13-Feb-2025

# Palo Alto Networks, Inc. (PANW)

## Q2 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.*

**Hamza Fodderwala**
*Analyst, Morgan Stanley & Co. LLC*

**Brian Essex**
*Analyst, JPMorgan Securities LLC*

**Gabriela Borges**
*Analyst, Goldman Sachs & Co. LLC*

**Jonathan Ho**
*Analyst, William Blair & Co. LLC*

**Peter Weed**
*Analyst, Bernstein Institutional Services LLC*

**Shaul Eyal**
*Analyst, TD Cowen*

**Tal Liani**
*Analyst, BofA Securities, Inc.*

**Andrew Nowinski**
*Analyst, Wells Fargo Securities LLC*

**Matthew Hedberg**
*Analyst, RBC Capital Markets 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' Second 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, Thursday, February 13, 2025 at 1:30 pm Pacific Time.

With me on today's call to discuss second 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 Q2 2025 supplemental information and the Q2 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 those 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 related 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 specifically noted otherwise, all results and comparisons are on a fiscal year-over-year basis. All per share figures have been adjusted for the 2-for-1 stock split that we announced November 20, 2024, and affected after the close of trading on December 12, 2024. We also note that management is scheduled to participate in the Morgan Stanley Technology, Media & Telecom Conference this quarter.

I will now turn the call over to Nikesh.

## Nikesh Arora

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

Thank you, Walter. Good afternoon, everyone. And thank you for joining us today for our earnings call. I'm excited about our Q2 results. Our teams did a phenomenal job of executing at scale. We've made considerable progress in platformization, allowing us to outperform both our top and bottom line expectations for this quarter. We delivered on our high RPO expectations towards the top of the range. This gave us strength in our NGS ARR and also allowed us to outperform our revenue expectations.

In Q2, growth was pretty broad across the entire portfolio, with strength across all three geographies and platforms. In particular, we saw strong performance from large deals internationally and also strong contribution from SASE, software firewalls and XSIAM.

On the profitability front, we delivered operating margins ahead of our internal target despite some onetime events. Our efficiency initiatives continue to bear fruit, including some promising early contributions from AI. These results allow us to raise our operating margin and EPS guidance for the year. We're also very happy with our free cash flow performance and continue to be confident in managing our free cash flow guidance for the next few years, as outlined. More from Dipak on this later.

From our vantage point, the outlook for cybersecurity seems to have been robust in Q2 and is likely to stay so over the rest of this year. Despite the settling in process of the new administration, we see signs that we are going to be able to see reasonable growth through the rest of the year. As the conversation around AI continues to get omnipresent and companies race to evaluate, experiment and deploy AI, they're discovering that some of the legacy architectures come in the way of their aspirations. Interestingly, this is resulting in a resurgence of cloud transformation projects, and consequently, demand for network security and network transformation.

While cybersecurity is a derivative effect, it is clear that the longer term trend towards AI is going to continue to underpin technology transformations and hence continue to drive demand for security. The transformations are all geared to embedding AI capabilities across infrastructure. Additionally, many of them involve changing strategies towards data and a growing understanding that data security will be more and more important in the future. We see that from the heightened interest in data security posture management, where our acquisition of Dig seems to be proving pre-signed.

To fully harness the power of AI, customers must unshackle their data from disparate legacy systems and providers and open up broader access and lean into the cloud. Cloud infrastructure is much more dynamic than on-prem IT, creating risk.

As cloud data volumes grow and customers utilize new services from the cloud service providers such as modern data repositories, they're doubling down and ensuring they're protecting their cloud environments from development to runtime, understanding who's accessing what data in the cloud and putting controls around these new services. In other words, the cloud is becoming an integral part of the enterprise, and the same level of security must be delivered.

A constantly changing attack backdrop is also compounding this inflection we have seen. There are tangible signs that bad actors use AI to accelerate attacks. Google recently found that adversaries can use generative AI to more rapidly create attacks, including custom payloads, iterate on malicious scripts, and use evasion techniques. Additionally, bad actors are using GenAI to do reconnaissance of target organizations, including their infrastructure and hosting providers, which are often exploited in attacks.

We have a new technological revolution that requires us to secure AI. As customers leverage the cloud, transform on-prem infrastructure, and respond to the escalating threat environment driven by AI, they're transforming how they manage security operations. Legacy offerings cannot unify SecOps across cloud and on-prem across multiple vendors and also take advantage of AI. AI is key for providing automation to help stitch together overwhelming volumes of data and generate the near real-time analysis and remediation needed to keep pace. As I said, security is a data problem and the data has to be all in one place for AI to have context and stop threats in their track.

Our industry has to change the paradigm by shifting from fragmentation to platformization to enable the best security outcomes. In a recent study we did with IBM, platformized organizations take 72 days less to detect and 84 days less to contain a security incident. Our teams are busy helping customers as they accelerate cloud

adoption and transformation across their environments. They need integrated security products and platforms for AI to be most effective in staying ahead of this active cybersecurity landscape.

A year in, we're pleased with our progress in driving our platformization strategy and the adoption and endorsement of platformization broadly across the industry. As I mentioned a few quarters ago, I wish we had made this move earlier. We're seeing some interesting behavior that reinforces our conviction that the future state of cybersecurity will have to be AI-enabled platforms that can markedly improve the speed of response.

We delivered approximately 75 new platformizations in Q2, up from approximately 45 in the year ago. We now have a total of over 1,150 platformizations within our top 5,000 customers. As you might expect, most of our platformizations start with network security and are from customers that are platformized in one area. However, our number of two-platform customers grew over 50% in Q2, and we're seeing our number of three-platform customers up 3 times year-over-year.

Also, the number of customers platformized in Cortex is up more than 3 times, reflecting our strong XSIAM momentum. We're excited to see the number of paths we have had success driving the strategy so far, and our Q2 performance keeps us on track to achieve our stated target of 2,500 to 3,500 platformizations by fiscal year 2030.

Investors have always asked me what platformization deals look like. So I wanted to provide a few examples based on deals we signed this quarter. A bank in Asia signed a transaction worth over $65 million in Q2, platformizing with us for the first time on Cortex was a significant XSIAM deployment. They have been leveraging XDR and other Cortex capabilities several years ago, who're also a network security customer and a QRadar customer. They had many point products in their SOC and were not getting the outcomes they needed, with limitations in the time to discover and remediate security incidents resulting in compliance issues.

In platformizing on Cortex, our NGS ARR with this customer increased by 5 times to over $12 million year-over-year. We look forward to driving a successful deployment here, which can be an avenue to platformizing a network or cloud security in the future for this customer.

A US municipality signed a transaction of over $60 million with us, which included a renewal of its network security estate and the expansion across our portfolio. The customer leverages all three of our four form factor – of our form factors within network security and is already platformized there. The deal also included Cortex and Prisma Cloud, which positions us well for future platformization in these areas. Our NGS ARR here increased over 40% in the last 12 months to over $11 million.

A European automotive manufacturer signed a $25 million transaction in Q2. They're already platformized with us in network security and cloud security. They added several capabilities as they renewed their firewalls and support footprints, including IoT, virtual firewalls and SASE. This is a complex customer, and we also secured business with them in Cortex with XDR, XSOAR and Xpanse as well as Prisma Cloud. In doing so, we are now well positioned in the future to consolidate the SOC opportunity with XSIAM. For this customer, the NGS ARR grew 50% to $9 million.

More broadly than these anecdotes, the growth in our large deals tells the story. We had 74 accounts that had transactions over $5 million in Q2, up 25% year-over-year, and 32 accounts that had transactions over $10 million, up over 50%.

Now moving on to an update about our first security platform network security, NetSec. Our Q2 NetSec momentum was driven by strong software demand. We continue to lead the market in network security, which is approximately 80% of our bookings. Our Zero Trust platform combines three best-to-beat form factors built on a consistent architecture. This is fast becoming a requirement as applications proliferate across data centers, hyperscalers, SaaS and leveraged AI.

Meanwhile, users are increasingly distributed across headquarters, remote locations at home and other places. And also, there are now soon to be nonhuman users in the form of AI agents, where interactions with applications must be secured. Disjointed network security offerings require significant resource to be applied to integration, creating the possibility of gaps in security policies given the disparity of control panes, and more importantly, unless we can harmonize the data across the network, it will be challenging for customers to adopt AI-enabled security capabilities in the future. We have to believe that in the future, all solutions will need to integrate, harmonize data and use that to train AI agents to solve security.

Looking deeper into firewall as a platform, our bookings accelerated and grew by 21%. Within this, we continue to see stable demand in the appliance market. That stability, coupled with us continuing to take market share, allowed us to grow our appliance bookings in the mid-single digits. There's a refresh cycle coming from many players in the industry, and we believe we are well positioned to benefit from it.

Software and SASE make up approximately two-thirds of our Firewall as a Platform bookings, and grew over 1.5 times faster than the rate of the total Firewall as a Platform business. We have been on a multiyear journey to reinvent our security subscriptions, which we use consistently across all three form factors. Each of these advanced subscriptions are cloud delivered and we believe significantly differentiates with what's in the market.

Delivering these incremental innovations into our platform like advanced subscription and network security makes our customers adoption seamless. This is core to our strategy of staying ahead of our customers' security needs with future-proof innovation. It's also a win-win for Palo Alto and the customer.

Next, let's dive deeper into SASE and our software firewall business. As customers transform their networks to keep pace with delivering first-class security capabilities for remote users and branch offices, we continue to see demand for SASE. Many SASE projects are large and comprehensive, which is well suited to our rich offering.

SASE continues to be our fastest-growing form factor in network security and a strong contributor to our growth. We grew SASE customers by over 20%, while we grew bookings well north of 50% and increased deals over $1 million in value by 2.5 times. We now have over 5,600 SASE customers and over 23 million individual seats. Across our SASE base as well as our GP customers, we have been chosen to help protect a base of over 100 million users.

Meanwhile, the drivers of our SASE momentum are broadening. Bookings of newer modules of the SASE platform, such as Autonomous Digital Experience Management, or ADEM; Cloud Access Security Broker, or CASB; Prisma Access Browser, which you just saw an ad for; and AI Access grew nearly fourfold this year. Customers who're happy with their initial SASE deployments are adding these to derive a more modern security environment and streamline their vendor landscape.

I'm particularly excited about the momentum we're seeing with Prisma Access Browser. Roughly one-third of the new Prisma Access seats we sold in the quarter were for our secure browser. We signed a transaction in Q2 for over north of $10 million with one customer, with a total of over $30 million in Prisma Access Browser bookings in Q2, and growing seats by 95% quarter-over-quarter.

We also continue to innovate in SASE, releasing the mobile version of our integrated secure browser. This browser, integrated with Prisma Access, offers mobile phone and tablet users same robust security and access to private applications.

We added capabilities to AI Access, ensuring organizations can apply controls to how their users interact with AI-based applications. We can now provide real-time visibility into over 1,800 applications, up from 500 six months ago. AI Access comes with out-of-the-box policies to manage functions such as uploads, downloads, and sharing capabilities.

In a short period of time, this quarter, we crossed 300 customers who use the AI Access capability. We can also provide comprehensive data protection to secure sensitive data, secrets and intellectual property.

Now turning to software firewalls. This has been a strong area of growth. We saw 50% bookings growth in our software firewall business with AI and public cloud adoption continuing to be the strongest driver. Approximately, 70% of our VM deployments are now in the public cloud.

We continue to see customers adopt our software firewalls alongside our hardware appliances. As a testament to this, about two-thirds of our software firewall customers are also hardware firewall customers, showing the hybrid nature of the solution and the need for platformization.

We also continue to innovate in this business. Early in Q2, we released our API-based AI runtime security capability, which added the ability of our product to directly secure AI applications without being in the traffic path. Later in Q2, we leveraged this capability to secure AI agents as many of our customers look forward towards the value propositions of agents, but need to secure them as they would need to secure any other user or application. This capability helped drive our first seven-figure software firewall transaction for AI in the quarter, and we have a healthy eight-figure pipeline for AI firewalls for the future.

Now moving on to Cortex. This morning, we had an exciting announcement. We took our industry-leading Prisma Cloud platform, evolved it with more capability, merged it with our CDR capability and our Cortex platform to announce the introduction of Cortex Cloud. Cortex Cloud is now the industry's first end-to-end cloud security platform, which deeply integrates into the SOC.

As we have been delivering cloud security, over time, we have learned that the customers are keen to ensure that they can trace the cloud security capability all the way into runtime and production and do real-time security against this. We're also delivering a powerful data security DSPM experience and real-time security capability with our cloud agent. Again, all of this is now natively connected to the Cortex platform. This is where cloud security is going.

We have anticipated the market change in cloud security, and it is one reason for our momentum and leadership in this space. Recall that in our early days, we entered the cloud security market in 2018 with two acquisitions and continue to build up these capabilities, pioneering the category and leading with our initial cloud posture capabilities. Soon after, it became apparent that too many security issues were reaching production and organizations could not keep up with remediating them once applications were deployed. We led the trend to shift left, connecting this to the cloud posture to address security issues before deployment.

Attackers took note as customer deployment of mission-critical applications and sensitive data accelerated into the cloud. Our own Unit 42 research shows that 80% of security exposures are found in cloud attack services, with a 66% increase in threats targeting cloud environments.

With these evolutions in the attack backdrop, we believe cloud security and security operations must be inextricably linked. Existing Prisma Cloud customers will have a seamless upgrade to Cortex Cloud to benefit from AI-powered prioritization, automated remediation and new simplified powerful user experience. Additionally, they can also adopt Cortex's best-in-class CDR capability to gain real-time cloud security capability.

The unification of enterprise to cloud can further drive the adoption of XSIAM into the customers' cloud environment. Cortex Cloud natively integrates with cloud data, context and workflows within Cortex XSIAM to significantly reduce the mean time to respond to modern threats as a single, unified SecOps solution.

More importantly, because we are natively integrating cloud solutions with SOC, XSIAM has now transformed into both a cloud and enterprise set. We're excited about the prospects for us to maintain and accelerate our strong XSIAM momentum.

As I mentioned, we are making this announcement on the back of strong momentum in our cloud security and security ops business. I want to give you some highlights. We drove bookings growth of approximately 50% in both Cortex and Prisma Cloud in Q2.

In Cortex, we had healthy momentum with customer growth of approximately 20%. Fueling this customer growth, we again signed hundreds of new XDR customers in Q2, which become opportunities for SOC transformation on the broader Cortex platform in the future.

Our XDR momentum continues to be fueled by the efficacy of our product. This quarter, we achieved further external recognition of this, achieving the leadership results in the most recent MITRE ATT&CK evaluations.

XSIAM, our AI-driven SecOps platform, surpassed the $1 billion cumulative bookings milestone in Q2. While we know we have a winning product with XSIAM, we're also starting to see external validation of our leadership with Frost & Sullivan and Omdia recognizing us as leaders in the SIEM category.

Contributing to our Cortex strength in Q2 was over $100 million in QRadar-related bookings. Our pipeline on QRadar is equally strong, leaving us optimistic about our IBM partnership as a driver of Cortex.

On the cloud side, we saw the adoption of our capabilities continue to broaden. With DSPM integrated into Prisma Cloud, we've seen early adoption to be one of the strongest one of any of our new cloud security capabilities in the past. We're excited to see this success continue with DSPM as part of the Cortex Cloud product we announced this morning.

We're also seeing particular success among some of the largest companies in strategic industries. For example, several SaaS companies signed significant cloud security deals with us in Q2. In this industry, SIEM is the top 10 SaaS companies outside of cybersecurity leverage our cloud security capabilities to secure the customers' environment.

As you can see, we saw strong momentum across the business in Q2. We're seeing customer imperatives around AI driving accelerated cloud adoption and infrastructure investment, which is supporting strong cybersecurity

demand. This healthy spending backdrop and strong execution from our team on platformization helped drive the healthy top line trends we saw in Q2 across RPO, NGS ARR and revenue.

We remain optimistic about sustaining this momentum as our sales teams leverage our ecosystem, continue to become more adept at aligning our many capabilities into a unique platformization journey for each customer. We remain confident in our long-term NGS ARR forecast.

Supporting this is a steady innovation stream and momentum across our portfolio. We're a leading early mover into new market categories like enterprise browser, secure AI-by-design, the AI-powered SOC, which are making it easy for our customers to adopt key new innovations with our platform approach.

Lastly, we're driving profitable growth, balancing operating margin improvements with strong cash flow. We continue to make progress in driving a culture of efficiency at Palo Alto Networks, and you've seen the results of this over the last few years. This focus on efficiency and some early success in AI-based initiates gives us the confidence to continue delivering profitable growth.

I will now pass on to Dipak for his remarks.

## 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 Q2. You can review the results in our press release and the supplemental financial information on our website.

In Q2, total revenue was $2.26 billion and grew 14%, above the high end of our guidance. Within revenue, product revenue grew 8%, while total services revenue grew 16%. Drilling into total services revenue, subscription revenue grew 20% and support revenue rose 8%. Our product revenue is approaching 40% software on a trailing 12-month basis. We expect healthy software contribution to product revenue in the second half of this year, which we expect will increase our product revenue into the double-digit growth range.

We also saw stable demand for firewall appliances in Q2, which we expect to continue through fiscal 2025, as the appliance market grows 0% to 5%, as we have previously discussed.

Moving on to geographies. We saw double-digit revenue growth across all theaters, with the Americas growing 13%, EMEA up 18% and JPAC growing 17%. We were particularly encouraged by the volume of large deals we closed with some notable large deals in EMEA and JPAC.

For example, we have our largest deals ever in both EMEA and JPAC this quarter, each in excess of $50 million. As Nikesh noted, these deals demonstrate the broadening of our large deal success in North America to our international theaters.

Also, I know many investors have had questions about the US federal market. We have had prudent expectations in this market this year, and we saw stable federal business in Q2. Much of our federal business is tied to renewals and existing programs with long-standing funding.

During the quarter, we also received FedRAMP High Authorization across our network, cloud and security operations platforms. We now have the most comprehensive suite of AI-powered cybersecurity solutions authorized for use in federal networks at the high-impact level.

Total RPO grew 21% to $13 billion at the high end of our guided range. Our current RPO grew 17% to $6.1 billion. The average duration of new contracts remained at approximately three years. It did trend towards the high end of our historical range in Q2 based on our performance in large platformization deals, particularly customers making longer-term commitments to XSIAM.

Our NGS ARR again delivered strong growth growing 37%, finishing Q2 at $4.78 billion. Our NGS ARR was driven by the strength across our advanced subscriptions, SASE and Cortex.

Moving down the income statement, gross margin of 76.6% was down slightly as we continued to see the impact of some of our newer SaaS offerings that are growing quickly but have yet to achieve scale. Also, we had some costs in Q2 related to inventory and product transitions that were higher than typical, and we don't expect that that will recur in the second half of the year.

It is worth noting we have been transitioning our contract manufacturing facility in Texas as our primary manufacturing and fulfillment center, not only to enable scale and innovation in our appliances, but also to take advantage of our foreign trade zone that can help mitigate tariffs and products we ship to international destinations as we assemble and manufacture all of our firewall appliance products in the US.

More broadly, we continue to see efficiencies across the company as we focus on driving profitable growth. We saw operating expenses as a percentage of revenue decrease by 120 basis points as we benefited from scale in our business model and initiatives as part of continuing to build our culture of efficiency.

We delivered $0.81 of diluted non-GAAP EPS, and our diluted GAAP EPS of $0.38 continues to grow along with our overall profitability. As a reminder, in the year-ago period, we had a significantly positive impact to GAAP EPS from the large $1.5 billion release of tax valuation allowance that happened only in fiscal 2024. We generated adjusted free cash flow of over $509 million in Q2.

On our balance sheet, you will see that our debt balance came down by over $100 million as we continue to see early conversions of our convertible debt, which occurred at the discretion of the debt holders and was settled by us in cash and equity. Our remaining debt of just over $500 million matures in June 2025, although we may continue to see some early conversions. We did not repurchase any shares in Q2, and our buyback strategy remains opportunistic. We have $1 billion in authorization remaining through December 2025.

As Nikesh mentioned, we are pleased with the momentum we are seeing in our platformization strategy and the outcome in driving our financial results. I wanted to update you on what we are seeing a year into this strategy.

As you all no doubt remember, we announced our platformization strategy a year ago. Over the last 12 months, we've learned from our success and adapted where it made sense. We launched a number of structured sales programs that we highlighted to jump start this initiative. Our goal was to remove friction, both related to technology risk and budget challenges for the customer. We have now embedded these practices into how we do business.

At year-end, we have seen both the industry rally around this approach as well as some of our key ecosystem partners also put significant resources behind platformization. This has helped leverage our own investments on the sales and marketing side and brings us closer to enterprise accounts where ecosystem partners have strong relationships.

Many of our large platformization deals have been pursued and closed with global system integrators. With these joint successes, partners collectively are putting more resources behind platformization.

When we initially announced platformization, we had piloted the program, helping us build conviction in our aggressive launch. Predating our broad announcement, some of our top reps were driving deals with the principles that embody platformization. A year in, we have seen rep participation significantly increase with approximately one-third of our sales reps having already participated in a new platformization deal win in the last 12 months since we launched our accelerated strategy.

Lastly, when we launched the program, we had assumed the platformization would enable us to increase our ARR per customer. As you can see in some of the large deal highlights that Nikesh covered, we have seen success signing larger deals and further expanding our ARR in platformized customers.

As you can tell from both the tone and some of the details that we provided, we are very happy with our progress here. I'll reiterate what Nikesh noted last quarter and earlier, our biggest learning is that we should have made this move earlier.

Now turning to the bottom line. Our confidence in future operating margin expansion is rooted in our visibility to continued leverage across our P&L. As Nikesh mentioned, we've seen some encouraging results from our AI-based initiatives across multiple areas of the company that give me greater confidence in this ability to drive leverage.

I wanted to provide you with an update of some of these AI-based initiatives and what we're seeing so far. In the areas that we are focused on, we've seen meaningful efficiencies which either manifest as lower spending, enabling us to drive incremental innovation or absorb expected increases in volume without additional spending.

One of our first AI-based initiatives was focused on our employee-facing processes. In the past, we have leveraged contractors in various business processes in IT. We are on track to reduce this contract labor by about 50% as we close out fiscal 2025, which will result directly in operating expense savings.

In our global customer support business, we've leveraged an internally developed copilot to assist in case resolution. So far, we have seen our support copilot used in about 85% of cases in network security which is where we first rolled out this technology.

We're seeing approximately 50% reduction in the time to resolve cases. This results in a better experience for our customers, and also our team is being able to absorb more case volume while adding less head count than in the past.

Lastly, we are deploying copilot tools for our developers earlier and are seeing some exciting results. We've recently deployed the technology to all of our engineers. These and other initiatives that are still in their early stages, give us consistent outcomes, and that gives me more comfort and confidence on the tangible benefits to our business, including our cost structure.

Before I turn to guidance, we have a lot of questions about how we get comfortable with the sustainability of our cash generation given some of the transitions happening in our business. We began to see an increase in deals with deferred payments in fiscal year 2022 and have seen a significant increase driven by larger transactions, particularly in our SaaS offerings over the last 3.5 years.

As we have absorbed an increase in deferred payments, our visibility into our free cash flow each year has increased. In fiscal year 2024, when we entered the year with $1 billion in deferred payments scheduled for the year, that was 32% of our fiscal year 2024 adjusted free cash flow. This year, that amount increased to $1.4 billion and our visibility increased to 41% of our expected adjusted free cash flow. Looking forward, we expect to enter fiscal 2026 with $2 billion in deferred payments scheduled for the year, further increasing our visibility into free cash flow in fiscal year 2026.

We've progressed substantially over the last several years through the transition of deferred payments. We've also spent significant time over the course of this year, ensuring that we're balancing this transition with other uses of cash and opportunities for cash flow optimization.

Because our appliance bookings and smaller bookings predominantly are paid upfront, and many of our large transactions already utilized deferred payments, we believe we can manage the trend towards more of our larger transaction bookings utilizing deferred payments as we have done over the last several years. Consequently, our expected increasing profitability as we scale and these financial dynamics give us improved confidence in our free cash flow generation.

Our confidence holds for fiscal year 2025, where we continue to expect 37% to 38% adjusted free cash flow margin as well as our cash generation beyond this year. We are comfortable that we can generate adjusted free flow margins for fiscal year 2026 and fiscal year 2027 of greater than 37%. As a reminder, we do not guide free cash flow on a quarterly basis and we do see year-to-year fluctuations in our cash flow seasonality.

In fiscal year 2025, relative to prior years, we expect to see fluctuations in seasonality driven by the timing of deferred payments from customers, the timing of bookings within the year and the timing of cash tax payments. But this year, we expect, relative to the Street, that more of our free cash flow will come in Q4.

With that, let me turn to guidance. For 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%; remaining performance obligation of $15.2 billion to $15.3 billion, an increase of 19% to 20%; revenue to be in the range of $9.14 billion to $9.19 billion, an increase of 14%; operating margins to be in the range of 28% to 28.5%; diluted non-GAAP EPS to be in the range of $3.18 to $3.24, an increase of 12% to 14%; and adjusted free cash flow margin in the range of 37% to 38%.

For the third fiscal of 2025, we expect NGS ARR to be in the range of $5.03 billion to $5.08 billion, an increase of 33% to 34%; remaining performance obligation of $13.5 billion to $13.6 billion, an increase of 19% to 20%; revenue to be in the range of $2.26 billion to $2.29 billion, an increase of 14% to 15%; and diluted non-GAAP EPS to be in the range of $0.76 to $0.77, an increase of 15% to 17%. We've included our typical modeling points in the presentation for you to review.

Before I turn back to Walter for Q&A, we will roll one more video.

[Video Presentation] (00:35:11-00:36:21)

# QUESTION AND ANSWER SECTION

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

A

Thank you. We ask in the Q&A that each analyst only ask one question. Our first question will come from Saket Kalia from Barclays, followed by Hamza Fodderwala from Morgan Stanley. Saket, go ahead.

**Saket Kalia**
*Analyst, Barclays Capital, Inc.*

Q

Okay. Great. Hey, guys. Thanks for taking my question here, and nice quarter. Maybe a question for Nikesh and Dipak together. It's great to see free cash flow margins at 37% plus expected now through fiscal 2027. Nikesh, can you just maybe talk about some of the success you're seeing in driving better profitability? And Dipak, can you just maybe go one level deeper into other drivers of that free cash flow like the deferred payments?

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

A

Yeah. No, Saket, first of all, thank you for the question. As Dipak highlighted, like we're beginning to hit scale. As you see, platform deals are actually a lot more efficient from a sales perspective because the larger deals, I think if you see if you look at the cybersecurity landscape, we're now clearly a large deal company compared to most of our competitors. So that definitely drives efficiencies for us from a scale perspective.

If you look at any P&L in any enterprise business, 50% to 60% of P&L is sales, marketing and customer support. If you can find efficiencies in that process, that's where leverage lies. So you've seen we've been improving our operating margins consistently now for over 2.5 years. That's being driven from that efficiency lens.

If you couple that with some of the early experiments we've shared on the AI front, we think this has tremendous potential in the future where enterprise companies should operate at a much higher operating margin in the future from now.

I'm not going to put a forecast just yet, but I think the trend is our friend. And that gives us tremendous comfort that we can underpin our performance with strong operating margins over the course of the next few years.

Couple that with the way Dipak and his team have been able to balance the deferred payment products, which he can talk about, which, as he said, gives us tremendous amounts of visibility. And we feel confident that the range for the next few years is there and possibly higher after.

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

A

If I can just build, Saket, a lot of this is in the prepared remarks, but we've had a lot more visibility with a growing balance of deferred payments already in the past few years. There's parts of our business that are really never going to go to deferred payments. The smaller transactions that have a multi-tier distribution network where everybody wants to get paid upfront. The appliance business, whether it's industry standard to pay upfront.

Then you're left over with everything else, and we've already made a significant transition already. So there's not as much left to actually do. We're quite far along the journey. That's what gives us confidence, and that's what I was meaning to convey in the prepared remarks.

**Saket Kalia**
*Analyst, Barclays Capital, Inc.*

Q

Very helpful. Thank you.

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

A

Thank you, Saket. Next question from Hamza Fodderwala from Morgan Stanley, followed by Brian Essex from JPMorgan.

**Hamza Fodderwala**
*Analyst, Morgan Stanley & Co. LLC*

Q

All right. Great. Thank you for taking my question, and good evening. Nikesh, I had a bit of a bigger picture question for you. Palo Alto...

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

A

Hey. [ph] You don't want to go through the quarter (00:39:29)?

**Hamza Fodderwala**
*Analyst, Morgan Stanley & Co. LLC*

Q

...I'll leave that to the others. No, obviously, Palo Alto Networks has been at the forefront of AI, whether it's AI for security operations when it comes to Cortex or securing AI now with Dig and Prisma Cloud.

DeepSeek was a big moment for the AI trend in the market earlier this year. I'm curious, what do you think this means for the proliferation of AI in general? And how this impacts security and specifically Palo Alto Networks?

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

A

That's a very good question coming from you, Hamza. Not that I wouldn't expect that from you, but it's a great question. Look, I think DeepSeek is a phenomenal pivotal moment for AI. Not just for us but across the industry. And if you look at it across three parameters, right, there's the question around quality. Is it as good as the models that people are using out there like OpenAI, Gemini or Llama, et cetera?

At least if you read the ratings out there, it seems like it's equally good, if not better, for technical answers. It does better coding, better math, better physics. So it looks like for sort of – it has a better reasoning engine out there. So that's interesting.

Then the next question becomes, great, if it's so good, if it's equally good, what are the economics? Did they actually get it done for a lot cheaper? Now, we can debate that, and I don't know if you'll ever get to the bottom of it. But what's interesting is, today, you pay $0.14 for about 1 million words and you pay $7.50 for every other model. So it's 2% of the cost of every other model.

Now, that's driving experimentation. I have talked to many SaaS CEOs recently, and everybody is experimenting, so are we to see if DeepSeek can deliver that degree of performance.

And the third question comes, okay, wait. This has come from a nation state, maybe from somewhere where we don't want to trust the model, we've got to figure out how secure it is. So look, any AI model that is going to be used by enterprises will be used in a sequestered fashion, either on-prem or in your own cloud instance, or require AI firewalls around it.

If you can guarantee that your data doesn't get out of that sequestered sort of space, and if you can guarantee that you can put guardrails around the model, I think you'll see a lot more experimentation. So from that perspective, I think it's going to be pivotal. My only recommendation to every enterprise out there is make sure you don't deploy AI without running firewalls around it, make sure you don't deploy it in a multi-tenant environment.

But I think this is great for AI. And look, any technology is great for security because any new technology requires you to put more security around it.

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

Great. Thank you, Hamza. Next question is coming from Brian Essex at JPMorgan, followed by Gabriela Borges at Goldman Sachs. Brian, go ahead.

**Brian Essex**
*Analyst, JPMorgan Securities LLC*
Q

Yeah. Good afternoon, and thank you for taking the question. I have a bit of a different AI question. And it comes from the perspective of leveraging AI across the platform to provide better security outcomes. And maybe if you could talk about what you're seeing in cloud security as an example, and win rates as you're able to provide code-to-cloud-to-SOC security across your entire platform.

How does that affect your ability to compete against point solution providers in that space? And how is that enabling you to kind of leverage the platform maybe as an example in that cloud security space? Thanks.

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

Hey, Brian. Is any point solution business left? Every security company seems to claim they're a platform now. So I don't think this – I think that breed of point solution is gone. But anyway...

**Brian Essex**
*Analyst, JPMorgan Securities LLC*
Q

There's a difference between calling yourself platform and actually being platform. So...

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

Yeah. That's what they say about us, too, right, those guys. But that notwithstanding, look, I was – I called Lee last night, and I said, you know what, I found a new raison d'être for platformization. Our earlier sort of narrative was that you need a platform so you get a single pane of glass. You can run Zero Trust networks. You can be harmonized across policies. There are no security gaps. But as we go down this journey, we're discovering and

we've been talking about deploying agents and why do we need human beings trying to do these complex tasks and trying to understand how security should be deployed?

Why can't we have agenetic personas that say, I'm your network configurator. I'm your phishing remediators. Why can't we design security agents? When very quickly realized you can't design an agent unless you have the data. We can't have the data across 17 disparate products and make sense of it. So what we're discovering is this strategy that we deployed of platformization about two years ago and really sort of put our weight behind a year ago, is resulting in us getting harmonious data, right?

These 1,150 customers who are platformized have data that is harmonized. We can run and build agents on top of that. So from that perspective, the more platforms we sell, it creates tremendous opportunities for us. But I'm going to talk to – let Lee talk about how this is helping us on the cloud security front.

**Lee Klarich**
*Chief Product Officer, Palo Alto Networks, Inc.*
A

Yeah. So you've seen what we've done in number of places, right, Brian. So the – in XSIAM, using AI for the SOC and reducing meantime remediation from days down to hours to minutes. You've seen us do this with – in NetSec and across network security and SASE and other places in cloud. What you can see is a couple of things.

First is in the individual area, so in AppSec how we use AI in order to have better detection and prevention of misconfigurations before they reach production. In production, how we use AI in order to better remediate – detect and remediate, prioritize, et cetera. And then with Cortex Cloud, which we announced earlier this morning, what that allows us to do is now not only apply AI automation within each of these areas, but now connect that across the full end-to-end from AppSec into cloud, into runtime, into SOC. And that is incredibly powerful when you think about trying to become much more proactive in real time in cloud security.

**Brian Essex**
*Analyst, JPMorgan Securities LLC*
Q

Is that translating into better win rates though? Like if you look against a point solution vendor like a Wiz in the cloud security space, are you starting to see the improvement in win rates?

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

Yes.

**Lee Klarich**
*Chief Product Officer, Palo Alto Networks, Inc.*
A

Sorry...

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

No. Please go ahead.

**Brian Essex**
*Analyst, JPMorgan Securities LLC*
Q

Nikesh jumped on that one.

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

A

I'm going to let him answer the question, but I'm going to say something else. Go ahead.

**Lee Klarich**
*Chief Product Officer, Palo Alto Networks, Inc.*

A

Yes. Because it not only achieves better security outcomes, but it also translates to more efficient security operations of the teams that actually are responsible for managing all this on a day-to-day basis.

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

A

What I was going to say, Brian, is that I think cloud security is going to go through one more evolution. And that evolution will be as it – it sort of started in the center, shifted left to go to code. Now it's doing a hard shift right. A hard shift right is you need to be in the sensor in production environments, understanding what's going on, protecting the production environment and using that to prioritize cloud security. So I think the bigger cloud security action is going to be in runtime with agents, and that's where more XDR players are playing. It's actually not the CNAPP players who won the last round, if that makes any sense.

**Brian Essex**
*Analyst, JPMorgan Securities LLC*

Q

Super helpful. Thank you.

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

A

All right. Thanks, Brian, for those two questions. We'll go next with Gabriela Borges from Goldman Sachs, followed by Jonathan Ho from William Blair. Gabriela, go ahead.

**Gabriela Borges**
*Analyst, Goldman Sachs & Co. LLC*

Q

Hey. Good afternoon. Thanks for taking my question. Dipak, you mentioned earlier, there are some deals that are always going to be upfront. Maybe just elaborate for us, what are the guardrails or what is the framework for your salespeople that determines when they go to multiyear versus one-year billings? And when they can offer financing versus when you don't want to offer financing? Thanks.

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

A

Yeah. So I think its all part of the actual sales motion and negotiation. So really, really where you see the majority of the requests for deferred payments is in the higher end. Like distributors don't really want to have to deal with lots of back and forth with customers at the lower end, and therefore, that's typically all upfront, right? So it's really at the higher end deal. And on firewall, we typically get the money upfront because that's being budgeted based on a refresh cycle.

So those cases apart, it then becomes a negotiation. Our sales team will basically go and they'll explain that there is value in the cost of money. We expect to be paid upfront, and then it becomes part of the negotiation based on what is required and what's not required.

We do have guardrails in place. Everything from sales comp to approvals that are in place to make sure that we manage that tightly. But it really is with a view of enabling platformization at scale, which is why we've been working on this for a while and managed the transition pretty well so far.

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

Great. Thanks, Gabriela, for that question. Next, we'll go with Jonathan Ho from William Blair, followed by Peter Weed from Bernstein. Jonathan, go ahead.

**Jonathan Ho**
*Analyst, William Blair & Co. LLC*
Q

Good afternoon. Just wanted to understand a little bit better the decision to add in CNAPP as part of the Cortex platform. And can you talk a little bit about the ability to accelerate adoption or accelerate platformization as you take on this tactic? Thank you.

**Lee Klarich**
*Chief Product Officer, Palo Alto Networks, Inc.*
A

Yeah. Look, as Nikesh was mentioning, a lot of the action in cloud is shifting toward real-time, which means shifting toward runtime and even SOC. It's really critical, though, from our perspective that we bring in as much context as possible in order to be able to take those automated actions, right? And that context often comes from CNAPP and even code security. That's the first critical reason.

Second is the cleaner your cloud environment can be from preventing issues from ever making into production or cloud posture where we're detecting and remediating those issues, the cleaner your cloud environment, the better that security posture is, the easier it is for the runtime and SOC capabilities to fire in real-time because it's easier to pick out the attacks using machine learning, AI, and other types of capabilities like that.

So ultimately, we believe that the best outcome for customers is achieved when they connect all of the aspects of cloud together, and so you see that show up in terms of how we package the offering as well.

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

Great. Thanks for that question, Jonathan. Next, we'll have Peter Weed from Bernstein, followed by Shaul Eyal from Cowen. Peter, go ahead.

**Peter Weed**
*Analyst, Bernstein Institutional Services LLC*
Q

Thank you. And congrats on the continued success on the platform. Maybe I ask the un-sexy question, which is on the product side, I think we saw some nice strength this quarter. And I know kind of the guidance is that's going to remain a less exciting from a growth standpoint portion of the business.

But that strength was important for delivering on the revenue. And if we look forward, is that type of strength something that we should be able to look at as a support as opposed to maybe a drag on the overall growth? Or is this kind of a onetime quarter? How will that evolve looking forward?

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

So Peter, I think it's probably one I would sound like a broken record. I've always been saying that the hardware industry, for us, at least our end is going to deliver somewhere between 5% to 8%. And sometimes it's been flat. In the post-pandemic, there was a sort of surge and it went back down. I think we're back to steady state. So I think easily, you can expect us to be growing in low-to-mid single digits on the appliance side.

But I think the real action for us is I think you have to understand, there's a series of transformations going on underneath, like Dipak highlighted, the cash flow transition. We've been transitioning our network security business, as you saw, from hardware to software. This is why you see that we're growing that category 21% between hardware and software. So that just over time reduces our reliance on hardware because I think that cloud transformation is underway, more and more cloud volume, but that's good news, the cloud volume is going up faster than the data center volume is declining.

So if we can manage this transition in a way we can drive more and more software firewalling capability and not just recompense for the hardware business being slow growth compared to that, we can also, over time, drive higher growth across the entire network security category for ourselves.

**Peter Weed**
*Analyst, Bernstein Institutional Services LLC*
Q

Thank you.

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

Great. Thanks for the question. Next up is Shaul Eyal from Cowen, followed by Tal Liani from BofA. Go ahead, Shaul.

**Shaul Eyal**
*Analyst, TD Cowen*
Q

Thank you. Good afternoon, guys. Nikesh, I'm interested in your views on the curator and overall IBM partnership this quarter. And is it coming in line or better than your initial views couple of quarters ago when you have gone after this asset? Thank you.

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

Shaul, we had our board meeting yesterday, and there was a comment that one day a Harvard Business School case would be written on this for the right reasons. I'll tell you, this has been a spectacular partner for us, not just our relationship with IBM, our go-to-market partnership together, where they are – we talked to a large deal. It's actually public in the UK, the home office deal where IBM and us partnered, and it's a very large modernization contract. We partnered really well.

Some of our very large deals, as we highlighted one of our largest deals this quarter, the Asian bank, was a QRadar customer, which now we were able to take the ARR up 5 times. So you can see that the sort of inroads in the partnership that IBM had with many of these customers has translated into very, very large opportunities for us. So it couldn't have been better.

**Shaul Eyal**
*Analyst, TD Cowen*

Q

Thank you so much.

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

A

Thanks, Shaul. Next, we'll go to Tal Liani from BofA, followed by Andy Nowinski from Wells Fargo. Tal, go ahead.

**Tal Liani**
*Analyst, BofA Securities, Inc.*

Q

Hi. I wanted to ask about the margins. Can you go over kind of what happened to margins this quarter? I saw a little bit of pressure. And then what's the outlook for the year? What are the puts and takes for margins? Thanks.

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

A

Tal, just a clarifying question, you're talking gross margins? Is that what you...

**Tal Liani**
*Analyst, BofA Securities, Inc.*

Q

Yes. Gross margin and also a little bit on the operating margin, I saw.

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

A

Yeah. So really, it's mainly in the gross margin. And it was all in my prepared remarks. Like we're – so there, the main parts were on the services gross margin. It was driven by like faster growth on the newer SaaS offerings, which just have more time to mature and scale. And on the hardware, we did have some onetime inventory write-offs [ph] C&Os (00:54:40) that will not repeat in the second half.

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

A

So I think it's – we had a 40-basis point onetime write-off, which impacted our gross margin on the hardware side, which is why – it's a onetime event. But we still outperformed our margin expectations, both internally and as per you guys.

**Tal Liani**
*Analyst, BofA Securities, Inc.*

Q

Thanks.

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

A

All right. Thanks, Tal. Next, we'll go with Andy Nowinski. And our final question will be from Matt Hedberg from RBC. Andy, go ahead.

**Andrew Nowinski**
*Analyst, Wells Fargo Securities LLC*

Q

Okay. Good afternoon. Thank you. And I thought your quarter overall was very good as well. I want to ask maybe a more difficult question on the net new ARR side. If you pull out the $74 million from QRadar in Q1, it looks like your net new ARR declined on a year-over-year basis for the last two consecutive quarters. And you have so many positive trends in these large platformization deals. Why aren't those translating into net new ARR growth over the last two quarters?

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

Yeah. So Andy, we talked about this a little bit last quarter. I mean we're very happy with the net new ARR growth. We did have some transitions of old attaches to cloud-delivered advanced subscriptions that led to a significant increase in net new ARR a year ago as we lapped flat. We don't have the same step-up, but the net new ARR on some of our newer products, what's driving a lot of the platformizations, continues to go from strength to strength.

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

Andy, I think just to add to that, like the software firewall strengths we talked about, the SASE strength we talked about, the cloud security strength, the XSIAM strength, all these things contribute to net new ARR. That's what's allowing us to get it to the – I still remember six years ago, this was zero. So we're very happy that it's driving up closer to $5 billion. And we still believe we are on track to get to $15 billion on NGS ARR.

**Andrew Nowinski**
*Analyst, Wells Fargo Securities LLC*
Q

Got it.

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

Great. Thanks, Andy. Our last question is from Matt Hedberg. Matt, go ahead.

**Matthew Hedberg**
*Analyst, RBC Capital Markets LLC*
Q

Sure. Thanks for taking my question, guys. Congrats on the results. Not an easy environment here. Yeah, I had kind of a high-level question, maybe Lee for you. I think we've all been talking about an agentic framework, and I think Nikesh you mentioned on the call. I guess, Lee, from your perspective, a lot of people look at identity as sort of maybe the tip the spear for agentic-based security. What's your perspective on the security foundation for a broader agent rollout?

**Lee Klarich**
*Chief Product Officer, Palo Alto Networks, Inc.*
A

I think it's a lot more complicated than that, Matt. Not necessarily in a bad way, but I think sometimes the industry can be quick to jump on a single magic bullet of identity, which is important, but there's a lot of other aspects to how these agentic platforms work.

And I would actually start with how do you secure the AI portion of the agentic platform and making sure that it's providing – if you're going to give it the authority to take independent actions, which effectively what agentic AI will

do, you better make sure that that AI environment is fully secured from attackers and you have the proper guardrails enforced and everything else.

Yes, that has to be combined with identity. All of that has to be combined with – it's going to ramp up even just machine-to-machine level communication, how we secure it. So there will be multiple facets to how agentic AI is secured as it matures.

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

A

And just to add to that, Matt, I think one of the things which is from our perspective, fascinating is that we have now sold XSIAM more than 200 times in the last 24 months, making it one of the fastest-growing products in cybersecurity. And in XSIAM, we see all the data. So we expect we will start seeing agentic activity in XSIAM.

So identity is two parts. Identity is validating your credentials to make sure you are who you are, whether you're an agent or human being, which is what typically MFA does or service accounts do in SaaS applications. But watching the activity and being able to control the activity and stop the activity and change permissions will have to happen in some sort of AI-enabled SOC.

So we think there is an opportunity for us in the future as the definition of agents and the deployment agents starts to settle in that we will be able to build agentic sort of detection remediation and management within the XSIAM capabilities that we have.

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

All right. With that question, Matt, thanks for wrapping it up for us. I will turn the call back over to Nikesh for his closing remarks.

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

I just want to say thank you very much to all of our customers, employees and our ecosystem partners for all their hard work. And thank you for all of you for taking the time to listen in our earnings call. We'll see you guys next quarter.