ONAPSIS

ERP Security for Oil and Gas Companies

Cyber attacks are targeting ERP applications within the oil and gas industry. These attacks can have financial and reputational impact and result in outages causing great human costs. They can disrupt oil and gas production, refinement, transportation, and delivery and put customer personally identifiable information (PII) at risk.

Oil and gas companies need to protect against these attacks while modernizing their systems and complying with an ever increasing number of government regulations.

$4.7M average cost of energy industry breach[1]

94% of energy industry breaches impacted personal data[2]

33% of energy industry data breaches espionage driven[3]

Key Risk Factors

Increasing ERP System Attacks

Cyber attacks targeting ERP systems of oil and gas companies are on the rise, and successful attacks have the potential to disrupt the flow and delivery of oil and gas and put customer personally identifiable information at risk.

Cloud Migration and Modernization

Organizations are migrating to the cloud and focused on modernizing systems that are linked to system data including gas/oil production, employee, and partner data. This gives them the ability to reduce costs, more easily create new applications to operate more efficiently and streamline processes.

Increased Government Regulation

Oil and gas companies are considered critical infrastructure and must comply with new oversight and regulation. Additional environmental legislation creates additional compliance headaches. Failure to comply can result in significant financial impacts to the organization as well as loss of reputation.

Key Challenges

Lack of Visibility

Security teams are challenged to understand ERP applications and their risk profile to secure disparate systems across the business. Teams lack adequate ERP tools and resources to discover these systems as well as new or migrated cloud assets.

Under-Resourced Teams

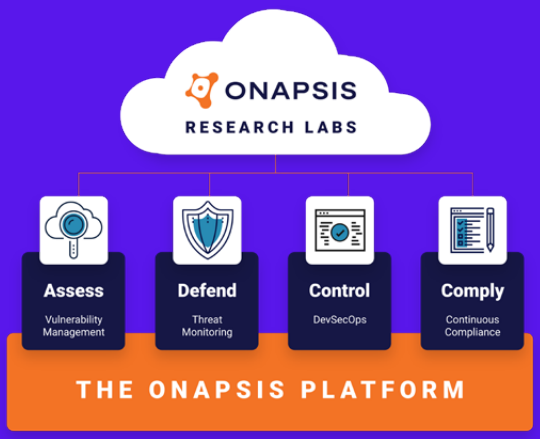
Workforce shortages in the security industry are further compounded by the difficulty of hiring staff in the oil and gas industry. Reduced budgets and cost pressures have also negatively affected the ability to hire and train staff.

Alignment of Security to Compliance

Compliance audits are mandatory and frequently result in time-consuming manual processes. Aligning security controls to compliance requirements for data and authentication for ERP systems can be a resource-intensive process.

[1] IBM Security Cost of a Data Breach Report 2022
[2] Verizon 2021 Data Breach Investigations Report
[3] Verizon 2021 Data Breach Investigations Report

Solution:
Onapsis Provides a Better Approach to ERP Security



Fortunately, securing your complex ERP landscape doesn't have to be complicated, even with all the advanced threats and attacks out in the wild. That's where Onapsis comes in. As the undisputed experts in business application security with the most prolific threat research team for SAP and Oracle, Onapsis has been on the frontlines securing the world's leading oil and gas companies for over a decade now. With Onapsis, you get complete 360 degree security for your critical ERP applications, helping you.

- ☑ Automate your ERP security helping you reduce time and resource costs for compliance audits
- ☑ Gain research-driven analysis and focused threat intel from industry experts, so even teams new to ERP security can quickly and effectively comprehend and act on risk
- ☑ Integrate with ticketing systems and SIEMs to bring ERP security into existing processes and SOC playbooks

Case Study

F1000 Gas Company Builds SAP Vulnerability Management Program, Reduces Remediation Time by 80%

Challenge: The company heavily relies on SAP applications for their business-critical processes, but the company had zero visibility into the actual security posture of these applications. They had a long, complicated patching process, and their existing vulnerability management solution and SAP tools didn't give them what they needed to effectively protect their value chain

Solution: Onapsis provided comprehensive, focused vulnerability management designed for SAP applications. Automated assessments, detailed solutions, and descriptions of business impact enabled the organization to easily identify and prioritize their risk, leading to a greater understanding of how to best respond while streamlining their patching process and reducing their overall time and costs while preparing for FERC compliance audits.

80%
Reduction in mean time to remediate (MTTR)

90%
Less time spent on patching

60%
Reduction in investigation time

Learn more about how Onapsis **helps oil and gas companies protect the systems and data supporting their ERP** and other business-critical operations from SAP and Oracle.

ONAPSIS

onapsis.com/oil-and-gas