CASE STUDY

How Oil and Gas Producers Tackle Cybersecurity Threats

Cybersecurity is of paramount importance in all kinds of companies. A successful cyberattack could halt operations or put customer information at risk, possibly costing the business huge amounts of money, damaging its reputation in the market, or conceivably even threatening the entity's survival.

For producers of oil and natural gas, the stakes are even higher. In addition to the potential business ramifications, a successful attack that unexpectedly shuts down OT equipment in the energy sector might result in an environmental disaster and injuries or loss of life for employees, bystanders, or nearby residents. Making the situation more dire, petrochemical companies are some of the biggest targets in the world, both for criminals looking for a financial windfall and for nation-states and political activists wanting to interrupt energy supplies in a certain part of the world. Look no further than the highly publicized Colonial Pipeline attack to see the threat oil-and-gas equipment is under.

Security teams in the sector have a tight focus on protecting the safety and reliability of their OT systems, and with very good reason. Oil and gas companies must utilize enterprise-grade security solutions they can easily deploy to remote locations worldwide.

OT-Specific Cybersecurity Threats

Fortinet's "2023 State of Operational Technology and Cybersecurity Report" reveals the prevalence of threats to OT systems.[2] The report is based on a worldwide survey of 570 OT professionals conducted by a respected third-party research company. It reflects that three-fourths of OT organizations reported at least one cyber intrusion in the past year, and nearly a third were victims of a ransomware attack.[3]

OT devices are notorious for their lack of sophisticated internal security controls. They typically do not have the processing or storage capacity to run complex software. Moreover, any controls built into their operating system may be updated infrequently, if ever, because downtime in OT production environments tends to be costly. According to the Fortinet research, fewer than a quarter of companies have encryption or user authorization capabilities on more than 75% of their programmable logic controllers (PLCs) and remote terminal units (RTUs).[4]

In years past, "air-gapped" separation of these devices protected them from any threats not manually delivered to the actual physical equipment. However, digital transformation (Industry 4.0), Internet-of-Things (IoT), and Industrial-Internet-of-Things (IIoT) devices have transformed OT networks, leading to closer connectivity with IT networks and the internet. Equipment often connects to cloud-based solutions for data sharing and analysis. The growing prevalence of 5G technologies makes connectivity possible even for OT devices in remote

75%

The proportion of OT organizations that reported at least one cyber intrusion in the past year.[1]

As manufacturers and other industrial producers connect their IT and OT environments, they gain visibility and improve efficiency in security management. They also introduce potential new threats to devices on both levels. That is a scary thought in a world where attacks targeting OT infrastructure are ever-present.

Details

Industry: Oil-and-gas production

Business Impact

- Increased security and better visibility into security events networkwide
- Effective segmentation of operational technology (OT) and information technology (IT) in compliance with the TSA Cybersecurity Directive

locations. In addition, third parties or employees often require remote access to OT devices for maintenance and troubleshooting. All these trends create new risks for OT networks.

As a result of the convergence of OT and IT over the past several years, FortiGuard Labs Global Threat Landscape Reports have noted an uptick in the detection of malware and malicious activity in OT systems.[5] Oil and gas producers and other OT-reliant organizations see connectivity as the future of efficient operations and key to building a competitive advantage. But that integration eliminates the air gap that previously kept most OT systems safe from cyberattacks.

Attack surfaces within OT organizations have expanded dramatically, and several high-profile attacks emphasize the risk this poses. Russian attacks on Ukraine's critical infrastructure have happened for nearly a decade. In December 2015, a cyber incident later attributed to Russian state actors resulted in widespread outages for Ukrainian power companies.[6] Such attacks have ramped up since Russia launched its ground war on Ukraine in February 2023 as part of what one threat intelligence analyst described as a "persistent, consistent campaign of disrupting Ukrainian critical infrastructure."[7]

Ransomware and other threats cast a dark cloud over companies relying on OT. Amid the gloom, the U.S. Transportation Security Administration (TSA) is lighting a path forward.

Meeting the TSA's Cybersecurity Pipeline Directive

In May 2021, the TSA released a cybersecurity directive for operators of "hazardous liquid and natural gas pipelines or liquefied natural gas facilities."[8] The directive is designed to protect national security, the economy, and public health and safety in the United States from the potential impact of a cyber intrusion that could affect the nation's transportation of crucial fuels.

The TSA security directive requires pipeline owners to take three key actions:

- Establish and implement a TSA-approved cybersecurity implementation plan that describes specific measures the company is using to thwart attacks. The plan should include network segmentation that prevents disruption to OT if the company's IT network is compromised and vice versa. Access control measures and continuous monitoring and detection processes must also be a part of the implementation plan. Development of the plan should entail a systematic identification of critical cybersecurity systems.
- Develop and maintain a cybersecurity incident response plan to reduce the risk of operational disruption and other potential impacts on pipeline capacity in the event of a cybersecurity incident.
- Establish a cybersecurity assessment program and submit a plan describing how the company will regularly assess the effectiveness of cybersecurity measures.

Leading oil and gas producers find that the Fortinet Security Fabric provides the capabilities they need to meet each TSA security directive's requirements. Fortinet's OT solution includes purpose-built hardware that empowers OT network administrators to take advantage of the benefits of IT-OT convergence while continuing to secure their assets. Moreover, across all OT and IT network resources, the Fortinet Security Fabric provides single-pane-of-glass visibility into security events and centralized management of security solutions.

The FortiGuard Enterprise Protection Bundle and a la carte services extend FortiGate Next-Generation Firewall (NGFW) intrusion prevention system (IPS) capabilities to support deep packet inspection (DPI). The FortiGuard OT Security Service also supports more than 70 OT protocols, including over 3,000 application and vulnerability signatures to protect OT networks and devices. The FortiGuard OT Security Service includes more OT IPS signatures than any other cybersecurity vendor offers.

Business Impact (cont.)

- Centralized and automated deployment and management of firewalls and switches bring tremendous staff time savings
- Overlap of services with standalone IPS and other devices enables the retirement of some legacy tools, further enhancing efficiency
- Widespread staff shortages in the industry are easier to manage thanks to efficiency improvements

Solutions

- FortiGate Next-Generation Firewall
- FortiSwitch
- FortiManager

FortiGuard Security Services

- Enterprise Protection Bundle
- OT Security Service

Overall, the Fortinet OT solution effectively supports the cybersecurity asset identification process, streamlines network segmentation, enables access control restrictions, and significantly improves breach detection and response.

Protecting OT All Along a Pipeline

One organization that has turned to Fortinet for help complying with the TSA's cybersecurity directive is a midstream provider of transportation and storage services to the natural gas industry in the southern U.S. A supervisory control and data acquisition (SCADA) system hosted in the organization's data centers manages OT equipment in its compressor stations—devices such as scrubbers, filters, and compressor units. The TSA directive requires that such equipment be completely segmented from the company's IT resources, so the midstream service provider partnered with Fortinet.

The company deployed high-availability pairs of FortiGate NGFWs in its data centers to separate and protect IT and OT traffic. The FortiGuard OT Security Service, an extension of the IPS security service, supports each NGFW. This ensures that all the data center north-south traffic is inspected using industrial signatures, which may reflect specifically OT threats. The company also deployed FortiGate NGFWs and FortiSwitch enterprise switches within its compressor stations to provide Layer 2 segmentation via proxy Address Resolution Protocol (ARP). As a result, the compressor stations' east-west traffic is also inspected with industrial signatures.

The midstream service provider intends to use Fortinet solutions to protect the more than 1,000 metering sites that measure gas flow along its pipelines. It will place a ruggedized FortiGate NGFW in a small cabinet at each metering site to protect its crucial OT equipment from attack.

Drill Down to the Benefits of Fortinet

One of the world's largest petrochemical companies took a similar path when it reached a crossroads with its legacy cybersecurity solutions. The company has locations worldwide that require leading-edge security, and its legacy vendor was not keeping up. Features and functionality were falling behind the competition, so the petrochemical company launched a due diligence process to choose a new security solution set.

Decision-makers selected FortiGate NGFWs and FortiSwitch enterprise switches for their network core for a few reasons. At the top of the list were the capabilities of the FortiGates in blocking and tackling threats. They also liked the performance of the FortiGate NGFWs in terms of throughput and efficiency of management.

The organization has corporate offices to protect oil and gas refineries dispersed globally. The centralized management capabilities facilitated by the FortiOS operating system eliminate the requirement that security team members travel to remote locations to log on to individual firewalls and switches. And the ability to automate firewall deployment further reduces the drag the security infrastructure places on the centralized team.

The facts that the Fortinet solutions are in the Leaders Quadrant of the Gartner® Magic Quadrant™ and that Fortinet offers excellent, high-touch support helped the petrochemical company finalize its decision: It would standardize on FortiGate and FortiSwitch devices for certain areas of its operations.

Protecting Oil and Gas Equipment Around the World

Today, thousands of FortiGate NGFWs are protecting all kinds of devices for the petrochemical company—devices from practically every vendor in the industrial space. Some NGFWs reside at the boundary between IT and OT networks, or Level 3 and Level 4—as defined by the Purdue model for industrial control system (ICS) security—of the company's network. Others protect the gateway, securing outbound traffic to the cloud and all inbound communications. The petrochemical company uses the FortiManager management solution to observe and control the Fortinet infrastructure.

The FortiGate NGFWs protect more than 1,000 locations ranging from refineries to chemical manufacturing plants to standard office environments. FortiGuard OT Security Service and Enterprise Protection Bundle secure all the OT equipment across the company's vast network. Deployment is ongoing for FortiSwitch switches, including ruggedized ones for some harsh industrial locations.

The FortiGate Next-Generation Firewall and FortiSwitch solutions fit well into a broader initiative by which the petrochemical company plans to expand automation throughout its technology infrastructure to improve operational efficiency. The Fortinet solutions accelerate implementation through automated and remote deployment of the FortiGate NGFWs and seamless integration with the FortiSwitches. The FortiOS graphical user interface simplifies security management across all Fortinet devices. In contrast, the inclusion of IPS, web security, content security, and OT and IoT security within the Enterprise Protection Bundle reduces the number of devices the oil and gas company's security team must manage. The FortiGate NGFWs can replace several devices that formerly provided those capabilities. Additionally, reducing reliance on original equipment manufacturers and systems integrators to secure their solutions gives the oil and gas company more control over managing its cyber risk.

In a sector widely known for staffing shortages, these improvements to employee efficiency are business-critical. In addition, the changes introduced by the Fortinet systems may reduce employees' need for external assistance. For the petrochemical company, cutting down on tickets with its managed service providers reduces IT costs.

Great Value for the Investment

Although the petrochemical company has not been using the Fortinet devices long enough to quantify the benefits, IT and OT improvements it is already achieving align with what the midstream service provider and other oil-and-gas companies have realized by rolling out a Fortinet infrastructure. They boil down to building secure connectivity among many locations and effectively segmenting IT and OT networks while streamlining the management of far-flung devices.

These are the same benefits reported by more than 52,000 customers using Fortinet's industrial-built solutions across various geographies and industry sectors, from regional oil-and-gas companies to multinational auto manufacturers to a massive Asian hydropower project. One U.S. business in the waste management and environmental services industry, which has been using Fortinet solutions to protect OT for several years, reports that the Fortinet infrastructure has reduced its overall cost by 65% while bumping up performance to nearly 38 times higher.

As industrial producers bring together Level 3 and Level 4 networking—in other words, bring together OT and IT—they gain visibility and improve efficiency in security management. They also introduce potential new threats to devices on both levels. That is a scary thought in a world where attacks targeting OT infrastructure are ever-present. Segmentation through a next-generation firewall is crucial for oil and gas companies. The right security solutions offer the latest cybersecurity technologies and great value for the investment.

[1] "2023 State of Operational Technology and Cybersecurity Report," Fortinet, May 24, 2023.

[2] Ibid.

[3] Ibid.

[4] Ibid.

[5] "2022 Global Threat Landscape Report," FortiGuard Labs, February 22, 2023.

[6] "Cyber-Attack Against Ukrainian Critical Infrastructure," CISA, July 20, 2021.

[7] Jenna McLaughlin, "Russia bombards Ukraine with cyberattacks, but the impact appears limited," NPR, March 3, 2023.

[8] TSA Memorandum, "Renewal with revision to the Security Directive (SD) Pipeline-2021-02 series: Pipeline Cybersecurity Mitigation Actions, Contingency Planning, and Testing," July 26, 2023.

www.fortinet.com

November 9, 2023 10:32 PM

2421101-0-0-EN