EXECUTIVE BRIEF

FROM CODE TO CONTROL

Mastering the Software Supply Chain in the Oil, Gas and Energy Sector

Overview

The Energy, Oil, and Gas industries are undergoing a digital transformation, but the shift introduces complex challenges in their software development and application security practices. For utilities, ensuring the safety and reliability of critical infrastructure is paramount, making robust security solutions a necessity, not an option. From managing embedded systems in remote substations to complex refining control software, this sector faces unique challenges in the management, security, and regulation of its software supply chain.

The New Standard: Why Universal Reliability and Traceability are Non-Negotiable

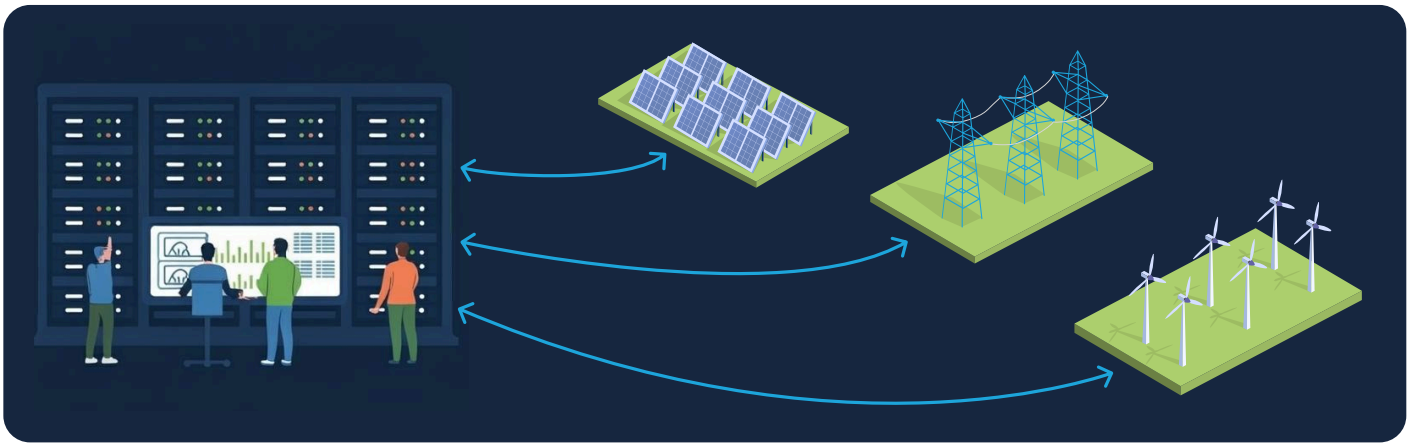
In the Energy, Oil, and Gas sectors, the distance between a developer's workstation and a remote edge device isn't just measured in miles - it's measured in risk. When software governs the flow of a pipeline or the stability of a power grid, the "move fast and break things" mentality is not an option.

To bridge this gap, DevSecOps teams are moving beyond basic security measures to Universal Reliability and Traceability (UR&T). This isn't just a workflow; it is a unified chain of custody that spans the entire software supply chain, ensuring that every binary, artifact, and dependency is accounted for from code creation to final deployment.

Ensuring Energy Continuity: How UR&T Protects the Software Supply Chain

Today's IT/OT software supply chain has become a key target for sophisticated threat actors. For utility providers, a single compromised open-source library can cause a shutdown of the entire grid.

UR&T addresses the expanding threat landscape by embedding security into every phase of the SDLC. By leveraging continuous security monitoring integrated with metadata integrity, the origin of every software artifact is identified and documented in the latest Software Bill of Materials (SBOM). This level of granularity allows security teams to move from reactive patching to proactive governance. If a critical vulnerability is discovered post-deployment, you don't have to hunt for it, but can instantly identify every instance of that component across all applications and enable remediation at source.



Ensuring Integrity from the Data Center to the Rig

In Operational Technology (OT) environments, the integrity of a deployment is paramount. A single corrupted instruction transmitted to a remote offshore rig could lead to catastrophic equipment failure or unexpected downtime. The question isn't just "did it deploy?" but "can we trust what we received?"

By implementing immutable artifact identification, JFrog ensures that the binary used in your application is the exact, bit-for-bit match of the one approved in your hardened CI/CD pipeline. Through rigorous checksum verification, utilizing standards like SHA-256, we eliminate the risk of tampering or accidental corruption. This creates a "gold standard" of deployment, guaranteeing that only authorized, tested, and verified code reaches your most critical assets.

Turning Compliance from a Burden into a Competitive Edge

For the Energy and Utilities sectors, meeting regulatory standards is a must-have. Traditionally, proving the security and quality gates of software running in sensitive environments has been a manual, months-long forensic exercise.

Universal Reliability and Traceability transforms this process by providing a digital audit trail that captures every action as immutable metadata, which can be leveraged to generate a complete traceability report for any asset on demand. Whether an auditor asks about software that you developed, that is running on a specific substation or a global fleet of sensors, you can provide immediate proof of what is running, who approved it, and even the scanning history to prove its integrity. This shifts the focus from "preparing for the audit" to maintaining continuous, automated compliance records available on demand.

Energy Software Supply Chain Security

Securing the software supply chain is one of the most critical and complex challenges facing DevOps and Security teams in the energy sector today. Like many other industries, this sector also relies on open source packages to ensure software development speed and efficiency. Unfortunately, attacks on critical infrastructure often target vulnerabilities introduced early in the development lifecycle through third-party or open-source components.

On average, 45% of security breaches hit the energy sector, highlighting the need for rigorous third-party package management and dependency scanning.

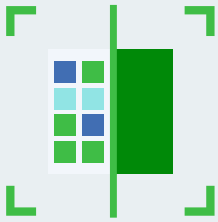
In the energy and oil sector, the bridge between Development and Operations is often where security risks are most acute. For security professionals working in these high-stakes environments, the primary pain point lies in the inherent fragility of Operational Technology (OT) and SCADA software management. Since these systems are frequently isolated or legacy-based, associated software packages often include hidden vulnerabilities that go undetected until they are already deployed in the field. This "blind spot" is further exacerbated by the risk of binary tampering, where a software artifact is altered while in transit from a development environment to production or once within production by an insider attacker or malicious actor. Ensuring software components remain untainted while in transit to a hardened, air-gapped OT environment is a significant logistical and security requirement for DevOps and Security teams at energy companies.

To secure these specialized software supply chains, JFrog provides a unified approach that integrates security directly into the artifact's lifecycle. By deploying JFrog Artifactory to manage all artifacts and JFrog Xray as a native extension of the universal repository, organizations can implement continuous security and compliance scanning for every binary and its associated dependencies. In addition, continuous monitoring alerts teams to new CVEs that were discovered after an application was deployed. This proactive approach allows teams to intercept packages with known vulnerabilities (CVEs) and license violations before they can reach your development environment.

Energy Sector Application Security Key Takeaways

Shift Left in OT

Vulnerability scanning is just as critical for SCADA binaries as it is for cloud-native apps.



Chain of Custody

Secure distribution ensures that everything you scanned during development is exactly the same as the components used in distributed applications.

Automated Attestation

Automated identification and documentation of all software artifacts during the development process eliminates the need for manual, labor-intensive post-mortem reports for critical internal and industry compliance.

Continuous Monitoring

Provides the ability to provide proactive alerting when new potential threats against systems in production, without having to scan the production environment.

Regulatory Compliance & Audit Readiness

In terms of regulatory compliance, the primary challenge lies in the "black box" nature of SCADA and Operational Technology (OT) software. These critical systems are frequently based on older legacy technologies that might include vulnerabilities that remain undetected throughout the development lifecycle, surfacing only after they are deployed into live, high-pressure, real-time environments.

Securing the Air-Gapped Supply Chain

Risks to the software supply chain are not limited to code itself, but also extend to the integrity of the binaries as they traverse the complex journey from secure development zones to isolated, air-gapped OT networks. Without a unified secure robust centralizer repo to manage these artifacts and the associated metadata, the chance of detecting if a binary is being compromised during transit increases exponentially. To defend against these attacks, DevOps teams at energy companies must have a "Single Source of Truth" that enables continuous vulnerability alerting and a proactive approach to application security, ensuring that every artifact is verified before it ever reaches development environments.

Automating Compliance for Pipeline Integrity

Beyond immediate security threats, Compliance teams in the energy sector must navigate a labyrinth of regulatory requirements. Maintaining a verifiable audit trail is no longer optional, as it has evolved into a core requirement for software production in the energy sector. The number of regulations that the energy industry needs to comply with and the volume of software they produce makes for a significant industry challenge: How can you collect and process such a large scattered amount of data? The solution is automating the process of collecting the auditable data and integrating the collection process with compliance validation prior to release.

By automating the collection of evidence for every application, organizations can simplify adherence to strict governance frameworks, including:

ISO standards for quality and security management.

NIST SP 800-218 part of the Executive Order 14028

NERC CIP for bulk power system protection.

FERC regulations regarding interstate infrastructure.

This automated governance doesn't just check a box for compliance; it builds a robust defense-in-depth strategy. By integrating binary control directly into the SDLC, energy companies can ensure that every piece of software governing their pipelines is secure, compliant, and fully traceable from code to “cloud" or code to “rig”:

Deployment Flexibility & Scalability

Energy infrastructure spans large networks across multiple remote locations, from offshore rigs to continental pipeline networks. This necessitates a deployment strategy that is flexible, highly scalable, and secure, often bridging the gap between traditional IT and restricted OT networks. In an industry where "the edge computing" could mean a remote offshore rig IT system with intermittent connectivity or a massive centralized refinery, a one-size-fits-all deployment strategy is not really viable.

Bridging the Rig to the Cloud

For DevOps and Security teams, achieving true flexibility means implementing a binary management strategy that supports a hybrid-cloud or multi-cloud architecture. By decoupling software from specific infrastructure, energy firms can ensure that mission-critical updates reach remote assets without disrupting local operations. This modular approach allows for "bursting" capacity during high-demand seismic data processing while maintaining a lean footprint for everyday monitoring.

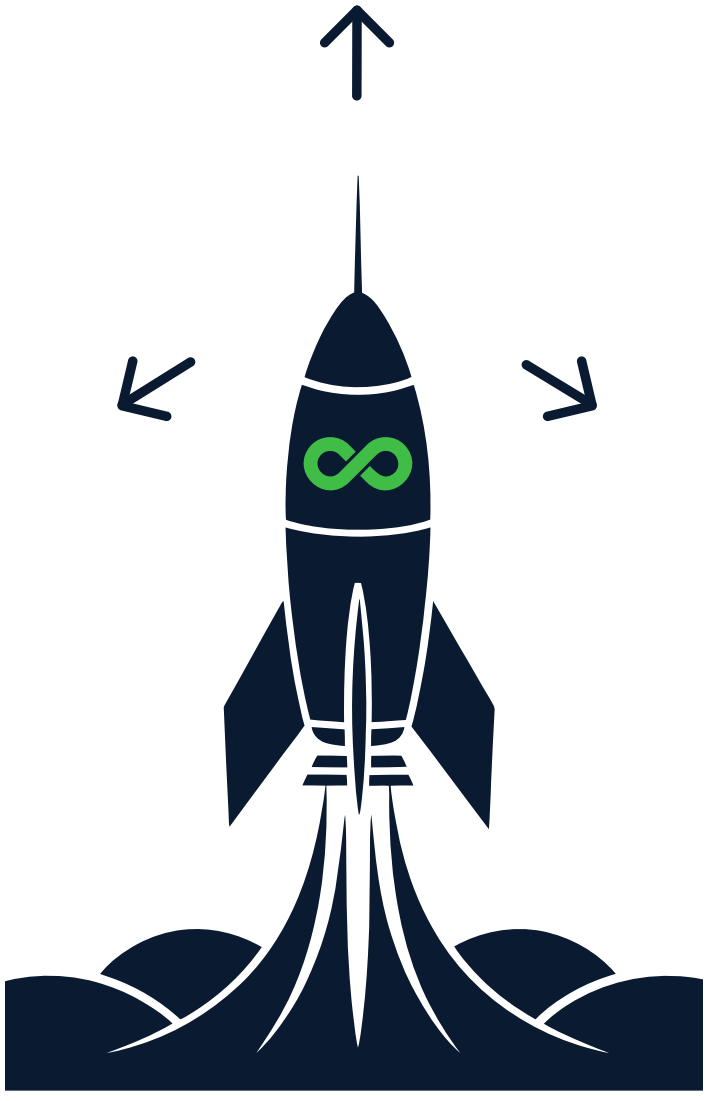
Scaling Security at the Speed of Demand

Scalability in the oil and gas sector isn't just about handling more data, it's about maintaining a rigorous security posture as your attack surface expands. As you scale from dozens to thousands of nodes across your global software supply chain, manual intervention becomes a bottleneck and a risk.

By leveraging automated promotion pipelines and a "single source of truth" for all binaries, DevOps and Security teams can ensure:

- **Immutable Releases:** Every software artifact is verified and consistent, whether it's deployed in a Tier 1 data center or a localized sensor at the wellhead.
- **Elastic Infrastructure:** Deployment targets can scale horizontally to meet fluctuating production telemetry without requiring a proportional increase in administrative overhead.
- **Global Distribution:** Low-latency access to tools and images is maintained through regional caching and federated repositories, ensuring that site reliability remains high even in geographically dispersed locations and remote regions.

Ultimately, by treating infrastructure as code and binaries as the ultimate unit of value, energy enterprises can transform their software supply chain into a competitive advantage, moving from legacy, monolithic updates to a fluid, scalable ecosystem that reacts to market demand and is scalable in real-time.



If you are a DevOps, Security or Compliance professional in the Oil, Gas and Energy Sector, then please take a tour, schedule a demo or start a free trial to see how JFrog can help, manage, secure and document your software supply chain.