08 – 06 – 2026

JFrog Ltd.

Second Quarter 2026 Results

TOTAL PAGES: 16

CORPORATE SPEAKERS:

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

PARTICIPANTS:

Unidentified Participant
Needham & Co.; Analyst
Miller Jump
Truist Securities; Analyst
Mark Cash
Raymond James; Analyst
Howard Ma
Guggenheim; Analyst
George McGreehan
BofA; Analyst
Radi Sultan
UBS; Analyst
Brian Essex
JPMorgan; Analyst
Andrew Sherman
TD Cowen; Analyst
Jason Celino
KeyBanc; Analyst
Sanjit Singh
Morgan Stanley; Analyst
Kingsley Crane
Canaccord Genuity; Analyst

PRESENTATION:

Operator^   Ladies and gentlemen, thank you for joining us. And welcome to the JFrog second quarter 2026 Financial Results Earnings Call. (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 second 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 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 third 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 revisions 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 risks and other important factors that could affect our actual results, please refer to our Form 10-Q for the quarter ended March 31, 2026, 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 June 30, 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 measures 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 a 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's CEO, Shlomi Ben Haim.

Shlomi?

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

We are pleased with our second quarter results which exceed the high end of our guidance across all metrics.

Our first half 2026 achievements reflect strong execution and the clear strategic importance of JFrog in enterprise software supply chains.

It is clear now that the world is moving at the speed of AI.

What began as a technology shift is becoming the foundation of every business and increasingly ambient infrastructure as they build and deliver software.

As AI accelerates software creation, engineering velocity and code quality, the challenge is no longer generating source code, but managing the tsunami of binaries compiled.

It is now about establishing trust in these software artifacts, models, agents and packages that AI and human increasingly produce without sacrificing speed. The JFrog platform is evolving for a future where AI agents become first-class citizens of the software supply chain.

By extending our platform to treat AI agents as trusted participants alongside human developers, we believe JFrog is building the control plane for the next generation of software delivery.

We see software engineering evolving into software supply chain engineering, not because every developer becomes a supply chain expert, but because every developer or AI agent must rely on a trusted software supply chain delivered by the organization.

For this new era, our customers are reaffirming JFrog as the single source of truth. And we believe this reality is fueling the momentum we are seeing across our business.

During the second quarter, JFrog's total revenue was $163.8 million, representing 29% year-over-year growth. Cloud revenue grew 53%, driven by increased secure binary consumption throughout the factory reinforcing its central role as the single source of tools for software supply chains.

In addition to continued strength in cloud growth, our enterprise-focused go-to-market strategy continues to deliver strong results at the high end of our customer base. Customers with annual spend exceeding $1 million grew to [97%], up from [61%] a year ago, representing 59% year-over-year growth. Customers spending more than $100,000 annually, grew to 1,291 compared to 1,076 in the prior year, an increase of 20% year-over-year.

On today's call I will walk you through the second quarter in more detail, and Ed will then follow with additional financial insights and outlook.

First, I will cover our cloud business where strong consumption trends continue to drive demand across traditional and AI software artifacts.

Second, I will discuss our security business. as software supply chain attacks grow in scale and sophistication, customers are looking for a unified security integrated with their system of record. Last, I will discuss governance and compliance. The era of genetic software development is driving the industry's next evolution devops.

I'll start with cloud.

In Q2, our cloud business continued to expand.

As we supported the scaling volume of software artifacts flowing through our customers' software supply chain pipelines.

As AI accelerates software development, customers are creating, storing and distributing more binaries than before.

Over the past several quarters and even more since the beginning of the year, we have observed the following key trends driving this change in cloud consumption.

First, the rapid adoption of AI tools accelerate software development activity and increases the volume of binaries moving through our platform as agents and tools consume more software at the pace and scale, no human work flow ever could.

Second, the increase in the number of AI-specific software packages, such as MCP, skills and others that organizations create and manage. Third, Continued uncertainty is making forecasting difficult for customers in the evolving AI economy, leading them to sometimes favor the flexibility of a consumption-based on-demand cloud model. These trends and the first half results validate our strategy and business model, continuing to reinforce the value of our cloud offering which enables customers to scale with demand while maintaining efficiency and operational flexibility.

Our enterprise sales teams remain focused on securing long-term enterprise commitments allowing customers better unit economics in the evolving AI spending environment.

At the same time and as always, we give customers the flexibility to determine the balance between committed capacity and on-demand usage.

Consistent with our guidance philosophy, we continue to exclude usage above committed levels from our outlook. Ed would refer to it later on the call.

Now to the continued momentum we are seeing in security, JFrog provides the infrastructure for creating, managing and securing software artifacts at enterprise scale.

By integrating comprehensive software supply chain security directly without the factory our customers' single source of truth.

We enable them to build and deploy software we trust at the scale and speed of AI.

As software supply chain threats continue to grow in scale and sophistication CSO team increasingly see JFrog Security as a mission-critical component of the software infrastructure, not an optional capability. Validating this fact, JFrog was recently named a leader in the Gartner Magic Quadrant for software supply chain security based not only on our highest rated ability to execute but also on our strategy of incorporating security alongside the software supply chain, single source of tools in one platform.

We continue to see strong momentum in our security business, reflected in higher attach rate on new customers win, continued expansion with existing accounts and an increasing number of larger security-led transactions.

In the second quarter, more than 80% of the customers that joined our over $1 million cohort added security. This momentum extends to our new logo business where over 40% of overall new logo wins included security as part of their initial land with JFrog.

In addition, AI-powered software supply chain attacks continue to escalate this quarter with threat actors increasingly targeting open source package ecosystems.

As AI accelerates software creation, it also accelerate the pace and sophistication of software supply chain attacks. Throughout these incidents, customers using JFrog curation remain protected.

By tightly integrating curation without the factory, JFrog delivers a trusted policy-driven software supply chain firewall that blocks malicious and risky packages before they enter the enterprise, allowing developers and AI coding agents to move fast without compromising trust or security.

In Q2, we will focus on making sure our security solutions become too integrated to pay powered by the AI ecosystem.

In the past, we focus on securing human developers Today we are extending that same trusted experience to AI agents that increasingly interact with the JFrog platform. Consistent with our universal trust layer strategy, we recently announced integrations with leading AI coding agents including cloud code and Carter, protecting our customers, developers and agents from vulnerable or malicious dependencies, enforcing enterprise security policies and receiving trusted remediation guidance in real time.

By embedding security directly into AI-driven development workflows, JFrog helps customers accelerate software delivery while preserving trust across the entire software supply chain. The continued validation of our strategy by security leaders, accelerating customers' adoption, expanding platform usage larger security-driven transactions and our deep partnerships across the AI ecosystem reinforce our confidence in JFrog's security roadmap.

We expect our security core to remain one of JFrog's most significant long-term growth drivers.

Finally, on security, we are excited to welcome Keynote security executive from both Entropic and Cursor as speakers at our annual Swamp Up user Conference this September in New York City. Next, I want to briefly address governance and DevGovOps.

It is becoming increasingly clear that AI will only be adopted at enterprise scale if it is trusted. That trust requires governance, compliance and auditability to be engineered directly into the software development workflows, not introduced as a separate manual step. The challenge is not whether these controls can be enforced, but how they can be enforced in a multi-agent and hybrid development environment without slowing AI-driven delivery.

This is why we believe DevGovOps represents the next evolution of software supply chain management and automation. Embedding governance into the software delivery life cycle, so organizations can move fast while remaining secure, compliant and auditable.

In Q2, a leading publicly traded provider of electronic design, simulation, validation and test solutions for AI infrastructure signed a 7-figure agreement with JFrog, adopting JFrog AppTrust bundled with our software supply chain security solutions. Building on JFrog's wall as the customers' system of record, they expanded their investment to embed the goop across the software delivery life cycle, enabling centralized governance, compliance trusted software consumption and policy enforcement to meet evolving global regulatory and audit requirements for distributed software assets.

As governance, compliance and DevGovOps continue to rise to the ballroom level, we believe JFrog is uniquely positioned to capture this opportunity.

As the infrastructure layer, powering the software supply chain, JFrog sits at the center of the software delivery life cycle, enabling customers to automate governance, in force policies and embed compliance natively into their development pipelines rather than relying on manual downstream processes.

As we execute on the security expansion of our platform, we continue to invest in expanding our platform to help enterprises not only build and secure software, but also govern it with the same level of control, automation, trust and scale.

Finally, I want to deliver comments on AI adoption and revenue. AI is meaningfully impacting our customers' software supply chain as they increasingly see the need for JFrog to function as their infrastructure for the software that both machines and humans build and consume.

We see the usage of AI-specific packages and their dependencies expanding on top of their traditional DevOps and detects workload growth.

In Q2, we were excited to announce partnerships and integrations that are solidifying JFrog as the enterprise standard for AI-powered software supply chain infrastructure. These investments included the tight integration with Anthoopic that brings JFrog security and governance solutions to the millions of Cloudco developers.

We also announced the partnership with [Carso] which powers over 1 million daily users that now have access to development and governance workflows directly in their development environment.

We also continued to expand our footprint with the world's leading AI native companies, welcoming a new logo, displacing a competitive solution that failed to scale with its growth. This customer migrated to JFrog platform as its software supply chain system of record and binary distribution engine across a multi-region hybrid deployment.

As AI leaders increasingly build software with AI for AI, this win further validates our strategy and reinforces JFrog's position as the trusted software infrastructure for the next generation of AI native autonomous and multi-agent software development. The accelerating adoption of AI development practices and coding agents across our customer base combined with our deep partnerships with the world's leading AI companies is also helping us navigate the enterprise shift toward token economy optimization.

As organizations increasingly govern and cap token consumption, the economics of software development are changing. JFrog's value proposition is fundamentally aligned with this transition because we are focused on the combined output of software, the binary, not on the number of prompts or lines of car generated. Whether software is written by a human developer and AIH and to both, it ultimately results in more trusted binaries that must be secured, managed, governed and distributed.

As AI reshapes how software is created, we remain focused not only on what is growing but also on why it's growing. And what matters most, the tasted binaries that power production. And with that, I will hand it over to Ed for a detailed review of our second quarter financials and our updated outlook for the third quarter and full year of 2026. Ed.

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

We are incredibly energized by our second quarter results which is slowly noted, exceeded the top end of our guidance range across every key metric. These results once again showcase our consistent strategic execution and operational discipline.

During the second quarter, total revenues equaled $163.8 million, up 29% year-over-year. These results demonstrate the continued execution of our go-to-market strategy, fueled by our cloud revenues, growing demand for our security core products and expansion in our Enterprise Plus portfolio.

Cloud revenues in the second quarter accelerated to $87.5 million, up 53% year-over-year, now representing 53% of total revenues versus 45% in the prior year.

Our outperformance in the cloud was driven by robust usage across our customer portfolio which continues to exceed contractual minimum commitments and increased adoption of our security core products.

We strategically work towards converting this usage into higher annual commitments.

During the second quarter, our self-managed or on-prem revenues were $76.3 million, up 9% year-over-year.

We continue to proactively engage our on-prem customers to migrate workloads to our cloud or hybrid offerings as they explore solutions better aligned with the rapidly changing security environment.

In Q2, 59% 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 at the JFrog platform revenue contribution from Enterprise Plus subscriptions grew 39% year-over-year in Q2 2026.

Net dollar retention for the four trailing quarters was 121% and representing a year-over-year increase of 3percentage points and a 1percentage point improvement sequentially. These results continue to highlight the strong adoption of our security core products, increased cloud usage and conversion of customers into higher annual contracts.

We continue to demonstrate the strategic value of JFrog as a mission-critical trusted system of record for our customers' software supply chain with gross retention of 97% as of the second quarter 2026.

Now I'll review the income statement in more detail. Gross profit in the quarter was $136.2 million, representing a gross margin of 83.2% versus 83.1% 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 annual gross margins to be in the range of 82% to 83% in 2026.

Operating expenses in the second quarter were $103.6 million, equaling 63% of revenues.

This is compared to $86.4 million or 68% of revenues in the year ago period.

Our operating profit in Q2 was $32.6 million or an operating margin of 19.9% compared to 15.2% operating margin in the second quarter of 2025. The continued balance between strategic investment and operational efficiency demonstrates our ongoing commitment to profitable growth.

Cash flow from operations equaled $57.1 million in the second quarter. After taking into consideration CapEx requirements, our free cash flow reached a record $53.8 million or 33% margin compared to $35.5 million or 28% margin in the year ago period.

Now turning to the balance sheet.

We ended the second quarter with $824.5 million in cash and short-term investments compared to $704.4 million at the end of 2025.

As of June 30, 2026, our RPO totaled $659 million, a 38% increase year-over-year, once again highlighting the successful execution of our go-to-market strategy as customers continue to make larger commitments to the JFrog platform.

As a reminder, RPO excludes any benefit from the customer's usage over contractual minimum commitments. And now let's turn to the outlook and guidance for the third quarter and full year of 2026.

As we enter the third quarter of 2026, we remain optimistic by the strength in our pipeline and the tailwinds of emerging AI workload trends driving increased cloud usage and security core product adoption. Even as usage trends accelerated through the first half of 2026, our guidance philosophy will remain unchanged as we continue to derisk large deals due to timing uncertainties and any benefit from cloud usage above contractual commitments.

Looking ahead, our outlook remains anchored by three key drivers: growing contributions from security core products, ongoing adoption of our 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 41% to 43%. Given the anticipated contribution from our security core products, and increased baseline cloud growth assumptions, we now expect our net dollar retention floor be 120% for 2026.

Turning to our operating expenses.

We continue to focus investments on innovation across our entire platform.

We remain committed to a disciplined spending philosophy and confident in our ability to drive ongoing operational efficiency in line with prior execution.

For Q3, we anticipate revenues to be in the range of $164 million and $166 million with non-GAAP operating profit anticipated to be between $27 million and $29 million and non-GAAP earnings per diluted share of $0.22 to $0.24, assuming a share count of approximately 130 million shares.

For the full year of 2026, we are again raising our revenue guidance now anticipating a range of $648 million to $652 million, representing 22% year-over-year growth at the midpoint.

Non-GAAP operating income is expected to be between $116 million and $120 million and non-GAAP diluted earnings per share of $0.96 to $1, assuming a share count of approximately 129 million shares.

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

Shlomi Haim^   Thank you, Ed.

Our second quarter reflected the strength of our strategy and the dedication of our team.

We delivered continued cloud expansion, security as a meaningful growth engine, strong enterprise execution increasing customer platform consolidation and solid free cash flow momentum, all while maintaining the discipline to grow responsibly and efficiently to every frog around the world. Thank you. These outstanding results are your achievements.

Together, you turn Q2 into a major windfall folk. Your passion, resilience and focus on our customers didn't just deliver another great quarter, but laid the foundation for future growth.

As we conclude today's call we look forward to welcoming many of you to swamp New York in just a few weeks. Together with customers and industry leaders from entropic cursor, Morgan Stanley, Microsoft, [Cowind], NVIDIA and many others will demonstrate how the software supply chain is evolving for the AI era. And how JFrog is helping enterprises control, secure, govern and scale software creation and delivery in a world powered by developers and agents alike.

May the frog be with you.

Operator, we are ready for questions.

QUESTION & ANSWER:

Operator^   (Operator Instructions) Your first question comes from the line of Mike Cikos with Needham.

Unidentified Participant^   This is Matt on for Mike Cikos over at Needham. Thank you for taking our questions.

We were hoping you could share some color on the conversations you've been having since the open AI models discovered the self-hosted Artifactory 0 days vulnerability.

It's worth noting that from our perspective, it seemed like the whole deal was very well handled.

But we were just curious if it's delayed pipeline conversions at all or if there's any plan to continue to leverage these AI models to search for other potential patches going forward?

Just anything you could share on that whole experience would be helpful.

Shlomi Haim^   Yes.

Well thank you for the question.

Obviously one that we were dealing with in the past two weeks and great partnership with OpenAI.

So as you mentioned, open AI have self-hosted factory and they ran model that worked on a sandbox with limited guardrails. AI models into the word should not be treated as free.

They should be treated with zero trust.

With the security practices that are required around that.

Once this AI model found a vulnerability within our factory, they contact the JFrog team immediately, we remediated fast worked in great partnership with the security researchers of OpenAI. And throughout the last week, kept improving this communication between us.

Obviously this is also a great opportunity to discuss the cloud solution, the SaaS solution that to remind everyone was not breach.

And also to discuss the security solution that JFrog can provide on top of the factory.

So great relationship will build a better product. More and more vulnerabilities will be fine as models are getting into the pipelines. And I think that what counts is how fast vendors are remediating.

We are very pleased, very honored with the relationship we built with OpenAI before and during the incident.

Operator^   Your next question comes from the line of Miller Jump with Truist Securities.

Miller Jump^   And congrats on the continued really strong momentum here.

I want to stay on security.

It was really great to hear about the momentum you saw in the quarter. There were a number of pretty significant open source vulnerabilities that came to light at the end of wondering like, did that have an impact on the Q2 security contribution in your view? And was there any of the second half pipeline of security that actually got pulled forward into the first half as a result of those vulnerabilities?

Shlomi Haim^   Yes, Miller, that's a great question that represent everything we've seen in the past few quarters. software supply chain attacks are becoming a daily thing, just two days ago, another massive attack over millions of open source packages coming from NPM yet another one.

So obviously we start to see that every CISO asks herself or himself what's the right firewall we should put from the get-go than what the right scanners we should put on top of our system effect cord.

Obviously this generates a lot of traction around JFrog because JFrog is one of the unique security solution that is not just providing a security solution but also the system of record that need to be protected.

So yes, the pipeline is impacted by it.

We were very pleased to see the results in Q2 that are showing yet another growth after the results of Q1.

It supports not only our penetration into the DevSecOps world, but also the growth in the cloud. And looking forward, we are very optimistic, as mentioned on the call that security will keep being a very strong growth engine for the company.

Operator^   Your next question comes from the line of Mark Cash with Raymond James.

Mark Cash^   Shlomi, if I can go back to the open air answer that.

Look, absolutely noble. Your team was great and transparent with disclosing what happened, had solutions in place, take care customers and I fully understand like this is a strong argument for adopting cloud and for security.

So I did want to ask, though, considering [47%] of your business is self-hosted. How have customers reacted?

What have you done to ensure customers are patched in the risk on spread? And then could you actually turn us to a positive for demand as we've seen with some other security companies that use incidents to actually get closer to customers and then drive broader platform adoption. And that's it for me.

Shlomi Haim^   Thank you, Mark. Great point.

So I'm thinking about how fast you remediate and how fast you take it to the market.

But there is also a very responsible way to treat your customers, and that's transparency. The moment it happened, the first thing that our team did was protecting our cloud customers and releasing a patch to the self-hosted customers.

Obviously this is not in our control.

So it can become a tailwind of customers that see the SaaS as a more secured environment.

But we immediately released the patch version.

It was confirmed by open AI as resolving the vulnerability.

We were very happy to see that they are keep running their models to check if Artifactory is secured and bulletproof and the answer was yes.

And just yesterday on a Black Hat stage, they shared with more transparency what happened there. And obviously some of it has to do with how you configure your environment and what guardrails you put around models.

I think that the entire industry is learning about it.

What I see inside JFrog is how fast we remediated the level of transparency with the market, no hidden stuff by going straight and bold to our customers and demand that they will protect the software supply chain.

But I also see an opportunity here to say hey, it can be much more secure in the cloud, you can even be more secure with security around model's behavior.

Now what we will see next and have no doubt about that. we will see more models, getting more sophisticated, finding more vulnerabilities.

It's not a matter of being the scanner anymore.

It's a matter of how fast and how efficient you are in remediating and communicating to your customers.

Operator^   Your next question comes from the line of Howard Ma with Guggenheim.

Howard Ma^   And congratulations on a really strong quarter and the full year guidance raise.

One for Ed, if you look at the Q2 outperformance, how would you compare the mix of higher commitments and overages relative to Q1? And if you could comment on if there was any contribution from the fourth Frontier lab customer that you added in the quarter and for the full year as well.

So kind of two questions there.

Ed Grabscheid^   Yes. Thanks for the question, Howard.

We don't necessarily split out in terms of providing guidance or updates of what was overcommitted revenue versus commitment revenue.

But what I can tell you is, in Q2, we saw something very similar to what we saw in Q1 which was strong usage across the customer, a diverse group of customers in our installed base continuation of packages going through the software development life cycle and Artifactory. And we didn't see a decline by any means in the usage of that minimum commitment.

And we're very pleased with the end result.

In addition to that, we also had as Shlomi talked about in the prepared statements, we extended the -- our foundational AI labs.

We have four of those customers, and Shlomi can share a little bit more about that customer that we landed during the quarter.

Operator^ Your next question comes from the line of George McGreehan with Bank of America.

George McGreehan^ This is George McGreen on for Koji Ikeda, Bank of America.

I wanted to ask about kind of the contribution you guys are seeing from your suite of security products between the three advanced security run time and curation, kind of how do you stack rank the contribution from those?

Shlomi Haim^ Yes.

I'll take it, George. And thank you for the question.

We spoke a moment ago about the amount of [soto] supply chain attack and the kind of I don't want to say panic, but alerted response from customers and prospects.

So obviously the first thing that they are applying is a firewall between the software supply chain, the organization and the open source hubs. This is JFrog curation and we saw JFrog curation being adapted rapidly and also referred on the call JFrog curation by itself is an amazing firewall.

But when it comes with the Artifactory integration, that's a bulletproof solution that prevents any malicious package, any vulnerability known any type of unrequired packages to come into your organization.

So because it's so simple, and because it's implemented in very high integration with Artifactory.

Obviously our customers and prospects are betting on curation. And as mentioned on the script, none of our customers got affected by this massive attack of software supply chain out there. The second thing is that what happened once you start to run your pipeline.

This is where JFrog X-ray JFrog Advanced Security are providing a comprehensive holistic solution on top of your -- sorry, on top of your system of record to make sure that all the binaries, all the software packages and everything that you will distribute will not only be secured, but also known, traceable and monitored.

So later on, when you need to govern it, when you need to audit it, you have all the information.

So obviously because of the amount of software supply chain attack, curation gets the spotlights now but our customers are requiring more and more security solution from JFrog, mainly because of the advantage that we also manage all the binaries for them, and we also play as the single source of tools.

George McGreehan^ That makes a lot of sense. And if I could follow up with the second question here. Last quarter, in cloud consumption, there was usage above commitment this quarter, you guys noted as well.

But I'm kind of wondering if there's any change in kind of customer behavior in terms of are customers kind of getting a better sense of maybe how much they're going to be consuming on JFrog over -- in the future and kind of getting more comfortable committing at higher levels of usage? Or is that maybe not the case?

Shlomi Haim^ Well George, this is a wonderful question.

What we see is what I'm going to share. A, we see more AI tools being part of the software supply chain that drives scale. B, we see more AI software packages, unique software packages, and we call some specifics like MCP and skills just half a year ago, you wouldn't hear those terms. There are new assets.

These are all binaries.

So new assets with new software packages. And the third thing is the uncertainty. JFrog provides this flexibility that is amazing, not only for the CIO, but also for the CFO, they need to settle on what is the right estimation, a moment before they decide what would be the budget of 2027.

Now with our philosophy of guiding you guys with the commitment only, if you combine that with the number of customers over $1 million, a number of customers over $100,000, the growth in the cloud, you probably understand that our team is doing great work converting those over usage to commitment.

But we provide you with the full predictability and the certainty around our model, and this is why we follow commitments and not usage. Usage -- usage over commitment is growing, and we will still be focused on the commitment and the cloud migration of our self-hosted customers to the cloud.

Operator^ Your next question comes from the line of Radi Sultan with UBS.

Radi Sultan^ Just one for me.

Shlomi, I wanted to ask on the shift we're seeing towards increased adoption of open source and open weight models. Like can you just walk through how you see that trend impacting demand and usage.

I imagine maybe it's increasing pull-through on the security side, but be curious if this could increase a need on Artifactory as well.

Shlomi Haim^ Well yes, if you refer to the security, you are very much right. That's a great driver that fuels the growth and the adoption of our security solution.

But it's not only because of the open source that is bring both to the organization.

It's also because of the new practices that requires new packages to be managed and secure.

Now every vendor provide an MCP software package.

You need to govern that. You need to have an MCP registry. And you need to make sure that it's secure. JFrog Security provide all of these assets on top of JFrog Artifactory which makes the solution far more comprehensive and holistic.

I'm not talking now about who has a better scanner.

I'm talking about the outcome, what's the real value that we bring.

So of course we see growth there, Radi. And the second thing, it's also the speed and how fast things are happening. And we also mentioned that AI starts to be a wallpaper.

It starts to be [nbn] infrastructure.

People just use AI every day for everything. And they expect the software supply chain to be secure, to expect the pipeline to be secured now with the amount of attacks that they see out there.

Our customers were not affected by it. Just think about the amount of time that they save for not having the need to remediate and recover.

So I think that more and more customers put their trust in JFrog security and the holistic solution and coming up next, also governance because you also need to trust those software packages that you mentioned before you ship them.

Operator^ Your next question comes from the line of Brian Essex with JPMorgan.

Brian Essex^ Congrats on the results.

I just want to follow-up to a previous question that was asked about the way that customers are -- may or may not be managing their overages.

It seems like demand is pretty healthy.

Shlomi, are you proving to any conversations with your customers in terms of how they might be addressing more efficient spend just in general, but also on your platform? That's question number one.

And then as we approach swamp up, just wanted to get a sense of -- sometimes it's difficult to time product releases with a specific conference.

Sometimes companies release products when they're ready. How should -- what should we expect as we head into swamp up being kind of relatively new to the story here?

Shlomi Haim^ Brian, thank you for bringing swamp up.

It's going to be an amazing conference. Again we already see the speaker lineup I'll start with that.

I'll just say that Obviously the main thing that we see at swamp up is that the world's biggest organization are using JFrog and willing to share their best practices. And this is gold for our users.

Alongside that, there are the JFrog announcement which are exciting, very much aligned with the future roadmap.

But in the world of AI, if I will wait for swap up to release our product, our company will go backward and not look forward.

So expect a lot of excitement also on stage, but also with the customers' conversation. Regarding the efficiency and management of budget.

So what is it that we see, right?

We see more token being spent that generate more software because AI agents are being fueled and that generates probably a higher cloud consumption.

But people are asking, will that be forever like that? The answer for sure not because now we are getting -- we are transforming from the CIO former which was around technology to the CFO former which is around budget control. And then we have to ask ourselves what is the desired outcome of software pipeline of software supply chain of the AI world.

What's the desired outcome?

The desired outcome is that you will have more software being shifted in a higher quality.

What I just said, equals binary. And this is what JFrog is monetizing on.

We are monetizing on binary traffic.

So we think -- we suspect that CFOs will be smart enough and disciplined enough not to block innovation inside JFrog, we keep saying that you can also optimize how much you want to pay for the electricity you consume at home, but you still don't sit in the dark, right?

You just train yourself to close the light before you leave. That's the difference between source code and binaries, the desired outcome of a better is better binaries in high quality and higher consumption.

Operator^ Your next question comes from the line of Andrew Sherman with TD Cowen.

Andrew Sherman^ Congrats on another quarter of acceleration here. and the billings in RPO were extremely strong. RPO added a record $84 million, Could you talk about the breadth and nature of the big deals that went into that? And was there any pull forward from the second half pipeline? And how is the second half pipeline looking?

Ed Grabscheid^ Yes. Thanks for recognizing that in the RPO.

We're very proud of that. And that actually comes from the efforts that we have around our security products. That's a driving increase in our ASPs.

And you saw that in the $1 million number, 80% of the $1 million customers that we added this quarter had security attached to it. And that, along with even the new customer lands, 40% of those customers was security are driving much of the RPO.

In addition to that, customers that land with security typically take a multiyear agreement as well.

So the construct is a larger ASP longer in duration, and that results in strong RPO. And that's what we're seeing.

We did not pull really anything in from Q3.

We just had strong build in the quarter and execution from the team. And that pipeline that we built really came from the shy that hold events that started in Q3 of last year and it continued to build the sales organization executed on those deals, and it's reflected in our results.

Shlomi Haim^ I might just add to it is that I completely agree with everything that I said, some of those macro impact of open source attack is out of our control.

Obviously these are awful things that are happening, but I also make the hacker more sophisticated. And this software supply chain rapid attack might expedite some of what -- some of the opportunities we have in the pipeline.

Operator^ Your next question comes from the line of Jason Celino with KeyBanc.

Jason Celino^ Shlomi, I don't think you had the opportunity to talk about your important force AI customer here.

It seems like the hybrid deployment model is unique and interesting. Maybe can you speak to why this is maybe different from your other AI native customer deals? And then secondly, we on -- the Street always feel as well more, right? I mean is there a pipeline or opportunity and other natives of this magnitude?

Shlomi Haim^ Yes.

Well listen, we are so honored and so excited to add more and more companies that are building the world of AI. And this one that we just won this quarter was a great win and it was sweeter also because of the fact that we displaced a competitor that couldn't scale. The amount of binaries and the traffic that needed to be supported was not something that they could do. This AI factory moved to JFrog.

And they moved to JFrog in a very interesting way. They took JFrog platform as their mother ship in the cloud and with some self-hosted Artifactory servers in their data center.

So they will not only have the power of the J platform supported by our services but also to have a super robust distribution mechanism from this mother ship to all data centers from Artifactory to Artifactory. Working with these companies that build with AI for AI makes JFrog better.

We spoke earlier about the open AI incident.

This is how JFrog becomes 100x stronger because these guys, they take you to the limit with the security scanning, with scaling with different deployment environment, and we are very pleased and very honored to have them on board.

Obviously they look at JFrog as the planners of their pipelines, the providers of the infrastructure to the software supply chain.

Operator^ Your next question comes from the question Sanjit Singh with Morgan Stanley.

Sanjit Singh^ Congrats on an awesome quarter.

It was great to see.

Some I think you and I discussed before in terms of some of the evolution that JFrog is going through. You guys were one of the key destinations for container registries and those kind of traditional software outer facts. You mentioned the initiative to be the home of models and some of the newer kind of AI-native artifacts.

And just to get a sense of how that trend is evolving in terms of winning those newer artifacts?

Shlomi Haim^ Yes.

Sanjit, Great to see you on the call. You are right, and you watch the JFrog transformation before AI and hopefully, with AI.

So what do we see happening? We see that the world of software supply chain management move from just managing the pipelines to also secure them and govern them.

And by being focused on the right asset, what we keep saying from the foundation days of the company, binary is the primary asset.

By being focused on that, we are not only providing our customers with the smart storage that can scale in the cloud and on-prem, but we also provide them with a comprehensive security solution. And now as you probably heard on the call we just started to win our first [DevGovOps] customers and deals. People understand and we saw it again this week with OpenAI, models need to be governed.

So to your point, Sanjit, we became the biggest container registry after Docker boom. And now we are becoming the biggest model registry for our customers, mainly because of the following. They can scale with us. They can trust and they can secure and they can govern.

So if we will provide them this fundamental, and it's on us to prove, then I think that you will see the next leap in our evolution.

What also matters is that the AI company, the AI native and the AI Labs companies trust JFrog for to do it for them.

So we are learning a lot.

We are improving a lot. Just to stay humble, we are in the beginning of the journey.

Operator^ Your final question comes from the line of Kingsley Crane with Canaccord.

Kingsley Crane^ Just to build off what we've been talking about earlier as novel agentic attacks, they become more apparent. How do you manage an intelligence that we don't necessarily fully understand that's now capable enough to be dangerous.

So you mentioned earlier that AI models should not be treated as free? Is it consensus that customers are treating coating agents with that same scrutiny to do with third-party packages? Or are they still adjusting to that?

Shlomi Haim^ Kingsley, I'll be honest with you.

With over 6,000 customers, you see everything. You see customers that are just kind of being attracted by the technology and adopt AI with no responsibility. And you see customers that are terrified and take it one step at the time.

I think that what is special for the experience that we get from companies like Open AI and other leading AI labs is that they are showing us not only what needs to be done, but also what happened if you don't do it right.

And if you don't do a drug, models are becoming sophisticated and even smarter than our more senior developers and engineers.

So I believe that the world will become mature and the regulation and guardrails and security around models will become a bit more powerful.

What we are discussing with our customers is how important it is not only to host the models and to host the binaries and the outcomes for them, but also how we secure the entire pipeline. And there is no better school then this AI labs to learn it from them.

It's a great privilege to have all of this as our customers.

Operator^ This concludes the question and answer session.

I will now turn the call back to Shlomi for closing remarks.

Shlomi Haim^ Thank you everyone, for joining our call.

Obviously Q2 was yet an amazing quarter for us.

We are focusing on delivering what we committed in 2026.

And looking forward to seeing you at swamp up, where we will host and investor meet up to keep answering your question in full transparency and with the right excitement and made the floor be with you.

Take care.

Operator^ This concludes today's call. Thank you for attending.

You may now disconnect.