18-Aug-2025

Palo Alto Networks, Inc. (PANW)

Q4 2025 Earnings Call

CORPORATE PARTICIPANTS

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.

Dipak Golechha
Chief Financial Officer, Palo Alto Networks, Inc.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

OTHER PARTICIPANTS

Rob D. Owens
Analyst, Piper Sandler & Co.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Saket Kalia
Analyst, Barclays Capital, Inc.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Shaul Eyal
Analyst, TD Cowen

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Joseph Gallo
Analyst, Jefferies LLC

MANAGEMENT DISCUSSION SECTION

[Abrupt Start]

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.

...August 18 at 1:30 p.m. Pacific Time.

With me on today's call to discuss fourth quarter results are Nikesh Arora, our Chairman and Chief Executive Officer; and Dipak Golechha, our Chief Financial Officer. Following our prepared remarks, Lee Klarich, our Chief Product Officer, will join us for the question-and-answer portion.

You can find the press release and other information to supplement today's discussion on our website at investors.paloaltonetworks.com. While there, please click on the link for Quarterly Results to find the Q4 2025 supplemental information and Q4 2025 earnings presentation.

During the course of today's call, we will be making forward-looking statements and projections regarding the company's business operations and financial performance, as well as the company's proposed acquisition of CyberArk. These statements made today are subject to a number of risks and uncertainties that could cause our

actual results to differ from these forward-looking statements. Please review our press release and recent SEC filings for a description of these risks and uncertainties. We assume no obligation to update any forward-looking statements made in the presentation today.

This presentation contains non-GAAP financial measures and key metrics relating to the company's past and expected future performance. Non-GAAP financial measures should not be considered a substitute for financial measures prepared in accordance with GAAP. The most directly comparable GAAP financial measures and reconciliations are in the press release and the appendix of investor presentation.

Unless specifically noted otherwise, all results and comparisons are on a fiscal year-over-year basis. We also note that management is scheduled to participate in the Citi Global TMT Conference this quarter.

I will now turn the call over to Nikesh.

Nikesh Arora

Chairman & Chief Executive Officer, Palo Alto Networks, Inc.

Thank you, Hamza. Good afternoon. Thank you, everyone, for joining us today for our earnings call. As you can all see, we had a strong finish to the fiscal year. We've just closed a landmark quarter, capping a year of disciplined execution and strategic acceleration. Our results this quarter are a direct reflection of a strategy we have been architecting for years, anticipating where the market is going and building the future of cybersecurity before it arrives. This is a moment of conviction, both for us and for our customers.

We're proud to be the first dedicated cybersecurity company to surpass a $10 billion revenue run rate. While this milestone is significant, it is not the ultimate goal. Our focus has already shifted to – sorry, excuse me. Yeah, our focus has already shifted to leveraging the scale to define the next decade of cybersecurity.

The very fabric of technology is being rewoven by AI, creating a vast, new and complex attack surface. In this new era, security is no longer a bolt on. It is a foundational enabler of transformational success. The record-breaking number of platformization deals this quarter demonstrates that customers are not just buying products, they are buying into a strategic partnership. We believe that integrated best-of-breed platforms deliver superior security outcomes, and our customers are validating this conviction by making larger, more strategic commitments with us than ever before.

During Q4, many of the deals our teams had been working on during our fiscal year came to fruition. We saw robust activity across the board. In Q4, our bookings growth turned the corner and was the highest we've seen in 2.5 years. This growth is driven by deals across our platforms and also as a result of strong renewals and upsells across our existing portfolio.

The robust booking growth was coupled with strong Next-Generation Security ARR and revenue performance. This, coupled with prudent financial management, allowed us to exceed our full year guidance metrics across the board.

RPO grew 24% year-over-year in Q4, an acceleration versus the prior year. It is early days, but we see the quality of revenue, ARR and retention is consistently higher across our platform customers. This bodes well for our long-term targets of Palo Alto Networks' platform business.

Next-Generation Security ARR grew 32% and net new ARR for the quarter was also up double digits year-on-year. We had strong contributions across our portfolio, particularly SASE, XSIAM and software firewalls. Our

investment in software firewalls and SASE are bearing fruit. As our customers end up in a hybrid compute environment across multiple clouds, we expect to continue to see strength in our software firewall business.

These offerings, each with very large TAMs, continue to gain momentum and reinforce our conviction in achieving $15 billion in Next-Generation Security ARR by FY 2030 on a standalone basis. This top line growth, coupled with scale effects and our prudent financial management, has allowed us once again to expand our operating margin.

Additionally, continued deft management of our deferred payments plan portfolio has allowed us to deliver 38%-plus free cash flow margins for the third consecutive year. Not just that, we now believe that structurally, we have visibility to go even higher on our free cash flow margins, more from Dipak on this later.

Demand for cybersecurity remains strong. Our customers are looking to us to help them secure their cloud and AI transformation journeys. We continue to see GenAI conversations as it becomes imperative for our customers to deploy productivity tools, coding tools or revamp their customer systems to enable natural language conversations.

All these use cases for AI need to be protected, no pun intended. Our timely acquisition of Protect AI, which we completed this quarter, coupled with our native abilities around our AI firewalls are driving conversations across many platform customers and prospects around securing the AI infrastructure.

Adoption of GenAI is happening faster than any previous technology trend. Recent internal study amongst our customers showed GenAI traffic is up over 890% in 2024. Following this, data security incidents related to GenAI more than doubled since last year.

With this rapid adoption of AI comes a new and complex attack surface. That's why, in early Q4, we introduced Prisma AIRS, industry's most comprehensive AI security platform. AIRS is a unified platform that empowers organizations to deploy AI bravely by providing end-to-end security across every AI app, agent, model and data set. It closes critical blind spots and secures AI deployments everywhere, ensuring confidence and compliance.

But securing the AI you build is only half of the equation. The other equally critical side is securing how employees use third-party AI. Our AI Access solutions provides the deep visibility and granular control needed for the safe adoption of those services. We are unique in providing a strategy for both sides of the AI landscape, each with integrated DLP controls to protect our customers' most sensitive data. This complete vision is resonating, and we have a strong combined pipeline for AI security offerings.

The chart you see here tells a powerful story. It's not just a graph of numbers going up. It's a visual representation of our customers' growing conviction in our strategy. The question is why is this happening? It's because we made a promise to our customers that when they partner with us, they are investing in platforms that are constantly evolving, and we are going to stay ahead of the threat landscape.

Time and again, you've seen the future first. You saw it with the tectonic shift to the next-generation firewall, which we pioneered 17 (sic) [7] years ago. You saw it with the move to the cloud and with the rise of SASE, where we're now the clear leader. You saw the inevitable shift from reactive SIEM to proactive AI-powered SOCs, as well as in XSIAM, a platform that is now our fastest growing offering ever. And you saw the market's ultimate shift towards the word we define platformization, integrated platforms that deliver superior security outcomes, a framework our peers once again are now rushing to imitate.

We continue to evolve our platforms, and this quarter was no exception. In our network security platform, we announced PAN-OS 12.1 Orion, which includes new appliances designed to provide an easy path to quantum readiness and multi-cloud security. We are anticipating threats of tomorrow, so our customers don't have to. This commitment to future proofing their investment is why we are seeing robust interest in integrated subscriptions like CASB and DLP.

Building on the launch of Cortex Cloud in Q3, we delivered powerful new capabilities like Application Security Posture Management, or ASPM, helping to redefine application security to meet the demands of the AI era. Natively built into our Cortex Cloud platform, ASPM provides a single source of truth, correlating data from our native scanners and third-party tools to secure the entire AI development life cycle. This allows our customers to break down the silos between their teams and focus on remediating the critical vulnerabilities that truly matter.

And our XSIAM platform continues to expand beyond its core wartime mission with new peacetime modules like Exposure Management that proactively identify and fix security gaps before an attack can ever happen. That confidence is translating directly into platformization traction you see here. These platformizations are driving superior financial outcomes for us and better security outcomes for our customers.

In Q4, our net retention rate amongst platform customers was an impressive 120% with nearly zero churn. This is the ultimate proof of the value we deliver and the deep strategic partnerships we are building. As we aim to more than double the number of platformization in the next five years, we believe our foundation for sustainable growth becomes stronger. This underpins our confidence in achieving $15 billion of NGS ARR on a standalone basis by FY 2030.

The clear validation of our strategy is in the landmark deals we're signing. These are not product sales. These are deep partnerships with the world's leading organizations to transform the security posture. We had one of our strongest large deals quarters ever. Customers with over $5 million and $10 million in ARR were up approximately 50% year-over-year and $20-million-plus ARR customers were up nearly 80% year-over-year. These types of large multi-platform deals hardly existed a few years ago and showcase our customers' growing commitment to us.

Let's look at a few examples. Leading global consulting firm signed a deal for over $100 million in Q4 on Cloud Security and SASE, including a purchase of our new AI Access Security product. The customer lacked identity entitlement controls over AI and cloud environments and also required a comprehensive secure access offerings that could scale globally across its employees, contractors and clients. Our deep relationship with that company's C-suite were also critical to landing a deal of this size. With this deal, this customer is now fully platformized and provides us an ARR of $50 million.

Next, a leading European bank signed a $60-plus million deal. This customer is going through a significant digital transformation and adopted XSIAM with multiple goals in mind, to address an expanding attack surface, while simplifying their security stack and keeping costs under control. Platformization was a competitive edge as part of this deal, and we have become a true security partner as now they have three platforms with us.

Finally, a leading US insurance company purchased $33 million across NetSec, SASE, SecOps, and Cloud Security. This customer needed to improve their security posture, level up their SOC analysts and drive further automation to reach their goals of 15-minute mean time to contain. This involved using AI. machine learning to assist their analyst teams, while also reducing their false positives. In addition to their existing Palo Alto Networks spend, this customer has now platformized on network security, cloud, and security operations.

There's a common theme developing across these platform deals. While customers are consolidating and simplifying their security stack in part to optimize costs, the larger benefit comes from their improved security outcomes. This includes faster incident response times, a better user experience, and removing the operational burden of stitching together point products. As our customers recognize the value of platformization, they're increasing their commitments with us, reaffirming our strategy and vision.

Now shifting to Network Security, which had a strong Q4. Network Security continues to account for over 75% of our bookings. Although over the last five years, we have transformed the nature of this business and now over 60% of our Network Security bookings are driven by software form factors across SASE and virtual firewalls.

In addition to having an integrated platform that allows for a consistent pane-of-glass policy and more than 10 software subscriptions, we also continue to lead the market and gain share across the capabilities as a singular best-of-breed solution of our customer, if our customers so desire. As enterprises look to secure increasingly hybrid workforces and IT environments and AI, we believe our platform is well-positioned to allow our customers of any of our products to consolidate in our platform.

Our growing mix towards software form factors once again drove better-than-expected growth this quarter. Our software firewall business had another strong quarter in Q4, with ARR up nearly 20% year-on-year and almost double the total contract value. As a result of the strong showing of our software firewalls and with our steady growth in hardware slightly ahead of industry growth, we saw product revenue growth of 19% year-over-year, which is market-leading in its category at scale.

Our software firewall market share is nearly 50%, and our product is native in all major public clouds. This quarter, we signed a $60 million deal, significantly expanded our partnership with a leading US-based cloud provider. All in, we generated nine figures in deals across the major cloud service providers in Q4.

As I shared earlier, we're also building momentum in AI runtime security with Prisma AIRS, as customers look to secure the growing AI attack surface. In Q4, this included an eight-figure deal with a global professional services company. With a strong pipeline, we see an opportunity for AIRS to become a growing contributor in the next five years.

We also continue to gain share in hardware firewalls. As mentioned earlier, this past week, we launched PAN-OS 12.1 Orion, a newer appliance that's designed to provide an easy path to quantum safe and multi-cloud security. We saw modest improvements in hardware demand in Q4, but expect this will continue to be a mid-single-digit grower in FY 2026.

All in, our next-generation Network Security business, which includes software form factors like SASE and software firewalls, reached $3.9 billion in ARR, up approximately 35% year-on-year. We believe this makes us the largest and fastest-growing next-generation network security player at scale.

Speaking of SASE, this continues to be our fastest growing product in Network Security. As customers transform their networks to keep pace with delivering first-class security capabilities for remote users and branch offices, we continue to see strong growth for SASE. Many SASE projects are large and transformational, which is well-suited for our comprehensive enterprise-focused expertise. This quarter, we won our largest SASE deal ever, a $60 million contract with a global professional services firm covering nearly 200,000 seats. This was in addition to record number of eight-figure SASE deals.

We're gaining share. For the last year, we displaced incumbent SASE vendors in over 70 accounts exceeding $200 million in TCV. Our SASE ARR grew 35% year-over-year, more than twice as fast as the overall market. We now have over 6,300 SASE customers and account for one-third of the Fortune 500.

Meanwhile, the drivers of our SASE growth are broadening. This quarter, we once again saw a particular strength in Prisma Access Browser. The browser is becoming the new operating system for the enterprise, the primary interface for AI and cloud applications. Securing it is not optional. We sold over 3 million licenses in Q4 alone, resulting in our cumulative seat count more than doubling on sequential basis to over 6 million. Notable deals include an over $3 million transaction with a leading US pharmaceutical company who purchased Prisma Access Browser for over 80,000 seats.

We are beginning to see browser wars as we see the adoption of AI. Understandably, this is a requirement as we march towards agent. Interestingly, it will become impossible to allow employees access to non-secure browsers in the future. And as more and more critical application and data reside within the browser, it naturally becomes a target for cyberattacks.

Prisma Access Browser's built-in controls and real-time visibility are designed to help ensure that sensitive data remains safeguarded during browsing sessions, regardless of the user's location or the application they're accessing. And we believe it is strategically positioned to be the future OS in enabling secure and productive work in an AI-driven world. We expect to see browsers become an integral part of the SASE stack for all of our customers.

Moving on to Cortex and Cloud, we saw broad-based strength in Cortex and Cloud as well, with combined ARR up nearly 25% year-over-year in Q4. For years, the industry has been stuck in an old SIEM paradigm, collecting logs, writing rules, and overwhelming analysts with alerts. We saw the writing on the wall, this model is not sustainable in the age of AI-powered attacks. It's a battle that humans alone cannot win, and our customers are seeing it, too.

XSIAM, our autonomous SOC platform and our fastest growing product ever, is modernizing and disrupting the SOC market AI, and we continue to see amazing milestones. This includes reducing customers' mean time to respond from weeks to minutes. Today, over 60% of deployed customers cite mean time respond in under 10 minutes.

We ended Q4 with approximately 400 customers on XSIAM and the average ARR per customer continues to be over $1 million. Nearly a quarter of XSIAM customers are represented in the Global 2000, creating a marquee list of referenceable customers across a number of major industries.

Beyond XSIAM, Cortex XDR saw deals over $1 million grow 30% year-on-year. As we continue to build on our industry recognition, we are seeing opportunities in larger accounts.

I also want to highlight the growing significance of Cortex Cloud. As the market shifts from static posture management to the urgent needs for real-time runtime security, our thesis on the convergence of cloud security and security operations is proving correct once again. This is when where we are fundamentally different from the competition. While others may offer a strong cloud posture tool or a separate SIEM, we're the only ones to natively unify a best-in-class CNAPP with our AI-powered SOC platform. This allows our customers to move beyond simply reporting on misconfiguration instead, actively stopping cloud attacks in real time.

Cortex Cloud allows our customers to not only shift left to secure applications during development, but also shield right, protect them in production. The platform is already gaining significant validation. It was recently praised for its ability to fully secure the entire life cycle of cloud-native applications and has achieved FedRAMP High Authorization, a critical credential for our public sector customers. This product set is resonating with the market and early interest has driven a strong pipeline, spanning hundreds of customers who understand they need to stop cloud attacks in real time.

Our platforms are powerful data-centric engine for organic innovation. Our core thesis is that the integrated data we capture from across network, cloud and security operations is the ground truth needed for a whole variety of security use cases. For AI to be effective, it needs this complete contextual data, a capability unique to our platform approach. This massive data stream is what makes our XSIAM platform so effective in its primary wartime mission of stopping active threats.

But as the slide illustrates, we are now leveraging the same powerful data to expand into new peacetime missions. By applying our AI to this rich data set, we are organically creating new modules and expanding into new TAMs like Exposure Management and Email Security. This represents an $18 billion opportunity for us in fiscal year 2026 and beyond.

We see significant upsell opportunities from these modules as they attach to larger XSIAM deals. We're encouraged by the early customer feedback on these new capabilities. This is our data-to-market engine in action, allowing us to explore new frontiers in security and deliver continuous value to our platform customers.

To close, we're exiting FY 2025 with strong organic momentum as we march along our path to that $15 billion target. Our bookings and RPO accelerated this quarter, driven by large deal traction and a sharp focus on excellence and execution. The results of our customer-centric strategy are clear. We're seeing more customers platformize with us than ever before, not just to save money, but achieve a level of security that a fragmented approach simply cannot provide in an AI-driven world.

This realization that platformization is the way forward is also the engine behind our strong Q4 results and our confident outlook. We see broad-based strength across our Network Security, Cloud and SecOps segment, and strong pipeline as majority of core sellers are now equipped to sell across multiple platforms.

With strong early traction with Prisma AIRS and with our relentless focus on innovation, we believe Palo Alto Networks can be the ideal partner to help organizations achieve and secure their AI transformation goals.

However, before I hand over to Dipak, let me also talk about what we see for FY 2026. Looking ahead, we have multiple tailwinds driving our business in FY 2026 and beyond. In Network Security, we've growing demand for software firewalls and SASE, which continue to grow well above the market. The higher mix of software gives us confidence in sustainability of double-digit product revenue growth in FY 2026. We have multiple newer products contributing to our growth, including Prisma AIRS, secure browsers, each with large pipelines.

In Cortex, XSIAM continues to deliver rapid growth at scale. AI is transforming the SOC, and we believe we are well positioned to capitalize and win. Our migration to Cortex Cloud continues to progress. We believe we are well positioned to capitalize as the market evolves from posture management to real-time security for AI.

Of course, we've heard the market, and it's clear our customers are asking for comprehensive security platforms. Over the last seven years, I have been asked often, why are we not a player in identity? And for the longest of time, I believe that identity was not at an inflection point. But as we saw the emergence of agentic AI, as we saw

AI getting mass adoption, we're beginning to reach conviction that the identity market will inflect in the next 12 to 24 months.

If you believe you believe that we have been able to identify inflections in a good way at Palo Alto Networks, it is important for you to believe that we have this one right as well. Similar to our roots in network, identity is a key enforcement point for enterprise security. Unlike most of the forms of security, like network firewalls, identity is also a real-time product. And because of this, we believe that the future for identity will actually be owned by somebody who is well prepared to take on the challenges of identity going forward as opposed to a new player.

Hence, we have diverged from our original approach of going and buying first-in-market best-of-breed products to go and own market or categories. Instead, we believe the future in this category is going to belong to somebody who's already established a strong reputation and is a leader in identity security.

So as the widespread deployment of AI agents makes privileged access more important, we believe security, not SSO focused identity vendors are best positioned to address emerging needs and that growth in PAM data and sensors will further solidify category leaders like CyberArk.

Second, with 90% of our breaches involving stolen or mismanaged credentials, every user machine and AI agent should be considered a privileged user, rather than just a small set of IT administrators. CyberArk's reach extends to over 8 million privileged end users and over 50% of the Fortune 500. With the right product strategy and go-to-market acceleration from Palo Alto Networks, we believe CyberArk will be able to both deepen their penetration in PAM and target a significantly larger base of global IAM users and machine identities.

Thirdly, the identity industry is lacking a broader platform. Today, over 100 vendors are vying to capture the customers' attention across multiple functional domains. These domains are converging as the complexity of stitching together disparate solutions and the rise in identity-related breaches push enterprises to favor better integration.

We believe Palo Alto can accelerate CyberArk's platform vision as they look to expand across multiple identity domains. By combining their leadership in identity security with our industry-leading AI-powered security platforms and our platformization approach coupled with our go-to-market, we will be able to offer the most complete integrated security solution in the market. We're building an evergreen security company that will define the industry for decades to come.

After many detailed conversations, we have strategic alignment with the CyberArk team and a common culture of innovation. Following the close of transaction, we will optimize our combined go-to-market resources and continue to lead innovation. To provide some context, we have nearly 10 times the number of core sellers, and we see an opportunity to expand CyberArk's presence into our much larger 75,000 customer base.

Overall, we believe this accelerates our mission to double the value of our joint businesses over the next five years. We are strategically entering this category now to define the next chapter of cybersecurity for the AI era. We look forward to providing more details on our strategy, once we close the transaction.

Before I hand over to Dipak, I want to take a moment to speak from the heart on the important leadership announcement we made today. Our founder, our first innovator and a true titan of this industry Nir Zuk has decided to retire after more than 20 years. When you think of Palo Alto Networks, you think of Nir. It is impossible to overstate Nir's impact. He didn't just start a company. He started revolution with the next-generation firewall, forever changing the security landscape. Personally, it has been a privilege to call him a partner and a friend.

The relentless competitive fire that defines our culture, that is his legacy. It is in our DNA. His legacy isn't just in our products, it is in our people. So, Nir, on behalf of every single one of us, thank you. This marks a seamless and natural transition as we pass the torch to Lee Klarich, who will now serve as both Chief Product and Technology Officer and as a member of our board.

For years, almost as many as Nir, Lee has been the chief architecture for our product strategy, masterfully turning our vision into the industry-leading platforms we have today. Appointing to him as both CPO and CTO and to our board of directors is a reflection of the profound trust we have in his leadership. This ensures the soul of our innovation not only continues, but accelerates into the future.

With that, let me pass on to Dipak.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you, Nikesh, and good afternoon, everyone. To maximize our time spent on Q&A, I will provide you with financial highlights of Q4. You can review the detailed results in our press release and in the supplemental financial information on our website.

In Q4 2025, total revenue was $2.54 billion and grew 16%, above the high end of our guided range. Within total revenue, product revenue grew 19%, driven by growth in software form factors, while total services revenue grew 15%. Within total services, subscription revenue grew 17% and support revenue rose 11%.

In the fourth quarter, 56% of product revenue was from software form factors, a significant driver of product revenue growth year-over-year. On a trailing 12-month basis, the proportion of our product revenue from software surpassed 40%, driven by growth in our software firewall form factors and PAN-OS SD-WAN. We continue to see firewall appliance growth in line with the ranges that we have described in past periods, namely 0% to 5%.

Moving on to geographies. We saw double-digit growth across all theaters, with the Americas growing 15%, EMEA up 19%, and JAPAC growing 13%. We saw strength across our major verticals and saw a year-over-year bookings growth improvement in our public sector business.

Remaining performance obligation, or RPO, grew 24% to $15.8 billion. This was our highest RPO growth in seven quarters at a significantly larger scale. Our current RPO was $7.0 billion, growing 17% year-over-year. As Nikesh noted, we saw customers making significant commitments to our platforms in Q4 as reflected by a large deal volume, net new platformizations and RPO growth. Contract duration in the quarter increased slightly on both the year-over-year and the quarter-over-quarter basis, but remains within our historical range at approximately three years.

Turning to Next-Generation Security ARR, where we continue to see very healthy growth. We ended the quarter at $5.58 billion in NGS ARR, which grew 32%. Q4 NGS ARR included approximately $17.5 million in support where customers also purchased Strata Cloud Manager.

For context, this AI-powered unified management platform, which utilizes rich telemetry to deliver deeper insights into threats, a significantly improved user experience and much faster mean time to resolve issues for our customers. We expect this to be a growing contributor going forward, but remain immaterial to total NGS ARR.

We added approximately $490 million in net new NGS ARR in Q4, up 12% from a year ago. Our momentum was broad based this quarter. Notable growth drivers included software firewalls, SASE and XSIAM. AI ARR is now approximately $545 million in Q4, up over 2.5 times year-over-year.

Moving down the income statement, total gross margin was 75.8%. Product gross margin was 76.8%. And as we closed fiscal 2025, we undertook a comprehensive review of our inventory, leading to Palo Alto Networks taking a reserve for excess and obsolete inventory and spares. This was a deliberate and prudent step, taking a disciplined and conservative view of our product lifecycle. This action solidifies our balance sheet and ensures we're well-positioned into fiscal 2026 and beyond. That being said, we expect product gross margins in fiscal year 2026 to increase relative to 2025 and be in the high-70s or low-80s.

As I have mentioned in prior quarters, we've been transitioning our primary manufacturing and fulfillment center to a contract manufacturing facility in Texas to provide us with the benefit from scale and innovation, as well as to take advantage of a foreign trade zone that can help us mitigate the impact of any potential tariffs on products we ship to international customers and destinations.

We continue to believe that we differentiate ourselves in the industry by being the only pure-play cybersecurity firm to assemble all of our hardware in the USA at scale. As a result, the impact to tariffs of our business have been immaterial.

Total services gross margin was 75.5%, a slight sequential increase from Q3. We are pleased by the sustained growth in our SaaS offerings and are executing on cloud cost efficiencies, including engaging with our cloud service providers to negotiate favorable procurement arrangements as the scale of our cloud host products continues to grow. We continue to deliver profitable growth through the expansion of operating margins, which encompasses the gross margins that I just discussed.

In Q4, we expanded operating margins by 340 basis points and delivered operating margins above 30% for the first time in the company's history. On an annual basis, operating margins of 28.8% came in above the high end of our guided range as we drove scale and efficiencies across sales and marketing, R&D, and G&A. Diluted non-GAAP EPS was $0.95 and also came in ahead of the high end of our guided range.

Turning to the balance sheet, you will see that our debt balance came down by $383 million, as our 2025 convertible notes reached maturity in June of this year. These notes were settled in cash and equity in Q4. We did not repurchase any shares in Q4, and our buyback strategy remains opportunistic. We have $1 billion in authorization remaining through December 2025.

As many of you have heard from me in the past, we are focused on delivering profitable growth. And every decision we make is made within the context of maximizing long-term total shareholder return. For that reason, I'm extremely proud that Palo Alto Networks has delivered results that were above the Rule of 50 for the last five years. We are unique in our ability to deliver top-line growth with leading free cash flow margins at a level that is best-in-class among scaled enterprise software companies. As you will see shortly, we expect to once again be above the Rule of 50 in fiscal year 2026.

As Nikesh discussed, our ability to deliver sustained growth can be attributed to both our continued focus on innovation and our platformization strategy, which is driving bigger deals for us and better outcomes for our customers. On the free cash flow side of the equation, we've been able to expand our operating margins, providing a higher floor for our free cash flow, while improving our visibility to said cash flows.

Critical to our ability to be a continued Rule of 50 company has been the scalability of our business across every line item of the P&L. Since fiscal 2022, we've expanded our operating margins by almost 1,000 basis points, and we expect to continue to deliver expanded operating efficiencies in fiscal year 2026 and beyond.

Our ability to expand operating margins have enabled us to deliver sustained high free cash flow margins, while steadily managing an increase in demand for deferred payments. We've been moving through this transition since fiscal 2021, and as we lap deals with deferred payments from prior period, we have an increased visibility into our future free cash flows.

As I mentioned earlier, we delivered $3.5 billion of free cash flow at 38% margin in fiscal year 2025. We had visibility to approximately 40% of that free cash flow from deferred payments on deals signed prior to the fiscal year. We continued through this transition to deferred payments in fiscal 2025, and we expect about half of our fiscal 2026 free cash flow to come from deferred payment deals signed in fiscal 2025 or earlier.

Looking forward, we continue to see future free cash flow supported by ongoing operating margin expansion and a continued smooth transition to deferred payments. Specific to that topic, we continue to see increasing demand for annual payments, particularly on larger deals. We're absorbing this transition whilst maintaining our best-in-class adjusted free cash flow margins and guiding 2026 adjusted free cash flow margin of 38% to 39%.

With that, let me turn to guidance. The Q1 2026 and fiscal year 2026 guidance I will provide is for Palo Alto on a standalone basis and does not include any anticipated impacts from the proposed acquisition of CyberArk announced on July 30, 2025.

For the fiscal year 2026, we expect NGS ARR to be in the range of $7.00 billion to $7.10 billion, an increase of 26% to 27%; remaining performance obligation of $18.6 billion to $18.7 billion, an increase of 17% to 18%; revenue to be in the range of $10.475 billion to $10.525 billion, an increase of 14%; operating margins to be in the range of 29.2% to 29.7%; diluted non-GAAP EPS to be in the range of $3.75 to $3.85, an increase of 12% to 15%; and adjusted free cash flow margin in the range of 38% to 39%.

For the first fiscal quarter of 2026, we expect NGS to be in the range of $5.82 billion to $5.84 billion, an increase of 29%; remaining performance obligation of $15.4 billion to $15.5 billion, an increase of 23%; revenue to be in the range of $2.45 billion to $2.47 billion, an increase an increase of 15%; and diluted non-GAAP EPS to be in the range of $0.88 to $0.90, an increase of 13% to 15%.

We've included our modeling points in the presentation for your review, but I would like to highlight two areas. Firstly, we expect Q1 2026 product revenue growth to be approximately 20% and we expect fiscal year 2026 product revenue growth to be in the low-teens. This is largely driven by strength in our software form factors within product revenue. Furthermore, we expect our top line seasonality to continue to be second half and Q4 weighted as we continue to platformize with our customers.

Finally, I'd like to give an update around our financial expectations for the combined Palo Alto Networks and CyberArk. As you can see, we are pursuing this acquisition from a position of strength and are excited about our integration efforts post-close.

Based on our continued operating margin expansion and visibility of free cash flow and our continued smooth transition to deferred payments, we're targeting adjusted free cash flow of 40% plus for the combined company in fiscal 2028, the first full year post-integration. This target assumes the impact of M&A-related synergies. We

intend to provide more details on the full scope of synergies post the closing of the transaction, which we continue to expect will happen in the second half of fiscal year 2026.

We're excited about the outcomes of the combined Palo Alto Networks and CyberArk businesses will deliver from a security perspective as well as from a TSR perspective for the shareholders of both companies.

With that, I will turn over to Hamza for Q&A.

QUESTION AND ANSWER SECTION

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.
A

Sorry about that slight technical difficulty. [Operator Instructions] The first question will be from Rob Owens from Piper Sandler, followed by Brad Zelnick from Deutsche Bank.

Rob D. Owens
Analyst, Piper Sandler & Co.
Q

Thank you, Hamza, and good afternoon. Thanks for taking my question. I was hoping to get a more strategic view on security consolidation, both from your perspective, where we're at now, as well as any anecdotes you can share from customers. As you well know, security is one of the most fragmented IT markets of scale with Palo as the independent leader, but still only kind of a mid-single digit share relative to spend right now. While platformization, your SecOps strategy was clearly aimed at playing to this convergence, can you speak to the rise of agentic right now and how it's catalyzing this market need? Thanks.

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.
A

Hey, Rob. Thanks for your question. I guess, we should be more strategic in our answers. So the consolidation is 99% perspiration and you see that. That's why we've set ourselves on this plan of platformization. And I think the reason we highlighted a $50 million ARR deal, that's a big number in technology, whether it's cybersecurity or anything else. That tells you the art of the possible. If one was able to consolidate the entire security spend of a large customer, you can get up $50 million in ARR. I think if you look around our landscape, many companies are still reporting million dollar customers, right? The art of the possible is $10 million, $20 million, $50 million in ARR. That shows you that's where consolidation is headed.

Now, historically, whether it's CRM, whether it's ERP, whether it's HR, workflow, it's ITSM, all these markets have started as fragmented markets. They've just been around 25 years longer than we have. So if you play this movie 10, 15 years out, there's no reason why our installed base of platform customers should not continue to rise at the pace we're trying to predict it's going to rise.

So, can I see us going from 6% to 8% market share to 15%, 20%? Yes, I can. Is it going to happen in one quarter? Unfortunately not, it's going to take us this sort of deft art of convincing our customers to platformize with us, giving them good experiences on one platform, evolving them to the next one. I'll tell you the benefit of AI is we're down to a 25-minute attack, right? So it's no longer how much money are you spending to protect ourselves. The question is how quickly you're going to find it and how quickly you're going to stop it? The answer

is more than 25 minutes, I got news for you. These wonderful agents are going to come and make sure they're able to exfiltrate data and breach an enterprise, it doesn't matter how much you're spending, in under 25 minutes.

To get there, the only way to get near real-time is to have some consistency in our platform where data talks to each other and are able to run agents on top of it. We can't run agents on top of disparate infrastructure. There's no agent out there that understands three different firewall vendors in infrastructure, two SASE vendors, a browser vendor and seven other vendors on top. Well, if there's one, we'd love to hire it.

So I think agentic is only going to make this worse because there are agents that bad actors can deploy to try and breach it. So I think from our perspective, AI is going to act as an accelerant towards the desire to consolidate. Customers are beginning to feel the value of consolidated data, not just in security and other areas as you can see. So I think it's all good, but it's going to have to be heads-down execution in that light, and I'm sorry for taking so long to answer your question, like that's what's driving us to say, look, we need to get identity as part of the fold, because identity is – I sort of have a word in my script, which I didn't say, maybe it's time for identity firewall. Why is there no real-time clearing of identities in an enterprise? It's disparate and spread across 7 or 10 identity providers. Thanks, Rob.

Rob D. Owens
Analyst, Piper Sandler & Co.

Q

Thank you.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.

A

Thank you, Rob. Next question will be Brad Zelnick from Deutsche Bank, followed by Saket Kalia from Barclays.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Great. Thank you very much for taking the questions and congrats on a monster near $5 billion bookings quarter. Nikesh, if you reflect back on the underlying drivers, how much of this is strong execution versus maybe improved macro since April versus seeing the fruits of platformization play out? Or is the platformization benefit still very much ahead of us? Thank you.

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.

A

Well, first of all, thank you, Brad, for your positive note on our stock most recently. You found a low point to reestablish your credibility with us. So thank you.

That notwithstanding, look, I want to say it's the platformization story. I think it takes a while to take our thousands of sellers out there, get them to understand that the value is in platformization, and being able to multiply and deploy all of our products in a consistent fashion. I don't think the macro is bad. I think macro is fine. I think the challenge that you've been seeing is something that Rob just talked about. We still have fragmented players in the industry. You get trapped in a hardware only business. If you only have a hardware business, you don't have a software firewall, where you have 50% market share, you're not going to have double-digit product growth on a consistent basis.

If you're not taking share in SASE and you only have SASE to deal with, then you're stuck in a situation where you're losing share in SASE and you're still fighting three vendors at every SASE sort of PoC or SASE deal. If

you're not innovating, you're not out on the browser game, then you've got to watch out because the world is moving to the browser.

I think it's a combination of the innovation roadmap, the conviction of the customer that we have now demonstrated over the last five years that we will rush to deploy and embrace a technology that's out in the market. Two years ago, we didn't have a browser. And a year ago, we didn't have an AI firewall. Our customers see that, say, look, I know that if I commit to your platform, I will see a path to the next technology out there. So I think it's partly us building conviction with our customers that we will provide them an evergreen path. I think it's partly the fact that people feel that there is a need to consolidate to get a better security outcome.

I think macro is still what it is. I think the Fed is finally coming out of its machinations of a new administration trying to figure out how to keep business as usual going and how to make sure that we continue to protect the nation.

So I think from all those perspectives, macro is fine. I think there's no big step up or step down in macro. And we'll see what happens going forward, but I don't see anything different in the market going forward. I think we can see – continue to see the benefits consolidation. And as always, look, there's always the Q4 magic, as you all know. There is no magic to July 31, but there is magic to Q4. So I think part of what you're seeing is our teams saw that they were executing really well and they put their foot in the accelerator.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Very helpful. Thank you.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.

A

Thank you, Brad. Our next question is from Saket Kalia from Barclays, followed by Gabriela Borges from Goldman Sachs.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Okay. Great. Hey, guys. Thanks for taking my question here. Nice finish to the year and congrats to Lee and Nir on their respective next steps. Nikesh, maybe for you. I'd love to dig into the Network Security ARR a little bit more, particularly the form factor shift in firewall. You've talked about sort of more of a move to software there driven by cloud transformation. Maybe the question is, why do you think Palo is taking share in the software part of the firewall market? And how do you think about lifetime value there versus appliances, if that makes sense?

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.

A

Well, let me have our new board member first answer the form factor shift from a technological perspective. You have to deliver visionary stuff as Chief Technology Officer. Then I'll talk to you about the numbers. Go ahead.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Thank you, Saket.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Hey, Lee. Congrats.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Thank you very much. Look, if you think about the hardware space, it started in 1994, 1995, just to give you a sense of like how long that space has been around, whereas the software network security market is much more recent. And as customers made their shift toward the cloud, a lot of the sort of incumbent vendors sort of treat it as a secondary market, possibly de-feature something that was hardware based, put a little spit and shine on it.

The reality, though, is the cloud environments require a lot more focus than that. It's not just someone else's network and you put a software firewall into it. There's a lot of unique innovation that has to be driven. And you saw this over the last few years from us. We launched Cloud NGFWs, which are designed to be sort of cloud native firewalls. So they're not just a virtual appliance. They're actually designed to fit seamlessly in the cloud.

With the PAN-OS Orion launch from last week, we talked about cloud networking and building out a whole cloud networking fabric that connects into that, not only for Cloud NGFWs, but also for our AI firewalls that run in the cloud as well. And so I believe our traction and success in software firewalls is the amount of dedicated attention we put on them to drive unique innovation that's specific to their deployment needs and we see it. We see it in the numbers and we see it in the customer traction we get. Nikesh?

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.

A

Look, I think part of what you're seeing from a why now is, originally, the view was that people will go with one cloud service provider, make that the mainstay of their cloud migration, and that's where you're going to get some of this network security capability. But today, I'd say if you look at Fortune 500, I'd say 80%, 90% of those customers are multi-cloud. It's hard to find a single cloud customer out in the market, unless you are the cloud provider yourself. Even they have sometimes, too, because to make an acquisition with somebody else who is using a different cloud provider.

So the moment you start having multiple cloud providers, then if you want a single pane of glass, you need to go off one of them and come to something like Palo Alto. We're the only player in the market which had native embedded software firewalls in all of the cloud providers. So you want one pane of glass, as a native firewall in all of cloud providers, you come to us, kind of that's one reason.

Two is what you've noticed now more and more production applications are in the public cloud. And when they get there, there is no excuse not to have a firewall protecting that instance. So I think from both those vantage points, it's that software firewall time has come now. And the good news is, as you'd appreciate, hardware, we ship a firewall, customer sandbox it, test it, deploy it takes six months. Software firewalls can get turned down overnight. You can provision them in under 24 hours. You can scale them as soon as you want. There's no lag. You can upgrade them from a software perspective instantaneously. As and when we deploy an upgrade, it gets deployed to all of our customers.

So I think from all those reasons, it's a much more efficient security appliance in a way, software appliance, than you could ever get for hardware. So you're seeing that. I think from a lifetime value perspective, it's kind of interesting. We announced a $60 million deal with one company for software firewalls TCV this quarter. It's been a

long time since we did a $60 million hardware firewall deal from a TCV perspective, because that will require you to buy, I don't know, at least 3,000 firewalls. And nobody is buying 3,000 firewalls.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Very helpful. Thank you.

Dipak Golechha
Chief Financial Officer, Palo Alto Networks, Inc.

A

Just to build on that, Saket, like we've said multiple quarters ago that the transition from a hardware firewall to software firewall is roughly the same in terms of revenue, and Nikesh talked about how it's much easier to deploy. On SASE, actually, the lifetime value ends up being about 2.5 times larger than it typically is on a hardware firewall.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Appreciate it. Thanks, guys.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.

A

Thank you. Up next is Gabriela Borges from Goldman Sachs, followed by Matt Hedberg from RBC.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Q

Hey, good afternoon. Thanks for taking the question. Dipak, I wanted to follow up on some of the mix commentary within NGS ARR from last quarter. Give us a little bit of a sense as we look through this year on how you're thinking about the advanced attach subscription versus the emerging portfolio mix in NGS ARR. And to Saket's question on virtual firewalls, do you think we can see similar step-ups in growth in virtual firewalls such that they contribute similar amounts to the growth algorithm for NGS ARR? How durable is that as a growth driver? Thanks.

Dipak Golechha
Chief Financial Officer, Palo Alto Networks, Inc.

A

Yeah. So I think, Gabriela, maybe just the meta point is, we're pretty much over a lot of the transitions of our advanced subscriptions at this stage, like we alter the definition really based on feedback from you to make sure that it's easier what's excluded at this stage, which is really just hardware firewalls and legacy subscriptions and support. We will continue to see step-up from those things that are legacy that we can transition over. But the reality is we're now more and more – the growth is coming from fast, durable, next-generation products, whether it be software firewall, whether it be SASE, whether it be XSIAM, and some of the newer products that we're launching like Prisma AIRS that will also be significant contributors to growth.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Q

Thank you.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.
A

Thank you, Gabriela. Next question is from Shaul Eyal at Cowen, followed by Joe Gallo from Jefferies.

Shaul Eyal
Analyst, TD Cowen
Q

Hamza, I think you had Matt ahead of me.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.
A

Oh, I'm sorry. Matt, please go ahead. And then from Shaul Eyal from TD Cowen.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Sure. Thanks, Hamza. The top line results are super impressive. I have a question for Dipak. The 40% free cash flow margins by 2028 is also equally impressive. Maybe a question for you or even Lee from a product integration perspective. Can you talk about some of the underlying components of how you get there and sort of your confidence level on that. Because that is obviously, I think, well above what a lot of us thought post-integration.

Dipak Golechha
Chief Financial Officer, Palo Alto Networks, Inc.
A

Well, let me start. I mean, like we wouldn't be guiding to it if we didn't have confidence in it, Matt. But I think, look, it's really underpinned by the operating margins. You've seen a lot of operating margin expansion occur over the last three years. We feel very confident that we have a business model that scales at every single line item of the P&L. I've talked through that before. We're a low capital-light business model, which always helps from a free cash flow point of view. So I'd say pretty high degree of confidence.

I think the meta point is when the strategy is to platformize and customers are buying into it and we're cross-correlating the data, that really helps us scale well as a company, and then that helps scale very well from a cash point of view as well. That's effectively what we're seeing, like as we guide into the future.

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.
A

I will add to what Dipak just said. I think he showed you a beautiful slide about how we feel like some of our free cash flow has been sat upon because of the transition from effectively – yeah, and towards annual billings. So now, given that a majority of our business has shifted towards annual billings, we know that the rest is still going to be upfront cash. So given that, we get a sense that we'll get some relief on the free cash flow margin in the next 24 months.

So I think putting all those together in a box and mixing it, we believe we definitely can achieve more than 40% margin. Of course, it will require some degree of work with our CyberArk colleagues and partners when we get this deal done. But we feel confident that they're equally aligned in terms of what we want to achieve.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Thanks, guys.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.
A

Okay. Great. Up next is Shaul Eyal, and we'll wrap it up with Joe Gallo from Jefferies.

Shaul Eyal
Analyst, TD Cowen
Q

Thank you. Good afternoon, everybody. Congrats to everybody. Nikesh, enterprise browser momentum and also browser wars. These wars, are these with privates? Are these with some other players out there? What's the thinking along these lines [indiscernible] (00:55:41)?

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.
A

Look, if you look at what's going on, it's kind of sometimes it's better be lucky than good, right? So we bought the browser because we felt there were certain use cases like VDI or third-party contractors or mobile devices which are not covered by SASE. So we literally bought the browser business thinking we were going to cover these edge use cases and life will go on as normal for regular employees of VPNs or SASE clients. And we built that strategy, and we see a lot of adoption from a third-party contractor as well as VDI perspective, and we continue to make progress there.

Now, what happened about six to eight months ago, you started hearing that the only way to deploy agents successfully for many consumer use cases is a browser. If you want to make a reservation on Booking.com and [ph] book an OpenTable (00:56:25) reservation or you want to so suddenly to run agentic tasks, you need to control the browser. That's what Anthropic is figuring out, that's what OpenAI is figuring out, that's what Perplexity is figuring out, that's what Google is figuring out.

Suddenly, you're beginning to see these, let's call it, consumer browser wars that are beginning to start. Microsoft is going to come back with more agentic features of browsers. Effectively, you deploy a browser in your device, which is going to start doing agentic tasks for you.

Now, what's great for the consumer is dangerous for the enterprise, right? No enterprise is going to love a do as you please browser, which can run agents without control. How do you control agents in a browser for enterprise employee or you need to secure browser? You literally will come to a point where companies will say, you cannot use a consumer version of this product. And think about it, happens in enterprise all the time.

You're not allowed to use a consumer version of Docusign. You're not allowed to use a consumer version of Dropbox. You're not allowed to use a consumer version of a SaaS app in enterprise because it's missing the enterprise controls. So if you believe that agentic true future is coming through browsers in the future for the desktop, then you have to believe that the case for secure browser just became a mainstream case in the enterprise use case. So that's what I meant by the browser wars and consumer are going to drive the acknowledgment that we need to solve the browser problem in enterprise, then it's going to become a critical part of your SASE stack.

Shaul Eyal
Analyst, TD Cowen
Q

Understood. Thank you so much. Appreciate it, guys.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.
A

Thanks, Shaul. And our last question will come from Joe Gallo from Jefferies.

Joseph Gallo
Analyst, Jefferies LLC
Q

Hey, guys. Thanks for the question. Saw the blended Cortex and Cloud numbers. But can you just talk more about Cloud Security specifically in detail? How is that doing? Are customers gravitating towards that runtime agent architecture and then any changes in the competitive landscape post the Wiz acquisition?

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.
A

Look, I think the thesis we had with Cloud Security when we decided to make the change and launch Cortex Cloud was that the different elements of Cloud Security are all interconnected from application security to cloud posture security and to runtime security and cloud SOC.

And I would say six months since the Cortex Cloud launch, our belief and conviction in that thesis is even stronger. It is very clear that attacks are happening faster. We know that as more and more enterprises move enterprise critical applications to cloud, that means cloud runtime protection becomes even more important than ever before.

And from that, and Nikesh made the comment of sort of both shift left and shift right. There's the shift left aspect, which is how do we shift left all the way to the beginnings of code writing and application security. You saw us a couple of weeks ago launch Application Security Posture Management, which is our approach to making sure that everything developed for the cloud is done in a secure way such that what is deployed in production is as secure as it can be. With Exposure Management, we can then tie that across not only cloud but enterprise, tie in with run time, et cetera.

And so, our conviction of that is still very, very strong. And we're seeing the response from our customers of being aligned with that strategy. And now, it's a question of lot of execution to take our customers through that transformation, that journey over to Cortex Cloud.

Joseph Gallo
Analyst, Jefferies LLC
Q

Thank you.

Hamza Fodderwala
Senior Vice President-Investor Relations & Strategic Finance, Palo Alto Networks, Inc.

Okay. With that, we'll conclude the Q&A portion of the call, and I'll turn it back to Nikesh for his closing remarks.

Nikesh Arora
Chairman & Chief Executive Officer, Palo Alto Networks, Inc.

Well, all I have to say is thank you again, everyone, for joining us today. I also want to once again say thank you to Nir for all his visionary leadership at Palo Alto Networks, and congratulations to Lee Klarich, our newest board member, who will continue our technological vision going forward.

And we look forward to seeing many of you at future conferences. I also, once again, want to thank our customers, employees and partners for helping us deliver a wonderful quarter and the end of the year, we look forward to FY 2026. Have a great day.