USE CASE

IRONGATE

THE STORY

As with many other commercial sectors (electric grids, water facilities, transportation), the oil and gas industry has increasingly become dependent on software systems for monitoring and control through drilling, production, and distribution. In the pipeline industry, for instance, 50 years ago, manned pump stations were standard and now regional and national software systems operate stations remotely.

Since oil and gas operations are geographically widespread – even offshore – remote IP-based SCADA (Supervisory Control and Data Acquisition) is essential in their operations, providing monitoring and control.

APPLICATION

Cyber Security

SCENARIO

The oil and gas industry is vulnerable to cyber attacks

Unfortunately, every additional piece of remote IP-connected SCADA equipment exposes a new interface for hackers to exploit. This includes the wireless solutions commonly used in oil and gas fields and pipelines. Until now, systems to protect IP-based SCADA communications have been expensive and only lessen, rather than eliminate, vulnerability to attack. SCADA communications over a network create vulnerabilities that require more than an IP-based solution.

THE SOLUTION

IronGate provides secure SCADA transmission over IP networks, including over the Internet. IronGate does not rely on standard networking or security methods. It is a purpose-built computing appliance. Its Hardened Ethernet Interface (HEI) is its only connection with the network.

The IronGate system is scalable and comprised of the IronGate Core server and any number of IronGate Edge devices. IronGate Edge devices are located remotely, and their main function is to send SCADA communications to and from devices located in the field and the main operations center, such as an oil and gas pipeline. Each Edge device can connect to hundreds of SCADA controls and sensors. Located at the main operations center and receiving communications via the Edge devices, is an IronGate Core server. The Core passes along the received SCADA data to supervisory systems for monitoring. Each IronGate Core can connect to more than 100 Edge devices. The Edge devices communicate with the Core solely via their HEI, which is their only connection to the network. The HEI protocol is encrypted, custom, and used nowhere else in the world. The tools and methods designed by hackers to penetrate standard networking equipment have no point of entry.

STORY

The oil and gas industry is vulnerable to cyber attacks, but every additional piece of remote IP-connected SCADA equipment exposes a new interface for hackers to exploit.

Challenge

Stop hackers before they cause damage to critical infrastructure systems.

Solution

Irongate - a purpose-built SCADA security solution.

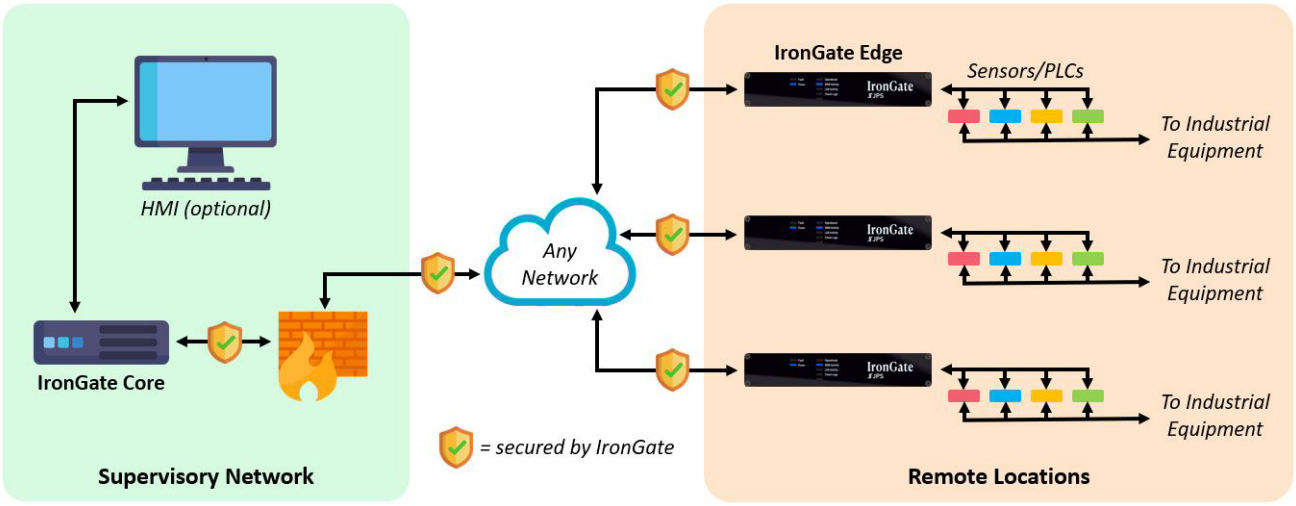
Benefits

Provides a scalable, brand agnostic, software secure approach to foil hackers.

THE RESULT

From drilling to final delivery, the oil and gas industry relies on a multi-step process for turning what comes out of the ground into gas, home heating oil, jet fuel, and other petroleum products. Each of these steps requires movement of the product from one location to another, as each of these stations is specialized. The movement and monitoring of oil or gas through the processing, pipelines, and delivery is constantly monitored and controlled. Sadly, SCADA monitoring and control has proven vulnerable to hacking.

The IronGate solution provides a scalable, brand agnostic, software secure approach to foil hackers. It distinguishes itself with its encrypted HEI custom protocol for communication, and its physical hardening which erases and "bricks" the Edge device if anyone tampers with it. Similarly, once the system is up and running, usernames and passwords (or other identifiers) cannot be used as an entry vector.



"IronGate was exceptionally hardened against attack and presented a minimal attack surface"

CYLANCE

Tested and ubreached by:

MANDIANT
A FireEye® Company

"...stood out from among the dozens submitted as a potentially groundbreaking solution to some of the most critical and high-priority challenges that the U.S. Intelligence Community faces

INNOVATORS' SHOWCASE 2020 HONOREE

INSA

KEY BENEFITS

+ Secure hardware and software design. Physical possession of an Edge device does not expose any vulnerabilities and the HEI is encrypted.

+ IronGate Edge devices are designed to be FIPS 140-2 level 4 and, the Core device is FIPS 140-2 level 2 compliant.

+ Remote control of Edge devices is available via RS-485A interface and relay and sensor inputs.

© 2022 JPS | JPS.COM