



CUSTOMER

Global Oil & Gas company
Headquartered in North America
100k+ employees


OBJECTIVES

Access patch intelligence and
secure OT assets

RESULTS

Successful replacement of
security controls
Implementation of a patch
management program
General improvement of OT
(Operational Technology) security

 Foxguard

 <https://foxguardsolutions.com/>

 requestinfo@foxguardsolutions.com

GLOBAL OIL & GAS COMPANY IMPLEMENTS PATCH MANAGEMENT SOLUTION

The global Oil & Gas company successfully deployed Foxguard's Patchintel at one of its largest refineries.

Context

The May 2021 ransomware attack on Colonial Pipeline, which crippled the systems controlling its pipeline operations, sent shock waves through the Oil & Gas industry, exposing critical vulnerabilities in its cyber defenses. To contain the attack, the company halted all pipeline operations, triggering widespread fuel shortages, panic buying, and ultimately, a state of emergency. Over the past five years, the Oil & Gas sector has seen a significant rise in cyberattacks, with 35 major incidents recorded during this period.¹

Cyber security challenges at a typical refinery often involve issues such as remote third-party contractor and vendor access, the use of removable media like hard drives and smart phones, outdated or unpatched operating systems, and more.

In this context, a U.S. refinery, part of a Global O&G company, reached out to Foxguard in 2022, as they were transitioning away from their existing systems and needed a new solution to replace their patch management program.

The customer challenges

This refinery is one of the largest in the U.S., with a production capacity of 300,000 barrels of crude oil per day. It faced several challenges:

Refineries often manage a vast array of assets from numerous vendors, requiring them to navigate multiple data sources—such as official vendors, regulatory agencies, threat intelligence repositories, and third-party intel—when searching for patch availability.

According to Deloitte, the average large-scale O&G company “uses half a million processors just for oil and gas reservoir simulation; generates, transmits, and stores petabytes of sensitive and competitive field data; and operates and shares thousands of drillings and production control systems spread across geographies, fields, vendors, service providers, and partners.”

¹ S&P Global Platts Oil Security Sentinel™ research project

Many of these assets are critical, either for production or safety protocols. Interrupting operations with unverified patches or leaving systems vulnerable due to missing patches is simply too risky, potentially leading to costly downtime or exposing the organization to cyberattacks.

The solution

Foxguard implemented the following solutions at the refinery:

Foxguard Patchintel: A monthly subscription-based solution that provides a detailed summary of the previous month's patches for each customer's critical assets. It ensures privacy by keeping customer data out of the cloud and securely safeguarding their asset list, while delivering the necessary patch binary files to help customers update their critical assets to the latest version. The patches are provided in a secure, easy to manage format and are verified using a custom hash tool to ensure customers can trust the authenticity and integrity of each binary file.

Foxguard Deploy: A centralized, secure patch distribution solution that enables customers to efficiently distribute patches across their entire fleet of assets.

Together, these solutions provide a single, secure source for patch management, ensuring a reliable and protected supply chain for all updates.

The results

The refinery now benefits from access to:

- Intelligence data on new software patches and updates for critical assets.
- A standardized and secure process to acquire patches from vendors.
- Patch, update, and firmware installers delivered via secure storage device(s).
- A hardened, purpose-built patch deployment platform designed to manage on-premises patching efficiently.

After retiring its initial solutions, the refinery enhanced its security posture by implementing a patch management program tailored to its specific environment. Security controls were seamlessly integrated with existing software and hardware.

As a result, the refinery saw a significant improvement in its OT security, allowing its personnel to focus more on maintaining operational continuity.

CYBER SECURITY SOLUTIONS PORTFOLIO

Program Development Services

Our Governance Program Development services provide a comprehensive approach to establishing a cybersecurity program aligned with your business objectives, identifying essential people, processes, and technologies.

Audit/Inspection Support Services

Our Governance Audit/Inspection Support services help organizations prepare for regulatory compliance by conducting thorough audit readiness drills, assessing governance frameworks, and identifying compliance gaps.

Tabletop Exercise Services

Our Tabletop Exercise services provide guided simulations, workshops, and activities with key stakeholders to assess your organization's readiness and ability to respond to business-impacting events.

Assessment Services

Our Assessment services offer comprehensive evaluations of assets, systems, and policies tailored to the customer's industry, regulatory environment, and security maturity level.

Asset Visibility Services

Our asset visibility services utilize automated tools and on-site resources to identify all network and non-network connected devices, delivering a comprehensive asset inventory report that includes asset inventory creation, network topology, and cyber hygiene assessments.

Hardening Services

Our Hardening services focus on securing operating configurations by assessing device-specific settings, implementing best practices, and configuring controls to reduce vulnerabilities across your environment. We also provide high-level programmatic guidance to ensure regulatory compliance.

Patch & Vulnerability Management Services

Our Patch & Vulnerability Management services use patch and vulnerability intelligence to develop targeted tactical mitigations or comprehensive strategies for identified vulnerabilities, creating mitigation plans and recommending technologies to close security gaps and strengthen your organization's cyber posture.