data, reputation and business loss, cyber attacks on the Oil and Gas industry can also cause major damage to plants, equipment, environment and public safety risks.

Duties and As-Is Situation for Oil and Gas Industry

Extensive use of operational technology which was not designed to be connected to the Internet and lacks robust built-in security also for remote connectivity

Wide use of unsafe ICS and SCADA systems, sensors as well as of traditional IT networks and networks of other companies, including the ones of clients

Collecting system data from various sources, such as network traffic logs and endpoint devices (oil drills, gas turbines, pipelines, generators, pumps etc.) which is transferred to central computation centers where it is processed and analyzed

Oil rigs and gas production plants are modern high-tech software-controlled installations and prone to vulnerabilities and attacks

Project Specification

The need of a comprehensive security framework to protect existing IT networks, endpoint devices and legacy systems from unauthorized access, intrusion, data breaches and sophisticated cyber attacks

Field service and maintenance workers need for their field diagnostic readouts and video inspection of critical assets by drones a secure and proteced data transfer

Deployment of an advanced threat detection and response system to monitor network traffic, identify potential threats and taking immediate action to mitigate risks is needed

Implementing endpoint device protection to secure voice/video calls, sensor data transmission and ensuring secure remote access to process data in data centers or cloud solutions

Project Implementation

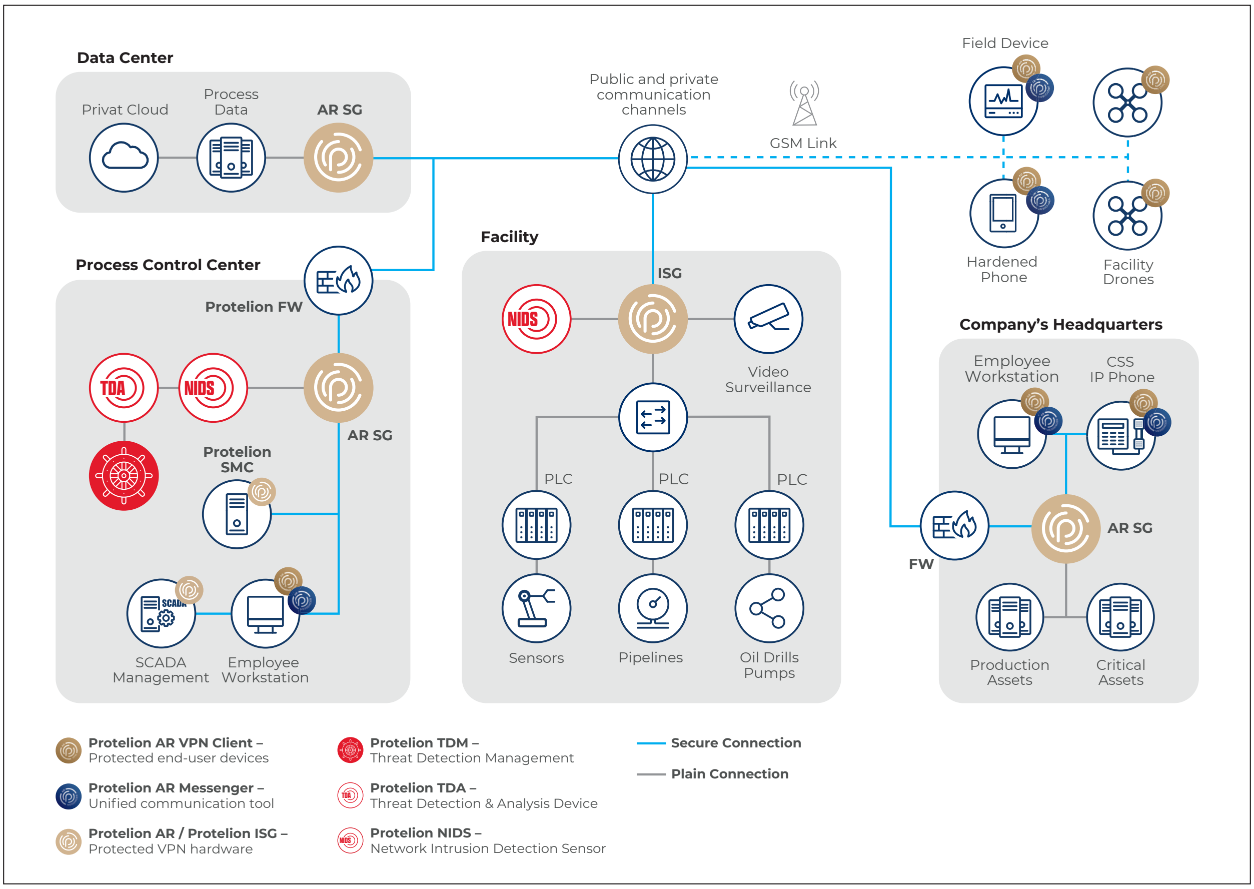
1 The Protelion TDR-System detects and analyzes malware activities and provides fast real-time alerts to security officers and makes cyber attacks useless. It can easily be integrated in an existing SIEM

2 Protelion Security Solutions protect endpoint devices, sensors, valves, ICS and SCADA networks against a multitude of cyber threats and attacks, ensuring continuity of production and distribution systems

3 Internal and external endpoint communication devices are hardened and protected against various types of cyber threats and malicious user behavior, enabling encrypted voice and video calls, chat, email and file exchange over unsecure channels between different headquarters, facilities and exploration sites

4 Access control system to the facilities' IT network, video surveillance cameras and patrolling drones. All systems and devices transmit their critical log data and image information encrypted over different physical communication channels

Scheme for Oil and Gas Industry



Protelion Features

Comprehensive Protection
Protelion Security Solutions offer comprehensive protection against a wide range of cyber threats, using advanced technologies to detect and respond in real-time and minimizing thereby the impact of cyber attacks

Customizable Solutions
High flexibility, interoperability and scalability of the Protelion Security Technology make it easy for each individual customer to create an optimal solution on top of its existing IT infrastructure

Endpoint Protection
All-in-one solution to secure endpoint devices from zero day exploits, unknown malware, ransomware, DDoS attacks and internal or external threats such as data theft, loss and alteration

Operation Security
Protelion Security Solutions provide a protected oil/gas production, ensure the continuity of distribution infrastructures as well as secure remote access to control and monitoring sensors. They also secure endpoint devices' firmware and sensitive update processes

PROTELION

Oberwallstrasse 24
D-10117 Berlin

+49 30 206 43 66-0
info@protelion.de

gov.protelion.com