Defend energy infrastructure against sophisticated cyberattacks

Gain 360-degree visibility to protect critical systems and reduce operational risk

Energy and resource corporations face increasing pressure to strengthen cybersecurity as hackers target oil and gas, utilities, chemicals, metals and mining, and other industrial infrastructure. With attacks reaching record highs and the average data breach costing $4.7 million,[1] organizations need smarter cybersecurity approaches that bridge IT and OT systems to ensure energy flows safely and securely.

1 **Prevent costly operational disruptions** like the Colonial Pipeline attack, which halted 2.5 million barrels of fuel daily, costing $225 million per day in losses while threatening the safety of employees, communities, and the environment.

2 **Gain comprehensive security visibility** across endpoints and network traffic to identify, triage, and investigate anomalous behavior before it impacts operations or leads to expensive "all-hands-on-deck" emergency responses.

3 **Bridge IT and OT security gaps** by integrating cybersecurity practices across operational technology systems that have traditionally focused on sophistication rather than protection against modern threats.

4 **Reduce security alert fatigue** as demonstrated by Dubai Electricity and Water Authority, which achieved a 30% reduction in alarms by embracing modern technologies and establishing an advanced security operations center.

5 **Detect and respond to threats in near real-time** with automated orchestrated responses that minimize damage by quickly identifying genuine threats and immediately implementing protective measures.

6 **Simplify security management** by consolidating vendors to reduce complexity and improve risk mitigation through comprehensive security platforms.

7 **Deploy AI-powered threat detection** that combines machine learning models with new detection approaches to automate responses to emerging threats and enable sophisticated behavioral threat hunting.

8 **Protect valuable energy data** with encryption of sensitive information at rest and in transit, preventing unauthorized access while ensuring regulatory compliance with NIS2 and other industry standards.

Resources

Learn more ›

[1] IEA.org, *Cybersecurity—is the power system lagging behind?,* July 2021

Copyright © 2025 Open Text • 05.25 | 269-000059-001