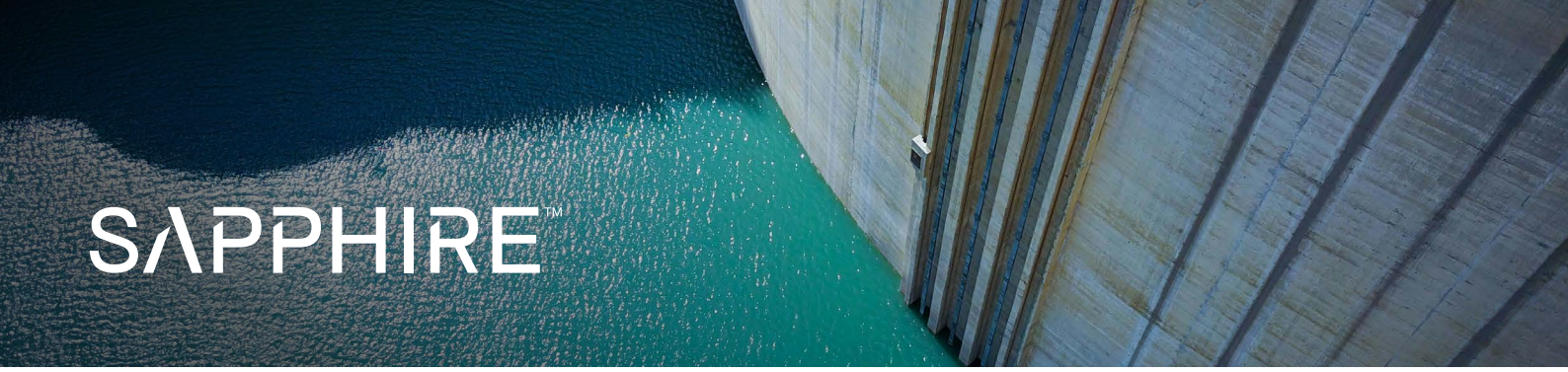

SAPPHIRE™

Safeguarding Our Powerhouses: Architect a Secure Energy Landscape

Energy companies in the industrial sector, spanning oil, gas, and renewable energy, play a key role in providing the essential resources needed to power our economies and meet consumer demands.

Its activities encompass diverse processes, each with their own distinct set of assets, critical infrastructure, and security requirements.

Oil and Gas

Oil and gas companies explore, extract, refine, and distribute fossil fuels. Their assets include vast oil and natural gas reserves, drilling rigs, refineries, pipelines, and storage facilities. The critical infrastructure involves offshore and onshore drilling platforms, refineries, petrochemical plants, and an extensive network of pipelines for transportation. Security requirements are robust, given the industry's geopolitical significance and the potential impact of disruptions. These requisites include securing drilling sites, implementing cybersecurity measures to protect operational technology (OT), and maintaining stringent safety protocols to prevent accidents.

Renewable Energy

Renewable energy companies focus on harnessing energy from sustainable sources such as wind, solar, hydro, and geothermal.

Their assets include wind turbines, solar panels, hydroelectric facilities, and geothermal power plants. Critical infrastructure encompasses renewable energy installations, often distributed across various locations. Security requirements involve protecting these plants from physical and cyber threats. While the environmental impact is a concern, ensuring the secure operation of control systems and protecting against cyber threats is paramount. This includes implementing cybersecurity measures specific to industrial control systems (ICS) and ensuring the resilience of smart grids.

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001

Shared Security Requirements

Although they may have bespoke security requirements, a shared set of security requirements exists across all three segments of the energy sector.

IT/OT Infrastructure Security

With increased digitisation and reliance on IoT devices, robust security measures are required to secure IT and OT systems to protect energy companies from emerging cyber threats that target critical infrastructure. Furthermore, compliance with industry standards such as ISO27001 and ISA/IEC 62443 is important to ensure they remain robust to adversarial pressures in their sector.

Physical Security

Protecting physical assets, including drilling sites, refineries, power plants, and energy distribution infrastructure, is essential to minimise widespread disruption that can impact local and nationwide populations. Using stringent access controls, surveillance systems and perimeter security safeguards can mitigate the potential of physical threats to critical infrastructure.

Supply Chain Security

Given the interconnected nature of the energy sector, ensuring the security of the supply chain is vital. This includes vetting suppliers, contractors, and third-party vendors to prevent attacks that originate from the supply chain and mitigate the impact that would be widespread across their service delivery networks.

Incident Response and Continuity Planning

Developing and testing incident response plans to ensure a swift and coordinated response in the event of security incidents, natural disasters, or accidents. The energy sector is often influenced by geopolitical factors, including potential cyber threats from nation-state actors seeking to gain a strategic advantage or influence global energy markets. Having a well-defined and tested business continuity plan that aligns with your business objectives can help you remain resilient from this angle in the face of further adversarial pressure.

Sapphire's Service Offering

Service /Offering	Introductory	Foundations	Intermediate	Advanced
NCSC Guidelines	✓	✓	✓	✓
Standards Compliance Review	✓	✓	✓	✓
Gap Analysis	✓	✓	✓	✓
Security Improvement Planning	✓	✓	✓	✓
Security Awareness & Training	✓	✓	✓	✓
Procedure & Policy Review	✓	✓	✓	✓
Network Configuration Review	✓	✓	✓	✓
Firewall Security Checkup	✓	✓	✓	✓
Framework Review (CyberEssentials, GovAssure)		✓	✓	✓
Information Security Management		✓	✓	✓
Authentication Review		✓	✓	✓
Business Continuity Planning		✓	✓	✓
Disaster Recovery Planning		✓	✓	✓
Incident Response Planning		✓	✓	✓
IT/OT Asset Discovery		✓	✓	✓
Identity & Access Management Review		✓	✓	✓
Threat Assessment		✓	✓	✓
Penetration Testing		✓	✓	✓
Internal/External Audit		✓	✓	✓
Threat Intelligence			✓	✓
Vulnerability Management			✓	✓
Third-Party Risk Management			✓	✓
IT/OT Consultancy			✓	✓
MXDR & Endpoint Management				✓
CISO as a Service				✓
Red Teaming				✓
Breach Attack Simulation (BAS)				✓
SIEM & SOC Advisory Services				✓

To find out more or to speak to an expert contact us today

CONTACT US TO FIND OUT MORE

Or call: 0845 58 27001