The State of Software Supply Chain Security in Energy & Utilities

Digital transformation is driving the energy sector's convergence of OT and IT. Protecting the software supply chain is now a critical cyber defense for essential national infrastructure.

Industry Snapshot:
The Critical Need for Software Supply Chain Security

The highly regulated nature of the energy industry, combined with high-value, high-impact targets, makes robust security mandatory.

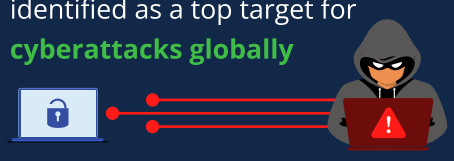
Key Trends & Statistics

Adoption Acceleration

97% of CIOs in the utilities and energy sector view extending a DevSecOps culture as key to accelerating digital transformation.
(Source: Dynatrace)

Target of Choice

The energy sector is consistently identified as a top target for **cyberattacks globally**



often due to geopolitical factors and the critical nature of its infrastructure.
(Source: IBM Security)

Software Supply Chain Risk

Energy organizations report an average of **20** supply chain attacks per respondent in a 12-month period, highlighting the need for rigorous third-party and dependency scanning.
(Source: Bridewell)

The Cost of Failure

The average cost of a data breach in 2024 is over **$4.8M** emphasizing the financial imperative of proactive security.
(Source: IBM Cost of a Data Breach Report)

> For us, it's about visibility and traceability but it's also really about auditability and being able to monitor in real time what people are doing – as a lot of them are in small self-contained silos. By pushing everything through the JFrog Platform, we're achieving the capability of really understanding what's happening internally with our technology at any time.
>
> **DevSecOps Team Lead, Leading Energy Company**

Apply the highest levels of security and governance continually across your application lifecycle without hurting your development velocity.

Learn more at jfrog.com