Protect critical energy and resources infrastructure against sophisticated cyberthreats

Comprehensive cybersecurity solutions establish 360-degree visibility across your organization, reducing operational risk, minimizing downtime, and maintaining compliance

Benefits

- Combat rising, sophisticated cyberattacks with adaptive defense
- Reduce security alarms by as much as 30 percent[1] to improve response
- Feel secure with the same protection trusted by 78+ million end users across 180 countries

Energy and resources corporations in oil & gas, utilities, chemicals, metals & mining, and engineering & construction face increasingly sophisticated cyberthreats. Energy assets account for a third of all incidents since 2017 and electricity networks make up a quarter.[2] Penalties for failure are massive. In 2024, a single attack on an energy firm lead to a $35 million USD loss.[3]

Gain comprehensive visibility across converging IT and OT systems

Smart oilfields, grids, and other industrial assets are only “smart” if they’re secure. As information technology and operational technology systems converge, organizations need cybersecurity solutions that provide 360-degree visibility across endpoints and network traffic. This comprehensive approach ensures energy flows safely and securely while protecting sensitive information from both external threats and insider risks.

1 OpenText, *Dubai Electricity and Water Authority success story*
2 PCIM News Platform, *Energy sector: more cyber attacks in 2022 than ever before*, 2023
3 SC Media, *5 critical infrastructure sectors hit hardest by cyberattacks in 2024*, 2024

Resources

Learn more ›

Deploy AI-powered detection to identify threats before damage occurs

Advanced threat detection capabilities combine new approaches with machine learning models to protect infrastructure from evolving threats. By reimagining cybersecurity with automated detection and response while enabling behavioral threat hunting, energy organizations can identify malicious activity earlier. Transforming security from reactive to predictive significantly reduces response time and limits potential damage.

Reduce complexity with an integrated cybersecurity framework

Energy and resource companies struggle with vendor sprawl that increases total cost of ownership for security investments. An integrated framework addressing network security, identity management, data protection, application security, and more delivers improved protection with less complexity. This comprehensive approach helps close security gaps without requiring costly “all hands on deck” scenarios.

Strengthen resilience against geopolitical and infrastructure risks

From the $225 million USD per day Colonial Pipeline shutdown to the $50 million USD Saudi Aramco cyber extortion,[4] attacks on energy infrastructure have had devastating consequences. Smarter cybersecurity embraces resilience and volatility management, ensuring systems can withstand pervasive disruptions and geopolitical risks while safeguarding the integrity of sensitive information.

Conclusion

The OpenText™ Cybersecurity Cloud protects more than 800,000 businesses across 180 countries with full-stack security solutions that address all critical components of a comprehensive program. As the world leader in information management, we serve thousands of energy and resources companies in their information management journey to organize, connect, protect, and automate data flows.

No platform is more secure or scalable to manage high volumes of information throughout the industrial asset lifecycle.

4 Power & Beyond, *More cyber attacks in 2022 than ever before,* 2023

opentext™