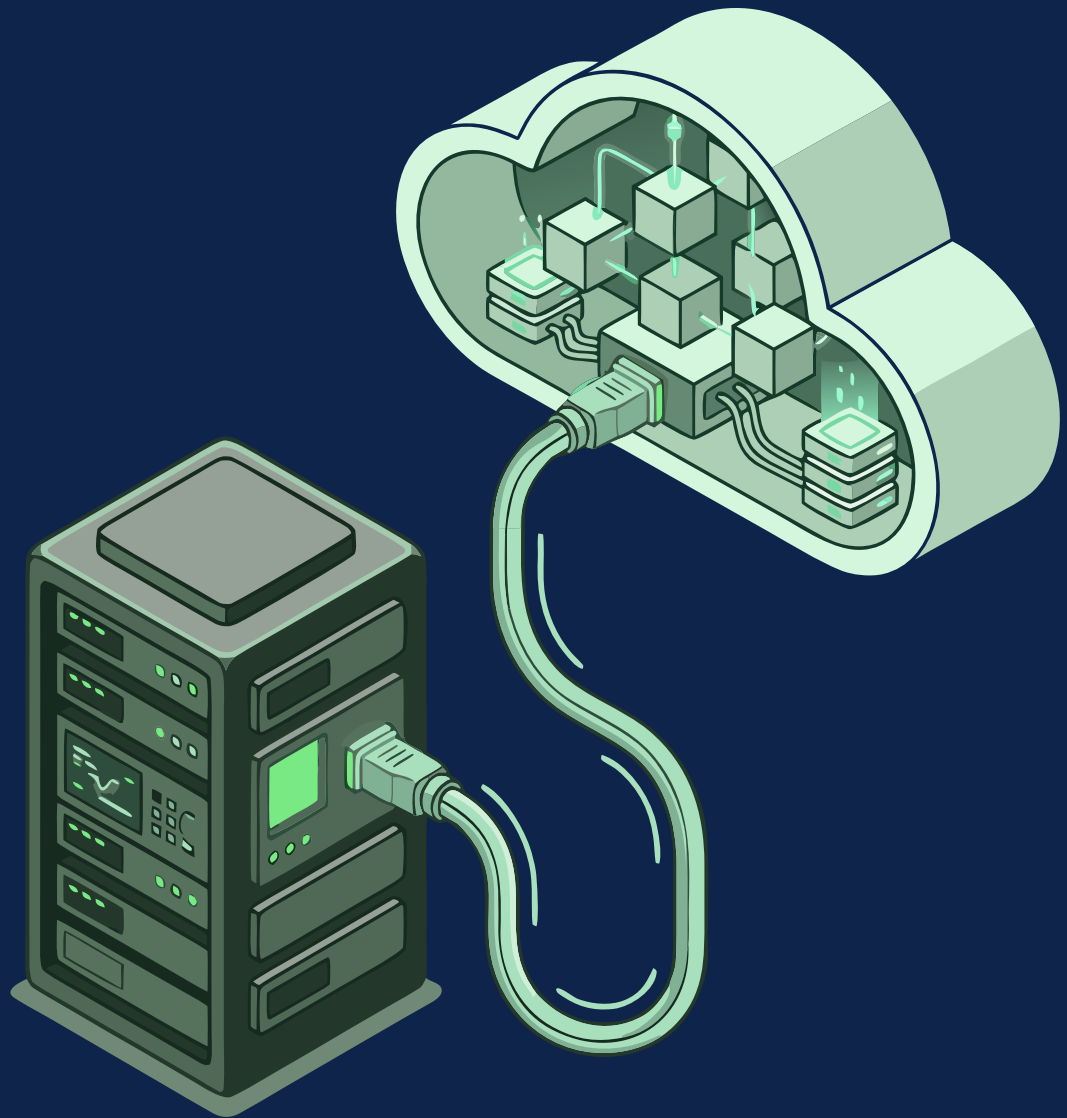




When SaaS Makes Sense

A Guide to Embracing the Cloud for
DevOps, DevSecOps, and AI Security



Introduction

Software teams are under pressure to move faster without breaking things. For DevOps, DevSecOps, and AI-dev teams, that pressure means constantly rethinking how they build, secure, and ship software. One of the biggest areas under review is the choice of deployment model and whether managing infrastructure yourself still delivers greater security control as software complexity and operational demands grow, or whether cloud and software-as-a-service (SaaS) offer a more secure, scalable operating model. While on-premises offers additional control, IT leaders face growing threats from frontier AI models weaponized by bad actors, the rapid spread of generative AI into enterprise applications across teams, and constant pressure to do more on tighter budgets. A SaaS model speaks directly to all three. It scales up or down as conditions change, it supports the infrastructure AI workloads demand, and it can replace large upfront investments with more predictable operating costs.

Add to this rising vulnerability volumes, shrinking exploitation windows, the burden of constant patching, and the fact that attackers can now reverse-engineer published fixes to craft working exploits faster than human security teams can manually test and deploy. All of this is leading teams to once again reassess the trade-offs of self-managed vs. SaaS.

This ebook explains why now may be the right time to move your Software Supply Chain tooling to SaaS. We'll walk through the benefits of making the switch, from always having the latest functionality to simpler operations to stronger security across your development teams, and show how JFrog can help at each step of your cloud journey.

Self-Managed vs. Cloud SaaS Environments

The following table compares self-managed and SaaS software deployments, revealing distinct advantages and limitations in key operational areas.

Feature / Aspect	Self-Managed Deployment	SaaS Deployment
Control & Customization	Granular control; tailored to specific or air-gapped needs	Managed infrastructure; dependent on cloud provider settings
Infrastructure	Relies on in-house hardware and software	Hosted on external, provider-managed infrastructure
Cost Model	High upfront costs and ongoing maintenance expenses	Cost-flexible; pay-as-you-go or subscription-based
Scalability	Limited by internal/managed hardware capacity; hard to support massive AI or traffic spikes	Highly scalable; rapidly expands to meet demand
Deployment Speed	Slower; can require physical hardware setup and configuration or other hosting configs	Rapid deployment speeds
Accessibility	Restricted to local network or configured VPNs	Accessible over the internet, with configurable access controls
Patch & Upgrade Effort	Requires internal pipelines, testing, downtime windows, and dedicated IT resources	Automatic, continuous updates for users, designed to deliver security fixes as quickly as possible
Exposure Window	Delayed upgrade cycles can leave environments exposed to reverse-engineered AI exploits	Vulnerability fixes and updates are applied by the platform provider

Ultimately, the choice comes down to balancing control with operational speed and risk management. Self-management works well for organizations with strict data-isolation requirements, but it forces your internal team to do all the heavy lifting, from maintaining servers to installing security patches and testing upgrades. Cloud SaaS optimizes for rapid deployment, continuous maintenance, capital efficiency, and **faster response time to emerging threats**. For cybersecurity teams, the appeal is clear: fewer systems to maintain and patches to deploy, freeing them to focus on access, policy, and threats to the business.

Cost Efficiency & FinOps

Deploying applications in the cloud can be significantly more cost-efficient compared to traditional on-premises and self-managed setups. Organizations can eliminate the high upfront capital costs of purchasing and maintaining physical servers, data centers, and related infrastructure. Instead, they benefit from a predictable subscription-based pricing model, making expenses manageable while avoiding unpredictable hardware investments. This is before we have even factored in the cost of human capital to “run” the on-premises deployment.

Cloud SaaS deployments excel in scalability, aligning with modern FinOps practices. Unlike self-managed or on-premises setups, cloud platforms dynamically adjust resources based on real-time needs. This model is designed to help companies pay for what they use, reducing wasted resources.

SaaS options can also reduce maintenance costs. On-premises setups require dedicated IT teams for hardware upkeep, updates, and security patches. SaaS providers manage these tasks natively.

Operational Simplicity Through Cloud Marketplaces

Adopting JFrog SaaS through cloud marketplaces streamlines procurement, deployment, and financial management.

- **Consolidated Billing:** Consolidate your software spend into a single invoice managed directly by your cloud provider.
- **Commitment Drawdown:** Where your cloud provider’s terms allow, utilize pre-committed cloud spending (such as AWS EDP or Azure MACC) to procure JFrog, which can help you use existing budgets and may reduce the need for new capital expenditure approvals.
- **Rapid Provisioning:** Skip lengthy hardware acquisition cycles. Teams can provision JFrog instances in a few clicks, then configure and scale them for production.

Scalability and Flexibility

In a self-managed setup, scalability can be physically constrained. Scaling up requires procuring and configuring additional servers, services, and potentially licences - a process that can span weeks, unless you have the budget and capacity to keep spare hardware on standby.

In contrast, cloud environments are designed to dynamically adjust computing resources in real time based on current workloads. They offer highly elastic scalability without the burden of maintaining excess capacity or idle licenses.

Deploying in the cloud also offers enhanced geographic flexibility. Cloud platforms support multi-region deployments, enabling businesses to distribute infrastructure globally. This can help lower latency, improve redundancy, and support data residency requirements under laws such as GDPR.

Serverless capabilities allow organizations to run custom code natively within cloud platforms, empowering teams to automate policies, process data, and handle heavy workloads seamlessly without managing external infrastructure.

Resilience and Reliability

Modern SaaS platforms deliver built-in high availability within your chosen cloud region, designed to support consistent uptime. For disaster recovery, additional cross-region options can be configured to maintain business continuity and protect critical data.

SaaS providers handle proactive maintenance, software updates, and security patches automatically. This removes foundational maintenance burdens from internal IT teams and reduces the risk of downtime due to delayed manual updates.

Cloud-based SaaS deployments benefit further from integrated monitoring and observability tools. Built-in management portals provide users with rich usage visibility, log streaming, and architecture mapping that help teams monitor availability and uptime.

Securing Your Software Supply Chain with JFrog SaaS

As software supply chain attacks grow more sophisticated and frequent, securing software deliverables requires visibility and governance across every stage of the development lifecycle. Transitioning to JFrog SaaS pairs the natural resiliency of cloud infrastructure with enterprise-grade DevSecOps capabilities, helping protect your artifacts, dependencies, and pipelines.

- **JFrog Curation:** Shift security left by automatically auditing and blocking malicious or non-compliant open-source packages and AI models before they enter your supply chain
- **JFrog Advanced Security:** Cut through alert fatigue with deep, contextual vulnerability analysis, exposed secret detection, container scanning, and Infrastructure-as-Code (IaC) security.
- **JFrog AI Security:** Provide centralized search, evaluation, and governance across AI models, MCP servers, agent skills, and other AI components to help developers discover and adopt trusted AI assets.
- **JFrog Xray:** Continuously scan binaries and dependencies for vulnerabilities and compliance risks, while generating and exporting Software Bills of Materials (SBOMs), including for supported ML models, to support your regulatory compliance work.

JFrog maintains its own security certifications, listed in the [JFrog Trust Center](#), which can help support your internal compliance work.

The Shared Responsibility Model

Security in the cloud is a partnership. JFrog manages platform infrastructure and core system security, allowing your team to focus on access governance and application lifecycle management.

- **JFrog's Responsibility:**
 - Cloud infrastructure hosting, maintenance, and uptime
 - Platform-level security, vulnerability patching, and system updates
 - High availability and in-region disaster recovery
- **Customer's Responsibility:**
 - User access management, identity controls, and role-based access control (RBAC)
 - Authentication enforcement (Single Sign-On, Multi-Factor Authentication)
 - Internal project permissions, repository access, and security policy configuration

Future-Proofing Your Supply Chain with AI Security

Clarifying platform responsibilities is only the baseline. Today, the software assets organizations must protect are fundamentally changing. As AI models and Generative AI integrate into modern applications, traditional software supply chains must evolve. Models are now core software artifacts that demand massive storage, dynamic compute, and dedicated security protocols - workloads that legacy on-premises infrastructure can struggle to support efficiently.

Through capabilities like the JFrog AI Catalog and native binary management, the JFrog Platform is built to provide holistic governance across software and AI assets. Organizations can discover, evaluate, secure, and manage open-source and internal AI/ML models right alongside traditional binaries, container images, and dependencies within a single, secure platform. This unified approach gives enterprise teams lineage tracking, automated vulnerability scanning, and trusted distribution across your environments.

Whether preparing for serverless computing, edge deployments, or autonomous AI agents, running JFrog in the cloud provides the elastic compute and global reach needed to scale continuous innovation while helping maintain security.

JFrog and Cloud Partners - Freedom to Choose

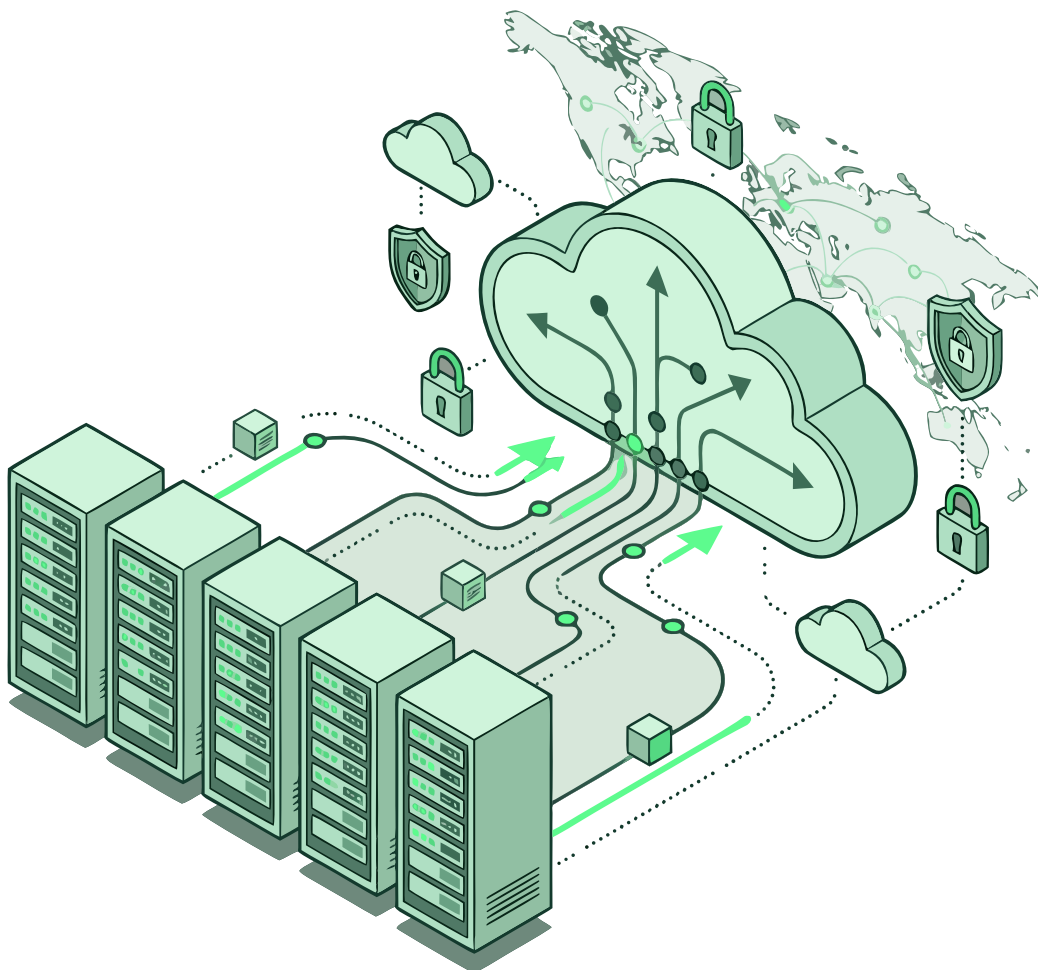
JFrog collaborates closely with major cloud providers to deliver deeply integrated, enterprise-ready software supply chain management across AWS, Microsoft Azure, and Google Cloud.

- Amazon Web Services (AWS): Combine the global reach of AWS with deep integrations across core storage and compute services and AI solutions such as Kiro, Amazon Bedrock AgentCore, and Amazon SageMaker for secure workflows.
- Microsoft Azure: Streamline development by pairing Azure infrastructure, Azure DevOps, Azure ML, and GitHub with JFrog to unify source code and binary management.
- Google Cloud: Harness Google Cloud's ecosystem by deploying JFrog alongside Google Artifact Registry, Google Kubernetes Engine (GKE), Cloud Storage, Cloud Run, and Vertex AI to power enterprise workloads at scale.

Next Steps

As AI accelerates software delivery and gives attackers new ways to find and exploit weaknesses, the time available to respond is shrinking. Moving to the cloud is more than a technology upgrade. It's a way to reach bigger business goals: faster releases, stronger security, and infrastructure that grows with you. Wherever you are in that journey, JFrog's universal cloud and hybrid deployment options give you the flexibility to move at your own pace, backed by deep experience helping organizations of every size make the shift.

Ready to see it in action? **Schedule a demo** with our team to explore how JFrog can support your move to SaaS.



This ebook is provided for general informational purposes only. It is not legal, compliance, or security advice and does not guarantee any security or product outcome. It reflects information available as of the publication date shown below and may not be updated. Results depend on your environment, situation, and configuration. Product capabilities vary by edition and deployment model and are governed by your agreement with JFrog. JFrog is a registered trademark of JFrog Ltd. in the United States. All other trademarks referenced in this document are the property of their respective owners.