

JFrog (Q1 2026 Earnings)
May 8, 2026

Corporate Speakers

- Jeffrey Schreiner; JFrog; Head of Investor Relations
- Shlomi Ben Haim; JFrog; Co-Founder and Chief Executive Officer
- Ed Grabscheid; JFrog; Chief Financial Officer

Participants

- Sanjit Singh; Morgan Stanley; Analyst
- Radi Sultan; UBS; Analyst
- Michael Cikos; Needham; Analyst
- Miller Jump; Truist Securities; Analyst
- Howard Ma; Guggenheim Securities; Analyst
- Mark Cash; Raymond James; Analyst
- Jason Salino; KeyBanc Capital Markets; Analyst
- Kingsley Crane; Canaccord Genuity; Analyst
- Shrenik Kothari; Baird; Analyst
- Brad Reback; Stifel; Analyst
- Lucky Schreiner; D.A. Davidson; Analyst
- Jason Ader; William Blair and Company; Analyst
- Andrew Sherman; TD Cowen; Director, Enterprise Software
- Koji Ikeda; Bank of America; Analyst

PRESENTATION

Operator^ Ladies and gentlemen, thank you for joining us and welcome to the JFrog First Quarter 2026 Financial Results Earnings Call.

After today's prepared remarks, we will host a question-and-answer session. (Operator Instructions)

I will now hand the conference over to Jeffrey Schreiner, Head of Investor Relations. Jeffrey, please go ahead.

Jeffrey Schreiner^ Thank you, [Nicole]. Good afternoon and thank you for joining us as we review JFrog's First Quarter 2026 Financial Results, which were announced following the market close today via press release. Leading the call today will be JFrog's CEO and Co-Founder Shlomi Ben Haim and Ed Grabscheid, JFrog's CFO.

During this call, we may make statements related to our business that are forward-looking under federal securities laws and are made pursuant to the safe harbor provisions of the Private Securities Litigation Reform Act of 1995, including statements related to our future financial performance and including our outlook for the second quarter and full year of 2026.

The words anticipate, believe, continue, estimate, expect, intend, will, and similar expressions are intended to identify forward-looking statements or similar indications of future expectations. You are cautioned not to place undue reliance on these forward-looking statements, which reflect our views only as of today and not as of any subsequent date. Please keep in mind that we are not obligating ourselves to revise or publicly release the results of any revision to these forward-looking statements in light of new information or future events. These statements are subject to a variety of risks and uncertainties that could cause actual results to differ materially from expectations.

For a discussion of material risk and other important factors that could affect our actual results, please refer to our Form 10-K for the year ended December 31st, 2025, which is available on the Investor Relations section of our website and the earnings press release issued earlier today. Additional information will be made available in our Form 10-Q for the quarter ended March 31, 2026, and other filings and reports that we may file from time to time with the SEC.

Additionally, non-GAAP financial measures will be discussed on this conference call. These non-GAAP financial measures, which are used as measure of JFrog's performance, should be considered in addition to, not as a substitute for, or in isolation from GAAP measures.

Please refer to the tables in our earnings release for reconciliation of those measures to their most directly comparable GAAP financial measures. A replay of this call will be available on the JFrog Investor Relations website for a limited time. With that, I'd like to turn the call over to JFrog CEO, Shlomi Ben Haim.

Shlomi?

Shlomi Ben Haim^ Thank you, Jeff. Good afternoon and thank you all for joining the call.

We entered 2026 strong. Our first quarter performance reflects both the clarity of our strategy and the discipline in execution. Our continuous focus on powering the world's software through JFrog Artifactory as a system of record for trusted binaries, software packages, and AI artifacts is resonating deeply with market demand. We are seeing growing adoption among the world's leading organizations and AI labs, which are choosing JFrog as they transform to adopt modern software supply chain practices.

Across industries, geographies, and deployment environments, whether cloud or on-prem, our customers are partnering with JFrog as their foundational platform while they navigate a complex transition of adding AI technologies and tools to their software supply chain. They tell us they are prioritizing AI adoption while simultaneously maintaining legacy pipelines and open-source packages, all as they demand stronger security, governance, and fast release cycles. We are working closely with our customers, the broader developer community, and AI-native companies to support them through this period of change. Our Q1 results reflect this momentum with AI redefining the software supply chain and powering our continued expansion.

In the first quarter, JFrog delivered total revenue of \$154 million, representing 26% year-over-year growth. Cloud revenue grew 50% year-over-year, underscoring the accelerating shift toward our cloud-first platform. This performance was driven by continuous strength across our core growth vectors, increasing consumption of our cloud services, rising demand for our software supply chain security solutions, higher ASP on new customer acquisitions, and robust expansion within our existing customer base. We also saw continued momentum at the high end of our customer portfolio. The number of customers with annual spend exceeding \$1 million grew to 80, up from 54 a year ago, representing 48% year-over-year growth.

Customers spending more than \$100,000 annually increased to 1,225 compared to 1,051 in the prior year, representing 17% year-over-year growth. These results reflect our alignment with the evolving needs of modern enterprises. Developers and increasingly AI agents are producing software at scale and speed. This surge in binaries fueled by AI is driving the need for a single, trusted system of record to manage, secure, and govern these assets across the entire supply chain.

On today's call, I will walk you through the quarter in detail, and Ed will follow with our updated outlook and additional financial insights. Now, I will highlight the key drivers behind our performance this quarter.

First, continued cloud growth, driven by increasing consumption and rising demand for a true system of record as a service, delivering scale and universality. Second, the sustained momentum in our security business, as customers prioritize end-to-end protection and governance amid rising software supply chain attacks. And finally, I will highlight our ongoing innovation that leads to solid adoption of our platform and Enterprise+ subscription growth.

Let me start with our cloud business. As mentioned earlier, cloud revenue in Q1 grew 50% year-over-year, an exceptional result that reflects not one single driver, but a broader trend we have been observing over the past several quarters.

As AI makes human-to-technology interaction nearly costless, and source codes itself increasingly commoditized, binaries become king. Organizations are actively encouraging developers to utilize AI coding agents, as well as explore agentic capabilities, causing software output to accelerate, resulting in more compiled code, a true AI-fueled tsunami of binaries. Observing our customers' consumption trends, we notice that this growth is not tied to one package type or a specific AI-native workload. It is not a spike in usage or a one-time increase in open-source caching. It is the result of a fundamental shift in how software is being generated, delivered, and consumed across the software supply chain.

We are seeing an acceleration in the volume of compiled software flowing through the JFrog platform. This trend, which began taking shape in 2025, is driven by two major forces. First, developers are being supercharged by AI coding agents. Simply put, the world is creating more software packages. In this AI mass adoption reality, we see organizations willing to accept budget overruns until they gain better clarity on long-term usage requirements and prior to increases in annual commitment.

Second, as AI drives more software creation, it is also accelerating the flow of all open-source components. Open-source consumptions by developers and AI agents is rising across nearly every software package we support. And as the ultimate Switzerland of binaries, JFrog sits at the center of this growth. Whether through on-demand increased usage momentum or annual commitments, we believe JFrog Cloud is positioned to benefit from these trends.

Now, to the continued momentum we are seeing in security. As we mentioned in previous calls, modern software supply chain security is moving beyond traditional DevSecOps and fragmented scanners. AI coding agents are increasingly securing, scanning, and even fixing code rapidly at scale. And while still evolving, we see agents replacing human skills in code protection. We believe a trusted software supply chain requires a single authoritative system of record for all binaries and AI artifacts.

Building on this foundation, we deliver protection and governance beyond traditional scanning, analyzing, tracking, and proactively blocking risk at the point of entry or before distribution to production. As AI adoption accelerates and binaries scale, the threat landscape is becoming more complex. Software supply chain attacks are rising, increasingly targeting open-source creators and package maintainers. This dynamic drives the growing demand for a trusted control layer and stronger DevGovOps practices.

In Q1, we again demonstrated that customers subscribed to JFrog curation were effectively protected from recent software supply chain attacks. Curation serves as a critical control point at the gate, enforcing policies that ensure only trusted packages enter the system, keeping Artifactory clean.

Once artifacts are stored, JFrog Xray and JFrog Advanced Security continuously secure and govern the binary flow, providing ongoing visibility and protection. In addition, as advanced AI models like OpenAI, GPT, Cyber, and Anthropic's Claude become increasingly embedded in development workflows, we believe modern software supply chain security and governance are defined by four core pillars.

First, a centralized system of record, a single source of truth across multi-agent environments. Second, universal governance, consistent visibility and enforcement across all types of artifacts, whether consumed or generated. Third, predictable and deterministic protection, continuous policy-driven guardrails that prevent malicious or vulnerable components from progressing. And finally, comprehensive coverage, securing both newly generated assets and the extensive base of existing mission-critical legacy binaries.

Our customers tell us they are accelerating software development and generating more binaries through the JFrog platform. As AI adoptions expands, JFrog provides a unified system of record to secure, govern, and manage AI-generated, open-source, or legacy binaries in one place. Our customers' adoption, Q1 results, sales pipeline, and future roadmap innovation are aligned with these observations.

Looking ahead, we expect security to remain a key growth driver for JFrog. This sets the stage for an update on the innovation we introduced at our annual LEAP Conference in New York this

past March. LEAP is JFrog's top customers, gathered by region, scheduled globally during H1 every year.

At LEAP New York, we demonstrated GA-ready solutions to concrete customers' need for a trusted infrastructure layer for software supply chain management in the AI era. We introduced the JFrog MCP Registry, the first enterprise-grade registry for MCP servers, extending our platform to support the growing AI ecosystem. As MCP adoption expands, customers need a centralized, trusted way to manage, secure, and govern these new assets, which logically sits Artifactory, as a system of record. MCP is rapidly adapted next to agent skills based on AI ecosystem demands. In Q1, we expanded our platform for AI-driven development with the introduction of the JFrog Skills Registry, providing a centralized way to manage and govern reusable AI capabilities.

In collaboration with NVIDIA, we announced the Skills Registry at GTC, enabling the governance and trust layer enterprises need to run agentic workflows securely and at scale. We further announced that JFrog Artifactory will serve as a registry for AI models and agent skills within NVIDIA AI-Q Blueprint, part of the NVIDIA Agent Toolkits. The Vice President of Enterprise Partnerships at NVIDIA, Pat Lee, noted, quote, "Security and governance are key to deploying AI agents in the enterprise. JFrog's Agent Skills Registry for NVIDIA NEMO-CLAW supports security and control for deploying long-running agents to help scale enterprise productivity with powerful new AI tools." End quote.

JFrog unifies all artifact types, binaries, models, skills, and MCP servers into a single platform governed by one framework, one set of policies, and complete visibility and traceability in one place. These innovations, combined with a growing ecosystem of strategic partnerships, are driving increased adoption across the enterprise, amplifying the value of our Enterprise+ subscriptions and accelerating its expansions within organizations.

With that, I will hand it over to Ed for a detailed review of our Q1 financials and our updated outlook for Q2 and the full year 2026.

Ed?

Ed Grabscheid^ Thank you, Shlomi, and good afternoon, everyone.

We are pleased by the results of our first quarter, which exceeded the top end of our guidance range on every metric. It was a strong start to the year, highlighting our consistent strategic execution and ongoing operational discipline.

During the first quarter, total revenues equaled \$154 million, up 26% year-over-year. These results demonstrate the continued execution of our go-to-market strategy, fueled by our cloud revenues, ongoing demand for our security core products, and growth in our Enterprise+ subscription.

Our first quarter cloud revenues grew to \$78.9 million, up 50% year-over-year, now representing 51% of total revenues versus 43% in the prior year. Our outperformance in the cloud was driven

by robust usage across our customer portfolio, which exceeded contractual minimum commitments. We strategically worked towards converting this usage into higher annual commitments.

During the first quarter, our self-managed or on-prem revenues were \$75.1 million, up 8% year-over-year. We continue to proactively engage our on-prem customers to migrate DevSecOps workloads to our cloud or explore solutions better aligned with their specific use cases, including hybrid and fit-for-purpose deployments.

In Q1, 58% of total revenues came from Enterprise Plus subscriptions, up from 55% in the prior year. Driven by the ongoing execution of our Enterprise go-to-market strategy and broader customer adoption of the JFrog platform, revenue contribution from Enterprise Plus subscriptions grew 33% year-over-year in Q1 2026.

Net dollar retention for the four trailing quarters was 120%, representing a year-over-year increase of four percentage points and one percentage point improvement sequentially. These results highlight the continued adoption of our security core products, increased cloud usage across a broad set of conventional software packages and AI workloads, and conversion of customers with usage over minimum commitments into higher annual contracts.

We continue to demonstrate that our customers view JFrog as a mission-critical system of record to their software supply chain, with gross retention that equaled 97% as of the first quarter of 2026.

Now, I'll review the income statement in more detail. Gross profit in the quarter was \$129 million, representing a gross margin of 83.8% versus 82.5% in the year-ago period. We remain focused on cloud hosting cost optimization as we anticipate a larger share of our revenues being generated from the cloud. Given our expected increase in cloud revenue contribution to total revenue, we reiterate our annual gross margins to be in the range of 82% to 83% in 2026.

Operating expenses in the first quarter were \$96 million, equaling 62% of revenues. This compares to \$79.7 million, or 65% of revenues in the year-ago period.

Our operating profit in Q1 was \$32.9 million, or an operating margin of 21.4%, compared to 17.4% operating margin in the first quarter of 2025. The continued balance between strategic investments and operational efficiency demonstrates our commitment to profitable growth.

Cash flow from operations equaled \$38.4 million in the first quarter. After taking into consideration CapEx requirements, our free cash flow reached \$37.3 million, or 24.2% margin, compared to \$28.1 million, or 23% margin in the year-ago period.

Now turning to the balance sheet, we ended the first quarter with \$741.2 million in cash and short-term investments, compared to \$704.4 million at the end of 2025. Given our strong balance sheet, consistent free cash flow generation, and confidence in our strategy to execute on durable growth opportunities, JFrog announced in late February our first-ever share repurchase authorization of up to \$300 million in ordinary shares.

As of March 31, 2026, our RPO totaled \$574.9 million, a 36% increase year-over-year, highlighting the successful execution of our go-to-market strategy as customers continue to make larger, multi-year commitments to our DevSecOps solutions. As a reminder, our RPO excludes any benefit from customers' usage over contractual minimum commitments.

And now, let's turn to our outlook and guidance for the second quarter and full year of 2026. As we enter the second quarter of 2026, we remain encouraged by the strength in our pipeline and emerging AI workload trends, driving increased cloud usage. Even as cloud usage trends accelerate, our guidance philosophy will remain unchanged as we continue to de-risk our largest deals due to timing uncertainties and any benefit from cloud usage above contractual commitments.

Our outlook reflects growing contributions from our JFrog Security Core products, ongoing adoption of a full platform, and cloud growth driven from higher annual customer commitments. We are raising our estimated full year 2026 baseline cloud growth to be in the range of 33% to 35%. Given the anticipated contribution from our Security Core and increased baseline cloud growth assumptions, we now expect our net dollar retention floor to be 118% for 2026.

Turning to operating expenses, we continue to prioritize investments and innovation across our platform. We remain committed to a disciplined spending philosophy and are confident in our ability to manage expenses and drive ongoing efficiency in line with prior execution.

For Q2, we anticipate revenues to be in the range of \$154 million and \$156 million with non-GAAP operating profit anticipated to be between \$28 million and \$30 million and non-GAAP earnings per diluted share of \$0.23 to \$0.25, assuming a share count of approximately 126 million shares.

For the full year of 2026, we anticipate a revenue range of \$628 million to \$632 million, representing 18.5% year-over-year growth at the midpoint.

Non-GAAP operating income is expected to be between \$112 million and \$116 million and a non-GAAP diluted earnings per share of \$0.93 to \$0.97, assuming a share count of approximately 128 million shares.

Now, I'll turn the call back to Shlomi for some closing remarks before we take your questions.

Shlomi Ben Haim^ Thank you, Ed.

AI is transitioning from experimentation to tangible revenue, and we are seeing stronger momentum across our business. Looking ahead, demand signals for JFrog remain strong, including the durable cloud growth driven by AI, which is accelerating usage. New logo ASP is rising, and demand for our security solutions amid the increasing frequency of software supply chain attacks is growing.

To my fellow Frogs around the world, thank you. This quarter, you didn't just deliver, you rose above. No matter the circumstances, you kept pushing forward, navigating with resilience, innovating with purpose, and triumphing where it mattered most, for our customers.

Because of you, we don't just move forward, we leap further. May the Frog be with you.

Operator, we are now ready for questions.

QUESTIONS AND ANSWERS

Operator^ We will now begin the question and answer session. Please limit yourself to one question.

(Operator Instructions)

Please stand by while we compile the Q&A roster.

Your first question comes from the line of Sanjit Singh with Morgan Stanley. Your line is open. Please go ahead.

Sanjit Singh^ Yes. Thank you for taking the question, and congrats on a fantastic start to 2026. I have two questions for the team. I wanted to start with Ed first.

Obviously great cloud growth, great total revenue growth in Q1. When I look at the outperformance versus what the estimates were, it seems like you guys came in about \$7 million above on Q1. Q2, you guys came in ahead by a couple million bucks, so roughly \$10 million.

When you look at the raise to the full year, it's somewhat less than that, and so I just wanted just to sort of sanity check any sort of revised assumptions about the second half ramp. That was sort of my first question, and then I had a more strategic one for Shlomi.

Ed Grabscheid^ Hi, Sanjit. Thank you very much for the question. It's a good question.

We had a very strong quarter in Q1, as you highlighted. The growth in the cloud is 50%. And more importantly, we now see the mix in our cloud above 50%. We delivered 51%.

First time, it's a milestone for JFrog, where we see more revenue coming from our cloud offering than we do from self-hosted. But we also are committed to our guidance philosophy, which we will only guide on those commitments. So, while we saw the strength in Q1, much of that was being driven by usage over minimum commitments.

We are deploying our sales organization, of course, to convert that into annual commitments, but until it becomes an annual commitment, it will not be part of our guidance aligned with our philosophy.

Sanjit Singh^ That's very clear. Thank you for that, Ed.

And then, Shlomi, the question for you is, it's a really interesting time, like some of our own field work on JFrog shows a real inflection in demand for the security side of the portfolio. It seems very clear to us, and I think you highlighted that in your script.

At the same time -- at the same time, there's more of this longer-term structural debate on security overall and what the model labs will subsume. And there seems to be a take that things like scanning, vulnerability management, vulnerability scanning, posture management, cloud security could be more the purview of model labs longer term. And so, to the extent that you guys have some exposure to those parts of security, I'd just love to get your latest thoughts on the long-term durability of those pieces of the security product portfolio.

Shlomi Ben Haim^ Thank you, Sanjit. Good question. So, what we see in the market is kind of flooding of software supply chain attacks coming mainly around open source maintainers, and the hackers are going after them.

JFrog is positioned to secure our customers with that quite strongly. We called that in the script when we said that all the JFrog curation customers were actually protected by those software supply chain attempt to be attacked.

Moving forward, what's the real question? The real question is that can you really secure and govern the binaries, the artifacts, the outcome of AI? And what JFrog provides is not only a place that scans.

Scanners are important, but the system of record of where you secure, manage, store, govern your artifact is actually more important, because in a world of multi-agents that are all building and scanning and protecting and even fixing software, you still need to host it in a secure place.

The second thing, you will have to protect yourself from the open source world that will still exist, the Python, the NPM, the Hugging Face, the Docker, which is JFrog's doing at the gate.

And the third thing is how you combine security of the new outcomes coming from agents or multi-agents with the legacy that is now being built. You still need to manage dependencies with the binaries of yesterday that are still hosted and still regulated and still are on the servers in your production.

The combination of the expertise that we build around binary security, not source code, because this is a big confusion in the market, coding agents are now securing source code, replacing human beings, the combination that we build with that, including the mold around the artifactories, the system of record in a multi-agent world, including the open source on top of it and including the legacy, I think gives JFrog customers the confidence to bet on us.

This is also one of the things we called out. New logos are now buying JFrog with security, knowing that this is the future.

Operator^ Your next question comes from the line of Radi Sultan with UBS. Your line is open. Please go ahead.

Radi Sultan^ Awesome. Thank you so much. And yet echo my congrats on a really strong start to the year.

Maybe just two quick ones. Shlomi, just on legacy code modernization, we've been hearing an uptick in JFrog getting pulled along in AI-driven legacy code modernization deals. So, Shlomi, if you could just talk through like how big of an opportunity is legacy code modernization for JFrog, and where do you expect to see the biggest potential pull-throughs to your business?

And then maybe just, sorry, one more quick one for Ed. Could you speak to how impactful your AI-native customers were to the cloud strength in Q1? Just want to get a sense of how broad-based the strength was.

Thank you, guys.

Shlomi Ben Haim^ Thank you, Radi. Maybe I'll stop and Ed will take it from there. When we speak about legacy, we speak about legacy binary code, not source code.

Basically, what you currently have in production is what we call legacy. What you have to regulate for the next seven years if you're a bank, or the next 45 years if you're an automaker, this is legacy. These are binaries that were built today or yesterday, and tomorrow with coding agents will still have dependencies that are in your servers in production.

This means that those binaries need to be also first-level citizens in the system of records. Otherwise, how can you protect what is secure to be shipped? What was made yesterday and approved and governed by the organization need to still be maintained in the system of record.

So, it's a very important asset that our customers are protecting still, while coding agents are building the new compiled code, the new binaries that are also scanned and protected by JFrog.

Ed Grabscheid^ Regarding the question on the native AI companies, we had a successful Q1 driven by a broad set of customers. So, not only AI native customers, but traditional customers as well, or non-AI native customers. You recall last year we talked about a million-dollar land that we had with an AI native customer.

That renewed, and we're in continuous conversations with many of the large AI native companies, and we'll explain more or update later.

Shlomi Ben Haim^ Radi, if I may add to it, serving the AI labs is important, and we take pride of it, and we are very honored. But I think that once you become the power grid of this AI labs software supply chain, you learn much more in how you should serve the rest of the portfolio, and that's the big plus. Not \$1 million here, \$1 million there, but mainly what we are building together with them as we power the software supply chain.

Operator^ Your next question comes from the line of Michael Cikos with Needham. Your line is open. Please go ahead.

Michael Cikos^ Hi, team. Congratulations on the strong start to the year here. Shlomi, maybe for you, and one of the things we've been going through this earnings season, which is still pretty quick on the heels of the SaaS apocalypse, which seems overinflated at this point.

But one of the things we're seeing is the budget is there for strategic vendors. And so, I'm wondering, when you're going to speak with customers, is it fair to assume that this evolution of the agentic stack or how AI is playing out is causing customers to rethink or the need to modernize their existing architecture, and as a result, JFrog is being pulled into that conversation and benefiting them with respect to cloud migrations? Can you talk to what the tempo of conversations you're seeing out there actually is like?

And then I just had a quick follow-up for Ed.

Shlomi Ben Haim^ Yes. Thank you, Mike. So, what is it that we hear from the market?

What we hear from our customers is that every application, to your point of SaaS companies, every technology that was built to have human interaction with technology is being questioned now. Everything, every application, even source code. Source code became cheap.

Source code is, as we mentioned in the script, source code is something that now you can do on an experimental level, and you can do it 1,000 times faster. But what happened when the machine language, the binaries need to be maintained, this is where they start to be a bit more cautious about how they plan the future. So, for example, in order to enable AI, you need to use MCP servers.

This is the interaction between machine and your solution. MCP servers are yet another binary. This is where, to your point, this is where JFrog comes into the question, can JFrog become my MCP registry for all the MCP servers?

The same thing happened with NVIDIA when they asked us about skills. Skills for agents, yet another binary. Can JFrog become the skills registry?

So, all of what we have hearing -- what we are hearing is that, how can I build a stronger, better, scalable, universal system of record to manage all of these binaries? Because in tomorrow's world, what matters would be the machine language, not source code, not human language, but zero and one. And this is what JFrog did for the past 17 years.

Michael Cikos^ That's great to hear. Thank you, Shlomi. And for a quick follow-up here, just trying to peel back layers of the onion as far as the strength in cloud that you guys saw, is there any way to further qualify?

I don't know if you could talk to either the size of the cohort that drove the magnitude of that upside or how cloud overconsumption trended through the quarter from a linearity perspective. Can you just put any finer parameters around that strength?

Ed Grabscheid^ It was a strong quarter from start to finish, Mike, to be honest with you. It was very broad-based. It wasn't concentrated on one geography or one industry.

I will say that what you saw in terms of the cloud was represented in our increase in the cloud guide. So, we were very happy. We're confident with what's happening right now in the cloud, and that's what gave us the ability to raise our guide from 30% to 32% to 33% to 35%.

Operator^ Your next question comes from the line of Miller Jump with Truist. Your line is open. Please go ahead.

Miller Jump^ Hey, great. Thank you very much for taking my question, and I will echo my congrats on a really strong start. Last year you guys were talking about AI experimentation driving consumption beyond commitments.

It sounds very different today from your prepared remarks. So, can you just talk about the difference you see in the amount of binaries in your system reaching production now versus a year ago? And I would also say it sounds like there's still a number of customers that are maybe waiting to commit bigger.

So what are you hearing in terms of their hesitancy? Thanks.

Shlomi Ben Haim^ [Oh], Miller, this is an awesome, awesome question, because basically you're saying source code is being produced at a completely different pace, completely different volume. Everything produced source code now. It's not just human developers, but all the coding agents together with the human developers.

So, the big question is do we see binaries going at the same time? So, you can think about it as like the digital photography replacing film. Film was expensive.

You would take one shot on sunset before you print it and now assume that you can take 200 of them. And instead of one printing, instead of one posting to your social network, you will now have five. Binaries are the asset that you will take to production.

Source code became cheap, and now you can make more binaries that need to be mutable. They need to be tracked. They need to be governed.

And you will see this growth in binaries and what you can take to production because of the change of AI. Same thing goes to governance. How do you make sure with the same metaphor, how can you make sure that the picture that you posted on your social doesn't carry your home address in the background?

This is what JFrog brings. Not only dealing with the volume of new secure pictures but also govern what goes out.

Operator^ Your next question comes from the line of Howard Ma with Guggenheim. Your line is open. Please go ahead.

Howard Ma^ Thanks, and congratulations on a strong quarter. I have two questions, but my first is I'd like to better understand how exactly JFrog's revenue benefits from curation and advanced security. And I believe there are a few parts.

The first being you need tier upgrades where you have to be on Enterprise X and Plus to qualify for buying those products. And then as you make commitments, you obviously get that. You get a commitment.

And then there's over-usage, I believe, that's driven by increased traffic from attacks. So, I just wanted to run that by you if those elements are correct.

Shlomi Ben Haim^ Yes, so I'll start speaking about JFrog Curation and JFrog Advanced Security and JFrog X-ray, and Ed can speak about the over-usage and what is counted. Well, listen, everything that comes from open source, whether pulled by agents, AI agents, or by human developers is something that needs to be protected before it steps into artifactory, your single source of truth. When we build curation, it was based on customer's request.

They asked us to give them a firewall that will enforce policy of what comes in. That was in a different, completely different volume when it was made by humans pulling open source packages. Now, when you have a thousand times faster pulling requests for open source packages from public hubs, whether npm, Docker, Hugging Face, Conda, PyPI, you know that you are subject to attack.

And the attackers are also using coding agents. They also became more sophisticated. They're also going after the maintainers that they know that by an order of magnitude will be spread their malicious packages.

So, what curation did very successfully, not only apply this firewall enforcing your policies, but also scaled to this level of AI. And this is why our customers not only embraced curation but also increased the demand for it. After every attack we saw since last quarter of 25, which I [allude] to this quarter with MCP and Python and others.

Regarding JFrog Advanced Security and JFrog X-Ray, once it's in, once it's inside your system of [record], once it's inside artifactory, you need to still maintain the security of your software supply chain. You need to look for secrets that were exposed. You need to look for composition analysis.

You need to look for dependency graph security. And this is what JFrog Advanced Security and X-Ray is doing. And then when you shift to production, you shift something that you can actually trust.

Ed Grabscheid^ And Howard, this is Ed. Regarding the monetization of curation, the monetization is based off of seats. This is a common currency in security.

And we monetize based off of the seats. So, regarding the attacks and an increase in attacks, it certainly drives a demand for our customer portfolio and new customers to take either an increased number of seats or adopt curation. But it doesn't necessarily drive data consumption.

Data consumption is being driven by packages coming in and out of the organization or going into production. So, curation itself is not driving the usage over minimum commits.

Operator^ Your next question comes from the line of Mark Cash with Raymond James. Your line is open. Please go ahead.

Mark Cash^ Great. Thank you. Hi. Shlomi, maybe I wanted to build off a few previous questions and ask about MCP registry and AI catalog because there's a lot of companies saying they'll provide the visibility and security for AI agents.

So, I guess where in the customer journey do organizations realize they need JFrog governance capabilities? Because what pain points are they seeing that others can't solve before coming to you? Thank you.

Shlomi Ben Haim^ Yes, thank you for this question, Mark. What's happening now is that every software provider already provides an MCP server because we all know that if agents will not have an interaction with your software, that would be -- that would be the end of your software usage. MCP servers are a binary code.

No matter who provides that, it's a binary code. So, our customers came to us and asked for MCP registry. As they trust npm packages inside Artifactory or Python inside Artifactory or Docker container inside Artifactory, they also want to have a list of MCP servers that they can put in an MCP registry, which is what we released this quarter.

And then they can tell all of their AI agents or human developers, this is a safe place to take your MCP servers from. Same thing happened with skills, which is a very growing trend when you use coding agents. And there is some kind of a movement now to CLI, which is the third technology.

All of the above are binaries code. All of the above are a natural expansion of our solution, and therefore they are stored in Artifactory.

Operator^ Your next question comes from the line of Jason Salino with KeyBanc Capital Markets. Your line is open. Please go ahead.

Jason Salino^ Great, thanks. Good afternoon. You know, the value proposition in curation is quite compelling, right?

And as you noted, these curation customers were protected in Q1 from the software supply chain attacks that we saw on the news. It seems like a no-brainer to me and to most investors, but to the customer, what might be the alternative if they don't choose curation or what factors are being considered that might be delaying that customer's decision? Given you are seeing this tremendous demand, do you have the capacity to kind of meet it?

Thank you.

Shlomi Ben Haim^ Jason, I think it's clear that for a very long time, JFrog said we are betting on a world of automation, a world where machines will have to manage the asset, and therefore we never shifted our focus from managing binaries. Every binary management tool is an alternative. So, I think that therefore the strong differentiators that JFrog brings, like universality, JFrog is the Switzerland of binaries.

JFrog not only serves all the binary type, but also all the coding agents, human beings, and other citizens that are using our solution. JFrog scale, we built 17 years of scalability. We went with the biggest organizations on the planet to scale to their level, and now we are even elevating it more because of AI.

So, scalability matters. JFrog is hybrid. We give you the freedom of choice of running it in the cloud, on every cloud, and on prem if this is what you prefer if you are in a highly regulated environment.

JFrog integrates with all your ecosystem tools when it comes to DevOps, DevSecOps, DevGovOps, which gives you also the freedom of choice in not getting into a vendor locking. So, if there would come a solution that provide all of this in a universal way and go so well complementing the AI change in a world of machine language binaries, that would be a threat over JFrog. I hope that we put the moat around what we build best, which is the system of records.

Operator^ Your next question comes from the line of Kingsley Crane with Canaccord. Your line is open. Please go ahead.

Kingsley Crane^ Hey, congrats on the results, and thanks for taking the question. So, on the Q4 call, you called out that the November npm attacks had driven both immediate curation revenue as well as building pipeline. I'm just trying to get a sense of if there's more urgency around procuring curation or advanced security versus some of these larger software architectural decisions that could take multiple quarters.

And I guess more specifically, just on Q1, like how much did curation drive the upside in cloud in Q1? Thanks.

Shlomi Ben Haim^ Yes. Well, listen, Kingsley, every time that there is some kind of a software supply chain attack, we see a rise in the pipeline, and obviously a lot of our customers are concerned, and that's an immediate impact. But what happens when it's happening every few weeks?

This is what's happening now. It's happening every few weeks, and it used to be solar wind, and then a year after, look for J, and then a year after, something else. Now you refresh your browser, there is a software supply chain attack.

And why? Because source code doesn't matter anymore. Source code scanning is something that used to be overappreciated.

Now people understand that what needs to be protected is what's going to production. And the hackers, the attackers, also understand that. So they go after the maintainer of the open source packages, and this is what you have to protect yourself from.

Now, will there be companies that will kind of react based on fear only? I think it's forever kind of the tradeoff, but we see more and more responsibility on the customer side, knowing that the magnitude that they are looking at is completely different than what it used to be yesterday.

Operator^ Your next question comes from the line of Shrenik Kothari with Baird. Your line is open. Please go ahead.

Shrenik Kothari^ Yes, thanks a lot for taking my question. So, Shlomi, Ed, you have been careful in the past not to oversell AI as an immediate sort of revenue windfall, and Ed's own words describe 2025 more as an initial spark than fire. And Shlomi, you drew a comparison now with the transition from, like, film to digital.

So as once this higher-quality AI code with Opus, Codex is likely reaching more production, and we are hearing anecdotes about it, that definitely creates more valuable binaries for you to act as a system of record. Just where are customers today on that journey from that AI code slop to production grade, and what specific indicators are you watching that would tell you that the fire has started or is going to start?

Shlomi Ben Haim^ Yes, good afternoon, Shrenik. I think that what we see today is more an experimental kind of mode. Everybody is trying everything.

Not so long ago, we would speak about Copilot and Cursor, and now everybody is speaking about Anthropic and Codex, and I think that a lot, a lot is being adopted on every organization. It means that, as we used in this metaphor before, like, you can take many more pictures. It doesn't cost you any film.

But what we also see is that not even a single customer has a full autonomous process. This is not yet there. It's still a combination of human developers with coding agent.

There is no coding agent that starts from scratch and pushes to production and maintains the production fully autonomous. So there is still some miles to do before AI will take over completely all of the developers' positions, but we start to see the collaboration between strong human developers and coding agent, and this is why there is a rise of the water on every front.

Operator^ Your next question comes from the line of Brad Reback with Stifel. Your line is open. Please go ahead.

Brad Reback^ Great. Thanks very much. Shlomi, back to your comment during the prepared remarks about customers willing to, I'll say, absorb meaningful overages in the cloud.

What do you think is the gating factor, or why are they willing to do that and not commit and get a better rate? Thanks.

Shlomi Ben Haim^ Yes. Hi, Brad. There is a race of AI adoption on every company now, no matter if you are a small or medium business or if you are one of the largest banks in the world with 50,000 developers.

It's coming from the board. It's coming from down. The board is asking about AI adoption, making sure that you are in the race and not kind of falling behind.

So, what we see now is that usage in the cloud is also part of this experiment. Now, if you go to the CFO and you say, JFrog asked me to commit, the CFO will ask, commit to what? And, therefore, they give you, they leave the meter on.

They let you use more and even pay more. And now our team mission is to make sure that we convert this over-usage into commitment to gain a win-win situation with our customers. It will come.

It will just take a bit more time because of the predictability that is now missing.

Operator^ Your next question comes from the line of Lucky Schreiner with D.A. Davidson. Your line is open. Please go ahead.

Lucky Schreiner^ Great. Thanks for taking my question and congrats from me as well. Very impressive quarter.

Maybe a bit of a follow-up there. Previously, you've spoken to some customers preferring to buy JFrog on a self-managed basis, given the better visibility and cost controls around that. But I didn't get a sense of those trends from the prepared remarks today.

So one, is that fair to say? And two, is there maybe any potential reason for a change in those trends? Thanks.

Shlomi Ben Haim^ Hey, Lucky. We still see customers asking for the self-hosted solution or on-prem solution. It's split into two profiles.

One is the big AI labs that are building their own data centers. They have enough money. They have enough capital.

They don't want to share anything with the public cloud for whatever reason you can imagine. And they will take an on-prem solution and embed it into their software supply chain architecture. The second group that we see is the group of the highly regulated companies, government institutes, or whatever organization that need to be highly regulated.

And they will, for sure, do a lot of these tests and experiments on an on-prem environment before they will go to the cloud or to FedRAMP. And the last, what we see, are companies that are well-established and kind of seasonal players at the on-prem environment. So, they are not looking to have now one or two entities in their world playing in the cloud.

They keep on extending their own on-prem. But as you can see in our numbers, it's not only part of our strategy to migrate our business to the cloud. And this is what we also announced the first time that it costs 50% of total revenue.

It's also a benefit that we keep in our pocket to become the only company that gives you a full hybrid solution with a full freedom of choice. Like, no matter what you are, no matter who you are, we can give you the freedom to embed AI or to adopt AI in your environment.

Operator^ Your next question comes from the line of Jason Ader with William Blair. Your line is open. Please go ahead.

Jason Ader^ Yes. Thank you. Good afternoon.

I wanted to kind of revert to an earlier question, which was asked about the risk that the LLM guys encroach into the binary layer. And Shlomi, I was hoping you could talk about some of the announcements that the labs made during the quarter where they started to talk at least a little bit about binaries. It was too technical for me, honestly.

So if you could help enlighten us and just talk about what they announced around binaries and why it's not something that you worry about.

Shlomi Ben Haim^ Hi, Jason. Let me start with the last sentence. I'm worried about everything.

There's nothing that I'm not worried about. But I have the confidence that what we are building alongside this company is completing and being complementary to what the world is demanding. What you have heard is reverse engineering binaries.

I guess that you refer to the open AI announcement about 5.4-Cyber. This is a way to kind of take the binaries themselves and reverse engineer it and to see what they were built from. That's not replacing JFrog's solution because even if you are running kind of fast forward two years from now, when every organization will use open AI next to Anthropic, next to Cursor, next to Copilot, next to Gemini, I guess that we will all agree that even if you have this environment, that they all build binaries, you need a government tool that provides a universal solution to contain them all.

The second thing, who will protect the open source? It's not reverse engineering the open source packages. It's what the agent built itself.

So when you bring something from NPM or something from Docker, how do you make sure that what you brought into the organization, past your firewall, how do you make sure that this is secure? The third thing is that this race is not just happening between the defenders and the vendors. This race is actually happening between the defenders and the attackers because the attackers will also use Cloud and they will use Codex in order to build a more sophisticated malicious attack.

So how can you make sure that the policies that you put to the gate are securing your system of record? And last, what happens when one authority should take a decision of what's going to production? Will it be one of the coding agents?

Will it be two of them? Will it be human beings? Will it be the company policy?

This is the infrastructure we provide. We are not the policy makers. We are the policy enforcers.

And we help you to make sure that what goes to production kind of came out clean from the non-poison reservoir. So while we are seeing this happening, it's mostly focused on what I built as an agent, replacing human being, replacing human language to what I need to secure at the end and to govern and to trust. So, that's how we see it now. And this is what our customers are telling us.

Operator^ Your next question comes from the line of Andrew Sherman with TD Cowen. Your line is open. Please go ahead.

Andrew Sherman^ Great. Thank you. Great.

Congrats on the Cloud numbers, guys. Shlomi, on the security side, we've gotten a lot of questions on how much of your revenue comes from Xray, since the labs now have similar products. It'd be great if you could clear that up for people.

How should we think about the contribution of that versus advanced security and curation and just the main barrier to entry for the latter, the curation and jazz? Thanks.

Shlomi Ben Haim^ Yes, great question. Xray forever was a part of our DevOps offering. And why is that?

Because we don't think that Xray by itself should stand alone and start to do study composing, sorry, software composing analysis, composition analysis. We think that Xray should run over your artifactory, making sure, for example, that your containers 40 years down are secured to be in artifactory. Can other tools replace that?

Yes. But if you get it as part of your package using artifactory built into artifactory, why do you need another tool? The second thing that Xray brings is this understanding of what's coming out from the open source environment and to be able to break that in pieces and to secure that.

Can it be something that brought from the outside like a point solutions tool on top of artifactory? Yes. But what we see is that thousands of customers prefer to take it as part of their DevOps subscription with JFrog knowing that this is a built-in solution on top of your system of record.

Operator^ Your final question comes from the line of Koji Ikeda with Bank of America. Your line is open. Please go ahead.

Koji Ikeda^ Yes. Hey, guys. Thanks so much for squeezing me in.

When I look at cloud, the net new revenue added this quarter I think is the most ever in a quarter, let alone a first quarter. And so that absolutely implies customers are spending above commitment levels like never before. And so why is it, or maybe the better question is, how long do customers typically take before they come to JFrog and start renegotiating their contracts for higher commitment levels, which presumably come with better volume discounts?

Thank you.

Shlomi Ben Haim^ Yes. Regarding the why, I'll make it simple. We called it before.

We would see more code means more binaries means more JFrog. And JFrog is well known for being the binary people. Regarding how long it takes, we actually we are not waiting, Koji.

This is part of our practices. Our enterprise practices changed something like two years ago. We are going to those customers with a better offer, with a better plan if they are committing.

The question would be how long this experiment will be mature to be discussed as a commitment. And this is something that I'm sure that we will keep on following and provide you with more clarity of where the cloud goes. But if you look at the confidence in our guidance, we raise the cloud.

Although we see that a lot of it comes from over -- from usage over commitment, we raise the guides for the year because we know that this is not the trend. This is not the spike. It's a few quarters already that we see the growth in the cloud.

Operator^ This concludes the question and answer session. I will now turn the call back to Shlomi for closing remarks.

Shlomi Ben Haim^ Everyone, thank you for your question. Thank you for your trust. May the frog be with you and may we have a great year.

Operator^ This concludes today's call. Thank you for attending. You may now disconnect.