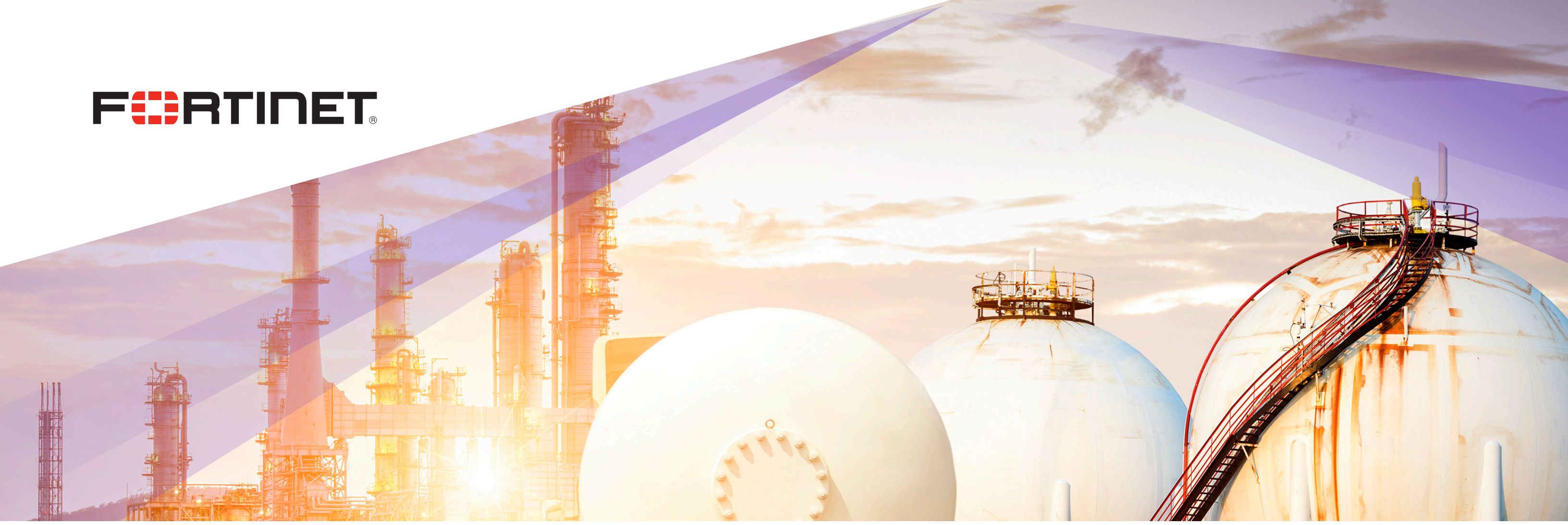

CASE STUDY

# Major Oil and Gas Company Leads the Pack in Securing Critical Infrastructure with Network Access Control

As critical infrastructure and utilities continue to evolve with the demands of their ever-changing marketplace, these organizations are also tasked with hardening their systems to ensure that delivery is never disrupted by security threats that take advantage of out-of-compliance endpoints. This can be a special challenge for energy providers, whose industrial control systems (ICS) are often highly distributed. Requisitioning IT staff to personally maintain and update wide-ranging systems is not practical. Yet visibility, control, and response over these systems is crucial.

A leading oil and gas company with 5,000 endpoints across 200 locations in North America chose the FortiNAC network access control (NAC) solution to help them secure their distributed endpoints and legacy equipment. Using the FortiNAC solution, this customer ensured uptime and reliability of service while gaining security and visibility across the entire network infrastructure. The solution provided for master control over disperse locations without difficult hardware installations or complex legacy equipment upgrades.

## The Challenge

This oil and gas customer had a difficult requirement: No unknown or noncompliant endpoints were to access the corporate production network. A noncompliant endpoint needed to be instantly quarantined from the rest of the corporate network until the issue was resolved (e.g., the endpoint was patched to a required level).

This requirement was hard to enforce since their network profile included both large corporate office locations tied to employee users, as well as extremely distributed, remote switches that rarely had any human interaction. For example, one switch was located in a remote oil field. Some of the company's remote ICS infrastructure consisted of legacy equipment that could not support 802.1X authentication, so a creative means of implementing network access control without using a RADIUS server or 802.1X was needed.

## Details

**Customer:** Major Oil and Gas Company

**Industry:** Power and Utilities

**Location:** North America

## Business Impact

- Full visibility into all managed and unmanaged IoT devices, endpoints, and users
- Zero-trust network architecture with endpoint validation and authentication
- Automated detection and isolation of unknown/rogue endpoints
- Comprehensive live inventory of network connections to share with IDS/IPS, SIEM, and CMDB solutions

## Solution

- FortiNAC

In addition, many of the company's remotely located endpoints had limited bandwidth, so being able to maintain network performance and integrity during NAC setup or maintenance was another key concern. In the past, when redirecting traffic to set up port mirroring, the customer had experienced cost-prohibitive performance degradation. Understandably, they wanted to avoid this when implementing any future NAC protocols.

## Finding the Right Solution

After extensive evaluations of three other "market-leading" NAC solutions, this customer chose the FortiNAC solution as one that would definitively meet their requirements, effectively addressing their organization's unique challenges. Plus, it would enable them to scale easily, taking advantage of additional, more advanced features in the future.

The customer successfully navigated their limited bandwidth concerns without appliance installations at remote sites, as the FortiNAC solution is centralized and has no bandwidth allocation requirement.

Fast, effective endpoint control was implemented with little ramp-up time. By deploying the vendor-agnostic solution, the customer's network security plans covered all new and legacy switches and endpoints, without lengthy setups or upgrades. The solution supports legacy equipment, so the customer had powerful network access control without using 802.1X protocols.

The robust security also came at a cost-effective price point—hundreds of thousands of dollars less than competitors' NAC solutions.

The customer was able to achieve complete visibility across their entire corporate network with a live inventory of all connections—including those highly distributed, remote switches—as well as endpoints and users at all 200 locations. This arsenal of comprehensive data proved invaluable in providing greater context and deriving increased value from their existing SIEM, IDS/IPS, and CMDB solutions.

The customer easily implemented and enforced robust NAC policies within the first year of deployment. They were able to validate all endpoints connecting to the corporate network and automatically deny access to any rogue device that had fallen out of compliance.

Thanks to the unparalleled visibility and control with the FortiNAC solution, this customer plans to expand their deployment to cover their SCADA network as soon as their corporate network reaches a fully managed state.

www.fortinet.com

November 11, 2019 10:30 AM
C:\Users\cyan\Documents\Creative Services - Misc\Document Edits\CS - Oil and Gas Co\cs-oil-gas-company Folder\cs-oil-gas-company