opentext™

POINT OF VIEW

Cybersecurity reimagined for energy and resources

Protect critical infrastructure with AI and security embedded everywhere at scale, with enterprise strength

Business backdrop

The energy and resources sector is facing a critical inflection point. Cyberattacks on utilities, oil and gas, chemicals, metals and mining and other industrial operators have surged, with ransomware attacks jumping by 46 percent from Q4 2024 to Q1 2025.[1] High-profile incidents like the Colonial Pipeline shutdown and the $50-million extortion of Saudi Aramco underscore the sector's vulnerability and the potential for catastrophic operational and economic consequences.

As energy and resource companies accelerate digital transformation and deploy smart, connected assets, their cyber risk exposure expands dramatically. The convergence of IT and OT systems—often built on legacy infrastructure—creates complex vulnerabilities that adversaries are increasingly exploiting. Regulatory mandates like the NIS2 Directive, Executive Order 13800, and frameworks such as NIST CSF and ISA/IEC 62443, are pushing organizations to adopt more integrated, risk-based cybersecurity strategies. Yet, many still rely on fragmented tools, lack real-time observability, and struggle to scale secure operations across hybrid environments. To stay ahead, organizations must anticipate cyber risk with advanced insights, protect against emerging threats, and simplify security with robust, unified platforms.

"By taking a different approach to visualizing our risk themes, embracing modern, business-enabling technologies such as OpenText Threat Detection and Response, and establishing an advanced Security Operations Center (SOC), we have experienced a 30 percent reduction in alarms, ensuring our resources are directed most effectively."

Jacob Jacob, Cybersecurity Specialist, Dubai Electricity & Water Authority

[1] Honeywell.com, Ransomware attacks targeting industrial operators surge 46% in one quarter, 2025

"With OpenText Enterprise Security Manager, we don't just detect real attacks quickly—we also automate orchestrated responses in near-real time."

Dmitriy Ryzhkov, Senior Information Security Analyst, NPC Ukrenergo

Smart industrial facilities and infrastructure are only smart if they're secure

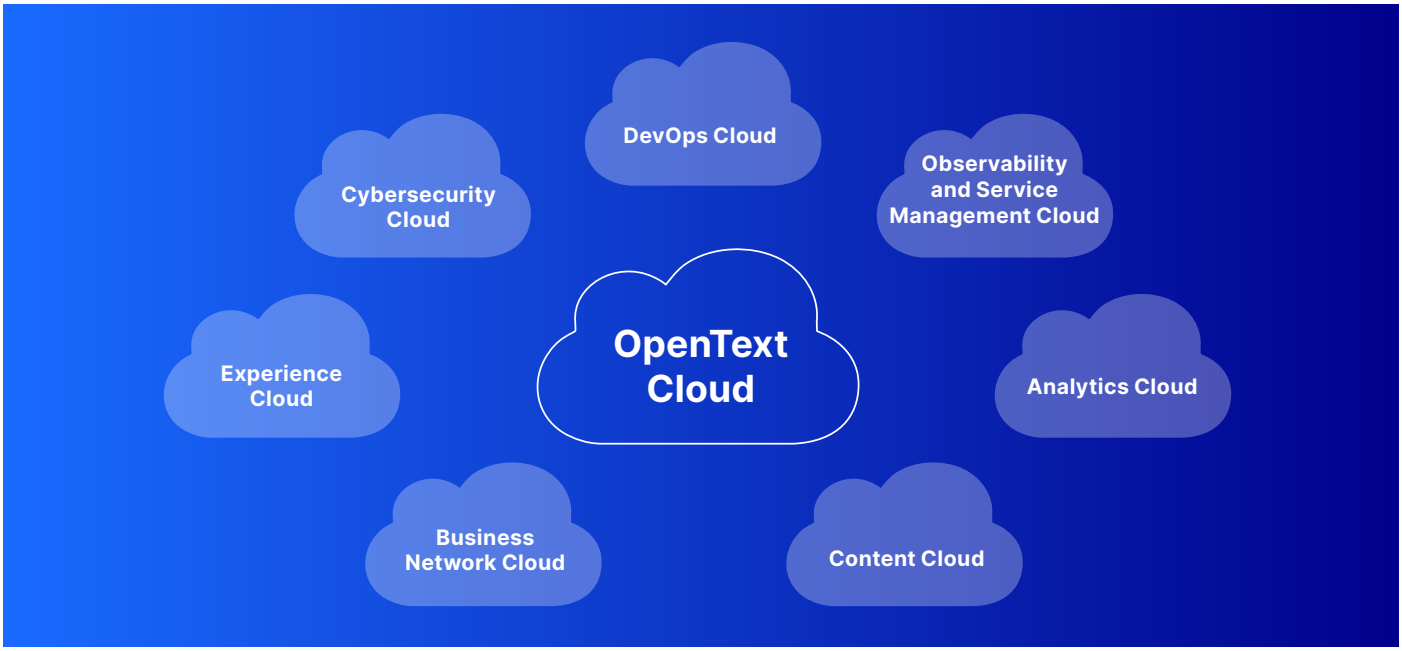
As cyberattacks surge across energy and industrial sectors, the growing interdependence between digital systems and physical operations exposes critical vulnerabilities. Vendor sprawl and siloed systems further complicate efforts to secure infrastructure and meet compliance mandates. Regulatory pressure is rising, but many organizations still lack unified visibility and control. Leaders must act now to anticipate risk, protect operations, and simplify cybersecurity before the next breach defines their future.

OpenText vision

OpenText envisions a future where cybersecurity is not just a defense mechanism but a strategic enabler of operational resilience and digital transformation. Our integrated approach combines AI-powered threat detection, full-stack observability, DevSecOps, and automated service management to help energy and resources organizations stay ahead of evolving threats.

With OpenText, energy and resource companies can:

- **Detect and neutralize threats in real time** using AI-driven analytics and behavioural threat hunting.
- **Accelerate secure innovation** by embedding security into DevSecOps pipelines, ensuring compliance and agility from code to deployment
- **Automate and orchestrate cybersecurity operations** with AI-powered workflows that reduce mean time to respond (MTTR) and improve SLA performance.
- **Remediate vulnerabilities and incidents faster** by integrating with third-party scanners, prioritizing risks using CVEs and EPSS scores, and automating patching and incident response at scale



OpenText solutions

OpenText solution	Benefits
Cybersecurity Cloud	Protect industrial operations with AI-driven threat detection and full-stack protection to reduce risk, accelerate response, and ensure compliance
DevOps Cloud	Embed security into development with automated DevSecOps to reduce risk, ensure compliance, and accelerate secure software delivery
Observability and Service Management Cloud	Unify insights and automate service operations to boost resilience, reduce downtime, and accelerate issue resolution across hybrid environments.
Analytics Cloud	Deliver smart, scalable, and secure insights with AI-driven analytics to enhance industrial performance, efficiency, and data security
Content Cloud	Securely integrate content and systems to streamline processes, deliver knowledge faster, and enhance work with AI-powered productivity and governance.
Business Network Cloud	Securely integrate people, processes, and things to automate operations and collaborate seamlessly across your entire industrial and supply ecosystem.
Experience Cloud	Optimize internal and external customer journeys with data-driven insights, empower teams to deliver value, and engage customers through personalized, preference-based experiences.
Thrust	Build secure, custom applications using proven OpenText information management technology

Business outcome

By implementing OpenText's integrated cybersecurity and information management solutions, organizations across the energy and resources sector can expect measurable improvements in both security posture and operational efficiency:

- **Stronger cyber resilience** through AI-driven automation, reducing the impact and frequency of security incidents.
- **Reduced operational risk** by consolidating vendors and achieving unified visibility.
- **Improved compliance** with global regulations like NIS2, GDPR, and Executive Order 13800.
- **Increased workforce productivity** through automated service management and secure, streamlined DevSecOps practices.

These outcomes translate into tangible business benefits: fewer outages, faster recovery, reduced costs, and stronger stakeholder trust. OpenText's approach helps organizations move from reactive defence to proactive resilience—ensuring that smart industrial operations remain secure, compliant, and operational.

"Just as every safety incident is preventable, so too are cyber breaches that disrupt operations and erode trust. The root cause of many security failures lies in fragmented systems, limited visibility, and reactive defenses. By embedding intelligence, automation, and resilience into cybersecurity, we can protect critical industrial operations—safely and securely."

— Phil Schwarz, OpenText Industry Strategist – Energy and Resources

Next steps

We invite you to continue the conversation with OpenText. Let's co-develop a roadmap to enhance your cybersecurity and information management maturity and align it with your digital transformation goals. Recommended next steps include:

- **Introductory meeting** with your security leadership and OpenText's Global Account Director or Sr. Account Executive.
- **Joint roadmap exchange** to align on cybersecurity priorities and explore solution fit.
- **Business Value Consulting workshop** to assess current gaps and quantify the impact of smarter cybersecurity.

Why OpenText?

OpenText is the global leader in information management, serving thousands of energy, utility, chemical, metals and mining, and EPC companies worldwide. Our secure, scalable information management platform is designed to manage the world's most complex data environments—empowering organizations to safely deliver energy and essential commodities to the world.

Contact us

Phil Schwarz
Sr. Industry Strategist - Energy and Resources
OpenText

pschwarz@opentext.com

opentext™