Google Cloud JFrog

From chaos to control

Mastering the AI supply chain for production success

Introduction

Artificial intelligence has moved from a promising experiment to a business imperative, transforming how enterprises compete and innovate. IDC forecasts that by 2028, AI will represent 16.4% of IT spending,[1] fueling advancements across security, operations, development, data engineering, and data science — especially with agentic AI use cases.

Despite this potential, most AI projects stall before reaching production. The complexity of operationalizing AI — intertwining data pipelines, infrastructure, and teams — outpaces traditional software delivery methods. This challenge is compounded by a critical gap in governance, with a lack of comprehensive model lineage tracking that renders audits, compliance, and reproducibility extremely difficult.

Fragmented operations expose enterprises to security vulnerabilities and compliance blind spots, threatening to erode trust, inflate costs, slow innovation, and ultimately undermine the transformative value AI promises at scale.

The sections ahead will explore the top challenges that hinder enterprise AI progress and offer practical recommendations for IT leaders seeking to operationalize AI securely, sustainably, and scalably. This ebook addresses the innovation-versus-control problem facing modern enterprises and introduces how JFrog, in partnership with Google Cloud, helps organizations centralize, unify, and govern their software supply chain and AI initiatives, while accelerating the ML development lifecycle and ensuring successful enterprise AI adoption.

1. IDC, "Worldwide Artificial Intelligence IT Spending Forecast, 2024–2028," 2024.

95%

of AI projects never progress beyond the pilot stage.

MIT, "The GenAI Divide: State of AI in Business 2025," 2025.

Google Cloud JFrog

Mind the gap: Common AI project pitfalls

As AI projects grow, enterprises often encounter a widening divide between pilot successes and reliable production deployments. Five critical challenges contribute to this gap.

01 Operational blind spots in production

02 Governance, security, and compliance gaps

03 Unpredictable outputs from model inconsistency

04 Fragmented model management and tool sprawl

05 The emergence of shadow AI

01: Operational blind spots in production

As AI initiatives transition from pilot to production, organizations often lose real-time visibility into models, pipelines, and AI agents. Traditional monitoring tools fall short in tracking these dynamic components, increasing the risk of security breaches and compliance violations. These operational blind spots make it difficult to scale AI reliably.

Autonomous AI agents running across platforms add complexity and opacity. Models often remain siloed, without end-to-end lineage or unified registries. This lack of insight causes delays, regulatory risks, and uncertainty about which AI systems to trust in production. Without clear answers to fundamental questions — such as which models are approved, under what conditions, and by which teams — pilots can stall, and AI initiatives fail to deliver expected results due to tensions between innovating fast and the need for robust enterprise governance and control. The resulting opacity hinders compliance with industry standards, exposes security vulnerabilities, and creates regulatory risks.

Recommendations

To close these blind spots, organizations must create a trusted source of truth for AI operations:

- **Create a single source-of-truth AI registry** to eliminate blind spots and ensure developers and IT teams have centralized visibility and insights.
- **Implement centralized AI governance** across models and pipelines to reduce complexity and strengthen enterprise trust. This integrated approach makes AI governance proactive, safeguarding innovation.
- **Prioritize a unified security platform** over fragmented tools to streamline governance, reduce friction, and strengthen the enterprise's defense posture.

02: Governance, security, and compliance gaps

The adoption of cloud-native architectures expands the attack surface for AI/ML components, introducing significant security and compliance challenges. Traditional, point-based security solutions struggle to keep pace, often resulting in alert overload and time-intensive remediation. Developers often integrate external models as APIs and connect to external model context protocol (MCP) servers from diverse sources, introducing substantial risk without consistent guardrails.

Effective governance requires end-to-end visibility of data lineage, access controls, and runtime activity. If security and compliance are not fully embedded from the start, projects risk failure due to increasing regulatory scrutiny.

Recommendations

1. **Implement a consistent system of record for AI workloads** that enables continuous oversight and accountability. A single system of record ensures consistent oversight, strengthens accountability, and builds confidence in AI-driven decisions.
2. **Embed security and compliance automation** within development and deployment pipelines to reduce alert fatigue and integrate governance across the innovation process.
3. **Establish cross-functional governance frameworks** with clearly defined responsibilities and collaboration across security, compliance, legal, and AI teams to maintain compliance with evolving regulations while preserving agility.

Google Cloud JFrog

03: Unpredictable outputs from model inconsistency

Even with strong infrastructure and governance, AI models can drift into unpredictable behavior, such as hallucinating, showing bias, or producing inconsistent results. Such issues erode stakeholder trust and delay adoption. The real risk lies in silent failure. Without real-time monitoring and explainable insights, performance degradation may go undetected until it causes operational or reputational damage. Lack of transparency hampers proactive risk management.

True AI maturity demands a continuous feedback loop: detecting anomalies early, providing clear reasoning behind model decisions, and automating remediation to fix problems quickly. These practices ensure accuracy and fairness while minimizing manual intervention. Proactive monitoring and explainability create trust across teams and leadership, enabling enterprises to confidently scale AI initiatives. By shifting from reactive troubleshooting to real-time assurance, organizations protect their investments and unlock AI's full potential.

Recommendations

- **Implement full model lifecycle management** to align innovation with accountability and govern every stage of AI development with clarity, reliability, and trust.
- **Integrate explainability and traceability into AI workflows** to generate actionable insights, detect drift, and maintain trust in model outcomes.
- **Maintain a unified, auditable record of AI assets** to safeguard data integrity, streamline compliance, and enable rapid, confident decision-making.

04: Fragmented model management and tool sprawl

When AI assets, such as models, binaries, and code, are spread across disconnected environments and tools, governance weakens, and productivity suffers. Valuable models and approved tools become fragmented across teams, causing duplication of effort and slowing time-to-market. This decentralization creates organizational overhead, as teams must navigate complex approval processes and manual steps just to find and utilize the necessary assets. As a result, the process of finding, evaluating, and getting approval for the right model can become a bottleneck.

To build enterprise-scale AI, organizations must address this sprawl by unifying AI asset management within a governed, scalable software supply chain. Centralizing models and tools under a single, authoritative system improves transparency, accelerates access, and streamlines governance.

Recommendations

- **Unify MLOps with DevOps and DevSecOps lifecycles** to create seamless, end-to-end workflows that streamline AI asset management and deployment.
- **Establish a single, authoritative registry for all approved AI assets —** models, tools, and computation providers — to eliminate silos, reduce approval delays, and enable instant self-service access for AI teams.
- **Utilize universal artifact repositories** supporting diverse formats to standardize lifecycle management, enhance governance, and accelerate time-to-market with consistent security and compliance controls.

05: The emergence of Shadow AI

Many organizations rely on allow/block lists to control AI assets managed manually in spreadsheets and documents as security recommendations, not enforcement. While this approach may appear simple and efficient, these static controls often create bottlenecks and frustrate developers, who lack clarity on what's allowed. This ambiguity stifles innovation and drives shadow AI — unmanaged models, personal subscriptions, and custom tools — adopted outside governance. Driven by a need for agility, these informal AI adoptions grow into an ecosystem of high-risk, unmanaged tools that breed compliance and operational risks.

The ease of deploying AI models through cloud-based APIs, prebuilt models, and personal devices exacerbates this challenge. Organizations face a new paradigm with this democratization and sprawl of AI tools. Governance must evolve from blocking access to enabling innovation — giving admins the control to prevent unapproved models while providing developers clear guidance on authorized assets — without sacrificing security or compliance.

Recommendations

- **Transition from gatekeeping to enabling governance** by implementing a centralized AI asset catalog paired with a secure gateway that enforces policies on access and usage with auditable controls.
- **Adopt lifecycle-aware governance with automated enforcement,** creating parallel tracks for standard and high-risk AI assets, preserving agility while ensuring compliance and reducing technical debt.
- **Embed governance into developer workflows** via a fast, pre-scanned, validated catalog, turning AI governance from a bottleneck into a value enabler fueling innovation.

Bridge the gap

Unifying the software supply chain for AI success with JFrog and Google Cloud

Google Cloud JFrog

Enterprise AI failures increasingly stem from fragmented workflows, inadequate security, and unpredictable model behavior. For enterprise AI to succeed, organizations must treat models and data pipelines as versioned, traceable, and continuously secured software assets while consistently applying the continuous integration/continuous delivery (CI/CD) principles.

JFrog turns this vision into reality by enabling organizations to build, secure, and release software and AI models faster and with greater confidence. With the JFrog Platform on Google Cloud, businesses can:

01 Unify workflows to bring together DevOps, DevSecOps, and MLOps to reduce silos and operational complexity.

02 Standardize production workflows and apply strict software supply chain controls on AI components to ensure quality, security, and compliance.

03 Centralize AI governance with the JFrog AI Catalog, a unified hub to discover, control, and monitor approved AI models across the organization.

> “People ask me how I managed to deploy so many models while onboarding a new team within a year. My answer is: JFrog ML.”
>
> **Idan Benaun,** Director of AI/ML, OpenWeb

Google Cloud JFrog

Achieving enterprise control with JFrog on Google Cloud

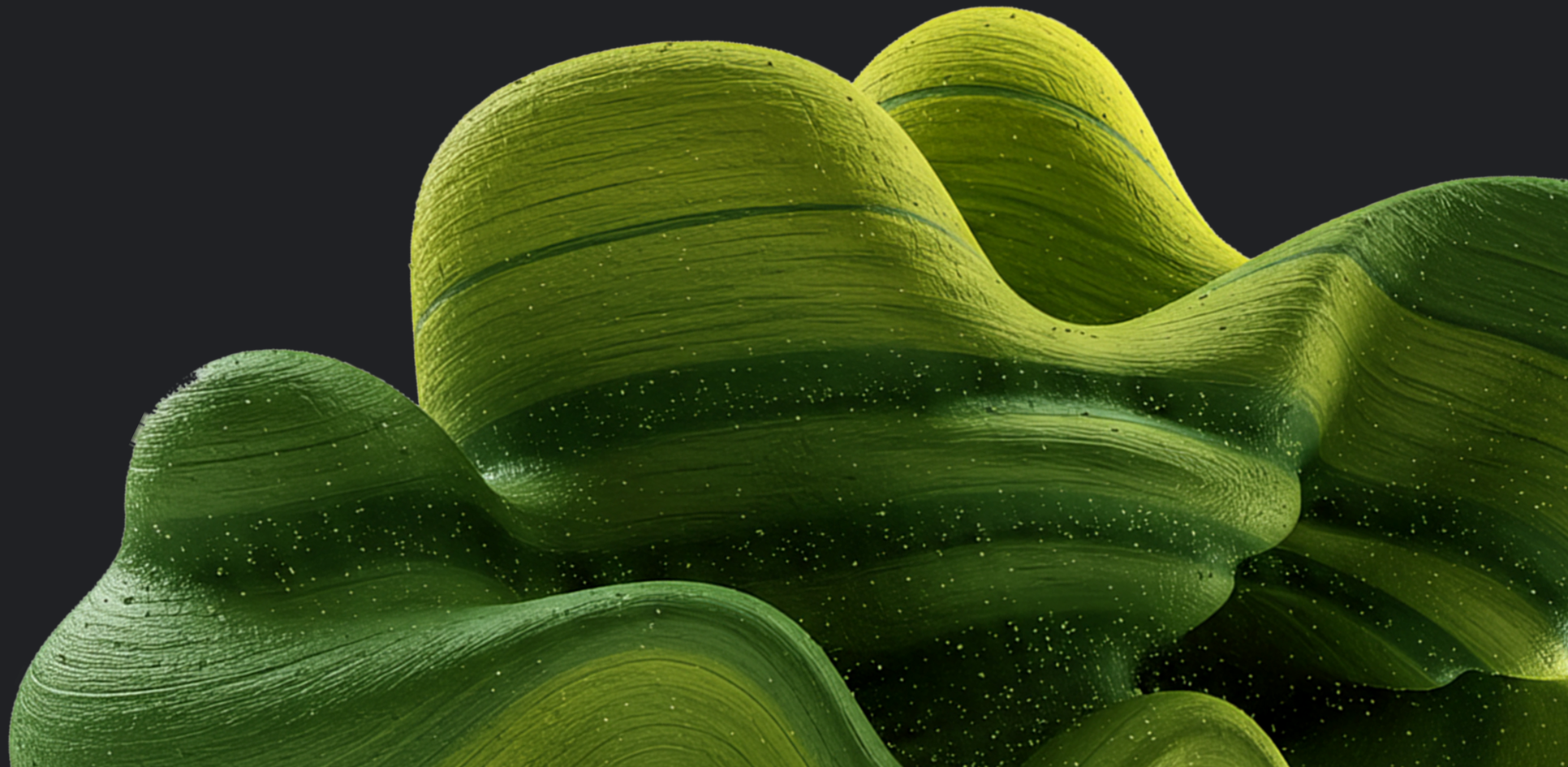
AI initiatives challenge	How JFrog and Google Cloud can help
Operational AI blind spots	**JFrog AI Catalog** provides centralized AI control, establishing comprehensive visibility and precise, auditable control over AI access and usage across the entire enterprise.
Governance, security, and compliance gaps	**JFrog AI Catalog** enables a secure, end-to-end AI supply chain by extending enterprise-grade security and governance to every AI workload. **JFrog Xray** automatically scans all models, datasets, and dependencies for vulnerabilities and license compliance. **JFrog Curation** enforces organizational policies by automatically blocking high-risk or non-compliant AI assets, providing the full visibility and traceability required for compliance.
Model inconsistency	**JFrog Artifactory** serves as the unified model registry, managing models as first-class artifacts alongside all other software binaries. This ensures robust **versioning, reproducibility, rollback capability,** and consistency across environments. **JFrog ML** further unifies and simplifies the MLOps lifecycle alongside DevOps and DevSecOps.

Google Cloud JFrog

AI initiatives challenge	How JFrog and Google Cloud can help
Fragmented models and tools management	**JFrog ML** extends the power of the JFrog Platform to the MLOps pipeline, bridging the gap between data science and production teams. It provides **end-to-end model lifecycle management** and acts as the **single, unified platform** to manage, secure, and deploy all AI assets — from models and data sets to accompanying MLOps tools — eliminating tool fragmentation and siloed workflows.
Shadow AI	**JFrog AI Catalog** provides a centralized platform to combat Shadow AI. It actively **detects and inventories every AI model and external API** call (e.g., OpenAI, Gemini) across the organization, instantly identifying unmanaged usage and eliminating security blind spots. The Catalog brings these assets under governance for **vetting,** allows for **policy enforcement** to block non-compliant models/APIs, and utilizes the **AI Gateway** to route all consumption through a single, standardized connection for unified control.
Ecosystem integration & trusted model sourcing	JFrog AI Catalog, part of the JFrog Software Supply Chain Platform **available on Google Cloud** and via the **Google Cloud Marketplace,** acts as the **centralized hub for all model types.** This includes securely connecting to external providers like **Google Gemini** and providing governance over **open models like Gemma.** By being natively available on Google Cloud, organizations can easily leverage JFrog's massive scale with **Google Cloud Storage** and integrate with core services like Google Kubernetes Engine (GKE) and **Cloud Build,** optimizing their AI/ML and DevSecOps workflows within a single, secure cloud ecosystem.

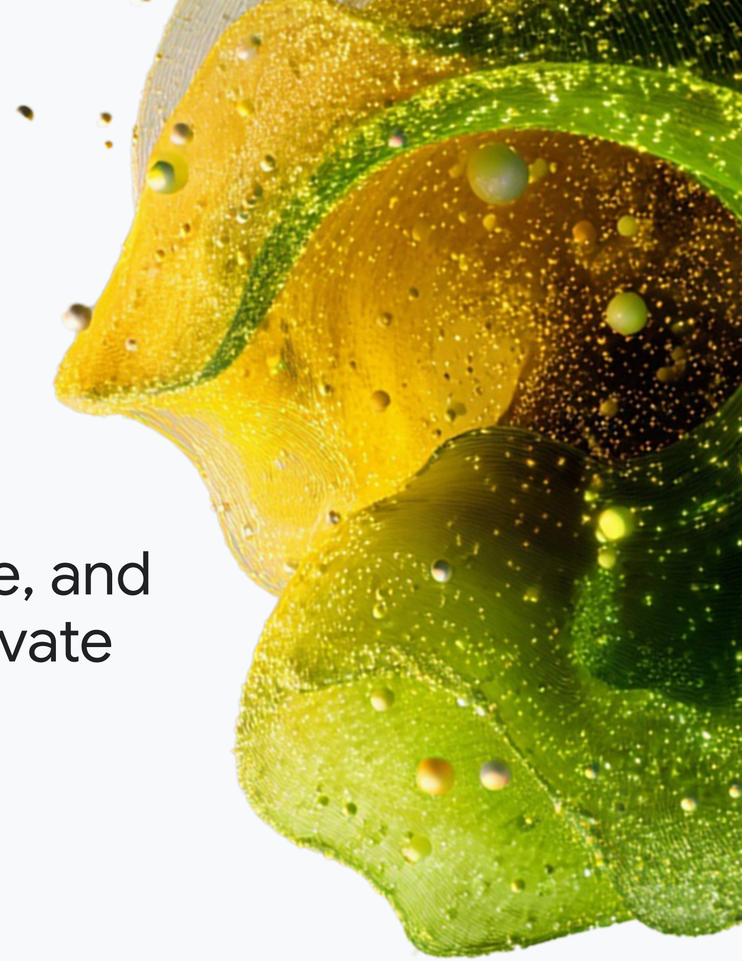
This powerful partnership delivers a unified, secure, and governed software supply chain platform specifically extended for AI/ML workloads, enabling organizations to move AI projects from pilot to production and ensure innovation happens securely and at scale.

Future-proof your AI strategy



Google Cloud JFrog

By integrating AI/ML workflows into the trusted, unified JFrog Software Supply Chain Platform running on Google Cloud, organizations can stop chasing AI trends and start controlling them. Teams gain both the necessary centralized governance and control and a secure AI supply chain end-to-end. This allows the enterprise to accelerate innovation with frictionless access to vetted AI assets and accelerate delivery from inception to AI applications.



> “Our platform ensures enterprises can trust their AI pipelines with end-to-end governance, compliance, and seamless automation — empowering them to innovate confidently and responsibly.”
>
> **Shlomi Ben Haim,** CEO, JFrog

For more information

To learn more, visit JFrog online or start a 14-day free trial.

About JFrog

JFrog Ltd. (Nasdaq: FROG) is the creator of the unified **DevOps, DevSecOps, and MLOps platform,** dedicated to frictionless software delivery. Its hybrid, multi-cloud platform is trusted by millions of users and **7K+ customers worldwide**, including a majority of the Fortune 100, for secure digital transformation.

About Google Cloud

Google Cloud accelerates every organization's ability to digitally transform its business. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology — all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems.

Google Cloud JFrog