

20-Nov-2024

Palo Alto Networks, Inc. (PANW)

Q1 2025 Earnings Call

CORPORATE PARTICIPANTS

Walter H. Pritchard

*Senior Vice President-Investor Relations & Corporate Development,
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 Officer, Palo Alto Networks, Inc.

OTHER PARTICIPANTS

Saket Kalia

Analyst, Barclays Capital, Inc.

Brad Zelnick

Analyst, Deutsche Bank Securities, Inc.

Hamza Fodderwala

Analyst, Morgan Stanley & Co. LLC

Brian Essex

Analyst, JPMorgan Securities LLC

Joseph Gallo

Analyst, Jefferies LLC

Matthew Hedberg

Analyst, RBC Capital Markets LLC

Gregg Moskowitz

Analyst, Mizuho Securities USA LLC

Rob D. Owens

Analyst, Piper Sandler & Co.

Gray Powell

Analyst, BTIG LLC

Andrew Nowinski

Analyst, Wells Fargo Securities LLC

Fatima Boolani

Analyst, Citigroup Global Markets, Inc.

Roger Boyd

Analyst, UBS Securities LLC

MANAGEMENT DISCUSSION SECTION

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

Good day everyone, and welcome to Palo Alto Networks First Quarter 2025 Earnings Conference Call. I'm Walter Pritchard, Senior Vice President of Investor Relations and Corporate Development. Please note that this call is being recorded today, Wednesday, November 20, 2024 at 1:30 p.m. Pacific Time.

With me on today's call to discuss first 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 1Q 2025 supplemental information and 1Q 2025 earnings presentation.

During the course of today's call, we will make forward looking statements and projections regarding the company's business operations and financial performance. 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 metrics and reconciliations are in the press release, and the appendix of the Investor presentation. Unless otherwise noted today, all results and comparisons are on a fiscal year over year basis. We also note that management is scheduled to participate in the UBS Global Technology Conference.

I will now turn the call over to Nikesh.

Nikesh Arora

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

Thank you. Walter. Good afternoon and thank you, everyone for joining us today for our earnings call. We're delighted to report a strong start to fiscal year 2025. In our first quarter of focusing on RPO, NGS, ARR, we saw strength in both metrics and saw them perform well ahead of our expectations. The market for cybersecurity continues to be robust and continues to grow faster than the overall technology market. Despite the acceleration of technology spend due to AI, cyber security continues to outpace technology spend. We saw particular strength in our next generation security offerings, notably in Cortex and in NetSec. NGS ARR grew 40% to over \$4.5 billion. It is still well ahead of our and the Street's expectations, independent of a one time increase due to the IBM deal.

On the profitability front, we expanded our operating margin by 60 basis points year over year as we continue to see benefits from our broad efficiency focus while making the necessary investments to sustain our growth. This translated into a 13% EPS growth and strong cash generation. We are particularly pleased with our continued execution at scale, where we are able to balance our growth initiatives within our financial investment envelope, allowing us to deliver upside to our EPS guidance.

We've been talking about the benefits of simplifying security architectures and consolidating point products into platforms for a while now. I'm sure all of you remember our eventful quarter where we changed gears on platformization, as I've said before, I wish we could have made our good decisions faster. We continue to see momentum across our partner ecosystem and our customers. More recently, our industry peers have been evangelizing the virtues of platformization and industry experts have begun to weigh in.

I had our teams go back and compare the growth in the mentions of the word platform on cybersecurity earnings calls this year versus last year. We found an overall 50% increase amongst our peers, as they say, imitation is the highest form of flattery. As another point of reference in recent research, Gartner sees 75% of security leaders actively pursuing a vendor consolidation strategy, although less than 15% of large enterprise customers have implemented at least any one security platform solution.

Gartner expects that by 2028, 45% of organizations will use fewer than 15 cybersecurity tools in their product portfolio, up from 13% of organizations in 2023. I do want to reiterate the definition of what we want to achieve as a platform, central to stopping threats of the future is a robust AI and automation platformization strategy and data is at the heart of it all.

Our approach is to ingest all relevant security data once, stitch and analyze this with precision AI technology, and natively automate end to end workflows. It's a tall order to take data from many different security vendors, analyze it on the fly, and make a decision to stop an attack fast enough. But we're encouraged with the early success of our XSIAM and cloud platform to do exactly this. In network security. We also collect all data across all Palo Alto Networks security products and enable our customers to operate on a single pane of glass with consistent services, which work across all our form factors.

We believe our network security strategy is the most comprehensive platform available in the industry, encompassing a majority of the use cases via a single, consistent interface. As one of our customers recently said, that's one pane of glass versus many glasses of pane.

So while many of our competitors are talking about their platform approach, we don't believe they're equipped to deliver it in the way we can. We feel the cybersecurity industry is embarking into its next phase, where the market will continue to converge towards a fewer set of platformization players over the next 5 to 10 years. Point solutions will continue to get subsumed in these platform plays. Having started this trend, we intend to be one of those few players.

With this being the first quarter of our fiscal new year, we further oriented our go to market enablement around platformization. Our goal is to broaden the effectiveness of our solutions selling across thousands of sellers, and arm them to sell the value of our differentiated security outcomes across network security, cloud security, and security operations. With platform-specific domain consultants and architects, we are able to bring tremendous focus to our go-to-market efforts.

I'm again pleased with the results we're seeing. These came through in our Q1 metrics. We added more than 70 new platformizations with about a third coming from our acquisition of QRadar SaaS, we ended Q1 with approximately 1,100 platformizations.

Beyond the number of new platformization in Q1, we also saw strength in ARR per platformized customer. Our Q1 ARR per platformized customer was up 6% versus the average we saw during fiscal year 2024. The improvement in ARR is driven not only by our success signing larger transactions, it is also driven by our team's ability to expand existing platformized deployments continuously with new innovation that is delivered.

For example, in network security, we have seen significant value from the adoption of advanced subscription services and uptake of add-on modules and SASE, such as ADEM or Autonomous Digital Experience Management or CASB. ADEM and CASB are essential for us to be able to deliver AI solutions and AI access capabilities in the future, and we believe this capability will become existential for all SASE customers. Our Q1 performance keeps us on track to achieve 2,500 to 3,500 platformization deals by fiscal year 2030.

We're happy with our continued strong growth in NGS ARR in Q1, fueled by our continued platformization momentum. We see multiple drivers here. Network security customers are increasingly deploying our software and SASE form factors, including adopting advanced Zero Trust security subscriptions across them. Over time, these customers have a significant incentive to converge their network security architecture towards adoption of our full suite of three form factors.

Outside of network security, where we now have well over \$2 billion in NGS ARR, we are also seeing our cloud security and Cortex security operations business become significant as well. Last quarter, cloud security crossed the \$700 million milestone, and this quarter, Cortex crossed the \$1 billion milestone.

Looking at the large platform deals, we see a variety of opportunities across all of our customers. We signed a transaction with a large technology firm for over more than \$50 million. This deal was headlined by a SOC transformation, where we both replaced multiple [ph] SIEMs and XSIAM and XDR. (08:13) The customer is facing rising costs in the SOC with little automation and [ph] inadequate (08:21) visibility into the rising number of tailored attacks that leveraged AI. The customer was a QRadar customer and a year ago had platformized with us in network security. In this transaction, they added SD-WAN as well.

Next, we had a deal north of \$15 million in value, with a national hospital system platformizing their network security, which include an ELA for our firewalls. The customer is focused on both preventing a breach, after observing the many high-profile incidents in the healthcare industry as well as reducing operating costs.

We displaced a legacy firewall vendor and also set ourselves up for future SASE deployments. In SecOps, we also have an initial Cortex footprint in this QRadar customer, with an XSOAR deployment. A financial institution customer standardizing our firewalls, including an ELA in a transaction for over \$20 million, after standardizing on our network security platform with SASE in fiscal year 2024.

While we had to win the firewall business based on the capabilities of our [indiscernible] (09:13) our SASE platformization and our consistent NetSec architecture across form factors was a big differentiator. With the benefit of our consistent network security architecture, we were able to streamline operations across the network and drive lower cost.

Last but not the least, [ph] we tried (09:29) the transaction greater than \$30 million with a physical security services company. The customer signed a large transaction with us last year, platformizing network security and

security operations. In this quarter, the customer expanded both XSIAM and XDR deployments and added SASE and network security. This is a challenging deal as there were significant changes [indiscernible] (09:46) customer with new IT Leadership, including someone who had previously deployed a SASE point product from a competitor.

We were able to show both cost savings and a better security outcome from our consistent NetSec architecture. Our expanded Cortex footprint was driven by the customer's confidence that we are helping them identify and stop attacks. Overall, these are representative of a large deal momentum, where we saw 305 transactions over \$1 million, up 13% and 60 transactions over \$5 million, up 30% this quarter.

Switching gears, let's take a look at our three platforms and how they're supporting our growth. In network security, we continue to see steady demand in our product business. The demand continues to be a function of customer refreshes, capacity expansion and selective competitive takeouts, driven by the customer's desire to deploy our network security platform across the category.

We're also seeing customers who as they move to the cloud are beginning to deploy more and more software firewalls to protect their cloud instances. With the recent upgrade of our products to be able to solve AI use cases, we continue to feel positively about strength in public cloud-deployed software firewalls. These represent 70% of our total virtual firewalls ARR and are driving our growth in this area.

SASE continues to drive transformation deals, as you saw in our customer stories. The true power of SASE and its extensibility now to our newer use cases helps validate the case from any of our new customers. Our SASE platform has recently integrated AI-based monitoring, incremental capabilities to manage AI applications, and even more recently, the Prisma Access Browser, which we will talk more about in a minute.

Whilst our SASE customers grew 20%, more interestingly, 40% of our SASE customers this quarter are net new to Palo Alto Networks. This is exciting, since it creates a future opportunity post-implementation to drive consistency by evolving these customers to the full network security platform. This was true for the financial services customer I mentioned. In addition to landing these SASE customers, we also have seen success driving large deals, with SASE transactions over \$1 million in contract value, up 40% in Q1.

Critical sustaining our NetSec performance are investments we're making in innovation. We released an enhanced security capability for operational technology environments to address the growing challenges our customers face as a number of non-IT connected devices accelerate. Challenges in OT environments include a need for more visibility, a lack of segmentation and unsanctioned remote access. We have brought precision AI to bear in this challenge, along with our new line of ruggedized firewalls.

We also saw strong interest from customers in our broad Secure AI by Design portfolio, with the AI Access leading the way. Our teams have been busy driving customer engagement. We have hundreds of customers leveraging AI Access. We currently secured over 750 AI applications, a volume which we believe leads the industry and are growing this figure by the day. We are also providing in-line data loss prevention for more than 65 applications, with this number growing as well.

Lastly, as part of our general availability release of our copilot capabilities across our three platforms, we rolled out the Strata Copilot. In our development process, we prioritize delivering superior accuracy and we've had fantastic feedback. The Strata Copilot trained on nearly 50,000 vetted sources, leverages best practices to help guide customers to faster decisions, and help accelerate remediation. We have made a version of this Copilot

available to our customer support teams, which is beginning to positively impact our time to resolving customer issues, which we believe will continue to improve significantly going forward.

I want to spend a few minutes on the Prisma Access Browser. We acquired Talon Cyber Security in December of last year. We knew this technology would become increasingly important to secure unmanaged devices such as those used by contractors. We saw an opportunity to acquire high-quality scarce asset and be first to natively integrate a secure browser into a SASE offering. Since then, we have been integrating the Talon browser with our leading security, DLP and access services, and leveraging our broader network security capabilities. This has resulted in a much more robust secure enterprise browser, our Prisma Access Browser.

What has been rewarding has been a surge in interest and emergence of various use cases. The browser is the ideal place to counter targeted attacks such as phishing, secure privileged users, and enable access to risky web applications. Customers are deploying Prisma Access Browser as an additional security control that is transparent to the end user. Customers running the [indiscernible] (14:06) SaaS applications and leveraging emerging AI applications are especially seeing the benefits of Prisma Access Browser as a critical end user security control.

Also, the replacement of Virtual Desktop Infrastructure, or VDI, is also starting to emerge as an opportunity. This is a legacy technology for which users are collectively unhappy. We are working to expand the pool of VDI users, which you can address by adding new protocols such as SSH and RDP and securely enabling mobile device users. Adding our ADEM capabilities browser can further enhance the end user experience with Prisma Access Browser compared to VDI.

We have seen significant commercial transaction for Prisma Access browser, with over 115 new customers and 1 million licenses sold since the time of the Talon acquisition. This traction with Palo Alto Networks SASE customers, including some of our largest customers, highlights our ability to successfully integrate the innovation and the innovative technologies that we acquire and rapidly take to market.

Prisma Access has about 16 million active licenses today. Our enterprise customers, the largest Prisma Access cohort, are now eligible to leverage this license to adopt Prisma Access Browser. We are seeing strong interest in this newly integrated capability.

Now moving on to Cortex. A strong momentum in this business continued with us crossing the \$1 billion ARR milestone in Q1, as I mentioned before. We have built the Cortex portfolio steadily over the last six years, starting with XDR. Our Cortex offerings have both been recognized as leaders in their markets, but also work together seamlessly as a platform that can deliver superior security operations outcomes for our customers.

In Q1, our leadership position continued to be reinforced by third-party recognitions, including from Gartner in Endpoint Protection, Forrester in Attack Surface Management, and KuppingerCole in Security Automation Orchestration Response, or SOAR.

XSIAM is a standout within Cortex, and we have made significant progress since its release with GA about two years ago. We continue to deliver both strong innovation and commercial momentum with XSIAM, released over 400 new machine learning detection modules leveraging precision AI to broaden the scope of our autonomous SOC capabilities. We now have over 150 active XSIAM customers, about 40 of which have more than \$1 million in ARR. We also rolled out a program for managed security service providers in Q1.

One of the key highlights this quarter has been our partnership with IBM, including the QRadar transaction that closed this quarter. This is an amazing burgeoning relationship. I'm excited about the early momentum we are

seeing from customers to migrate from QRadar to XSIAM. Following the close of the deal at the end of August, we have added over 550 QRadar SaaS customers to our Cortex customer base.

Since announcing the transaction, we have seen a number of customers sign QRadar to XSIAM transaction for a total TCV of so far over \$80 million, as we execute against our well-planned go-to-market programs. Over 500 active XSIAM customer opportunities and the pipeline across the full SaaS and on-prem QRadar base worth over \$1 billion in total value.

We're also seeing further opportunity across this customer set with our broader Cortex offerings. This opportunity we see is global with over half of the installed base outside the United States. We believe that this deal will help us to become one of the top three players in the SIEM space over the upcoming years.

Beyond our success in Cortex and with XSIAM specifically, I wanted to highlight another trend we see in the market. Many of the attacks we see on our customers are targeting their cloud environments. The pace of change in cloud is far faster than on-prem is challenging for security teams to keep up with, as new code is sometimes being pushed multiple times per day and new cloud services are constantly being adopted by developers.

This demand for real-time cloud security is driving us to bring together the capabilities of our leading CNAPP portfolio, Prisma Cloud and our Cortex security operations capabilities to stop cloud attacks. Against this backdrop, we have sold millions of cloud detection and response agents with these deployments up 10x in the two quarters since the April launch of our new offering. This has helped drive our combined Prisma Cloud and Cortex customer base, which is up 15% year-over-year. Interestingly, about a third of our Prisma Cloud customers already use at least one Cortex product.

Our combined portfolio can bring superior security, value and operational improvement to our customers. We recently released a new capability, integrating our XSOAR automation capability in Cortex with our Data Security Posture Management or DSPM in cloud to automate the remediation of data security risks identified. We also released our AI Copilot for Prisma Cloud and Cortex to general availability. While early in their adoption, we see significant promise here, driving towards security operations that are machine-led and human empowered.

In our Cortex Copilot beta, nearly half of users trusted to take security action on their behalf. With the recent flurry of conversations around Agentic AI, we have begun embedding Agentic capabilities across our copilots. We believe this Agentic vision of AI will be hugely impactful in security, and we're moving swiftly to adopt that into our products. We continue to drive innovation in our cloud security offerings. We released DSPM from our Dig acquisition. We integrated that into Prisma Cloud to counter the rise in cloud data attacks.

These critical DSPM capabilities enable customers to trace potential attack paths in their cloud environment to determine what sensitive data is at risk, appropriately prioritize their response and remediate automatically. Along with our overall launch of Secure AI by Design, our AI-Runtime and AI-SPM offerings targeted at cloud environments have also seen positive early traction. Lastly, we also launched another program for managed security providers as customers to enable partners to deliver security service in their customer cloud environment.

Before I wrap up and hand the call over to Dipak, I want to leave you with a few thoughts. One, we're seeing growing industry validation of our strategy with Q1 marking yet another steady quarter progress. Platformization is fueling the growth of our NGS ARR and puts us on track to hit our long-range targets as we drive sustainable, profitable growth. We're signing large transactions with leading global organizations because our approach delivers better security outcomes than the alternative.

Over the last six years, we have integrated our solution across three AI-powered platforms, and this approach is driving our business. We believe we have the best network cloud and security operation platforms, and we will continue to invest across these areas and keep them ourselves at the forefront of the nexus of cybersecurity and AI. Over time, we will steadily bring these platforms closer together to solve problems, leveraging our integrated capabilities and common data. We hear our customers asking for it and we are delivering on it today with real-time security across cloud and Cortex.

We also intend to lead these platform convergence opportunities that arise in the future. As you can see in Q1, our conviction in platformization and momentum gives us the confidence to make significant investments, notably in innovation. I believe we are the only dedicated cybersecurity company with resources and focus to drive consistent innovation and harness a substantial dedicated go-to-market capability to fuel our differentiated strategy.

We are releasing capabilities that our single form factor competitors network security are not able to offer such as our natively integrated browser in SASE. Our leading cloud and SecOps portfolio position us to lead in real-time cloud detection response. We're also seeing good early signs from our product and go-to-market investments around the opportunity to create our customer base to exceed our XSIAM momentum further.

As for securing AI itself, our Secure AI by Design portfolio is off to a great start, enabling organizations to confidently and securely leverage AI in the enterprise. If I look at the broader technology industry, we have seen evergreen companies that successfully execute on the platform approach in markets such as CRM, HR, ITSM. We think this will happen in cybersecurity, and we are poised to be that company.

Boiling this down to the impact on our fiscal year 2025 outlook, we are raising our full year 2025 NGS ARR, revenue and EPS in the back of a strong performance. Also reflecting our belief in the company's future and the momentum and confidence we have in our strategy, we announced a 2-for-1 stock split. This is also done to help ensure our shareholders accessible to all – our shares are accessible to all employees and investors.

I'll now turn the call over to Dipak to give you more details of our Q1 performance and our guidance.

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 highlights of Q1. You can review the results in our press release and the supplemental financial information on our website. Note that we have removed billings and added NGS ARR and RPO to our supplemental financials, reflecting our focus on the latter metrics.

In Q1, total revenue was \$2.14 billion and grew 14%, above the high end of our guidance. Within revenue, product revenue grew 4%, while total services revenue grew 16%. Drilling into services revenue, subscription revenue grew 21% and support revenue rose 8%.

As Nikesh mentioned, the demand for firewall appliances was stable in Q1, and we continue to expect growth of 0% to 5%, as we have previously discussed. Our support revenue is mainly tied to our appliance form factor.

Moving on to geographies, we saw double-digit revenue growth across all of our theaters with the Americas growing 12%, EMEA up 21%, and JPAC growing 13%. Total RPO grew 20% to \$12.6 billion. We added approximately \$68 million in RPO sequentially from the acquisition of QRadar SaaS business. Approximately \$30 million of this RPO was also included in our deferred revenue.

Our current RPO grew 18% to \$5.9 billion. The average duration of our new contracts remained at approximately three years, in line with the year ago quarter and slightly down from Q4.

Our NGS ARR grew 40%, finishing Q1 at \$4.52 billion. We added \$74 million in NGS ARR from QRadar SaaS. We expect this QRadar NGS ARR to decline to approximately half this amount by Q4 as we focus on upgrading these customers to XSIAM and growing our XSIAM ARR.

Also, it is worth noting that about a third of our new platformizations in Q1 came from QRadar. These customers have both – both have over \$100,000 in QRadar ARR and are active customers of Cortex XDR and/or Cortex XSOAR. That is a one-time increase as we completed the acquisition.

Moving down the income statement. Gross margin of 77.3% was down slightly as we saw the impact of some of our newer SaaS offerings that haven't yet scaled. We continue to see efficiencies across the company as we focused on driving profitable growth. This resulted in 60 basis points of operating margin expansion and along with some higher interest and other income, drove upside to our earnings per share.

Our diluted GAAP EPS continues to grow along with our overall profitability, and we generated strong free cash flow in Q1 based on collections of our substantial Q4 bookings.

On our balance sheet, you will see that our debt balance came down by over \$300 million. We have continued to see early conversion of our convertible debt, which occurred at the option of the debt holders and was settled by us in cash and equity. Our remaining debt matures in June 2025, although we may continue to see early conversions. We did not repurchase any shares in Q1, and our buyback strategy remains opportunistic. We continue – we have \$1 billion in authorization remaining through December 2025.

Before I turn to guidance, I wanted to touch on the early impact we saw as we shifted our focus squarely to RPO and NGS ARR as our top line metrics. We did this believing it would help further drive company-wide behavior to optimize our business for long-term value creation, and we are encouraged by the early results in Q1.

As we drove sales enablement and training to kick off the year, we focus the teams on maximizing exit ARR and deal profitability as compared to specific invoicing structures. I'm encouraged by some early signs we saw in Q1, where we reduced cycle times within certain steps of our deal close process. We also saw a handful of larger deals that work their way through the process, more smoothly than in the past. For example, a seven-figure SASE deal with one of the world's largest semiconductor companies accelerated through our process after we structured the deal around annual billings as compared to prior PANFS proposals, which would have needed longer scrutiny and approvals at our customer.

In another seven-figure transaction for XDR with a healthcare customer, we were able to structure a deal to accommodate the customer's payment terms requirements, while focusing on maximizing exit ARR. We look forward to building on this to drive further improvements in predictability in our business as we focus squarely on NGS ARR and profitability in our deals.

In Q1, we focused our PANFS financing capability on transaction where it was best suited, resulting in a meaningful reduction in the volume of these transactions. Instead of PANFS, we leveraged annual invoicing, which can be simpler for customers, especially when procuring SaaS offerings.

Last quarter, I mentioned to you that we would have expected our billings to grow 12% this fiscal year, if we did not change any of the practices in our business that impact billings. After reviewing Q1 results, this would continue to be true under the same assumptions. The quarterly analysis of billings is no longer meaningful as it does not reflect how we now run the business. Based on our Q1 performance, we also remain confident in our cash flow outlook for the year.

With that, let me turn to guidance. For the fiscal year 2025, we expect NGS ARR to be in the range of \$5.52 billion to \$5.57 billion, an increase of 31% to 32%. As a reminder, this guidance includes the contribution of QRadar SaaS of about half of the approximately \$74 million in ARR from QRadar in Q1, as well as incremental momentum in our NGS offerings, Nikesh and I discussed. Remaining performance obligation of \$15.2 billion to \$15.3 billion, an increase of 19% to 20%. Revenue to be in the range of \$9.12 billion to \$9.17 billion, an increase of 14%. Operating margins to be in the range of 27.5% to 28%. Diluted non-GAAP EPS to be in the range of \$6.26 to \$6.39, an increase of 10%, 13%. And adjusted free cash flow margin in the range of 37% to 38%.

For the second fiscal quarter, we expect NGS ARR to be in the range of \$4.70 billion to \$4.75 billion, an increase of 35% to 36%. Remaining performance obligation of \$12.9 million to \$13.0 billion, an increase of 20% to 21%. And revenue to be in the range of \$2.22 billion to \$2.25 billion, an increase of 12% to 14%. We expect diluted non-GAAP EPS to be in the range of \$1.54 per share to \$1.56 per share, an increase of 5% to 6%. We included our typical modeling points in the presentation for you to review.

Finally, as Nikesh noted, we announced today a 2-for-1 split of Palo Alto Networks common stock. This decision is supported by underlying confidence in our continued business momentum and by our desire to make our stock more accessible to our employees and the broader group of investors.

Shareholders of record at the close of trading on December 12, 2024, will receive one additional share after the close of trading on December 13, 2024, for every outstanding share held on December 12. Our stock will begin trading on a split-adjusted basis on December 16, 2024.

With that, we will roll one more video, and then we will start Q&A.

[Video Presentation] (00:30:49-00:31:55)

QUESTION AND ANSWER SECTION

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

To allow for broad participation in the Q&A, I ask that each analyst only ask one question. Our first question will come from Saket Kalia from Barclays, followed by Brad Zelnick from Deutsche Bank. Go ahead, Saket.

Saket Kalia

Analyst, Barclays Capital, Inc.

Q

Okay, great. Hey guys, thanks for taking my question and a nice start to the year. Maybe this is a question for both you, Nikesh and Dipak. The platformization strategy is clearly starting to hit its stride. And we've talked about the ARR implications of that longer term, specifically the long-term ARR target. But I'm curious if we can just talk about the margin implications from platformization long term, as those deals tend to be bigger and also tend to have higher lifetime value.

Nikesh Arora

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

A

Well, I'm going to ask Dipak to add. But, look, we look at margin. If you look at the biggest cost on any enterprise company's P&L, it's cost of sales, by far. The second largest cost is your COGS as it relates to cloud spend.

Now we are privileged to have some amazing deals with two large cloud service providers, which allow us to maintain margins that are consistent almost with on-prem solutions that other people do because of our scale. And we expect that to continue to improve over time. So that – at one end, that's a significant factor.

The second significant factor towards margin improvement is, as I mentioned, cost of sales. So the more we can platformize with existing customers and have large deal sizes with customers, it reduces our effort, because you don't have to get 20 deals to get \$200 million, like some of our peers, you get one deal for \$200 million, which means the cost of sales is lower on an incremental basis, as we established a land and expand strategy from a customer perspective.

And last but not the least, I sort of alluded to it, we're noticing some very interesting outcomes from a customer support perspective, which ends up being the third largest area of cost. We're seeing, in some cases, our Tier 1 support cases are getting solved by support Copilots, which our support team they are using. So we're significantly reducing the time to resolution of support tickets, at least on the sort of simpler end for now. But as I said, we've trained 50,000 data points into our network security copilot.

I think as we get better and better at training our models and training their customer support copilots, where we have fully revamped the way we collect data on customer issues, I think there's tremendous potential there to give us future margin expansion. So I think across the board, margin expansion on COGS, margin expansion from lower cost of sales, and margin expansion from customer support automation.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thanks, Saket, for the question. Next up is Brad Zelnick from Deutsche Bank, followed by Hamza Fodderwala from Morgan Stanley. Go ahead, Brad.

Brad Zelnick

Analyst, Deutsche Bank Securities, Inc.

Q

Great. Thanks so much and congrats on a strong start to the year. Nikesh, your NetSec competitors are talking about hardware refresh cycles. And I appreciate hardware is a much smaller part of your mix. So I won't bother asking why you're not expecting a refresh benefit like they are.

Nikesh Arora

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

A

But we look forward to their refresh cycle, so we get a chance to take out their customers' replacement to Palo Alto. So I'm delighted there's a refresh cycle in the market.

Brad Zelnick

Analyst, Deutsche Bank Securities, Inc.

Q

And that's exactly what I wanted to ask. Instead, how should we think about their refresh impacting your opportunity, both in the positive sense that you can go in and displace them as their boxes reach end of life, but also perhaps as a headwind, if they're using the event to bundle in SASE, SecOps, and other next-gen capabilities? Are you running campaigns actively to go after this? Thank you.

Nikesh Arora

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

A

So Brad, let me parse that out. Actually, I know I spoke faster and English is my second language. So, I did try to suddenly land in there that I am positive about hardware, where I said we're seeing steady growth in hardware, both from refreshes of boxes for our customers. We are seeing expanded demand for new use cases like ruggedized and IoT, et cetera. And last but not the least, we are seeing slow and steady take-outs of other customers.

So what's happening is our SASE cohort from two or three years ago, we landed with SASE. As that end of life happens in that customer base for firewalls, they turn to us and say, now I know the Palo Alto security interface, I don't have to learn it and they can just put firewalls, hardware firewalls against that SASE management pain, because we have the same security management pain across SASE.

So, it's not going to be revolutionary, but it is going to be evolutionary. If you look every year, our market share in hardware firewalls goes up 200 basis points to 300 basis points. So we think there are donors in the market of market share, who will constantly give – donate market share as they hit their refresh cycles. And there are acquirers of market share, and we're hopefully one of those. So, I actually have a steady expectation from product hardware, which I think is going to underpin our growth across the board over the next few years.

Brad Zelnick

Analyst, Deutsche Bank Securities, Inc.

Q

Great.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Thanks for the question, Brad. Next is Hamza Fodderwala from Morgan Stanley, followed by Brian Essex from JPMorgan. Hamza, go ahead.

Hamza Fodderwala

Analyst, Morgan Stanley & Co. LLC



All right. Great. Good afternoon. Thank you for taking my question and great to see the success with Prisma Access Browser year into that acquisition. Nikesh, I wanted to get your – just maybe early view into 2025. I mean, on the one hand, there's some optimism on the macro. You have a lot of new products. On the other hand, CIO, CISOs, they still want value for what they're spending. There's some talks about the incoming administration looking to perhaps roll back certain regulations, maybe cut entire civilian agencies. You're a big seller into the federal government. So, I'm just curious how you weigh those puts and takes as you look into 2025? Thank you.

Nikesh Arora

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



Thank you, Hamza, for a great question. Look, I think the most – if you separate signal and noise, the biggest signal is AI in the next 12 to 48 months. And AI is already having significant impact both on the attack side, attacks are getting faster and faster and quicker as AI is possibly being used to evaluate what are the more vulnerable parts of your infrastructure, so we can go now after that.

So I think from a cyber incident perspective, unfortunately, it's not going to slow down, right? And that's the biggest driver of improved security posture and improved higher spend from CIOs. I think you're right. There is a consolidation. Let me spend less money for security. And there, we are discovering – it's a more top-down motion than it is a bottom-up motion. And as you're aware, we are expending a lot of effort towards interacting with CIOs and C-level executives.

And actually, we're spending a lot more time with our GSI partners trying to address that issue, because they are typically involved in the transformation stage where say, let's take all of the stuff and put it together and replace it. So we're seeing early success.

As I said, we should have done that sooner, because when you sit across this, as I say, look, you have nine different products, you could bundle it together, take it down, have one management pane and you'll save a lot of cost because they understand, because we're not ingesting data nine times across nine products or in just to get once analyzing it 9 times, and giving them the outcomes they want. So I think the trend is in our favor.

As regards the incoming administration, I think, clearly, a higher standard deviation administration by the sounds of it, and higher standard deviation implies more risk and more risk implies possibly a more return.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.



All right. Thank you, Hamza. Next up is Brian Essex from JPMorgan, followed by Joe Gallo from Jefferies. Go ahead, Brian.

Brian Essex

Analyst, JPMorgan Securities LLC



Great. Thanks, Walter, and thanks for taking my question and great to see the strong profitability and cash flow, by the way. I want to ask about the integration between Cortex and Cloud. And I wanted to understand when did that kind of hit the market? Is it typically led by Cortex or cloud? And how should we think about how that positions you competitively, not just in the cloud security market, but across all of Strata, Prisma, Cortex segments of the business?

Nikesh Arora

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

A

So look, at a higher level, the Cloud market is effectively right now, three parts, right? There's the entire configuration management part, which is the CNAPP part and posture management part. There is the blocking real-time threats and protecting enterprises part, which is the CDR Cloud Detection and Response part. And then there's a cloud, the network traffic that needs to be inspected from a firewall perspective.

We're clearly leaders in the network traffic part. As we talked about, 70% of our use case is now public-facing cloud service provider traffic. We are still one of the leaders in the CNAPP space from our early start in Prisma Cloud. But what I think is going to happen in the next few years, this market is going to shift more and more towards the real-time security side on cloud, which is where CDR, Cloud SOCs, XSIAM become more and more important.

So, almost every one of our XSIAM deals there is a portion of that that is deployed towards cloud security now. And having that data together allows us to prioritize all the configuration issues and separate again signal from noise. So I'm going to let Lee describe a bit more about how we see that evolving. But I think that will change the cast of characters who are going to win in cloud security in the future.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

A

Yeah. Thanks, Nikesh. Thanks, Brian, for the question. Picking up where Nikesh left off the, if you think about sort of end-to-end cloud security, there's the – all of the work that goes into sort of the cloud posture side, generates a lot of data and understanding about what assets are deployed, what workloads are deployed, how they're configured, how they might be vulnerable or susceptible to attack. And by connecting that with CDR, it allows us to both leverage that for better protection of the cloud workloads in real-time. And vice versa, it allows us to leverage all the run-time, cloud run-time components back into posture from a remediation perspective.

And so, we initiated this earlier this year with the initial launch of CDR, which basically connects Prisma Cloud with Cortex. And then since then, we've been continuing to iterate on that and drive closer and closer integration between those two platforms.

Brian Essex

Analyst, JPMorgan Securities LLC

Q

Okay. Great. Thank you.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thanks, Brian. Next up, Joe Gallo from Jefferies, followed by Matt Hedberg from RBC, go ahead, Joe.

Joseph Gallo

Analyst, Jefferies LLC

Q

Hey guys. Thanks for the question. I think you could characterize cyber guidance broadly for calendar 4Q, is tepid at best. But yet your F 2Q guide calls for an acceleration in RPO and really strong ARR. So I mean, what are you seeing with budget flush or Fed or pipeline that's allowing you to kind of defy the gravity that others are feeling? Thanks.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

A

Well, I think we covered a lot of these, Joe, in our prepared remarks. I mean, we've got a product portfolio that we feel very proud of. We've just recently done an IBM acquisition, where we have a lot of additional pipeline that's coming through the pipe there.

And hopefully, we've proven over the last few years that we have a forecasting process that we feel comfortable, like manages the business. So I don't want to comment about others, but we really focus more on what we see. And maybe your comment is just proof positive that our platformization strategy is working and is somewhat unique.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thanks for the question, Joe. Matt Hedberg, go ahead, followed by Gregg Moskowitz after that.

Matthew Hedberg

Analyst, RBC Capital Markets LLC

Q

Thanks for taking my questions, guys. What stood out to me, the large deal success was striking. I know you spent a lot of time talking about platformization. It seems like Q1 brings a whole another level to it. Could you talk about specifically on the SIEM side of it?

The NGS, it really does seem like there's a next-gen SIEM replacement opportunity here. And we've talked a lot about some of the competitors with Splunk. Can you talk about just like what could – what are some of the catalysts that could unlock some of these large replacement deals? I know they take a long time, but curious if there's anything that you guys can do to accelerate that.

Nikesh Arora

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

A

Matt, look, we're very happy in two years since going GA on XSIAM. We're positively enthused about the progress we've made. We've crossed \$1 billion in ARR in Cortex. We're seeing larger and larger XSIAM deals. We have 150 customers. And as we mentioned, we have a robust pipeline north of \$1 billion. This is the fastest-growing product in the history of cybersecurity at scale.

Now the good news is, there are two or three very interesting characteristics of the SIEM market. If you look at the SIEM market, 90% of the SIEMs are of technology that is 10 to 15 years old. If you go back and look at the history of what SIEMs are, whether it's QRadar, LogRhythm, Exabeam, [ph] Jazz, (44:54) Sumo Logic, Splunk, these things are 10 – 7, 10, 15 years old.

I think there's a new breed of SIEM players that is fast coming in to replace these legacy SIEMs. I think we're going to go through a SIEM replacement cycle that we went through the endpoint replacement cycle from Symantec and McAfee to the XDR vendors. I think it is a moment of SIEM now for the next five years.

Now interestingly, every SIEM deal that we see, we are able to deliver a much better security posture and median time to remediate and detect, which is better than the current deployment and we're able to save cost. So from a compelling proposition perspective, this is a no-brainer.

You come and say, I know you're spending \$10 million a year running your SOC. I can do it for \$9 million. I can consolidate and I can improve your median time to remediate from four days in many cases from 19 minutes to four hours. So that's a compelling proposition.

We are seeing tremendous amount of interest in the market. We have created a compelling event in the case of QRadar customers, because they have to migrate to us or elsewhere, and we're seeing enough traction where people are considering Palo Alto instead. So I think in the next three to five years, you will notice that the entire \$20 billion TAM of SIEM is going to go through upheaval.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thanks for the question, Matt. Next up, Gregg Moskowitz from Mizuho followed by Rob Owens from Piper Sandler. Go ahead, Gregg.

Gregg Moskowitz

Analyst, Mizuho Securities USA LLC

Q

Great. Thanks for taking the question. Nikesh, now that we're a few quarters into the platformization go-to-market, I'd love to get a little more of a flavor of how it's going. Is there, and ask that for two of the strategy that's been most successful so far. For example, if you were to look at traction with legacy trade-ins versus introductory offers or more multi-product incentives. What would you say is resonating the most with customers?

Nikesh Arora

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

A

The thing that seems to resonate the most, Gregg, is elimination of execution risk. And what I mean by that is when I go to a customer saying, okay, let's go do this in a phased manner. We'll replace your SASE, or we'll deploy SASE for you. And then phase two we'll come in and replace your firewalls, they like that.

If I say don't worry, I'll start executing today and you can start paying me when you stop paying the other vendor, that's kind of the -- that's like the golden bear hug, because the biggest risk they have is wait, I have to go extend another deal by one year.

Guess what, that you're sending a signal to the other vendor. You're out in air, so the prices go up. And when I say, don't worry about it. Let's start executing now, when we're deployed, you can pay me when the current contract expires. So that elimination risk is resonating, the most.

Again, the customers fully understand that we're going to get our pound of flesh in the year two or year three of that deal. So they understand there is no free lunch, but eliminating that execution risk goes a long way.

I think the -- as I said to Hamza and I said in our prepared remarks, it really helps us step back and say, like, what are you trying to achieve? I mean, in many cases, we've been able to converge, XDR and SIEM RFPs for example, saying, listen, 50% of the data is going to go into XDR, which is going to be one vendor, that data is needed for AI-based or machine learning-based analysis across the entire stack. Why wouldn't you make sure that that data can be part of the SIEM and be used to improve your posture and get better, faster outcomes?

Gregg Moskowitz

Analyst, Mizuho Securities USA LLC

Q

Thank you.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thank you, Gregg. Next question, Rob Owens from Piper Sandler, followed by Gray Powell from BTIG.

Rob D. Owens

Analyst, Piper Sandler & Co.

Q

Yeah. Thanks. Walter. And Nikesh, as part of your prepared remarks, I love for you to build on the data security. And another one of the holy grails alongside next-generation SIEM, of course, is data that everybody is chasing. So what you're seeing from end customers, I know you made acquisitions of a DSPM capability in the space. But how you see Palo Alto's evolution longer term relative to the data opportunity? Thanks.

Nikesh Arora

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

A

Rob, this is my perfunctory question. I have to give to Lee otherwise [indiscernible] (48:50).

Rob D. Owens

Analyst, Piper Sandler & Co.

Q

Sounds good.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

A

Thanks, Rob. Look, if you take a step back, data securities is a longstanding sort of product category that's often been very painful. It's difficult to be accurate in data classification. It's difficult to figure out what policy is to enforce, and it's difficult to do that holistically everywhere the data might exist and need to be protected, right?

So there's two pieces to our data security strategy you've seen us evolve. First is around getting coverage of all the places where data might exist and improving the data classification capabilities within those. So, over the last six months, we've launched AI-based data classification, leveraging large language models, machine learning models to get more and more accurate in the data classification, being able to apply that to all different places where data can exist and move.

The second piece, and very importantly, is the tie-in with Prisma Access Browser. The way that users interact with data, access it, download it, share it, is one of the highest risk areas for data security. And historically, it's been very difficult to get all of the necessary context for enforcing an accurate policy.

Within the secure browser, we get all of the context needed. And what we're already seeing with the early adopters of Prisma Access Browser is the realization that this one component of what it does is effectively a next-gen data security component for how they secure data interaction with all of their employees. And this is part of the reason why the browser is expanding from being primarily focused on unmanaged device and third-party contractors to actually being something that applies to all devices and all users across the entire enterprise.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thanks, Rob, for the question there. Next up is Gray Powell from BTIG, followed by Andy Nowinski from Wells Fargo. Go ahead, Gray.

Gray Powell
Analyst, BTIG LLC

Q

All right. Great. Thanks for letting me ask a question in the call. Really appreciate it. So I have to admit, I'm a little confused on the NGS ARR statistics. If I look at the numbers and back out the QRadar deal, you added around \$230 million in net new ARR this quarter versus \$270 million a year ago. That metric has never been down on a year-over-year basis before. So, is there something I'm missing or something with the acquisition that maybe I'm not thinking about? Or just like what was the driver there? And then for the full year increase in NGS ARR, how much of that is organic versus full visibility on the QRadar asset?

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

A

So let me answer both, Gray, and let me just start off with the NGS ARR was above our guidance. So some of this, we already knew when we provided the guidance, but some of the products that move into NGS ARR have also been the advanced versions of our cloud subscriptions from a year ago, so things that were attached to our firewalls, where we made them cloud-enabled. Some of that happened last year, which is what led to a lot of the increase in the ARR. We're now lapping that. So that's really the bigger explanation of the base. We knew that. That's why we included that in our guidance to begin with.

When it comes to what's happening with QRadar, we talked about the one-time benefit. Our strategy is to convert all of the customers to XSIAM over time. We expect about half of that to occur within this year. So we would expect maybe half of that additional NGS ARR to be there by the end of the year.

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

A

Gray, I think to recast what Dipak said, you have seen the peak inorganic NGS ARR this quarter at \$74 million, or is that the number, from IBM. And half of that, we will migrate to us, and we expect half of that still stay on QRadar through the end of this fiscal year. So, there's no more net new inorganic NGS ARR expected this year.

Gray Powell
Analyst, BTIG LLC

Q

Understood. Okay. Thank you.

Walter H. Pritchard
Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

All right, Gray. Thanks, Gray. Next up, Andy Nowinski from Wells Fargo, followed by Fatima Boolani from Citi. Go ahead, Andy.

Andrew Nowinski
Analyst, Wells Fargo Securities LLC

Q

Great. Thank you. Good afternoon and great results this afternoon. I wanted to ask you about the Prisma SASE. You highlighted a number of large deals that either deployed SASE or they expanded with SASE. And I know it's bringing a lot of new customers, which is great. But I was wondering if you could provide an update on the growth of ARR from that solution, whether those new customers you're bringing into Palo Alto onto the platform are coming at the expense of other vendors. Or are those – were they just not using any SASE solution previously? Thank you.

Nikesh Arora

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

A

So, Andy, all of the above. There are some customers who are going through a network transformation, and they are now replacing their legacy VPN clients or other solutions they've had in the past. In some cases, there are competitor vendors who only had a Internet proxy-based deployment with the legacy VPN, or in some cases, Palo Alto VPN, which is converting to a full SASE solution from us. So we see all variants of that, as we said, 40% of them are net new logos to us, which means they were not deploying a Palo Alto VPN. They are deploying our SASE solution. So we're seeing all of that.

I just think the SASE market, as I said in the past, is a fast-growing market. We have clearly established ourselves as one of the top three players in the market. I think we're definitely growing faster than some of the others, or at least one more of the other top three players in the market. And we particularly like the SASE space, because we're always innovating, providing new stuff as we basically – as I said in my remarks, we've made it available to every existing SASE customers. They can deploy Prisma Access Browser for the unused licenses. So they can actually experience the browser. It's integrated. It's in the same management pane. It's the same UI.

Yeah. So I guess, I feel positive about it. We haven't quite reached \$1 billion yet as what we told you, but we're looking forward to it.

Andrew Nowinski

Analyst, Wells Fargo Securities LLC

Q

Thank you.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Great. Thanks, Andy. Fatima Boolani from Citi is up next. And our last question will be from Roger Boyd from UBS. Fatima, go ahead.

Fatima Boolani

Analyst, Citigroup Global Markets, Inc.

Q

Thank you. Good afternoon. I appreciate you taking my questions. I think the topic du jour is definitely QRadar and a lot of the momentum that you've been seeing that \$80 million, or more than \$80 million of bookings that you've already seen in the short amount of time.

What I wanted to actually shift gears on is on the on-premise side of the QRadar business. And Nikesh, some of your commentary, which I think is so apropos, there is just a stodgy stale technology in the SIEM market, right?

So, that \$500 million or so of revenue that is just still captive in the QRadar on-premise space, what is the thought process, the strategy to really forklift those customers to the goodies in XSIAM? And as you think about the arc of the next 12 to 24 months, how should we think about a multiplier effect on that business to really give Cortex booster shot to have it potentially be your biggest pillar?

Nikesh Arora

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

A

Yeah, Fatima, we had our Board meeting yesterday, and one of my Board members and I had this debate about which deal is going to look like the best deal Palo Alto ever did. And my bet is in the IBM deal, he bet on the Talon deal. Of course, I like both of them, they are equally successful.

But specifically, as it relates to QRadar, our teams are very focused. Since closed, we've called the top 500 customers and reached out to see if we can support the migration from QRadar to Palo Alto. This is irrespective of whether they are QRoC or on-prem. I mentioned \$1 billion pipeline. That \$1 billion pipeline is a hybrid pipeline of both QRoC and on-prem customers. The message is out there to on-prem customers that this technology will also over time be migrated.

And I have to say IBM is doing a phenomenal job working with us and being proactive with those customers where we go – I had a call yesterday with the CIO where IBM and us were together in the room where we're talking with the customers saying they will provide the migration services, they'll work on the migrating the rules from QRadar to Palo Alto XSIAM and we're going to do it together.

So look, it's – we haven't done a partnership like this ever in the history of our company. I haven't seen one in the cybersecurity industry yet. We have a lot of expectations, but it's a lot of execution, a lot of hard work. It's not going to happen, because I snap my fingers, but our teams are focused, we're dedicated. We're trying to do that. I think this will propel us into the top three SIEM players in the market in the next two years from nowhere. We did not play in this space two years ago.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Thank you, Fatima.

Fatima Boolani

Analyst, Citigroup Global Markets, Inc.

Q

Appreciate that.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

A

Last question, Roger Boyd to wrap it up. Go ahead, Roger.

Roger Boyd

Analyst, UBS Securities LLC

Q

Great. Thanks Walter. Dipak, you noted that contract duration on new business remained constant at roughly three years. Can you comment on what you're seeing with renewal and upsell business? And particularly when customers are renewing on platform deals and adopting XSIAM, which carries longer duration, I guess as we look to gauge the success of some of these platformization deals, shouldn't we expect to see contracts lengthen as customers place more strategic bets on your platform? Thanks.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

A

Yeah. So I think, Roger it's -- thanks a lot for the question. Look, at the end of the day, we're a large company with lots of different customers. We're definitely seeing the dynamic that you mentioned on some customers. We also see dynamics where other customers are saying, look, I know there's a lot more innovation to come. Let me go shorter duration on the renewals, because that could be ahead of the large platformization in the future. So we see a little bit of everything. I think on the renewals, just the data trended slightly up, but nothing significant.

Roger Boyd

Analyst, UBS Securities LLC



Got it. Super helpful. Thank you.

Walter H. Pritchard

Senior Vice President-Investor Relations & Corporate Development, Palo Alto Networks, Inc.

Great. Thank you, Roger. And that will end the Q&A. I'll turn the call back over to Nikesh for his closing remarks.

Nikesh Arora

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

Thank you, everyone, once again for joining us. As I said, I'm very excited of our great start to FY 2025. We look forward to seeing many of you at upcoming investor events. I also want to thank all of our employees who put a lot of hard work to help us deliver these amazing results. And also, of course, I want to thank all of our customers who trust in Palo Alto for delivering cybersecurity solutions to them. With that, have a wonderful day.

Disclaimer

The information herein is based on sources we believe to be reliable but is not guaranteed by us and does not purport to be a complete or error-free statement or summary of the available data. As such, we do not warrant, endorse or guarantee the completeness, accuracy, integrity, or timeliness of the information. You must evaluate, and bear all risks associated with, the use of any information provided hereunder, including any reliance on the accuracy, completeness, safety or usefulness of such information. This information is not intended to be used as the primary basis of investment decisions. It should not be construed as advice designed to meet the particular investment needs of any investor. This report is published solely for information purposes, and is not to be construed as financial or other advice or as an offer to sell or the solicitation of an offer to buy any security in any state where such an offer or solicitation would be illegal. Any information expressed herein on this date is subject to change without notice. Any opinions or assertions contained in this information do not represent the opinions or beliefs of FactSet CallStreet, LLC. FactSet CallStreet, LLC, or one or more of its employees, including the writer of this report, may have a position in any of the securities discussed herein.

THE INFORMATION PROVIDED TO YOU HEREUNDER IS PROVIDED "AS IS," AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, FactSet CallStreet, LLC AND ITS LICENSORS, BUSINESS ASSOCIATES AND SUPPLIERS DISCLAIM ALL WARRANTIES WITH RESPECT TO THE SAME, EXPRESS, IMPLIED AND STATUTORY, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, ACCURACY, COMPLETENESS, AND NON-INFRINGEMENT. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER FACTSET CALLSTREET, LLC NOR ITS OFFICERS, MEMBERS, DIRECTORS, PARTNERS, AFFILIATES, BUSINESS ASSOCIATES, LICENSORS OR SUPPLIERS WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR PUNITIVE DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES FOR LOST PROFITS OR REVENUES, GOODWILL, WORK STOPPAGE, SECURITY BREACHES, VIRUSES, COMPUTER FAILURE OR MALFUNCTION, USE, DATA OR OTHER INTANGIBLE LOSSES OR COMMERCIAL DAMAGES, EVEN IF ANY OF SUCH PARTIES IS ADVISED OF THE POSSIBILITY OF SUCH LOSSES, ARISING UNDER OR IN CONNECTION WITH THE INFORMATION PROVIDED HEREIN OR ANY OTHER SUBJECT MATTER HEREOF.

The contents and appearance of this report are Copyrighted FactSet CallStreet, LLC 2024 CallStreet and FactSet CallStreet, LLC are trademarks and service marks of FactSet CallStreet, LLC. All other trademarks mentioned are trademarks of their respective companies. All rights reserved.