SOLUTIONS OVERVIEW

Fortinet Oil and Gas Cybersecurity Solution

Protecting Critical Infrastructure and Assets against 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 risks, and adversaries target them with varied motivations.

For 10+ years, Fortinet has delivered cybersecurity solutions for the oil and gas industry with end-to-end cyber- and physical security integration for global networks. At upstream, midstream, and downstream locations, our ruggedized appliances can survive the worst environmental conditions. For oil and gas company headquarters, the Fortinet Security Fabric has a holistic approach to security. And that security architecture extends to gasoline retailers, providing secure networking to and within locations.

Ransomware attacks are increasingly successful and have risen 150% in the past year alone.[1]

Oil and gas companies own and manage major critical infrastructures that are vital to company operations and the nation's economic and military well-being. While the oil and gas industry powers the global economy and is vital to national security,[2] it isn't new to supply disruptions and price volatility. Today's situation is unique. A confluence of economic, geopolitical, trade, policy, and financial factors have exacerbated the issue of underinvestment and triggered a readjustment in the broader energy market.[3]

With a heavy reliance on technology and information systems to operate, a successful cyberattack against an oil and gas company could have serious consequences, such as operational disruptions, economic losses, reputation damage, and even environmental harm.[4] These might include expensive damage to facilities, lengthy supply disruptions, and even injury and loss of life for employees, bystanders, and nearby residents.

Cyberthreats will likely increase. Oil and gas companies' corporate infrastructures will also remain a high-value target. Enhancing cybersecurity will be a challenge as the world's energy system grows ever more complex, but it's also imperative. If an attack is successful, it could expose intellectual property, such as exploration data surveys, and pose data security risks for financial and personnel information. Beyond the business problems such attacks can create, they also expose companies to regulatory risk.[5]

Fortinet provides comprehensive security solutions for the oil and gas industry, whether for land-based and offshore drilling sites, refineries, pipelines, or the corner gas station. At the core of what Fortinet provides is the Fortinet Security Fabric, which enables end-to-end security integration across the expansive oil and gas company infrastructures.

Key Oil and Gas Cybersecurity Challenges

The major issues that currently challenge oil and gas company cybersecurity teams include:

Cost optimization

Petroleum markets are notorious for their wild fluctuations in the selling price of 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 costs 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.

Nearly every organization faces an uphill battle when it comes to finding qualified security practitioners due to the growing cybersecurity skills shortage.6 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.

Attack surface expansion

Industrial-Internet-of-Things (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, which has historically kept SCADA systems relatively safe from cyberattacks. However, removing the air gap raises a security issue by expanding a company's attack surface.

The problem is exacerbated because many IIoT devices are headless and thus cannot be protected with client security software or even get firmware updates. Additionally, older control networks may not contain routable traffic. Newer security and infrastructure solutions are required to provide the needed visibility into aging control deployments.

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 legal, procurement, and finance teams 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 cyberthreats 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

The following are some of the most widespread 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 difficult extremes of drilling and exploration sites on land and in water. These NGFWs receive a threat feed specific to industrial control systems (ICS) and SCADA systems from FortiGuard Labs.

FortiCamera and FortiRecorder video surveillance systems protect against physical intrusion, while Fortinet Secure SD-WAN and Fortinet SD-Branch provide secure networking to and within remote sites. FortiManager, FortiAnalyzer, FortiSIEM, FortiInsight, FortiClient, FortiEDR, FortiPresence, and FortiNAC, usually delivered from the corporate infrastructure at headquarters, provide layers of security including centralized monitoring, reporting, management, and policy reinforcement for these vulnerable remote sites.

- **FortiManager** provides centralized device management and security policy implementation for FortiGate appliances across IT and OT. It enables consistent security policy enforcement and software updates across all FortiGate appliances from a single, streamlined user interface.
- **FortiAnalyzer** provides centralized monitoring, logging, and reporting for FortiGate appliances deployed across IT and OT.
- **FortiSIEM** security information and event management ingests and analyzes log data from IT and OT, enabling correlations for threat actor behavior that spans both environments. FortiSIEM can also show threat activity in the ATT&CK framework for enterprise IT and ICS environments.
- **FortiInsight** provides user and entity behavior analytics (UEBA), minimizing insider threats using forensic machine learning.
- **FortiClient** is a Fabric Agent that delivers protection, compliance, and secure access in a single, modular lightweight client for endpoint management and zero-trust network access (ZTNA).
- **FortiEDR** endpoint detection and response provides real-time, automated endpoint threat detection, protection, orchestrated incident response, and forensics.
- **FortiPresence** provides presence and positioning analytics using the existing on-site Fortinet access points to detect each visitor's smartphone Wi-Fi signal.
- **FortiNAC** network access control provides visibility, control, and automated response for everything that connects to the network.

"To keep up with this business demand, providing good quality and secure OT services organizations need to ensure they have built solid digital foundations."[8]

"State-sponsored hacking groups and hacktivists have a track record of breaking into industrial OT systems causing maximum disruption and damage."[9]

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 using SCADA systems, one can control processes in real time and obtain data from sensors, devices, and other associate equipment. In short, SCADA systems help an organization manage and operate an industrial plant efficiently.[7] A successful attack can be catastrophic, with the potential for massive environmental damage and loss of life.

The Fortinet Security Fabric protects midstream infrastructure with the same integrated cybersecurity, physical security, and secure networking it does for securing upstream infrastructure. For example: 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.

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 third parties. And while some insider attacks may be deliberate, others may be accidental.

The Fortinet Security Fabric secures the downstream infrastructure in the same integrated and holistic way and with the same Fortinet products and solutions that it safeguards the upstream and midstream infrastructures.

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. Accelerated by the 2020 COVID global pandemic, the dispersion of employees from their workplaces led to the great expansion of the hybrid workforce and the need for updating existing work-from-anywhere (WFA) policies and creating new ones. In addition to protecting these resources from external attacks, it is crucial to protect against well-intentioned or malicious insiders exposing confidential data.

> "OT assets must be closely monitored to identify configuration issues and to prioritize vulnerabilities when they are detected."[10]

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 more 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. It eliminates 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.

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.

Finally, the Fortinet Zero-Trust Access architecture supports identifying and having oversight of which users and devices are accessing the network. As more users work remotely and Industrial-Internet-of-Things (IIoT) devices proliferate in OT environments, IT teams are able to continuously verify all users and devices as they access applications and data.

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 is 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 Secure Networking 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 other vendors require as an additional hardware purchase. 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. This infrastructure is supported by integrated artificial- intelligence (AI) and machine-learning (ML) capabilities to help detect and remediate unknown threats.

"To secure SCADA systems, stay alert for issues and prepare accordingly. In today's business world, investing in a strong defense is a necessity."[13]

Fortinet Differentiators

Below are differentiators that make Fortinet cybersecurity solutions 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 are capable of working in complex, remote environments and delivering 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[11] and positioned highest in the ability to execute.[12]

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 nearly two decades of work. To detect zero-day threats, Fortinet has been analyzing files using AI and ML for nearly a decade, 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.

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.

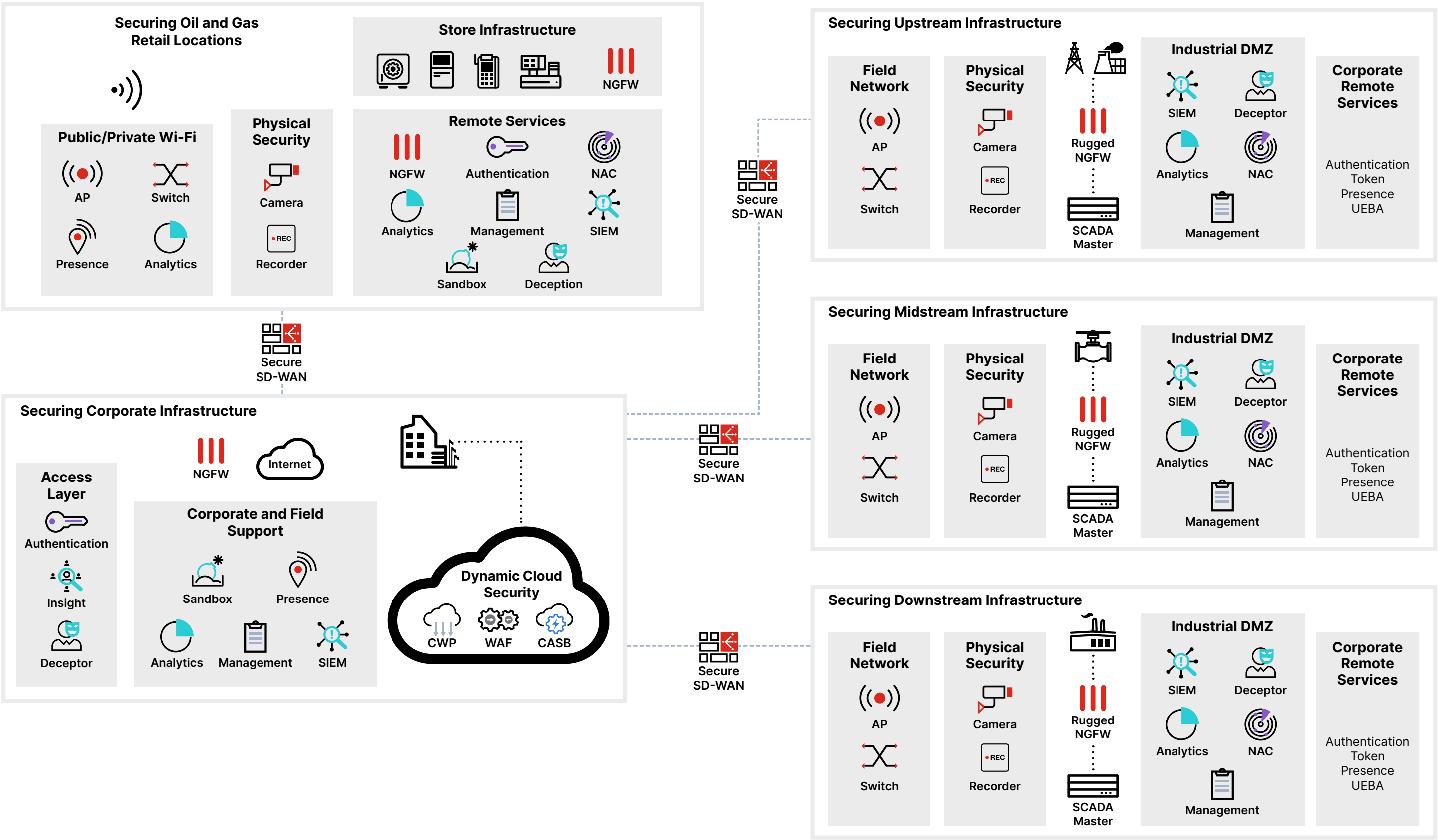

Figure 1: Fortinet cybersecurity solutions for oil and gas companies

[1] Diana Davis, "5 Big Cyberattacks in Oil and Gas," Oil & Gas, November 1, 2022.

[2] "Strengthening Cybersecurity in the Oil and Gas Industry," World Economic Forum, January 19, 2023.

[3] "2023 Oil and Gas Industry Outlook," Deloitte, 2023.

[4] "Strengthening Cybersecurity in the Oil and Gas Industry," World Economic Forum, January 19, 2023.

[5] "Outlook: An industry Reinventing Itself," PwC. 2023.

[6] "2023 Cybersecurity Skills Gap," Fortinet, March 2023.

[7] "Complete Guide to SCADA Security," Security Boulevard, September 25, 2022.

[8] Tomasz Szalach, "We Got It! What Does the Future of Operational Technology Management Look Like?" EY, May 30, 2023.

[9] "Why Failing to Extend Cybersecurity to the Production Line is a Serious Threat to your Business," Petroleum Economist, June 8, 2022.

[10] Ibid.

[11] "Gartner recognized Fortinet a Leader in the 2022 Magic Quadrant for Network Firewalls," Fortinet, December 19, 2022.

[12] Ibid.

[13] 21 Steps to Improve Cyber Security of SCADA Networks, US Department of Energy, 2022