Trellix

SOLUTION BRIEF

Securing the Oil and Gas Digital Frontier

For the oil and gas industry, a cyber breach is no longer limited to data loss. It can create operational disruption, safety exposure, environmental risk, and broader national energy security concerns.

Given that ransomware attacks targeting the sector increased by 935% between 2024 and 2025, and unplanned downtime costs an average of $125,000 per hour, oil and gas leaders need a resilient cybersecurity strategy that protects both enterprise IT and mission-critical operational technology (OT).[1,2]

To enable that strategy, Trellix delivers an integrated security architecture that extends from corporate IT to OT-adjacent and critical industrial environments across upstream, midstream, and downstream operations. By combining threat intelligence, endpoint protection, network detection and response, data security, security operations, consulting services, and strategic partnerships, Trellix helps oil and gas organizations strengthen operational resilience, protect sensitive industrial data, and maintain asset availability across the value chain.

Trellix also helps customers improve visibility and control in support of strict regulatory and standards-driven requirements. This includes helping covered pipeline operators align with the U.S.'s TSA Pipeline Security Directives for network segmentation, access control, continuous monitoring, and cybersecurity implementation planning; supporting faster investigation and response for SEC cyber incident disclosure readiness; and helping customers align with ISA/IEC 62443 principles for industrial cybersecurity, including defense-in-depth, network separation, asset visibility, and risk-based security design.

[1] Dragos OT Cybersecurity Report: Adversaries Increase Real-World Impact, Map Control Loops Across Industrial Infrastructure, 2026

[2] IBM, Cost of a data breach: The industrial sector, 2024

Providing integrated solutions tailored for IT/OT convergence

As oil and gas operations become increasingly connected through cloud technologies, remote access, automation, and digital operations, organizations face growing cybersecurity risks across both enterprise IT and industrial OT environments. These risks include:

- Weak IT/OT segmentation
- Legacy OT vulnerabilities and insecure protocols
- Insecure remote access
- Limited asset visibility
- Exposure to ransomware and nation-state threats
- Shortage of specialized OT cybersecurity expertise

Trellix helps address these challenges by delivering integrated cybersecurity capabilities designed for converged IT/OT environments, with a strong focus on endpoint protection, network detection and response, data security, and security operations. Trellix solutions can support fully on-premises deployments, including highly restricted or air-gapped environments, while also extending protection across hybrid and cloud-connected architectures.

This allows oil and gas operators to improve visibility, strengthen protection, detect threats earlier, and respond faster across upstream, midstream, and downstream environments without compromising the availability and stability requirements of critical operations.

Delivering layered detection and response architecture

Unlike fragmented point solutions, Trellix provides an integrated, OT-aware security architecture designed to support uptime, operational control, and cyber resilience. The core of this defense is a layered detection and response framework that brings together endpoint protection, network visibility, threat intelligence, and security operations.

- **Endpoint Security:** Trellix endpoint security solutions help protect servers, workstations, engineering systems, jump hosts, field devices, and OT-adjacent endpoints across upstream, midstream, and downstream environments. These capabilities support prevention, detection, investigation, containment, and recovery, while helping reduce the attack surface through controls such as application control, device control, allow/deny lists, host firewall policies, and forensics-driven response. Trellix can also support on-premises and disconnected deployment models where cloud connectivity is limited or restricted.
- **Network Detection and Response:** Trellix Network Detection and Response (NDR), together with OT ecosystem capabilities from partners such as Nozomi Networks, helps improve visibility across IT, OT, and SCADA-connected environments. By monitoring network communication patterns, identifying suspicious behavior, detecting anomalies, and supporting asset visibility, Trellix helps security teams identify lateral movement, unauthorized access attempts, and advanced threats targeting industrial environments.

- **Security Operations:** Trellix connects endpoint, network, data, threat intelligence, and security operations telemetry through an integrated security platform. AI-assisted capabilities such as Trellix Wise help analysts prioritize critical alerts, reduce alert fatigue, and accelerate investigation and response. For OT environments, this enables security teams to correlate activity across enterprise IT, OT-adjacent systems, industrial networks, and SOC workflows while helping preserve the availability and stability of critical operations.

Together, these capabilities help oil and gas organizations move from isolated detection to coordinated defense across the full value chain, improving visibility, reducing response times, and strengthening resilience against ransomware, unauthorized change, lateral movement, and targeted attacks.

Shielding sensitive data

Oil and gas companies handle large volumes of sensitive and operationally critical information, including pipeline telemetry, seismic data, production records, refinery data, engineering designs, commercial contracts, trading information, customer records, and regulated data.

Trellix helps protect this information through Data Loss Prevention (DLP) and Database Security capabilities that secure data across endpoints, networks, cloud repositories, and databases. These solutions help monitor sensitive data movement, detect unauthorized access, audit database activity, monitor privileged users, and reduce the risk of data leakage.

This is especially important in IT/OT convergence zones where operational data is increasingly shared with enterprise systems, cloud platforms, historian databases, analytics environments, and data lakes. By protecting data both **at rest and in motion**, Trellix helps oil and gas operators safeguard intellectual property, maintain compliance, and reduce the risk of operational or commercial exposure.

Fortifying the full oil and gas value chain

Trellix solutions help address the distinct cybersecurity challenges across upstream, midstream, and downstream oil and gas operations by strengthening protection, visibility, detection, and response across IT, OT-adjacent, and industrial environments.

- **Upstream—Securing the Intelligent Edge:** Trellix helps protect remote exploration and production environments, including offshore rigs, drilling operations, field endpoints, engineering workstations, and contractor access. This includes helping secure data flows from wellhead sensors, field systems, and edge environments to enterprise and cloud platforms, while protecting high-value intellectual property such as seismic data, well data, production data, and engineering designs.
- **Midstream—Enforcing Pipeline Integrity:** To help safeguard highly distributed infrastructure, Trellix improves visibility across pipeline operations, terminals, pumping stations, compression stations, and SCADA-connected environments. Network detection and response, endpoint protection, and threat intelligence help identify suspicious activity, unauthorized access attempts, lateral movement, and potential threats targeting transportation and storage infrastructure.

- **Downstream—Driving Safety-first Refinery Protection:** In refineries and petrochemical plants, where uptime, safety, and process continuity are paramount, Trellix helps protect OT-adjacent systems, engineering workstations, plant endpoints, data repositories, and network traffic. By correlating endpoint, network, data, and security operations telemetry, Trellix helps detect anomalies, prioritize critical alerts, and accelerate investigation and response without disrupting critical industrial operations.

Enhancing security with Trellix consulting and partnerships

Technology alone cannot fully secure highly complex, mission-critical oil and gas environments. Many organizations face gaps in specialized OT cybersecurity expertise, architecture design, deployment readiness, operational governance, and incident-response planning. These challenges become even more critical when security controls must be implemented without disrupting production, safety systems, or plant availability.

Trellix helps bridge this gap through experienced Professional Services, advisory support, and a broad ecosystem of technology and industry partnerships. Trellix Professional Services can help customers assess their current IT/OT security posture, design practical deployment architectures, validate segmentation and visibility requirements, support implementation, tune detections, and align security operations with business and operational risk.

Through consulting-led engagement and partner collaboration, Trellix helps oil and gas organizations move beyond product deployment toward measurable security outcomes, including improved visibility, stronger control of critical assets, faster threat detection, reduced operational risk, and more resilient upstream, midstream, and downstream operations.

Trellix Professional Services

Trellix Professional Services helps oil and gas organizations maximize the value of their Trellix investments through custom scopes of work, deployment expertise, and specialized methodologies designed for complex IT/OT environments. These services help customers assess risk, design resilient architectures, implement controls, and operationalize security without compromising uptime, safety, or production continuity. Key services include:

- **OT Environment Assessments and Inventories:** Trellix consultants support OT security assessments, asset visibility reviews, baseline analysis of network and endpoint behavior, and IT/OT segmentation reviews. These activities help reduce the risk of enterprise-side compromises spreading into production environments and improve the customer's understanding of critical OT dependencies.
- **Incident-response Readiness:** Trellix experts help develop OT-aware incident-response playbooks, escalation models, and response templates aligned to industrial operating requirements, safety considerations, and applicable regulatory obligations. This helps security and operations teams respond faster while minimizing disruption to critical systems.
- **Data Security Rollouts:** Trellix Professional Services can support data classification initiatives, database risk assessments, and DLP policy design for sensitive oil and gas data, including seismic data, well data, production data, engineering documents, commercial contracts, and operational records. These services help reduce the risk of intellectual property exposure and unauthorized data movement.

- **Continuous-monitoring Deployments:** Trellix consultants assist with the deployment and configuration of endpoint, EDR, NDR, and security operations capabilities across upstream, midstream, and downstream environments. Services may include sensor placement guidance, detection tuning, integration with SOC workflows, threat-hunting enablement, and operational handoff to internal SOC teams or managed service partners for ongoing monitoring.

Strategic OEM and integrator partnerships

Trellix collaborates with technology partners, OEMs, system integrators, and managed service partners to help oil and gas organizations extend security across complex industrial environments. These partnerships are especially important in OT environments, where cybersecurity controls must be deployed carefully to preserve safety, uptime, system integrity, and vendor supportability.

- **OEM and Technology Partners:** Trellix works with technology and infrastructure partners to help align security controls with industrial architectures and operational requirements. Where supported by the customer's architecture and vendor ecosystem, Trellix capabilities can help strengthen endpoint protection, access control, data protection, encrypted communications, and monitoring across OT-adjacent systems, engineering workstations, servers, and critical operational infrastructure. This helps improve resilience while supporting operational integrity and compliance requirements.
- **System Integrators:** Trellix partners with system integrators that understand oil and gas operations, OT networks, SCADA environments, and industrial deployment constraints. Through partner enablement, architecture collaboration, and delivery support, Trellix helps system integrators plan and execute safer deployments across areas such as OT security assessments, asset visibility, endpoint protection, network monitoring, segmentation reviews, SOC integration, and operational handoff.

Together, these partnerships help customers move from isolated technology deployment to a coordinated security model across upstream, midstream, and downstream operations.

Conclusion

By combining a unified security architecture with deep consulting expertise and a strong partner ecosystem, Trellix helps oil and gas leaders protect their operations, people, data, and reputation. Whether operating in isolated or air-gapped environments, remote upstream locations, highly distributed pipeline networks, or converged IT/OT environments, Trellix provides the visibility, protection, threat detection, and response capabilities needed to strengthen operational resilience.

With Trellix, oil and gas organizations can reduce cyber risk across the full value chain, improve security operations, protect sensitive industrial data, and support safer, more resilient upstream, midstream, and downstream operations.

To learn more, contact us or visit trellix.com.