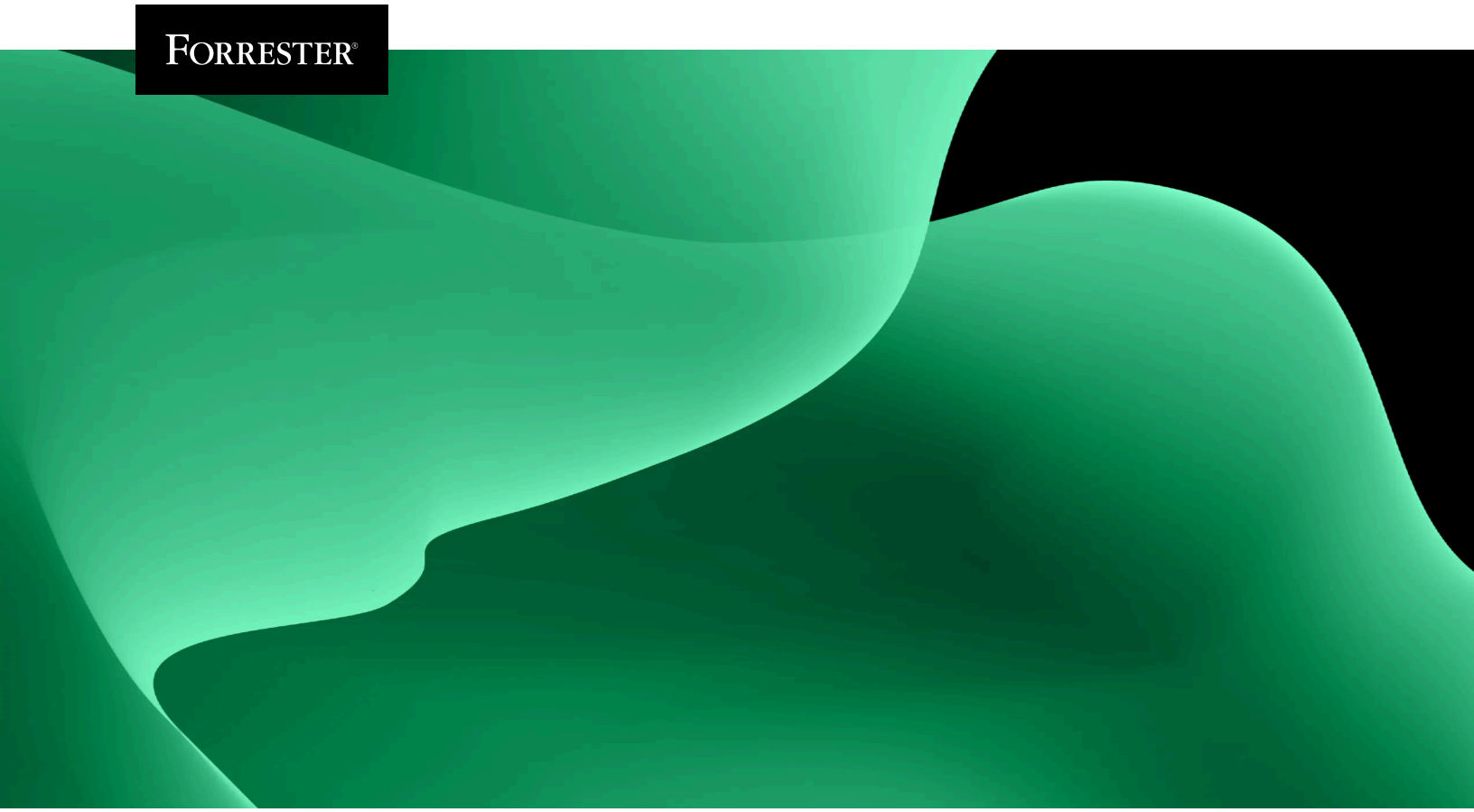
Total Economic Impact

The Total Economic Impact™ Of JFrog Software Supply Chain Security

Cost Savings And Business Benefits Enabled By JFrog

A FORRESTER TOTAL ECONOMIC IMPACT STUDY COMMISSIONED BY JFROG, JANUARY 2026



Executive Summary

Today's software supply chains are under siege, from surging open-source vulnerabilities and regulatory pressure to the rising cost of downtime and delayed releases. As development accelerates, organizations can no longer afford reactive security or fragmented tooling; they need to shift security left, embedding it early and seamlessly throughout the development lifecycle and beyond release. This study explores how integrated platforms are enabling teams to reduce risk, streamline compliance, and empower developers to build securely at scale.

JFrog provides a unified platform for managing the software supply chain, which can help organizations build, secure, and deliver software with greater speed and confidence. The platform supports integrated workflows across DevOps; development, security, and operations (DevSecOps); and emerging machine learning operations (MLOps) practices. This can help secure management of application and AI/ML artifacts within a single solution. The Artifactory solution supports DevOps teams with scalable artifact management, while Curation, Security Essentials (Xray), and JFrog Advanced Security can help DevSecOps teams proactively block risky packages; detect vulnerabilities and prioritize remediation through contextual analysis; detect secrets exposed in source code and binaries; natively integrate with developer tools (IDEs); and generate software bill of materials (SBOMs) for compliance and dependency management. For machine learning workflows, JFrog ML offers secure model cataloging, development, storage and deployment capabilities, extending the platform's reach into AI and MLOps environments.

JFrog commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying JFrog.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of JFrog on their organizations.

282%

Return on investment (ROI)

$4.0M

Net present value (NPV)

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using JFrog. For the purposes of this study, Forrester aggregated the experiences of the interviewees and combined the results into a single composite organization, which is a global enterprise operating in a regulated industry with 500 engineers and $2 billion in annual revenue.

Interviewees said that prior to using JFrog, their organizations relied on fragmented toolchains for artifact management, vulnerability scanning, remediation, and compliance reporting. These siloed approaches led to inconsistent security practices, delayed remediation cycles, and manual, error-prone audit preparation. As a result, their organizations' teams struggled to maintain visibility into their software supply chains, often discovering vulnerabilities late in the development cycle or after release, which increased operational risk and slowed delivery and compliance reporting.

After the investment in JFrog, the interviewees described a more unified and proactive approach to software development and security. Their teams benefited from integrated vulnerability scanning, contextual analysis, prioritized remediation, and automated SBOM generation embedded directly into continuous integration and delivery (CI/CD) pipelines. Key results from the investment include faster vulnerability remediation, improved audit readiness, reduced tool sprawl, and greater developer autonomy through shift-left security practices.

Key Findings

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Reduced vulnerabilities, worth $2.5 million.** JFrog Curation, Advanced Security and Xray together help minimize risk for the composite across the software supply chain. Curation acts as a gatekeeper, blocking malicious or noncompliant open-source packages before they enter development environments. JFrog Xray SCA tools and JFrog Advanced Security with contextual analysis provide ongoing oversight, enabling developers to detect and prioritize exploitable vulnerabilities earlier in the lifecycle. Prior to implementation, the composite's security teams spent days manually investigating common vulnerabilities and

exposures (CVEs) and tracing dependency trees. With JFrog, developers receive real-time feedback, reducing the number of vulnerabilities reaching production and accelerating remediation from days to hours. The composite experiences a 65% reduction in critical vulnerabilities driven by shift-left practices, automated exposure validation, and proactive package curation. These improvements reduce security exposure, lower remediation workload, and free up engineering resources to focus on innovation.

- **Faster vulnerability remediation, worth $1.2 million.** While Curation reduces the volume of risky packages entering development at the composite, Xray and JFrog Advanced Security accelerate remediation for vulnerabilities that do surface. The composite organization reduces the time required to remediate vulnerabilities by automating detection and streamlining response workflows. Prior to implementation, its security and development teams spent hours manually tracing dependencies and validating exposure. With JFrog, contextual analysis and real-time scanning are embedded directly into CI/CD pipelines, enabling near-instant identification and resolution. The composite experiences an 80% reduction in remediation time, with developers now resolving issues in hours instead of days. These improvements enhance operational agility, reduce risk exposure, and free up engineering capacity for higher-value work.
- **Improved onboarding of software developers, worth $1.4 million.** The composite organization accelerates developer onboarding by standardizing toolchains, automating environment setup, and streamlining access to repositories and permissions. Prior to JFrog, onboarding new developers could take several days due to manual configuration and inconsistent processes. With JFrog, developers gain immediate access to preconfigured environments and integrated security workflows, enabling them to become productive within hours. The composite saves 38 hours onboarding each new software developer as integrated security workflows during onboarding helped standardize DevSecOps practices and reduce configuration errors, reinforcing secure development from day one. These improvements reduce ramp-up time, accelerate time to productivity, and allow engineering teams to scale more efficiently. Integrated security workflows during onboarding help standardize DevSecOps practices and reduce configuration errors, reinforcing secure development from day one.
- **Tool consolidation savings, worth $337,000.** The composite organization reduces software development tool spend and administrative overhead by consolidating best-of-breed point solutions and outdated legacy tools into the JFrog Platform. Prior to implementation, teams relied on a fragmented toolchain, including separate tools for artifact management, vulnerability scanning, license compliance, and application security testing. This created redundant licensing costs, integration complexity, and inconsistent security practices. With JFrog, the composite retires overlapping solutions and standardizes on a single platform that embeds software supply chain security capabilities natively. It saves nearly $136,000 annually by eliminating legacy tools. This consolidation not only lowers direct costs but also strengthens security posture by replacing siloed tools with an integrated platform approach, simplifying operations and freeing up engineering resources.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified for this study include:

- **Greater developer confidence and autonomy.** By embedding real-time feedback and contextual vulnerability analysis into developer workflows, JFrog enables the composite organization's engineers to identify and resolve issues independently. This reduces reliance on security teams, accelerates development cycles, and improves code quality.
- **Faster and more consistent audit readiness.** The composite organization benefits from automated SBOM generation and continuous scanning, which streamline compliance reporting and reduce manual effort. These capabilities support audit readiness in regulated environments and improve transparency with internal and external stakeholders.
- **Reduced noise in vulnerability management.** JFrog's contextual CVE analysis and AI-driven filtering allow the composite organization to focus on exploitable risks, minimizing time spent on false positives. This improves operational efficiency and ensures that remediation efforts are directed toward high-impact issues.
- **Improved cross-functional collaboration.** The composite organization uses JFrog as a shared platform across DevOps, DevSecOps, and security teams. Unified dashboards and visibility into security posture enhance communication, reduce silos, and support coordinated responses to security and operational challenges.
- **Enhanced resilience and business continuity.** JFrog's SaaS-based architecture, federation, and caching capabilities ensure uninterrupted access to critical tools and artifacts. The composite organization can maintain development velocity and deployment continuity even during outages or connectivity disruptions.
- **Improved technological performance through modern architecture.** The composite organization benefits from JFrog's cloud-native design, broad package support, and integration with infrastructure-as-code tools. These capabilities reduce technical

debt, simplify toolchain management, and support modernization initiatives.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Initial implementation and setup, totaling $22,000.** The composite organization incurs a one-time implementation cost to deploy the JFrog Platform. This includes internal labor from DevOps, security, and platform engineering teams, as well as a possible limited package of professional services from JFrog to support configuration and best-practice alignment. Implementation was straightforward for the composite, with automation and infrastructure-as-code tools like Terraform accelerating deployment. It purchases a limited package of professional services from JFrog to accelerate configuration and best-practice alignment. The composite organization benefits from faster time to value and a scalable foundation for long-term platform adoption.
- **Annual license fees, totaling $1.2 million.** The composite organization pays $467,500 annually for access to the JFrog Platform, including Enterprise X tier, JFrog Advanced Security, and Curation modules. These license fees support approximately 500 developers across DevOps, DevSecOps, and development, governance, and operations (DevGovOps) teams and cover multiple federated deployments. While pricing varies based on deployment scope and optional modules, the composite organization benefits from predictable, scalable licensing aligned with its enterprise needs; bundled pricing model simplifies procurement and scales with usage. The composite also experiences the ability to consolidate multiple tools and reduce administrative overhead.
- **Ongoing professional services costs, totaling $205,000.** The composite organization invests in customer success services to ensure successful adoption, continuous enablement, and long-term platform value. These services include onboarding support, technical training, strategic guidance, and access to dedicated account and support teams. The composite organization benefits from proactive support, faster time to value, and improved platform utilization across teams.
- **Ongoing labor and management, totaling $30,000.** The composite organization allocates a small portion of internal resources to manage the JFrog Platform on an ongoing basis. This includes monitoring usage, provisioning repositories, managing access, and supporting developers. It experiences minimal administrative overhead due to JFrog's SaaS delivery model, automation features, and integration with infrastructure-as-code tools like Terraform. Platform management is shared across teams and requires only a few hours per month. Compared to self-hosted alternatives, the composite organization benefits from reduced operational burden and improved efficiency in managing its DevSecOps toolchain.

The financial analysis that is based on the interviews found that a composite organization experiences benefits of $5.4 million over three years versus costs of $1.4 million, adding up to a net present value (NPV) of $4.0 million and an ROI of 282%.

> *"We want people to know right away that they've got an issue and with JFrog, as soon as they scan something or push something, we'll know right away."*
>
> **Principal engineer, telecommunications**

Key Statistics

282%

Return on investment (ROI)

$5.4M

Benefits PV

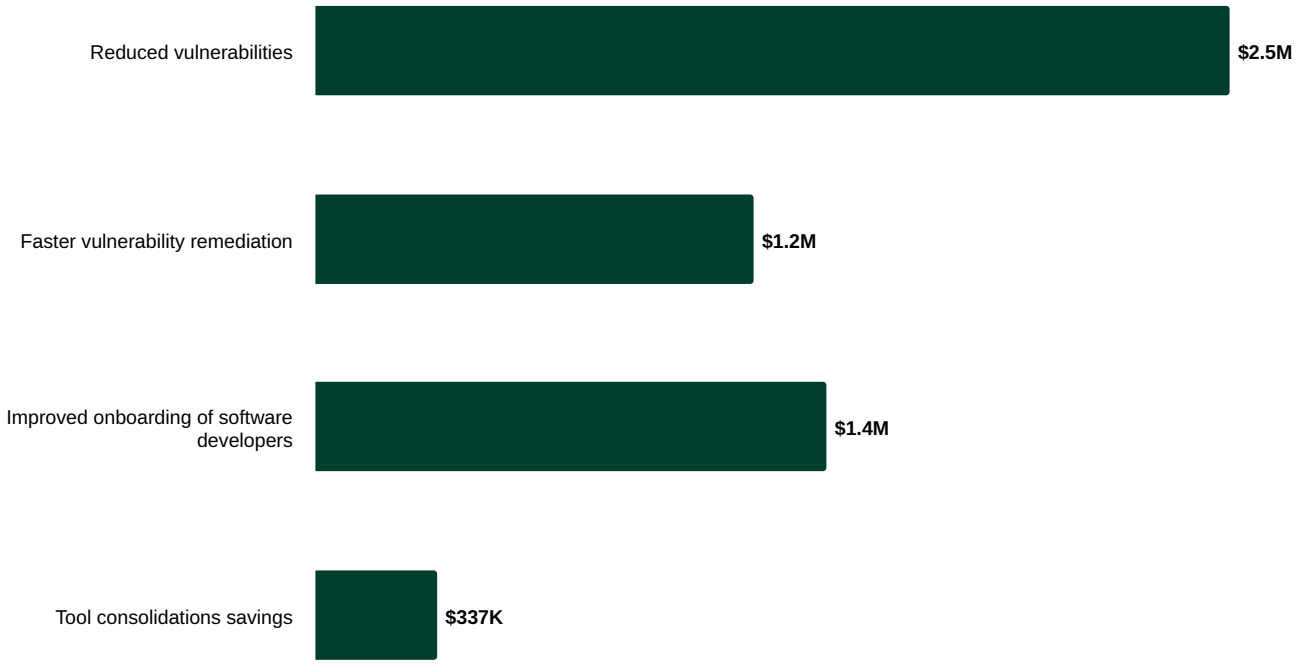
$4.0M

Net present value (NPV)

<6 months

Payback

Benefits (Three-Year)



The JFrog Software Supply Chain Security Customer Journey

Drivers leading to the JFrog investment

Interviews					
Role	**Industry**	**Headquarters**	**Geographic Focus**	**Annual Revenue**	**Employees/Users**
Principal engineer	Telecommunications	US	Global	$1B	3,600 employees; 200 users
Senior chapter lead, DevOps and cloud	Insurance	UK	UK	$6.5B	15,400 employees; 500 users
Head of R&D information systems	Healthcare	Israel	Israel	$1.5B	10,000 employees; 20 users
Software supply chain manager	Telecommunications	US	Global	$68M	285 employees; 50 users
Director of software development	Pharmaceuticals	US	Global	$470M	750 employees; 23 users

Key Challenges

Before implementing JFrog, interviewees' organizations relied on fragmented, inconsistent, and often manual approaches to software development and security. Their teams used a patchwork of tools for artifact management, vulnerability scanning, and compliance reporting, which created inefficiencies, blind spots, and operational risks. These limitations made it difficult to scale secure development practices, respond quickly to vulnerabilities, or maintain audit readiness — especially in regulated industries.

Interviewees noted how their organizations struggled with common challenges, including the following:

- **Toolchain fragmentation hindered collaboration and standardization.** Interviewees said their teams used different tools for artifact management, vulnerability scanning, and CI/CD integration, resulting in duplicated effort and inconsistent results. This lack of a unified platform made it difficult to enforce shared practices or maintain governance across teams and geographies.
- **Manual vulnerability triage overwhelmed security teams.** Without contextual analysis, security teams at the interviewees' organizations had to investigate each CVE manually — tracing dependency trees, reviewing code paths, and validating exposure. This process was time-consuming, error-prone, and often delayed remediation by days.
- **Inconsistent security practices created blind spots.** Some interviewees noted their teams used open-source scanners, while others used commercial tools and many had no scanning at all. Security was often bolted on late in the development cycle, making it difficult to enforce policies or ensure compliance across the organization.
- **Delayed remediation cycles increased risk and rework.** Vulnerabilities were frequently discovered after code had shipped, requiring emergency patches and formal documentation. One interviewee noted that patching in production could take days and required coordination across multiple teams.
- **Limited supply chain visibility impeded risk management.** Teams at the interviewees' organizations lacked a centralized view of open-source usage, license compliance, and transitive dependencies. SBOMs were generated manually — if at all — making it difficult to respond to zero-day vulnerabilities or customer security audits.
- **Audit readiness was reactive and labor-intensive.** According to interviewees, preparing for audits required manual report gathering, package validation, and risk justification. In some cases, interviewees' organizations relied on external consultants due to the lack of automation and centralized reporting, increasing both cost and effort.

> *"We spent two or three days on a number of vulnerabilities before we used JFrog to figure out if we were using the piece of code where the vulnerability existed."*
>
> **Software supply chain manager, telecommunications software**

> *"Before JFrog, there was just a complete ban on using any open-source platform inside the company. … Every time you wanted to use one, you had to manually approve it with the security guys. It could take weeks."*
>
> **Head of R&D information systems, healthcare**

Solution Requirements

The interviewees searched for a solution that could:

- **Proactively manage vulnerabilities and reduce risk exposure across the software supply chain.** Interviewees said their organizations sought capabilities to block high-risk or malicious open-source components before they entered development environments, while also embedding scanning and contextual analysis earlier in the lifecycle to prevent issues from reaching production.
- **Streamline and consolidate fragmented toolchains.** Interviewees said their teams sought to eliminate redundant tools for artifact management, vulnerability scanning, and compliance reporting, aiming for a unified platform that could support DevOps, DevSecOps, and MLOps workflows.
- **Automate and simplify audit and compliance processes.** Interviewees wanted to reduce the manual burden of audit preparation by generating SBOMs and vulnerability reports automatically, ensuring readiness for customer and regulatory reviews.
- **Accelerate vulnerability remediation without slowing down delivery.** Interviewees' organizations required real-time feedback and contextual prioritization to help developers and security teams identify and resolve issues quickly and efficiently.
- **Empower developers with secure, self-service workflows.** The interviewees' teams looked for tools that would enable developers to act independently with confidence, reducing reliance on security teams and improving development velocity.
- **Standardize DevSecOps practices across teams and geographies.** Interviewees emphasized the need for consistent policies, pipelines, and access controls to scale secure development practices across distributed environments.

After evaluating multiple vendors through a business case and RFP process, the interviewees' organizations selected JFrog and began deployment. Several interviewees said their organizations initiated implementation with a focused rollout to high-priority teams, such as platform engineering or DevSecOps, before expanding to broader development groups. In many cases, adoption was accelerated by developer enthusiasm for integrated tooling and security automation, with some teams beginning to use the platform even before formal licensing was finalized.

> *"We were looking to streamline our toolchains and reduce complexity. Having a unified platform helped us eliminate redundant tools and improve consistency."*
>
> **Senior chapter lead, DevOps and Cloud, insurance**

> *"We needed to proactively manage vulnerabilities and reduce risk exposure. Embedding security earlier in the pipeline was a key requirement for us."*
>
> **Head of R&D information systems, healthcare**

Composite Organization

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the interviewees' organizations, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

- **Description of composite.** The composite organization is a global enterprise with $2 billion in annual revenue. It is operating in a regulated industry with a strong emphasis on software quality, compliance, and security. The composite employs 6,000

people, including 500 engineers across development, DevOps, QA, and security roles, and supports a hybrid mix of cloud-native and on-premises applications with growing adoption of microservices and DevSecOps practices.

- **Deployment characteristics.** The composite organization deploys a SaaS-based solution using an enterprise-tier license, integrating artifact management, vulnerability scanning, and advanced security into CI/CD pipelines and developer workflows. The rollout began with platform and security teams and expanded to development groups across multiple geographies with federated repositories and automated policy enforcement supporting global collaboration and scalability.

KEY ASSUMPTIONS

- $2 billion in annual revenue
- 6,000 total employees
- 500 engineers across DevSecOps and QA
- Hybrid cloud/on-prem architecture with global operations and growing DevSecOps adoption

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Reduced vulnerabilities	$1,017,900	$1,017,900	$1,017,900	$3,053,700	$2,531,367
Btr	Faster vulnerability remediation	$462,840	$462,840	$462,840	$1,388,520	$1,151,015
Ctr	Improved onboarding of software developers	$565,326	$565,326	$565,326	$1,695,978	$1,405,882
Dtr	Tool consolidation savings	$135,660	$135,660	$135,660	$406,980	$337,366
	Total benefits (risk-adjusted)	$2,181,726	$2,181,726	$2,181,726	$6,545,178	$5,425,630

Reduced Vulnerabilities

Evidence and data. Interviewees shared that prior to implementation, their organizations faced significant challenges in identifying and managing software vulnerabilities. After adopting the solution, they experienced measurable improvements in both the volume of vulnerabilities getting into the developer environment and reaching production and the speed at which they could be remediated.

- Interviewees said their security teams spent days manually investigating CVEs, tracing dependency trees, and validating exposure before JFrog. A software supply chain manager at a telecommunications company shared, “We spent two or three days on a number of vulnerabilities before we used JFrog to figure out if we were using the piece of code where the vulnerability existed.”
- After implementation, interviewees’ organizations embedded contextual analysis into their CI/CD pipelines, helping prioritize and remediate issues that were the most applicable to their business.
- A director of software development at a pharmaceutical company noted: “After implementing JFrog within a few months, we started narrowing things down. We saw like a 30% reduction in critical vulnerabilities that were exposed.”
- A principal engineer at a telecommunications company added, “We want people to know right away that they’ve got an issue, and with JFrog, as soon as they scan something or push something, we’ll know right away.”

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization experienced 4,000 vulnerabilities annually prior to implementation.
- With the solution in place, the composite organization reduces vulnerabilities by 65%, avoiding approximately 2,600 issues per year.
- The average cost to remediate a single vulnerability is estimated at $435.
- These avoided vulnerabilities represent a reduction in security exposure and remediation workload driven by early detection and contextual analysis integrated into CI/CD workflows.

Risks. The value of this benefit can vary across organizations due to the following:

- The baseline number of vulnerabilities may differ depending on the size and complexity of the software portfolio.
- The percentage reduction in vulnerabilities may vary based on how effectively contextual analysis and shift-left practices are implemented.
- The cost per vulnerability may fluctuate depending on labor rates, remediation processes, and the severity of issues encountered.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.5 million.

65%

Reduced vulnerabilities reaching production through early detection and contextual analysis integrated into CI/CD pipelines

> *"We saw a significant reduction in critical vulnerabilities that were exposed after implementing the platform within a few months."*
>
> **Director of software development, pharmaceuticals**

Reduced Vulnerabilities					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	Vulnerabilities before JFrog	Composite	4,000	4,000	4,000
A2	Reduction in vulnerabilities attributable to JFrog	Composite	65%	65%	65%
A3	Vulnerabilities after JFrog	A1*(1-A2)	1,400	1,400	1,400
A4	Avoided vulnerabilities due to JFrog	A1-A3	2,600	2,600	2,600
A5	Average cost of each vulnerability	Composite	$435	$435	$435
At	Reduced vulnerabilities	A4*A5	$1,131,000	$1,131,000	$1,131,000
	Risk adjustment	↓10%			
Atr	Reduced vulnerabilities (risk-adjusted)		$1,017,900	$1,017,900	$1,017,900
	Three-year total: $3,053,700		**Three-year present value: $2,531,367**		

Faster Vulnerability Remediation

Evidence and data. Interviewees reported that JFrog significantly accelerated their ability to identify and resolve vulnerabilities. This improvement was attributed to automation, better visibility into dependencies, and streamlined workflows.

- A senior chapter lead of DevOps and Cloud at an insurance firm shared: "Before JFrog, we had to manually trace dependencies and patch vulnerabilities. Now, it's largely automated and much faster." This highlighted a shift from manual, time-intensive processes to automated remediation.
- A head of R&D information systems at a healthcare company noted: "JFrog helped us cut our remediation time dramatically. We're now able to respond to threats in near real time." This emphasized the platform's impact on response speed and operational agility.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization remediates 1,400 vulnerabilities per year, with each requiring 1 hour after JFrog implementation.
- This reflects an 80% reduction in remediation time compared to pre-JFrog processes, saving 4 hours per vulnerability.
- The fully burdened hourly rate for a software developer is $87.
- These assumptions are based on consistent patterns observed across interviewees and are expected to remain stable over the three-year analysis period.

Risks. The value of this benefit can vary across organizations due to the following:

- The number of vulnerabilities remediated annually may vary depending on the organization's size, industry, and threat landscape.
- Time savings may differ based on the complexity of vulnerabilities and the maturity of existing remediation workflows.
- Regional differences in labor costs could impact the overall financial benefit.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.2 million.

80%

Faster vulnerability remediation

> *"We no longer spend days chasing down vulnerabilities. JFrog gives us the visibility and automation to act within hours, not days.*
>
> **Software supply chain manager, telecommunications**

Faster Vulnerability Remediation					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	Time required to remediate vulnerability prior to JFrog (hours)	Composite	5	5	5
B2	Percentage of time saved per vulnerability with JFrog	Composite	80%	80%	80%
B3	Time required to remediate vulnerability after JFrog (hours)	Composite	1	1	1
B4	Time saved per vulnerability (hours)	Composite	4	4	4
B5	Fully burdened hourly salary for a software developer	Composite	$87	$87	$87
B6	Vulnerabilities after JFrog	A3	1,400	1,400	1,400
Bt	Faster vulnerability remediation	B4*B5*B6	$487,200	$487,200	$487,200
	Risk adjustment	↓5%			
Btr	Faster vulnerability remediation (risk-adjusted)		$462,840	$462,840	$462,840
	Three-year total: $1,388,520		**Three-year present value: $1,151,015**		

Improved Onboarding Of Software Developers

Evidence and data. Interviewees shared that JFrog helped streamline the onboarding process for new developers by reducing setup time, improving access to tools, and eliminating manual configuration steps. These improvements led to faster productivity and reduced ramp-up time.

A senior chapter lead of DevOps and Cloud at an insurance company said: "Before JFrog, onboarding a new developer could take days. Now, they're up and running in a matter of hours with everything they need already integrated." This interviewee continued: "We used to spend a lot of time configuring environments and permissions. JFrog standardized that process and made onboarding much more efficient."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization onboards 180 software developers annually.
- Each developer saves 38 hours during onboarding due to streamlined setup and access to preconfigured environments.

- The fully burdened hourly rate for a software developer is $87.
- These assumptions reflect consistent feedback from interviewees and are expected to remain stable over the three-year analysis period.

Risks. The value of this benefit can vary across organizations due to the following:

- The number of developers onboarded annually may vary depending on hiring trends and organizational growth.
- Time savings may differ based on the complexity of the development environment and existing onboarding processes.
- Labor costs may fluctuate by region or role, affecting the financial impact.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.4 million.

38 hours

Time saved per developer

> *"New hires used to spend their first week just getting set up. With JFrog, they're contributing code by day two."*
>
> **Senior chapter lead, DevOps and Cloud, insurance**

Improved Onboarding Of Software Developers					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
C1	Time saved onboarding each software developer (hours)	Composite	38	38	38
C2	Fully burdened hourly salary for a software developer	Composite	$87	$87	$87
C3	Software developers onboarded per year	Composite	180	180	180
Ct	Improved onboarding of software developers	C1*C2*C3	$595,080	$595,080	$595,080
	Risk adjustment	↓5%			
Ctr	Improved onboarding of software developers (risk-adjusted)		$565,326	$565,326	$565,326
	Three-year total: $1,695,978		**Three-year present value: $1,405,882**		

Tool Consolidation Savings

Evidence and data. Interviewees shared that JFrog enabled them to eliminate redundant tools and reduce the overhead associated with managing multiple platforms. These changes led to direct cost savings and operational efficiencies.

A software supply chain manager at telecommunications company shared: "We were able to retire several legacy tools after adopting JFrog. That alone saved us tens of thousands annually." This interviewee also noted: "Tool sprawl was a real issue. JFrog helped us consolidate and simplify our toolchain, which also reduced the time we spent managing licenses and integrations."

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization reduced its annual DevOps and DevSecOps tool spend from $180,000 to $52,200 after adopting JFrog. This reflects a 71% reduction in tool spend.
- In addition to license savings, the composite organization realizes $15,000 annually in reduced management effort due to fewer tools and simplified administration.

- These assumptions are based on consistent patterns observed across interviewees and are expected to remain stable over the three-year analysis period.

Risks. The value of this benefit can vary across organizations due to the following:

- The extent of tool consolidation may vary depending on the organization's existing tool landscape and contractual obligations.
- Some organizations may retain certain tools due to team preferences or integration dependencies.
- Savings from reduced management effort may differ based on team size and administrative complexity.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $337,000.

71%

Reduction in software development tool spend

> *"We eliminated overlapping tools and cut down on license costs. JFrog gave us everything we needed in one platform."*
>
> **Software supply chain manager, telecommunications**

Tool Consolidation Savings					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Spend on software development tools before JFrog	Interviews	$180,000	$180,000	$180,000
D2	Reduction in software development tool spend with JFrog	Interviews	71%	71%	71%
D3	Spend on software development tools after JFrog	D1*(1-D2)	$52,200	$52,200	$52,200
D4	**Subtotal: Cost savings from tool consolidation**	**D1-D3**	**$127,800**	**$127,800**	**$127,800**
D5	Additional savings from reduced management effort	Interviews	$15,000	$15,000	$15,000
Dt	Tool consolidation savings	D4+D5	$142,800	$142,800	$142,800
	Risk adjustment	↓5%			
Dtr	Tool consolidation savings (risk-adjusted)		$135,660	$135,660	$135,660
	Three-year total: $406,980		**Three-year present value: $337,366**		

Unquantified Benefits

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Greater developer confidence and autonomy.** Multiple interviewees cited that developers no longer had to wait on security teams to identify issues late in the cycle. Instead, IDE-level integration and early detection with real-time feedback and contextual vulnerability analysis allowed them to self-manage dependencies and remediate issues proactively, accelerating development without compromising security.
- **Faster and more consistent audit readiness.** Interviewees from organizations in regulated industries like healthcare and finance emphasized that JFrog's automation significantly reduced manual effort in audit readiness due to automated SBOM generation and continuous software composition analysis (SCA). Terraform-based configurations and regulatory-ready SBOMs were also specifically mentioned as key enablers for consistent, repeatable compliance reporting.

- **Reduced noise in vulnerability management.** Interviewees consistently praised JFrog's AI-driven filtering and contextual prioritization with its contextual CVE analysis, which helped them avoid wasting time on irrelevant vulnerabilities and instead focus on real threats. This improved trust in the tooling and reduced unnecessary remediation cycles.
- **Improved cross-functional collaboration.** Interviewees noted JFrog has shared dashboards and unified toolchains. It also serves as a common platform across DevSecOps teams. Interviewees highlighted how shared visibility into security issues and standardized practices — especially in globally distributed environments — improved alignment and reduced friction at their organizations.
- **Enhanced resilience and business continuity.** Teams emphasized that JFrog's cloud-native model ensured uninterrupted access across time zones and geographies. Federation and remote proxies enabled builds to continue during outages, while secure access and continuous scanning supported both software and IoT teams in maintaining operational continuity.
- **Improved technological performance through modern architecture.** Interviewees emphasized JFrog's SaaS delivery model, broad package support, and Terraform-based configuration as key enablers for reducing operational overhead and simplifying toolchain management. These features helped the interviewees' organizations standardize DevOps, DevSecOps, and MLOps practices and accelerate modernization efforts.

> *"We're spending a little to get a lot more engineering time. JFrog takes work out of developers' hands and lets them focus on what matters — building secure, high-quality software faster."*
>
> **Principal engineer, telecommunications**

Flexibility

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement JFrog and later realize additional uses and business opportunities, including:

- **Accelerated onboarding and scaling of engineering teams.** Multiple interviewees noted that JFrog's standardized toolchains, role-based access controls, and federated repositories enabled faster onboarding of new developers and smoother scaling of teams. One director of software development at a pharmaceuticals company shared that onboarding time was reduced by a full week per engineer, while a principal engineer emphasized that "people could go to other people's build jobs or look at their build specs and copy them exactly," accelerating productivity across distributed teams.
- **Improved resilience and business continuity in distributed environments.** JFrog's federation, caching, and proxying capabilities allowed teams at the interviewees' organizations to continue building and deploying even during outages or connectivity issues. A software supply chain manager at a telecommunications organization described how JFrog kept development running during a sitewide internet shutdown: "People that were doing it directly to the internet, things were broken. If you pull too many Docker containers down, you run out of tokens, you'll get shut down. Artifactory keeps us afloat even when we cut access to the internet to our sites."
- **Expanded DevSecOps standardization across global teams.** Interviewees' organizations used JFrog to unify Dev, Sec, and Ops practices across geographies and business units. A senior chapter lead of DevOps and cloud in insurance noted, "We've managed to simplify [access] by how JFrog is configured. We've got six different roles in JFrog across the whole of our engineering department of just under 500 engineers." This standardization reduced tool sprawl and enabled consistent security and compliance practices at scale.
- **Future-ready platform for MLOps and AI integration.** While not yet fully deployed in all interviewees' organizations, several interviewees cited JFrog's potential to support AI/ML workflows. One principal engineer at a telecommunications company described how their MLOps team was already using Artifactory as a model registry, reducing latency and improving collaboration: "People were using half their shift just downloading these gigantic models. Now they push to the closest Artifactory, and it federates back. Their models are already there and ready to go."
- **Support for customer-facing innovation and edge deployments.** A director of software development shared plans to use JFrog to support customer-facing edge devices: "We have customers that want to pull from our servers. Instead of putting something on a big SFTP [secure file transfer protocol] site, they want to connect to our registries directly. This is something we're looking at, and it was a requirement from one of our customers."

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Total Economic Impact Approach).

> *"People could go to other people's build jobs or look at their build specs and copy them exactly. It gave us a good-quality pattern to follow."*
>
> **Principal engineer, telecommunications**

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Initial implementation and setup	$22,050	$0	$0	$0	$22,050	$22,050
Ftr	Annual license fees	$0	$467,500	$467,500	$467,500	$1,402,500	$1,162,603
Gtr	Ongoing professional services	$0	$82,500	$82,500	$82,500	$247,500	$205,165
Htr	Ongoing labor and management	$0	$11,865	$11,865	$11,865	$35,595	$29,506
	Total costs (risk-adjusted)	$22,050	$561,865	$561,865	$561,865	$1,707,645	$1,419,324

Initial Implementation And Setup

Evidence and data. Interviewees described implementation as relatively lightweight, with most of their organizations completing setup within one to two months.

- A principal engineer at a telecommunications company shared: “We had five deployments and got up and running quickly. Our tiger team did a side-by-side comparison with other tools, and once we validated JFrog’s contextual analysis, adoption was easy.”
- A senior chapter lead of DevOps and Cloud at an insurance firm noted: “We configured everything using Terraform, which made the setup scalable and consistent. The biggest delays were legal and procurement, not technical.”
- Across interviewees’ organizations, implementation typically involved three to eight internal resources, including DevOps, security, and platform engineers, contributing between 25% and 50% of their time over a four- to six-week period.
- A head of R&D information systems in healthcare emphasized: “We were fully integrated in about a month. JFrog supported us even before procurement was finalized, and we didn’t need external services.”
- Pricing may vary. Contact JFrog for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- It has a team of five internal resources support implementation over a six-week period, each contributing 50% of their time.
- The composite also purchases a limited package of professional services from JFrog to accelerate configuration and best-practice alignment.
- Based on these assumptions, the total cost of initial implementation and setup is estimated at $21,000.

Risks. The value of this cost can vary across organizations due to the following:

- The scope and complexity of the deployment (e.g., number of sites, repositories, or integrations).
- The availability and skill level of internal DevOps and security resources.
- Whether professional services are purchased to support implementation.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $22,000.

Initial Implementation And Setup						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Initial implementation and setup	Composite	$21,000			
Et	Initial implementation and setup	E1	$21,000	$0	$0	$0
	Risk adjustment	↑5%				
Etr	Initial implementation and setup (risk-adjusted)		$22,050	$0	$0	$0
	Three-year total: $22,050				**Three-year present value: $22,050**	

Annual License Fees

Evidence and data. Interviewees reported a wide range of license fees depending on the number of deployments, product tiers, and add-ons such as Advanced Security and Curation.

- Interviewees emphasized that pricing was generally aligned with usage and scale and that JFrog's bundled pricing simplified procurement.
- Several interviewees noted that license fees were justified by the consolidation of multiple tools and the ability to scale usage across globally distributed teams.
- Pricing may vary. Contact JFrog for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite organization pays $467,500 annually in license fees. JFrog provided the annual license fees for the composite organization, which also includes customer success costs. Forrester has broken out customer success costs separately and will detail them later in this section of the study.
- This includes access to the JFrog Platform (Enterprise X tier), Advanced Security, and Curation modules, but excludes Runtime.
- The license also covers multiple federated deployments and supports approximately 500 developers across DevSecOps teams.

Risks. The value of this cost can vary across organizations due to the following:

- The number of users, deployments, and repositories supported.
- The inclusion or exclusion of optional modules such as Runtime or Curation.
- Contract length, discounting, and regional pricing differences.

Results. To account for these risks, Forrester adjusted this cost upward by 0%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $1.2 million.

Annual License Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Annual license fees	Composite		$467,500	$467,500	$467,500
Ft	Annual license fees	F1	$0	$467,500	$467,500	$467,500
	Risk adjustment	0%				
Ftr	Annual license fees (risk-adjusted)		$0	$467,500	$467,500	$467,500
	Three-year total: $1,402,500				**Three-year present value: $1,162,603**	

Ongoing Professional Services

Evidence and data. Interviewees described JFrog's customer success services as a critical enabler of successful adoption and long-term value realization, highlighting a blend of onboarding, technical support, and strategic guidance.

- Interviewees consistently emphasized the value of JFrog's customer success support, including onboarding, technical enablement, and ongoing account management.
- A senior chapter lead of DevOps and Cloud at an insurance firm shared: "We purchased 152 hours of professional services at a discounted rate of $48,000. That included onboarding, enablement, and ongoing support. It was worth every dollar."
- A principal engineer in the telecom industry noted: "We had direct access to JFrog's developers and principal engineers. They helped us troubleshoot licensing issues and optimize our federation setup. That level of support is rare."
- A head of R&D information systems at a healthcare organization reported: "We received unlimited support and enablement as part of our Enterprise X package. JFrog was responsive and proactive, even before procurement was finalized."
- Interviewees described customer success as a blend of technical support, training, and strategic guidance. Several interviewees highlighted the importance of JFrog's white-glove onboarding and the ability to engage directly with product experts.
- While some interviewees said their organizations bundled customer success into their license agreements, others purchased it as a separate line item or through professional services packages.
- Pricing may vary. Contact JFrog for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite incurs $82,500 annually in customer success costs. This includes onboarding and implementation support, customer success management, technical support services, and ongoing training and enablement.
- These services are delivered through a combination of bundled support and dedicated professional services hours.

Risks. The value of this cost can vary across organizations due to the following:

- The level of internal expertise and need for external onboarding or enablement.
- Whether customer success services are bundled into license fees or purchased separately.
- The complexity of the deployment and number of federated environments supported.

Results. To account for these risks, Forrester adjusted this cost upward by 0%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $205,000.

Ongoing Professional Services						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Ongoing professional services	Composite		$82,500	$82,500	$82,500
Gt	Ongoing professional services	G1	$0	$82,500	$82,500	$82,500
	Risk adjustment	0%				
Gtr	Ongoing professional services (risk-adjusted)		$0	$82,500	$82,500	$82,500
	Three-year total: $247,500			**Three-year present value: $205,165**		

Ongoing Labor And Management

Evidence and data. Interviewees reported that the ongoing management of the JFrog Platform required minimal effort, with most of their organizations allocating only a small fraction of internal resources to monitor usage, manage repositories, and support developers. Despite the platform's broad adoption, administrative overhead remained low due to automation, SaaS delivery, and intuitive tooling.

- A senior chapter lead of DevOps and Cloud at a financial services / insurance firm shared: "We spend maybe half a day per week across our entire platform team. It's not one person - it's a shared responsibility across 70 engineers."

- A principal engineer in the telecom industry noted: “We’re using JFrog for everything — storage, scanning, release — but the day-to-day management is light. We check usage, provision new repos, and that’s about it.”
- A software supply chain manager at a telecom firm said: “I spend maybe one to 2 hours a month checking usage and responding to the occasional request. We don’t need to manage upgrades or infrastructure anymore.”
- Interviewees emphasized that the SaaS delivery model and automation features significantly reduced administrative overhead compared to self-hosted alternatives.
- Several interviewees noted that repository provisioning, access control, and policy enforcement were largely automated or managed through infrastructure-as-code tools like Terraform.
- Pricing may vary. Contact JFrog for additional details.

Modeling and assumptions. Based on the interviews, Forrester assumes the following about the composite organization:

- The composite allocates a portion of one full-time equivalent (FTE) to ongoing platform management. This includes time spent monitoring usage, provisioning repositories, managing access, and supporting internal users.
- The composite organization leverages automation and SaaS delivery to minimize manual effort, resulting in an estimated annual cost of $11,300.

Risks. The value of this cost can vary across organizations due to the following:

- The number of federated environments and repositories managed.
- The degree of automation and use of infrastructure-as-code.
- The internal support model and volume of developer requests.

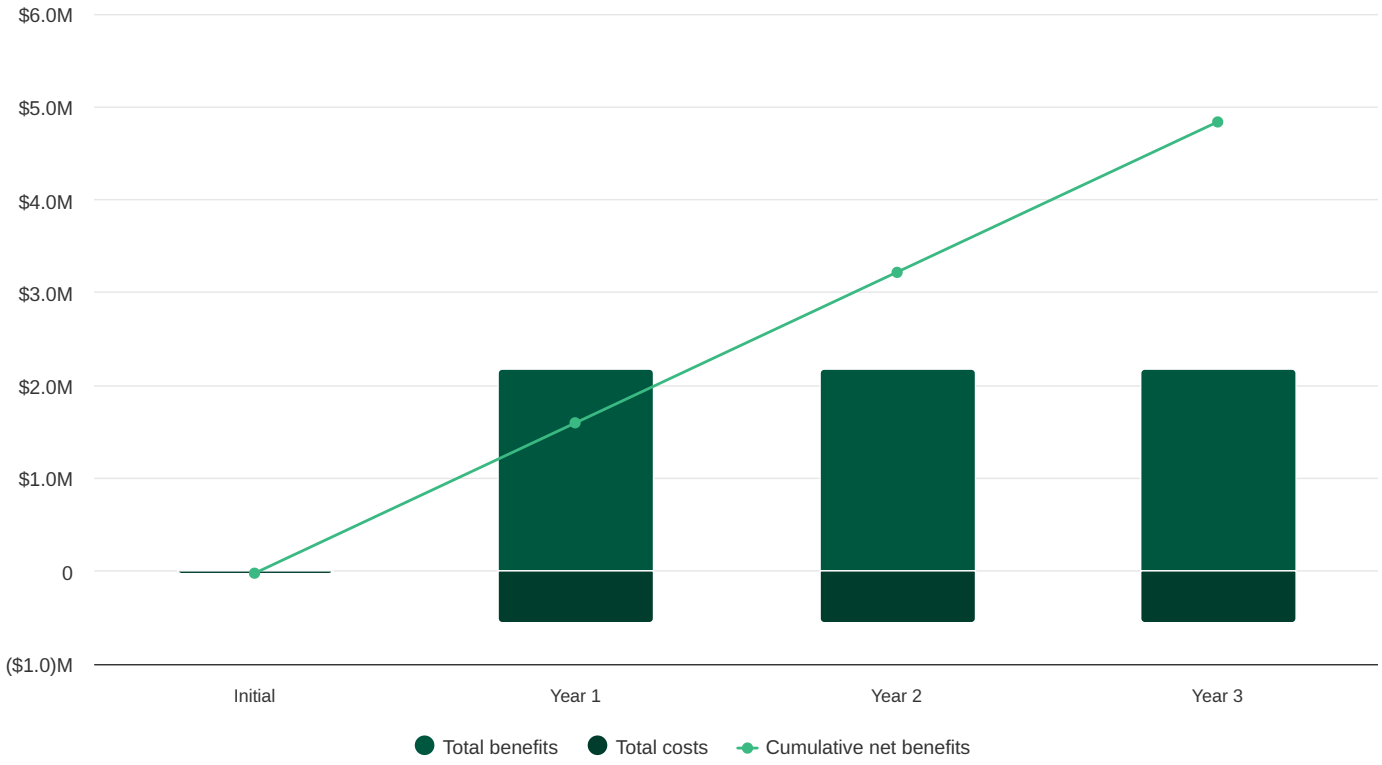
Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $30,000.

Ongoing Labor And Management						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
H1	Ongoing labor and management	Composite		$11,300	$11,300	$11,300
Ht	Ongoing labor and management	H1	$0	$11,300	$11,300	$11,300
	Risk adjustment	↑5%				
Htr	Ongoing labor and management (risk-adjusted)		$0	$11,865	$11,865	$11,865
	Three-year total: $35,595			**Three-year present value: $29,506**		

Financial Summary

Consolidated Three-Year, Risk-Adjusted Metrics

Cash Flow Chart (Risk-Adjusted)



Cash Flow Analysis (Risk-Adjusted)						
	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($22,050)	($561,865)	($561,865)	($561,865)	($1,707,645)	($1,419,324)
Total benefits	$0	$2,181,726	$2,181,726	$2,181,726	$6,545,178	$5,425,630
Net benefits	($22,050)	$1,619,861	$1,619,861	$1,619,861	$4,837,533	$4,006,306
ROI						282%
Payback						<6 months

Please Note

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI, NPV, and payback period for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI, NPV, and payback period values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

TEI Framework And Methodology

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in JFrog.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that JFrog can have on an organization.

Due Diligence

Interviewed JFrog stakeholders and Forrester analysts to gather data relative to JFrog.

Interviews

Interviewed five decision-makers at organizations using JFrog to obtain data about costs, benefits, and risks.

Composite Organization

Designed a composite organization based on characteristics of the interviewees' organizations.

Financial Model Framework

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

Case Study

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

Glossary

Total Economic Impact Approach

Benefits

Benefits represent the value the solution delivers to the business. The TEI methodology places equal weight on the measure of benefits and costs, allowing for a full examination of the solution's effect on the entire organization.

Costs

Costs comprise all expenses necessary to deliver the proposed value, or benefits, of the solution. The methodology captures implementation and ongoing costs associated with the solution.

Flexibility

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. The ability to capture that benefit has a PV that can be estimated.

Risks

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

Financial Terminology

Present value (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PVs of costs and benefits feed into the total NPV of cash flows.

Net present value (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

Return on investment (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

Discount rate

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

Payback

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendixes

APPENDIX A

Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

APPENDIX B

Endnotes

[1] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists solution providers in communicating their value proposition to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of business and technology initiatives to both senior management and other key stakeholders.

Disclosures

Readers should be aware of the following:

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in JFrog.

JFrog reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

JFrog provided the customer names for the interviews but did not participate in the interviews.

Consulting Team:
Roger Nauth

PUBLISHED
January 2026