



# Why OT Security is Critical for the Energy Industry

OTORIO enables a more confident and connected energy and oil & gas future. Our OT security platform delivers automated, context-aware industrial OT security risk management for safer and more efficient operations.



# The Importance of OT Protection for Energy Companies


OT cyber security risks in the energy, oil and gas industry are ever-present, with each threat potentially affecting millions of people around the world.

While there has been an increase in industry regulation, there is a long way to go, and this leaves many companies open to attack.

There is also still a significant divide between IT-OT-IIoT posture within the energy, oil & gas industries as old infrastructure and machinery digitize to catch up and better connect with advanced IT.

OTORIO works globally with energy, oil and gas companies and understands the scale of digitizing the industry and implementing a holistic OT security strategy. It is critical for organizations to protect everything they operate across the entire operational environment, bringing IT and OT together to proactively ensure true operational resilience.

OTORIO empowers operations personnel, IT security teams, and CISOs to work together effectively to ensure resilient operations and business continuity.

- 
- **In 2022, over 60% of IT intrusions impacted OT systems.<sup>1</sup>**
  - **How many could have, should have, been prevented?**
  - **67% of OT security professionals are more concerned about ransomware than other intrusions.<sup>2</sup>**

# Energy Industry Overview

The top 5 leaders in the global energy market have a \$3 trillion market cap.<sup>3</sup>  
Some of the most important commodities in the world depend on oil and gas.

Who relies on Oil & Gas	Products and services
Industrial manufacturers	Chemicals, medical (drugs & medical supplies), auto plants, food & beverage
Critical infrastructure	Electricity, water treatment, transit (air/railroad/shipping)
Consumers	Cars, packaged food, clothes, consumer products (TVs, electronics, homes)
Businesses	Computers, furniture, electronics, offices, commercial, retail, entertainment
Governments	Offices, emergency services (police/fire/public transit), schools, playgrounds

**40% share of US electricity is from power plants that rely on natural gas.<sup>6</sup>**



3%

Industry share  
of Global GDP<sup>4</sup>



13%

Energy cost  
of global GDP<sup>5</sup>



# How Energy Companies Are Targeted for Attack



**Phishing**  
Colonial pipeline<sup>7</sup>



**Malware**  
2017 Triton attack<sup>8</sup>



**Ransomware**  
Colonial pipeline<sup>7</sup>



**Device vulnerabilities**  
2017 Triton attack<sup>8</sup>



**Network vulnerabilities**  
IIoT wireless networks<sup>9</sup>



**Espionage**  
Nation-states<sup>9</sup>,  
competitors<sup>9</sup>,  
ransomware gangs



**Internal threats**  
Colonial Pipeline<sup>7</sup>



**Third-party providers' security gaps**<sup>10</sup>

## Colonial Pipeline

The Colonial Pipeline ransomware attack in May 2021 is a stark reminder of how malicious threat actors can exploit cyber security gaps and vulnerabilities to harm energy and oil and gas operational environments. After its IT systems were breached by cyber criminals, the company halted production, distribution operations, and deliveries for five days until it paid millions in ransomware, restored its affected systems, and got operations up and running again.<sup>7</sup>

## Wind-Energy cyber attacks

Three Germany-based wind-energy companies were victims of cyber attacks shortly after Russia invaded Ukraine.<sup>11</sup>

# Who Conducts Oil & Gas Cyber Attacks?



## Nation-states

### Motivation:

- Geopolitics<sup>12,13</sup>
- Espionage
- Economic damage
- Harm government, civilians, and industry



## Advanced Persistent Threat (APT) Actors

### Motivation:

- **Financial**<sup>14,15</sup>  
(ransomware, extortion, blackmail)
- Data theft<sup>14</sup>
- Terrorism<sup>16</sup>
- 'Hired guns' acting for nation-states<sup>17</sup>



## Employees Current & Former

### Motivation:

- Lack of knowledge
- Grievances
- Espionage
- Financial gain



## Hacktivists

### Motivation:

- Political protest<sup>15,18</sup>
- Social protest<sup>18</sup>
- Economic grievances<sup>15,18</sup>

The U.S. is currently the world's top producer of oil and natural gas energy, according to the Council on Foreign Relations.<sup>19</sup> America surpassed Saudi Arabia's oil production in 2018, and overtook Russia's natural gas production in 2011.<sup>20</sup> When Russia invaded Ukraine in 2022, the U.S. became the world's largest exporter of liquid natural gas (LNG).<sup>20</sup>

# Key OT Security issues for the Energy Industry

Energy companies, especially oil and gas, face OT security risks that can impact operations and result in downtime that affects supply chains:



## Visibility

Real-time visibility of asset inventories and processes is increasingly complex. It is vital to understand operational context, including the asset's role and impact on the environment.



## Excessive noise and alert fatigue

Many OT security tools generate high volumes of low-priority and irrelevant risk alerts that creating a flood of noise and alert fatigue for security professionals.



## Safety

Worker and operational safety are critical issues that impact employees, uptime, regulatory compliance, insurance qualification, and more.



## Cyber insurance

The high level of potential cyber risks and consequences means that oil and gas companies find it difficult to obtain cyber insurance. To qualify, they must rigorously quantify and assess risk, and maintain regulatory compliance at all times.



## Maximizing availability and operational continuity<sup>21</sup> by preventing interruptions and downtime that impact

- Supply chains and deliveries
- Revenue loss

## Case Study:

# Eliminating Real-World Alert Fatigue at an Oil Refinery

A U.S. oil and petrochemical refinery with geographically-dispersed assets invested in OT cyber security solutions, but its security team experienced alert fatigue from them due to a high volume of false-positive security notifications. The flood of security alerts and an inability to accurately prioritize them was a major challenge that needed to be solved.

OTORIO's OT security platform transformed the way data sources were presented to show only legitimate, relevant, and high-priority alerts that impact operations and business (e.g., 76 high-priority alerts out of 27,000+ events).

**Read the case study** to see how OTORIO's OT security platform helped the oil refinery eliminate alert fatigue.

**Raw asset information**  
PLCs, RTUs, Sensors

**Security systems**  
EDR, Firewall, NAC, AD, SRA

**Industrial solutions**  
OPC, DCS, Historian

**Logs**  
Windows event logs, Servers, HMI

**Network monitoring**  
IDS, Traffic, Netflow



**27,000+**  
Events

- Excluding Ghost
- External Multicast
- Broadcast assets



**2,441**  
Indicators

Turn data source legitimate alerts into indicators (non-working hours, legitimate tasks got verified, etc.)



**76**  
Alerts

Represent alerts that should be addressed or checked (repetitive, high impactful assets, abnormal behavior)



**29**  
Insights

Correlate insights based on indicators and alerts (pattern based analysis, defined insights, etc.)



- **Improved MTTD** (Mean Time To Detect)
- **Improved MTTR** (Mean Time To Response) with automated mitigation steps
- **OT context-based prioritization**

# Partner and Client Testimonial

OTORIO has extensive global OT industrial-native cybersecurity experience working with energy companies, critical infrastructure operators, and industrial manufacturers.

We proudly enable a confident and better-connected energy future via automated, context-aware cyber risk management for safer, more efficient operations. Our energy clients are diverse; they include oil and gas, electric power, hydroelectric power, solar power, wind power, mining, and other companies.

**“Before being introduced to OTORIO’s solution, it was hard to detect real security threats due to the high volume of false-positive security alerts created by our existing IDS solutions. OTORIO’s OT security platform managed to present only relevant alerts, reducing alert noise so that the security team can focus and prioritize efforts where they are most needed.”**

OT Manager,  
U.S.-based energy and refining company



# Achieve Operational Resilience with OTORIO

OTORIO's OT security platform efficiently enhances the security posture of energy operational environments, including oil and gas downstream and midstream settings.



**Empowers the proactive identification, management, and mitigation** of risks that impact physical operations, supply chains, and revenue



**Equips IT and OT teams with clear, practical mitigation playbooks** and expert-defined guidance for oil and gas OT environments



**Orchestrates data from cross-domain sources** to provide consolidated visibility of the entire OT network and enhance the security posture



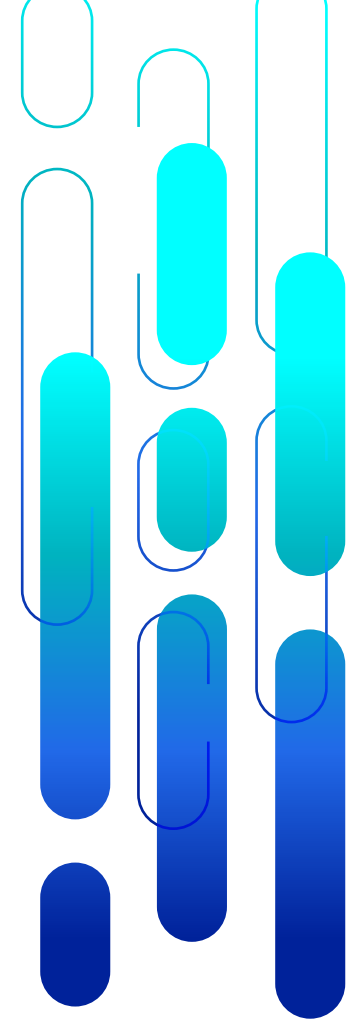
**Contextualized risk prioritization identifies the most important risks** first to ensure operational processes remain safe and efficient



**Prevent downtime and financial losses** via proactive risk management to ensure your operational environment is ransomware-ready

# References

- 1 [2022 State of Operational Technology and Cybersecurity Report](#), Fortinet, June 21, 2022
- 2 Id.
- 3 Aramco, Exxon Mobil, Chevron Corp., Reliance Industries, Ltd. Shell, plc (Publicly available data as of Jan. 17, 2023)
- 4 [Why do oil prices matter to the global economy? An expert explains](#), World Economic Forum, Feb.16, 2022
- 5 [Energy Costs Set to Reach Record 13% of Global GDP This Year](#), Bloomberg, Mar. 16, 2022
- 6 [Russian hacking threat hovers over U.S. gas pipelines](#), Politico, Mar. 2, 2022
- 7 [Hackers Breached Colonial Pipeline Using Compromised Password](#), Bloomberg, Jun. 4, 2021
- 8 [Cybersecurity Threats Facing the Oil & Gas Sector](#), OTORIO, Oct. 14, 2020
- 9 [Hacked](#), Houston Chronicle, March 3, 2017
- 10 Market Guide for Operational Technology Security, Gartner, by K. Thielemann, W. Voster, et al. 4 Aug. 2022 - ID G00743794
- 11 [European Wind-Energy Sector Hit in Wave of Hacks](#), The Wall Street Journal, April 25, 2022
- 12 [A perfect cyber storm against critical infrastructure](#), Daniel Bren, OTORIO, April 4, 2022
- 13 [Pro-Iranian hackers attack Israeli gas company website](#), Jerusalem Post, Oct. 9, 2022
- 14 [Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data](#), Lillian Ablon (Rand Corp.), Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, on March 15, 2018.
- 15 [Meet the Environmental Hacktivists Trying to ‘Sabotage’ Mining Companies](#), Vice, Aug. 16, 2022
- 16 [Nasrallah warns Hezbollah missiles are ‘locked on’ offshore Israeli gas field](#), Times of Israel, Sep. 22, 2022
- 17 [Assessing Russia’s role and responsibility in the Colonial Pipeline attack](#), Atlantic Council, Jun. 1, 2021
- 18 [Rivers community protests neglect by oil firm, demands N120m damages](#), The Guardian (Nigeria), Jan. 12, 2022
- 19 [How the U.S. Oil and Gas Industry Works](#), Council on Foreign Relations, Aug. 11, 2022
- 20 [The United States became the world’s largest LNG exporter in the first half of 2022](#), U.S. Energy Information Administration, July 25, 2022
- 21 [Offshore Oil and Gas: Strategy Urgently Need to Address Cybersecurity risks to Infrastructure](#), U.S. Gen. Accounting Office, GAO-03-105789.



## About Us

OTORIO pioneered an industrial-native OT security platform that enables our customers to achieve an integrated, holistic security strategy for industrial control systems (ICS) and cyber-physical systems (CPS).

Together with our partners, we empower operational security practitioners to proactively manage cyber risks and ensure resilient operations. OTORIO's platform provides automated and consolidated visibility of your entire operational network, enables you to take control of your security posture, eliminate critical risks, and deliver immediate business value across your organization.

Our global team brings the extensive mission-critical experience of top nation-state cyber security experts combined with deep operational and industrial domain expertise.

Visit [OTORIO.com](https://OTORIO.com)

