Fortinet Oil and Gas Cybersecurity Solutions

Protecting Critical Infrastructure and Assets Against Cyber and Physical Threats with End-to-end Integration
Executive Overview

Infrastructure owned by oil and gas companies contributes not only to the profitability of one firm but also to economic and geopolitical stability for the entire world. From drilling sites to pipelines to refineries, the petroleum production process is rife with all kinds of risk, and adversaries target them with varied motivations. Fortinet has delivered cybersecurity solutions for the oil and gas industry for more than a decade, offering end-to-end integration of cyber and physical security for far-flung networks. At upstream, midstream, and downstream locations, ruggedized appliances can survive the worst environmental conditions, and layers of security protect vulnerable remote sites. For oil and gas company headquarters, the Fortinet Security Fabric enables a holistic approach to security. And that security architecture extends to gasoline retailers, providing secure networking to and within locations.

Oil and gas companies own and manage major pieces of critical infrastructure that are vital not only to company operations but also to the nation’s economic and military well-being. Upstream, midstream, and downstream operations are valuable targets for cyber adversaries with a variety of motives—from personal profit to industrial espionage to economic disruption. As one writer puts it, “Every part of the oil and gas value chain is currently exposed, and conventional static defenses no longer suffice.”

While this statement might seem to be hyperbole at first glance, the risk is real. An attack on the supervisory control and data acquisition (SCADA) system that operates an offshore rig, oil well, pipeline, or refinery—or for that matter Internet-of-Things (IoT) devices that provide monitoring data to such systems—can have devastating consequences. These might include expensive damage to facilities, lengthy supply disruptions, and even injury and loss of life for employees, bystanders, and nearby residents.

Such attacks targeting operational technology (OT) infrastructure are becoming more frequent, and oil and gas companies’ corporate infrastructure is a target as well. Successful attacks could expose intellectual property such as exploration data surveys, and pose data security risks for financial and personnel information. Beyond the business problems that such attacks can create, they expose companies to regulatory risk as well.

For more than a decade, Fortinet has provided comprehensive security solutions for the oil and gas industry—whether for land-based and offshore drilling sites, refineries, and pipelines, or for the corner gas station. At the center of what Fortinet provides is the Fortinet Security Fabric, which enables end-to-end security integration across the expansive infrastructure oil and gas companies manage.

Key Oil and Gas Cybersecurity Challenges

Key oil and gas cybersecurity challenges include:

Cost Optimization

Petroleum markets are notorious for their wild fluctuations in the selling price for oil, gasoline, and natural gas. This volatility means that a company can easily go from significant profitability to an operating loss in a matter of days. As a result, minimizing cost is always a priority for oil and gas companies, as they try to structure operations to survive periods of low prices.

In this environment, replacing expensive, older equipment due to security vulnerabilities is sometimes out of the question, necessitating creative approaches to keeping them secure. Whatever this requires, the solution must be designed in such a way as to not impede operations. Many companies have multiple pieces of infrastructure with these kinds of vulnerabilities, putting a greater burden on cybersecurity team members.

The cybersecurity skills shortage is getting worse, with an estimated shortage of more than 4 million workers—compared with 2.8 million currently working in the field. This means that hiring additional team members to address these issues is costly, and it may be impossible to find some specific skills in the labor market at any price. Regardless, adding more staff does not address the core problem that manual security processes are inadequate to deal with threats that move at machine speed.
Visibility Across IT and OT Systems

Industrial IoT (IIoT) devices have changed the game for the security of supervisory control and data acquisition (SCADA) systems used to manage drilling sites, pipelines, and refineries. Internet-connected sensors and connected controller devices eliminate the air gap from the internet that has historically kept SCADA systems relatively safe from cyberattacks.

This, of course, expands a company’s attack surface. The problem is exacerbated by the fact that many IIoT devices are headless and thus cannot be protected with client security software—or even get firmware updates. To plug these security holes, organizations often deploy multiple point products. The resulting security silos create complexity and obfuscate visibility, delaying threat detection, prevention, and response. This increases the risk that a fast-moving threat will get through before manual processes detect it.

Operational Efficiency

This architectural fragmentation also increases operational inefficiencies for the cybersecurity team. Automation of security processes is impossible without end-to-end integration of all security elements. This requires manual security workflows that waste the time of highly paid security engineers. It also increases security complexity and requires security leaders to have a wide variety of product skills within the team. As an example, some teams must pull multiple employees from other tasks in the days before an audit so that reports can be prepared manually.

Architectural silos also create redundancies in the management of applications and even in software and hardware licensing, decreasing the efficiency of teams in legal, procurement, and finance that manage those licenses. Organizations may also find that their technology spend is higher because of the use of multiple vendors and overlapping features in different products that a company might own.

Customer Experience

Fuel retailers engage with their customer base through a variety of electronic means, including self-service point-of-sale (POS) infrastructure, mobile apps, and loyalty cards. For any POS transactions, they must be compliant with Payment Card Industry Data Security Standards (PCI DSS), with integrated reporting to demonstrate compliance. The performance of IoT sensors that monitor tank levels, refrigeration temperatures, and the like also impact customer experience. Protecting a store’s infrastructure against cyber threats is paramount for both compliance and maintenance of brand value. And that brand value primarily reflects on upstream, midstream, and downstream providers, given that these retailers typically carry the logos of major producers.

Compliance Reporting

Energy companies are subject to a wide array of regulations and standards, from environmental requirements for drilling and refining to cybersecurity regulations. Unfortunately, a disaggregated security architecture makes preparing reports difficult and time-consuming. Failure to demonstrate compliance can damage brand reputation and result in substantial fines and penalties.

Use Cases

Following are some of the most prevalent cybersecurity use cases for oil and gas companies:

Securing Upstream Infrastructure

Organizations involved in energy extraction must protect a complex infrastructure in remote locations, both on land and offshore. These sites are valuable targets for hackers whose objective is operational disruption, environmental terrorism, or even injury and loss of life for employees and members of the surrounding community.

To protect these sites, every aspect of security, from industrial control systems to physical security, must be integrated for centralized visibility and control. Surveillance infrastructure at a small drilling site should be as heavily protected as at headquarters—if not more so—and equally visible to the security operations team.

The Fortinet Security Fabric offers comprehensive, integrated cyber and physical security for the oil and gas industry. FortiGate Rugged Series next-generation firewalls (NGFWs) and FortiAP Outdoor Series wireless access points provide robust security protection while withstanding the rugged extremes of drilling and exploration sites on land and water. These NGFWs receive a threat feed specific to industrial control systems (ICS) and SCADA systems from FortiGuard Labs. FortiCamera and FortiRecorder protect against physical intrusion, while Fortinet Secure SD-WAN and Fortinet SD-Branch provide secure networking to and within the remote site. FortiManager, FortiAnalyzer, FortiSIEM, FortiInsight, FortiClient, FortiEDR, FortiPresence, and FortiNAC, usually delivered from the corporate infrastructure at headquarters, provide layers of security for these vulnerable remote sites.
Securing Midstream Infrastructure

The wholesale transport of petroleum expands an organization’s physical attack surface by hundreds or thousands of miles. Pipelines are subject to both accidental leaks and physical sabotage, and the SCADA systems and IIoT devices that monitor and control them are often vulnerable. A successful attack can be catastrophic, with the potential for massive environmental damage and loss of life.

Midstream operators do well to utilize the Purdue Enterprise Reference Architecture as a standard in designing their electronic infrastructure. But while the Purdue standard helps to define where security is located in the architecture, it gives little guidance for how the cybersecurity architecture should be designed.

The Fortinet Security Fabric makes this possible with integrated cybersecurity, physical security, and secure networking. FortiGate Rugged Series NGFWs and FortiAP Outdoor Series wireless access points provide robust security protection while withstanding the remote outdoor environments that pipelines run through. FortiCamera and FortiRecorder protect against physical intrusion, while Fortinet Secure SD-WAN and Fortinet SD-Branch provide secure networking to pumping stations and other remote sites. A wide range of tools delivered from headquarters provide layers of protection: FortiManager, FortiAnalyzer, FortiSIEM, FortiInsight, FortiClient, FortiEDR, FortiPresence, and FortiNAC, to name a few.

Securing Downstream Infrastructure

Refineries turn crude oil into a variety of combustible materials, and this adds even more physical danger to the process. Like upstream and midstream operations, downstream ones are targets for both physical and cyberattacks. Either type of attack can pose significant physical danger to employees and the general public. Successful attacks can also impact the national economy with supply shortages. Threats can emanate from the outside, the inside, and from third parties. And while some insider attacks may be deliberate, others may be accidental.

To provide protection in such a volatile location, security teams need single-pane-of-glass visibility into the entire network, as well as the surveillance infrastructure. The Fortinet Security Fabric protects cyber and physical security at these facilities in an integrated and holistic way. FortiGate Rugged Series NGFWs and FortiAP Outdoor Series wireless access points withstand a variety of environmental challenges. FortiCamera and FortiRecorder integrate physical security into the integrated Security Fabric. A wide range of security tools deliver layers of protection, including FortiManager, FortiAnalyzer, FortiSIEM, FortiInsight, FortiClient, FortiEDR, FortiPresence, and FortiNAC.

Securing Corporate Infrastructure

Oil and gas companies’ corporate infrastructures contain a variety of business-critical data, from geological and exploration data to financials to the personal information of employees and consumers. Most companies have remote and traveling workers, third-party partners with access to corporate resources, and services in multiple clouds. In addition to protecting these resources from external attack, it is crucial to protect against well-intentioned and malicious insiders exposing confidential data.

While a disaggregated security architecture and mobile users impede both security and operational efficiency, single-pane-of-glass visibility and centralized control enhance both. End-to-end integration of the security infrastructure unlocks automation of threat detection, response, and reporting, freeing up time for well-paid security personnel to focus on strategic tasks.
The **Fortinet Security Fabric** provides an integrated security architecture that makes this possible. Fortinet covers the entire attack surface, from the data center to multiple clouds to the network edge, with broad, integrated, and automated protection. **Fortinet Dynamic Cloud Security** solutions break down silos between multiple public and private clouds, enabling consistent policy management. **FortiManager**, **FortiAnalyzer**, and **FortiSIEM** provide comprehensive management and analytics. **FortiInsight** and **FortiDeceptor** help protect against insider threats. And companies can protect devices and applications and detect and respond to attacks with **FortiWeb**, **FortiMail**, **FortiClient**, and **FortiEDR**. Finally, in the case of mobile users and their devices, **FortiAuthenticator** and **FortiToken** provide them with secure access to the corporate network. Intent-based segmentation, enabled by **FortiGate** NGFWs, enhances the security posture of remote users by restricting their access to only the data and systems to which they have been granted authority to access.

### Securing Oil and Gas Retail Locations

Oil and gas retailers usually sell other items as well, and they face similar challenges to other brick-and-mortar retailers. In addition, they have numerous IoT devices to track tank levels, refrigerator temperatures, and IP cameras. Fuel tanks on the property add extra safety and compliance requirements that other retailers do not have, and self-service, outdoor POS infrastructure presents another risk. As a result, the integration of cyber and physical security is critical, as are compliance with PCI standards and providing a pleasant in-store experience.

Such a complex set of business and security needs makes end-to-end integration of the security architecture especially important for gasoline retailers. Such an infrastructure eliminates the need for manual processes and workarounds that slow threat response and take staff members away from their mission of customer service.

Fortinet networking and security solutions help connect different locations in a chain, providing robust network security and automated compliance reporting. **FortiGate** NGFWs deliver robust protection for the entire attack surface, with many features built-in that require an additional hardware purchase with other vendors. **Fortinet Secure SD-WAN** provides secure networking to all store locations without the need for expensive multiprotocol label switching (MPLS) bandwidth. And **Fortinet SD-Branch** solutions, including **FortiAP**, **FortiSwitch**, and **FortiNAC**, extend Fortinet security into the infrastructure within each store.

This infrastructure also allows for shared security services to be delivered from headquarters, including the **FortiAuthenticator** identity and access management tool, **FortiClient** and **FortiEDR** advanced endpoint security solutions, **FortiInsight** user and entity behavior analytics, and **FortiDeceptor** deception technology. In addition, the **FortiManager**, **FortiAnalyzer**, and **FortiSIEM** management and analytics tools enable single-pane-of-glass visibility and automated reporting for compliance with standards like the PCI Software Security Framework (SSF). This infrastructure is supported by integrated artificial-intelligence (AI) and machine-learning (ML) capabilities to help detect and remediate unknown threats.

### Fortinet Differentiators

Below are some differentiators that make Fortinet the best choice for oil and gas companies:

#### Integrated Architecture

The **Fortinet Security Fabric** provides a single-vendor, end-to-end, integrated security architecture across IT and OT, for every phase of the production process, from protection to detection to response—for greater visibility and control.

#### Networking, Cybersecurity, and Physical Security

Fortinet delivers the ability to consolidate networking, cybersecurity, and surveillance functions into a single pane of glass—whether at headquarters, a remote drilling site, or the corner gas station.
Ruggedized Security Appliances
Fortinet offers a broad selection of ruggedized appliances to fit all environmental needs, to provide cybersecurity protection for all phases of the production and delivery process.

High Performance
FortiGate NGFWs have capabilities for working in complex, remote environments and deliver top performance even with secure sockets layer (SSL)/transport layer security (TLS) inspection activated. Fortinet is recognized as a Leader in the Gartner Magic Quadrant for Network Firewalls and achieved the best score in the NGFW Security Value Map from NSS Labs.

Robust Threat Intelligence
In addition to identifying IT-specific threats, FortiGuard Labs provides robust intelligence on threats specific to OT systems as a result of 15 years of work in the field. To detect zero-day threats, Fortinet has been analyzing files using AI and ML for eight years, with unparalleled accuracy.

Extensive Partner Network
The Fortinet Fabric-Ready Partner program includes the industry’s largest network of partners with specific experience in OT and industrial systems.

Broad Security with Minimal Devices
Fortinet delivers a wide variety of security and networking functions delivered in a single box, when competitive solutions often require multiple devices—and multiple license expenditures—for the same capabilities.

“The key to defending SCADA systems effectively is to be aware of potential issues and plan ahead. Investing in effective defense is no longer simply ‘nice to have’—it is a business imperative.”

Figure 1: Fortinet cybersecurity solutions for oil and gas companies address use cases that span the entire process from exploration to retail distribution.
Conclusion

Oil and gas companies are responsible for some of the world’s most critical infrastructure, and successful attacks can bring economic disruption, environmental catastrophe, and even loss of life. Fortinet delivers a broad, integrated, and automated cyber and physical security solution that reduces risk and protects a sprawling infrastructure.

4. Ibid.