20-May-2025

Palo Alto Networks, Inc. (PANW)

Q3 2025 Earnings Call

CORPORATE PARTICIPANTS

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

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

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

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

OTHER PARTICIPANTS

Saket Kalia
Analyst, Barclays Capital, Inc.

Brian Essex
Analyst, JPMorgan Securities LLC

Keith Weiss
Analyst, Morgan Stanley & Co. LLC

Joseph Gallo
Analyst, Jefferies LLC

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Shaul Eyal
Analyst, TD Cowen

Jonathan Ho
Analyst, William Blair & Co. LLC

Joel P. Fishbein
Analyst, Truist Securities, Inc.

Andrew Nowinski
Analyst, Wells Fargo Securities LLC

MANAGEMENT DISCUSSION SECTION

Hamza Fodderwala

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

Good day, everyone, and welcome to Palo Alto Networks' Fiscal Third Quarter 2025 Earnings Conference Call. I am Hamza Fodderwala, Senior Vice President of Investor Relations and Strategic Finance. Please note that this call is being recorded today, Tuesday, May 20, 2025 at 1:30 PM Pacific Time.

With me on today's call to discuss our fiscal third 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 Q3 2025 supplemental information and Q3 2025 earnings presentation.

During the course of today's call, we'll be making 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 measures 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. We also note that management is scheduled to participate in the Bank of America Technology Conference this quarter.

I will now turn the call over to Nikesh.

Nikesh Arora

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

Thank you Hamza. Good afternoon, everyone, and thank you for joining us for our earnings call. I'm delighted with our Q3 results. We continue to make progress on our platformization strategy while releasing a number of unique innovations in Q3 that set the pace for our industry. It is becoming increasingly clear that as organizations aspire to simplify and modernize their security architectures in the age of AI, with data at the center, our strategy is resonating, resulting in larger deals.

Most notably, we crossed an important milestone of $5 billion in Next-Generation Security ARR, up 34% year-over-year, delivering industry-leading growth at scale. Our net new ARR growth also showed positive momentum in the third quarter.

We believe we have reached an inflection point in our Next-Generation Security story as a growing majority of our incremental growth this year is derived from our AI-powered XSIAM, SASE and software firewalls. These

offerings, with large TAMs, should help underpin your confidence in the sustainability of our NGS ARR growth as we march towards our $15 billion ARR target for FY 2030.

On the profitability front, Q3 continues to show the leverage in our business model as we drive efficiencies from our scale and benefit from the economies of larger, multi-product deals, in addition to continuing to drive AI efficiency benefits slowly and steadily. We also generated healthy free cash flow while continuing to manage our transition from a billing focus to RPO. As such, we remain confident in our – achieving our adjusted free cash flow margin targets over the next few years.

Let's be clear. You can't walk around a street corner or a conference without hurting – hearing the words AI. The urgency to adopt AI is omnipresent in all of our customers. It no longer seems to be a choice. It's becoming a strategic imperative for every customer as the risk of inaction is too high. During every conference, every customer conversation, the topic of AI transformation is more and more frequent. And now the conversation is shifting to agentic AI.

What's fascinating is this is actually creating a higher sense of urgency amongst our customers to undertake their technology transformation, transformations that require a fundamental change in your infrastructure. Traditional IT architectures weren't built for the scale, speed or complexity of AI. To truly capitalize on AI's potential, enterprises need modern, cloud-delivered platforms that can ingest vast amounts of data and operate in real-time at scale. We've seen customers who were previously delaying their cloud migrations are now reaccelerating their investment. This is good news for cybersecurity.

And as AI becomes more deeply integrated into our customers' businesses, the need to protect the underlying data, models and infrastructure will become paramount. Over the next year, an estimated more than $300 billion will be spent on AI infrastructure alone. That kind of spend doesn't just power models. You saw the video we opened with Glean, and we're hard at work enabling secure adoption of this next wave of AI-powered applications. This is precisely why industry must change the paradigm, shifting away from today's fragmented security landscape and towards consolidation. The cost of fragmentation is friction. Friction causes latency. Latency is the enemy of real-time cybersecurity.

Now more than ever, bringing data together into a unified platform is critical. At its core, security is a data problem. We believe our depth and breadth of data is amongst the largest in the industry, and is something that point solutions simply cannot access. This leads to superior threat detection efficacy, reduced false positives, and faster incident response times, all critical metrics for our customers and key drivers of our market leadership.

The volume and complexity of threats are not slowing down either. Bad actors are using AI to move faster than ever. Recently, our Unit 42 team was able to simulate an entire ransomware attack in under 25 minutes using AI at every stage of the attack chain. That's a staggering increase in speed, powered entirely by AI.

Over a year ago, we doubled down on our platformization strategy. We're pleased with the large deal momentum we've had since, and the endorsement of our strategy broadly across the industry. Our platform approach is working well with customers slowly and steadily. Our approach, which favors better and speedier security outcomes and lower cost of ownership, is being adopted by more and more of our customers. In Q3, we delivered over 90 net new platformization deals, and now have a total of approximately 1,250 platformizations within our top 5,000 customers.

Digging deeper, the number of customers with multiple platformizations grew nearly 70% year-on-year in Q3. In particular, the number of customers platformized on Cortex was up nearly three times, reflecting strong momentum with XSIAM.

The overall growth in largest customers also reinforces our success. We had 130 customers with over $5 million in NGS ARR in Q3, up over 40% year-over-year and 44 customers with over $10 million in NGS ARR, up over 60%.

To give more color on what these platformizations look like, I want to take a look at a few examples from Q3. Of particular note, beyond the size and scope of our deals is the customers' ability to consolidate a significant number of products with Palo Alto Networks. A leading global consulting firm signed a transaction worth over $90 million in Q3. This customer platformized on Cortex for XSIAM, replacing a legacy incumbent SIEM provider. Our differentiated value was centered in our ability to materially reduce mean time to respond. We also reduced costs by consolidating a total of four products in this deal. As a result, our NGS ARR with this customer nearly doubled year-over-year.

A leading financial services company signed a $46 million transaction with us. The customer recognized the value of XSIAM and consolidated four products with us, including the displacement of their well-established EDR and SIEM vendors. Beyond XSIAM, the customer also expanded and extended their platformization on our network security platform in the quarter.

A US financial services firm signed a $32 million transaction with us. This customer platformized on network security and consolidated cloud security vendors, driven by a company mandate to consolidate their security tools and reduce complexity in their cybersecurity stack. In this deal, they consolidated four products.

Now moving on to an update on Cortex. As you can tell from earlier comments, I'm particularly excited about the momentum we're seeing with XSIAM, which saw accelerating growth in Q3. XSIAM is not only our fastest-growing product ever, it is now more impactful to our overall growth rate. I believe that from a strategic perspective, XSIAM has the potential of being the game changer for both the industry and Palo Alto Networks, in the first innings of baseball, not cricket, of transforming the cybersecurity industry with XSIAM. By consolidating security data into a single AI-driven SOC platform, XSIAM is modernizing and disrupting the traditional SIEM market. We're continuing to see amazing milestones, including customers' mean time to respond from weeks to minutes. As security teams face growing complexity and talent shortages, we believe XSIAM is well positioned [ph] to be (00:09:41) operating system for modern SecOps.

The numbers speak for themselves. We now have approximately 270 customers in XSIAM and the average ARR per customer is over $1 million. This already makes it one of the most successful products in the history of cybersecurity.

What's even more remarkable is that we've generated – reached this level of adoption and impact just 30 months after XSIAM was made generally available to customers. XSIAM ARR grew over 200% year-over-year in Q3, nearly twice as fast as our closest next-generation SIEM competitor.

On a trailing 12-month basis, XSIAM bookings are now approaching $1 billion. About three years into our XSIAM journey, our sustained strong momentum bolsters our confidence in a long growth runway as we increasingly tap into this estimated $40 billion SecOps TAM. Last quarter, we unveiled Cortex Cloud, our breakthrough in unifying cloud posture and SOC operations. Over the last three months, we have seen strong early customer interest in Cortex Cloud with a nine-figure pipeline, spanning hundreds of customers.

This quarter, we also announced two products that will enhance our ability to further expand XSIAM and its capability. XSIAM, once deployed, has become the foundational security data platform for our customers.

We now understand the data we're capturing in this is the data you actually need for a whole variety of use cases. In April, we launched Advanced Email Security to help stop threats before they reach the inbox, and our exposure management capability was launched as well, designed to cut through the noise and focus security teams on the risks that truly matter.

That's not all. Think of XSIAM as our data to market engine. Every byte on nearly 12 petabytes of telemetry we ingest daily around Cloud Identity endpoints in email and more act as high-octane fuel. This massive data stream isn't just powering XSIAM; it's igniting our ability to identify and accelerate our entry into entirely new markets, unlocking additional TAM in the tens of billions we're now uniquely positioned to address.

Through our comprehensive understanding of data sources and broad data ingestion capabilities, we're beginning to deliver solutions using multiple content capabilities of XSIAM. Every piece of telemetry we ingest makes our platform smarter. The more data we [ph] pull (00:11:58) in, the further our engine can go, and the smarter it gets, the faster we can build and trial new capabilities on top of it. We're encouraged by the early customer feedback and look forward to continuing to discuss this more in the future.

Now shifting our focus to network security. We continue to lead the market in network security and gain share across all three of our best-of-breed form factors. As enterprises look to securely, increasingly secure hybrid workforces and IT environments spanning headquarters, branch offices, data center and the cloud, we're uniquely positioned with a consistent security architecture.

In Q3, our product revenue grew 16% year-over-year. This growth was broad-based, with software continuing to increase in the overall mix. We also saw stable demand in the appliance market.

Software firewall ARR grew approximately 20% year-over-year in Q3 with public cloud deployments continuing to be the primary driver. AI is accelerating cloud adoption, and we believe this trend will expand the long-term need for software firewalls that scale modern workloads.

Shifting to SASE, which continues to be our fastest-growing form factor in network security and a strong contributor to our overall growth. As customers transform their network to keep pace with delivering first-class security capabilities for remote users and branch offices, we continue to see robust growth for SASE. Many SASE projects are large and comprehensive, which is well suited to our rich offering and enterprise-focused sales expertise. In Q3, our SASE ARR grew 36% year-over-year, more than twice as fast as the overall market and ahead of our key SASE competitors.

Furthermore, 40% of new SASE customers were net new to Palo Alto Networks in Q3. We now have approximately 6,000 SASE customers, up 22% year-over-year.

Meanwhile, the drivers of our SASE momentum are broadening. This quarter, we saw particularly – particular strength in Prisma Access Browser, which again accounted for a third of our Prisma Access seats sold in the quarter. In just 18 months since our Talon acquisition, we have now sold approximately 3 million license seats on Prisma Access Browser, up more than 10x from a year ago, and we have a healthy nine-figure pipeline.

As AI drives more data and applications to cloud, the browser is becoming the primary interface to accessing these resources, acting as the application runtime environment. The operating system in this scenario becomes less about local resources and more about securely connecting to and managing cloud-based services. And as more and more critical applications and data reside within the browser environment, it naturally becomes a target for cyberattacks.

Prisma Access Browser's native controls and real-time visibility are designed to help ensure that sensitive data remains safeguarded during browsing sessions regardless of the user's location or the application they're accessing. And we believe Prisma Access Browser is strategically positioned to be the future OS in enabling secure and productive work in an evolving AI-driven world.

Now shifting to our newly launched Prisma AIRS, our AI runtime security. As I mentioned earlier, it's more important than ever to bring data together in order to leverage AI and enable customers to stay ahead of the attackers. We're also seeing customers demand for us to help them secure their AI transformation journey. In this mad rush for AI in the industry, many of our customers are experimenting with AI.

At Palo Alto Networks itself, our teams are leveraging over 35 models across multiple products, each of which [ph] and their (00:15:21) AI artifacts need to be discovered, scanned, constantly tested and protected against. Prisma AIRS allows for just that. It helps enterprises discover, scan and test all the AI artifacts to ensure they're safe. It allows for world-class data security posture deployment. And once in production, it ensures that applications using AI are constantly monitored and any security flaws are both protected against as well as remediated across the enterprise. Prisma AIRS extends our existing capability in posture management, runtime security and will add security for AI agents in the future.

And we recently announced the intent to acquire Protect.ai, an early innovator leader in security for AI, providing AI model scanning and AI red teaming to further bolster our capabilities. Customer interest has been strong. We currently are in conversation with hundreds of prospects and already have an eight-figure pipeline since making the announcement last month.

In summary, we see strong momentum heading into our fiscal year-end, driven by continued transformation, and we look for of our first north of $4 billion quarter. We see strong desire for consolidation and the desire to implement AI securely, including a robust Q4 pipeline. We continue to take share across multiple security categories, driving strong growth in NGS ARR at an industry-leading scale.

Our platformization strategy translates into tangible business benefits for customers, including a strong security posture and improved operational efficiency throughout – through vendor consolidation. With our relentless focus on innovation, we believe Palo Alto Networks is the ideal partner to help organizations achieve and secure their AI transformation goals. I'm particularly proud of our teams for driving phenomenal success in a Q3 which was fraught with geopolitical discussions, tariff discussions. Yet our teams kept our heads down and continued to execute, setting us up for what we hope will be a great Q4.

Let me hand it over to Dipak to review the quarterly results in detail.

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 Q3. You can review the detailed results in our press release and the supplemental financial information on our website.

In Q3, total revenue was $2.29 billion and grew 15%, at the high end of our guided range. Within total revenue, product revenue grew 16%, while total services revenue grew 15%. Within total services, subscription revenue grew 18% and support revenue rose 10%.

On a trailing 12-month basis, the proportion of our product revenue from software is approaching 40%, driven by our growth in our virtual form factors and SD-WAN. We continue to see stable demand for firewall appliances, with market growth in the 0% to 5% range, as we have discussed previously.

Moving on to geographies, we saw double-digit growth across all theaters, with the Americas growing 12%, EMEA up 20%, and JAPAC growing 23%. Our remaining performance obligation, or RPO, grew 19% to $13.5 billion. Our current RPO was $6.2 billion, growing 16% year-on-year.

The average duration of new contracts remained at approximately three years. Contract duration decreased slightly on both a year-over-year and quarter-over-quarter basis. Customers continue to make significant commitments to Palo Alto Networks, through our platformization deals, particularly when adopting XSIAM to transform their security operations center.

We continue to see increasing demand for annual payments, particularly deals over $1 million, but we are absorbing this transition while maintaining the high end of our fiscal year 2025 annual adjusted free cash flow margin guidance, as well as reiterating confidence in our adjusted free cash flow margin targets of 37% plus in fiscal year 2026 and 2027. In line with what we talked about earlier in the year, we saw a year-over-year increase in bookings that went into annual billings in Q3, and a decrease in deals leveraging PANFS, with a neutral impact on cash flow.

Turning to Next-Generation Security ARR, as Nikesh highlighted, we surpassed the $5 billion mark in Q3 and ended the quarter at $5.09 billion in NGS ARR, a growth of 34%. Within NGS ARR, we continued to see significant momentum around our Cortex platform, and our AI ARR is now approximately $400 million in Q3, up over 2.5 times year-over-year.

I'm particularly excited about the trends driving the NGS ARR, and I wanted to provide some additional insights around the evolution of our net new NGS ARR. We've made a number of significant investments over the last several years to both continue to lead the network security market, as well as build leadership positions in new markets. You've seen the results of this effort in our NGS ARR.

Over the last several years, in network security, we invested in advanced cloud-delivered versions of our subscriptions that attach to our appliances. We saw strong adoption of these advanced subscriptions, as customers saw the value of adding these to their existing network security deployments, and this is meaningful – and this has driven meaningful NGS ARR growth. In addition, we have NGS product offerings beyond those advanced subscriptions in new markets across network security, cloud security, and security operations. We refer to those as our new market offerings, as they have also fueled our NGS ARR growth.

We continue to see momentum from our advanced subscriptions in fiscal year 2025, driving a healthy and relatively consistent level of net new ARR compared to prior years. At the same time, we've seen our net new NGS ARR from new market offerings grow significantly, and these are becoming a larger proportion of our total net new NGS ARR dollars. This is a result of our strengthened position in these markets, our large sales team becoming more adept at selling these offerings, and platformization taking hold with our customers and in the industry.

As we look forward, we expect to see the new market business to be the stronger driver of net new ARR dollars. It is this dynamic that gives us confidence in our long-term targets.

Moving down the income statement. Total gross margin was 76%. Product gross margin was 78.4% in the quarter. As a reminder, we have been transitioning to a contract manufacturing facility in Texas as our primary manufacturing and performance center to benefit from scale and innovation as well as to take advantage of a foreign trade zone that can help us mitigate tariffs in products that we ship to international destinations.

As we said on our previous call, we continue to believe that we differentiate ourselves by being the only pure play cybersecurity firm at scale to assemble all of our hardware in the USA. As a result, tariff impact to our business has been immaterial. We expect product gross margins to remain in the high 70% or low 80% margins in Q4.

Our total services gross margin was 75.4%. We are excited to see continued strong adoption of our SaaS offerings. We continue to execute on cloud cost efficiencies, including engaging with our key cloud service providers to negotiate favorable procurement arrangements as the scale of our cloud-hosted products continues to increase.

Encompassing those gross margin dynamics, we continue to focus on executing our operating margin targets, which delivered year-over-year improvements in operating margin. As I have often said, our business scales well across every single line item of the P&L.

On an operating expense as a percentage of revenue basis, we saw 340 basis points of year-over-year leverage this quarter as we drove scale and efficiencies across sales and marketing, R&D and G&A. We delivered $0.80 of diluted non-GAAP EPS and diluted GAAP EPS of $0.37, our 12th consecutive quarter of positive GAAP EPS. We generated $578 million in adjusted free cash flow in Q3.

Turning to the balance sheet, you will see that our debt balance came down by $151 million as we continued to see early conversion of our convertible debt, which occurred at the discretion of the debt holders and were settled by us in cash and equity. As a reminder, our convertible notes reach final maturity in June and our convertible notes can no longer be early converted. We will settle the remaining convertible debt in cash and equity in Q4.

As Nikesh mentioned, we announced our intention to acquire Protect AI for a total consideration of $700 million in cash and replacement equity awards. We expect the transaction to close by our first quarter of fiscal year 2026. We did not repurchase any shares in Q3 and our buyback strategy remains opportunistic. We have $1 billion in authorization remaining through December 2025.

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%; remaining performance obligation of $15.2 billion to $15.3 billion, an increase of 19% to 20%; revenue to be in the range of $9.17 billion to $9.19 billion, an increase of 14%; operating margins to be in the range of 28.2% to 28.5%; our diluted non-GAAP EPS to be in the range of $3.26 to $3.28 per share, an increase of 15%; adjusted free cash flow margin in the range of 37.5% to 38%.

As we noted last quarter, we do expect a higher Q4 contribution to our annual free cash flow. And for Q4 specifically, 80% of the collections are from deals that have already been booked. Our annual cash flow seasonality is more second half and Q4 weighted this year, influenced by the timing of deferred payments from customers that signed deals in prior periods and the timing of bookings within the year.

For the fourth fiscal quarter of 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 $2.49 billion to $2.51 billion, an increase of 14% to 15%; and diluted non-GAAP EPS to be in a range of $0.87 to $0.89, an increase of 16% to 19%. We've included our typical modeling points in the presentation for your review.

With that, I will turn it back to Hamza for the Q&A portion.

QUESTION AND ANSWER SECTION

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

Okay. Great. Thank you. To allow for broad participation, I would ask that each analyst ask only one question. The first question will come from Saket Kalia followed by Brian Essex of JPMorgan.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Okay. Great. Hey, guys. Thanks for taking my questions here, and congrats Hamza on the move over. Nikesh, maybe for you. Lots of things.

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

There is life after, you can see.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Absolutely. Nikesh, maybe for you. Lots of things to be excited about with XSIAM. I wanted to dig into one part of that opportunity in particular, which is the QRadar on-premise customer base. Clearly, a big base there that you can upgrade. Maybe the question is how are customers thinking about that upgrade and how big of an ARR opportunity could that be for Palo Alto Networks on that path to $15 billion?

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

Well, Saket, first of all, thank you for the question. Look, I think we had this debate last quarter, how big is XSIAM going to be versus Prisma Access Browser, because we believe they are both new trends in the industry, primarily driven by the AI wave we're seeing around us. And whilst we started the XSIAM journey and then we did the deal with IBM, where the first set of conversion we saw were from QRoC where people who were already adapted SaaS, already in the sort of cloud-delivered SIEM market, we saw that conversion.

But we've had a phenomenal partnership with IBM where we have been able to go with them to many of their large customers and work them through the transformation of going from an on-premise SOC to what is effectively now a cloud-delivered SOC. So the QRadar on-prem transition is not just moving [ph] QRadar to (00:28:45) XSIAM; it's also moving from an on-prem delivered solution to cloud-based solution.

And clearly, you've seen the ARR uplifts. We announced the large deal, one of the largest deals, $90 million deal, which had a XSIAM component to it. The second largest deal we had also had an XSIAM component. So, clearly, large deals on XSIAM are possible. I mean, if you think about it, you've been covering security for a long time. Which is the last product that came out where the average ARR was $1 million a year, right? There are companies out there in security who start and say – claim they have $10 million customers, or we say, every customer XSIAM is a $1 million ARR customer. So I think the opportunity is huge.

If you go back historically, and I've said this in cybersecurity, certain swim lanes reach inflection points where the next set of products are so much better that everybody has to be shaken out of their stupor and their old solutions to go replace. I mean you saw that happen in the endpoint market where we had players who had to be replaced over time. You saw that historically when we came out with the next-generation firewall.

And I think this is the moment of the SIEM market. It's a $40 billion TAM. I think in the next three to five years, it will get replaced. It will be replaced by new age players. The legacy players will try their darndest to hang on to it, but the architectures are fundamentally different and the architectures of yester years, and it's not their fault because we designed a product 17 years ago. It was designed where data was expensive to store, latency was high, things were done offline. Today, we live in a world with low latency, and so you see hyperscalers announcing real-time translation this morning. So, you can see that we can process data at immense speeds and deliver results immensely.

If you concatenate that with what I said, we were able to regenerate a [ph] sudden (00:30:23) ransomware attack in 25 minutes, right? If that's the pace of the bad guys, the pace of the good guys has to be faster. So, there's no way to get to the other side from an incident response and a management perspective if you don't transform what is fundamentally a legacy technology.

So, I think XSIAM is a huge potential, one, and I apologize for taking longer than I should for your answer. But I said this in my prepared remarks, I want to make sure I emphasize is that what we've covered is once we ingest all the data in an enterprise, we can actually go and make peacetime products better. So, our launch of Email is actually a multi-context launch. Email security products are traditionally swim lane products. I look at your email, I protect you. We're able to look past the email in the SIEM and say, wait, when somebody clicked on that email link, what happened? So we have the entire organizational context from the data that we have that allows us to go back and make the e-mail product spectacularly better.

So, we think there are many, many new swim lanes which will get discovered as we deploy XSIAM on our customers. We've seen early examples of exposure management and e-mail management. We think those are the first two use cases, but I think there's many use cases behind it. Eventually, we think something like XSIAM becomes the underlying security fabric of enterprises.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Very helpful. Thanks.

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

A

Right. Next, we have Brian Essex from JPMorgan, followed by Keith Weiss from Morgan Stanley.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Great. Thank you. Thank you, Hamza, and congrats on the move from me as well. Thank you for taking the question, I was wondering if you could unpack, Nikesh, the details behind the product revenue growth. Really strong quarter of growth there, and I heard Dipak's comment that approaching 40% software in terms of mix. But I was wondering if maybe you can shed some light on how much of that is share shift? How much of that is pricing increase and how much of that might be refresh?

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

A

Brian, as you know that our product revenue growth is a combination of hardware and software. So, it's not just the hardware part. I think the core hardware business still continues to grow at – I sound like a broken record. I've always maintained 5% to 8%. And I think the core hardware business is still growing at 5% to 8%. We highlighted software firewalls in our prepared remarks for a reason. We think the software firewall business is going to inflect.

And I said this and I want to reemphasize that. In the last six months, you always ask what changed this quarter. What changed this quarter is there is so much buzz about AI that even the people who are reluctant to deploy AI are dipping their toes on it. Now, what's fascinating is if you want to stay on the bleeding edge of AI innovation, it's all coming cloud delivered, right? If you want to do an on-prem AI implementation, it's about six months behind because there's no Gemini for on-prem, there's no OpenAI for on-prem, there's no Lambda for on-prem. You can deploy Lambda on on-prem, but you have to be very smart, technically, to go put all the bells and whistles required. So, even the most reluctant of organizations are going to have to move to the cloud to be able to leverage the AI models that are coming out fast and furious.

Now, the moment you say, I have to go in the cloud, I have to go deploy real-time in the cloud, you have to secure it. And today, we have the best technology in a multi-cloud basis for cloud network traffic in our software firewall. So part of what we're seeing is the software firewall business is beginning to inflect, which is underpinning both the transformation from hardware to software, but also bolstering our product revenue at Palo Alto.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Thank you.

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

A

Next question will be Keith Weiss from Morgan Stanley, followed by Joe Gallo at Jefferies.

Keith Weiss
Analyst, Morgan Stanley & Co. LLC

Q

Excellent. Thank you, guys...

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

A

Why did he pick – Keith, why did he pick you third?

Keith Weiss
Analyst, Morgan Stanley & Co. LLC

Q

I know, that's a good question.

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

A

This is what you get.

Keith Weiss
Analyst, Morgan Stanley & Co. LLC

Q

That being said, Hamza, if you ever realize you made the wrong decision, there's always room for you [indiscernible] (00:34:17). It's never too late. It's never too late to come back. But congratulation guys on a really solid quarter. I wanted to kind of expand on that last question on what you were talking about in terms of the AI imperative and what that opportunity means for Palo Alto Networks.

When you're talking to customers that are looking to secure these new AI infrastructures, is this just about ARRs, or is there a wider opportunity? What is it like pull through from the Palo Alto portfolio when people are looking to secure this new surface area? And to what degree does this help give you guys' confidence in the growth in like the next-generation of ARR into next year? That's where I hear the most concerns from investors. Are they too aggressive for next year? Is it AI? Is it platformization? Like what are the elements that give you confidence in that how you forecast?

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

A

That's a great question, Keith. So I think if you take the software firewall example and extend it, so our conversations now are beginning with, well, we've got to secure this AI implementation. And I highlighted, we had a board meeting last week and our InfoSec team presented how much AI are we using within Palo Alto.

I was amused and amazed to find, we have 35 models under evaluation and deployment right now at Palo Alto. It's not one model. It's 35 models because we use various models for different things. Now the moment you talk about 35 models, our board starts getting worried about, oh, my God, how are you securing these models because they could be from anywhere?

And what you discover is that to be able to secure those models, you actually effectively have to envelop them with a runtime firewall or AI firewall, which is actually an extension of our software firewall capabilities, right? So what's going to happen? The AI firewall is going to do a pull-through on the software firewall, and customers are going to lose the distinction between AI traffic and traditional cloud traffic. Call it traditional cloud traffic because – [ph] I don't know (00:36:08).

So, what's [ph] heartening (00:36:09) to see is we are beginning to see the faster adoption of cloud firewalls because of the AI trend, which is what I highlighted to Brian in terms of how that is driving some of the hardware to software transformation. So the transformation wave [ph] is sort of (00:36:22) be slowly chugging along for the last five, six years, moving to a more balanced portfolio, [ph] be it (00:36:28) hardware and software is getting accelerated, which will cause the NGS ARR shift from hardware to software, because that depletes our traditional ARR and increases our NGS ARR. So there is sort of tailwinds associated with that on the NGS ARR front from a software firewall perspective.

And Keith, one of the other things I'll say is that we learned our lesson in cloud. In cloud security, we dwelled too long on the peacetime capabilities of cloud security or the posture capabilities of Prisma Cloud. But in the firewall sort of AI business, we've actually doubled down on the production capability. So we are aggressively starting with runtime security, which actually was 18 months later in the cloud security industry, right? We are out of the gate with a runtime capability. And as you can see with our acquisition of Protect.ai, we're not going to let this one go. We will relentlessly innovate and make sure that we don't get sideswiped by any vendor in the market.

Keith Weiss
Analyst, Morgan Stanley & Co. LLC

Q

Excellent. Thank you, guys.

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

A

Thank you, Keith. Next up, we have Joe Gallo from Jefferies, followed by Gabriela Borges from Goldman Sachs.

Joseph Gallo
Analyst, Jefferies LLC

Q

Hey, guys. Thanks for the question, and congrats Hamza on the new role. Nikesh, you briefly alluded to executing through geopolitical volatility. You're the first off-quarter cyber name to report. Can you just elaborate on your conversations with CIOs, CSOs? Is it back to business as usual after the first couple of weeks of April, or is there still a lot of uncertainty? Maybe just kind of talk through the pipeline conversations and what's embedded in 4Q guide.

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

A

That's a great question, Joe. I don't – the reason I didn't dwell on it in our prepared remarks is because April was an anomalous month. I think we're back to normal, in a way. But there was, as you can imagine, not too far long ago, there was conversations around tariffs around the world. There were all kinds of supply chain shocks that were anticipated, which did cause some of our customers to think, oh, my God, what's going to happen? Next time I ship a car across the border, it's going to be twice as expensive. Or I can't ship anything. What am I doing over here?

So you saw that little sort of uncertainty in the market, which happened to be in the last month of our quarter. So that's why I'm particularly delighted that our teams got their heads down and executed. It was not an easy quarter to execute. Had we not had the tariff conversations or geopolitical tensions, it would have been much easier to sail through it. But we had our lessons from the pandemic. We had our lessons from the supply chain crisis. So we had to go back and pull up our shorts and execute the same practices that we did then.

And we're kind of like on the same sort of cadence now in Q4 because we are trying to stay ahead of the curve because I don't think many of our customers changed their plans from a transformation perspective. But there was a pause for a few days where they were trying to figure out where the market goes. And thankfully, as you see, that we seem to have overcome that as a global economy. So there's a little more, I'd say, stability in the business climate than there was towards the sort of, I'll say, the early to mid-part of April. But our teams did execute through it, so I'm very proud of that.

Joseph Gallo
Analyst, Jefferies LLC

Q

Thank you.

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

A

Right. Next up we have Gabriela Borges from Goldman Sachs, followed by Matt Hedberg from RBC.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Q

Hey, good afternoon. Thank you. Nikesh, I wanted to follow-up on your comment on learning your lesson from cloud. Maybe just a little bit more on how you think about the AI product portfolio evolving from here. How do you think about what this looks like couple years out, the mix between organic and inorganic? And on your plan being sideswiped, how do you think about insulating yourself from being leapfrogged in AI technology specifically, given how quickly the technology is evolving? Thanks.

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

A

Thanks, Gabriela, for the question. I think in the cloud world, if you go back five years ago, which is when I'd say – five or six years ago when the whole cloud security evolution started, there was an over-indexation and focus on cloud posture. Trying to understand what's going on, trying to understand where the misconfigurations are, trying to understand how do you configure GCP, how do you configure AWS, et cetera. And there was a whole flurry of companies, the Dome9, Evident, RedLock, Twistlock, all the companies that some of us bought and turned into our core cloud portfolios. But there was a lot less focus on runtime because everybody was experimenting. Everybody was trying to figure out what to do with cloud and deploying it. So, clearly, that's where the market was, that's where all of us focused.

But I think we did ourselves a disservice by not indexing harder on the runtime scenarios, which is where eventually the market has evolved, as you can see. Now we see more action in cloud detection and response and cloud SIEMs than we see in cloud posture. And over time, cloud posture is getting commoditized. Every vendor in our industry has a cloud posture module, whether you're in SASE, you're in endpoint detection, or you're a cloud security vendor. So it's a very commoditized industry, and you've seen pricing sort of get rationalized because of many players in the market, and it being an extension of many existing categories.

In AI, I think we're going to see an accelerated version of that, because AI is moving a lot faster than any other technology transformation that's happened. And we are sort of – it's better to be very lucky than good sometimes, and we were lucky that we deployed native firewalls in every public cloud provider that allows us to expand that capability, because if we want to watch AI transactions midstream [ph] align (00:41:35), you have to be where the traffic is. The traffic is in the cloud service providers, right? If you think about it, 90% of AI implementations are running through cloud service providers, not on-prem. If that's the case, that traffic has to be looked at, it has to be bidirectional traffic, because these things are going to have a brain of their own, right? They're going to have agency. When that happens, you have to look at what that brain is doing, because sometimes it can be erratic.

So from that perspective, AI runtime security becomes a very important pillar. And we sat around the team and [ph] we have (00:42:04) done a really good job on our AI firewall, and then you discovered, customers wanted to understand the veracity of the models, they wanted them scanned, they wanted to persist in red teaming and say, oh, my God, it's going to take us six months to build it. Like, no, let's go look at who's the best in the market. We found Protect. We were lucky that the founders found a fit with our team in terms of how they were going to work with us, and we're going to close that acquisition. And that team is actually going to run our AI security business.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Q

Excellent. Thank you.

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

A

Thank you. Next up, we have Matt Hedberg from RBC, followed by Shaul Eyal from Cowen.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Q

Hey. Thanks Hamza for the question. Congrats on the results, guys. I had a question for Lee. Walking around RSA, it really felt increasingly like it was an AI conference versus a cyber conference. And you guys talked about $400 million in AI ARR, which is great. I guess my question is, from an agentic world, talk about why Palo Alto is best positioned to help customers think through that, which is a – obviously, a whole new paradigm shift. But talk about some of the foundational aspects that you feel really good about from that, from an agentic perspective.

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

A

Yeah. Great question. I think two years ago, RSA was AI. A year ago, it was AI security. And this year, it was agentic AI, right? We're cycling through the different forms of AI. Look, with agentic AI, I think the way I think about it, it starts with this idea that AI is going to move from being a sort of helper function to having autonomy. Like it's going to be able to take actions on its own. Obviously, those actions will be metered out and increased over time as trust is built up.

And when you think about that in concept, one of the – there's a few key building blocks that are going to have to be present. And one of those is it's not just going to be sort of a open-ended, let AI kind of create and do whatever it wants to. There'll have to be certain guardrails and constraints on that from an enterprise perspective, and certainly from a cybersecurity perspective.

And so the first aspect of that then that positions us very well is our breadth and strength across everything related to automation, right? Our export platform has over 1,000 integrations. We know how to integrate with all the different systems in the enterprise. We know how to programmatically approach this in a consistent, reliable way. What happens then if we put a AI engine behind that, and that's the agentic piece that can actually start to actually create and evolve and improve and learn over time? So, no one else really has that same level of integration and automation capabilities that can be paired with AI.

The second piece is the biggest concern that I heard from just about every customer I talked to was the sort of the permission infrastructure for how do you make sure that these agentic systems are actually allowed to do what they're allowed to do. And the – our footprint in understanding the interconnectedness of all different applications and enterprise puts us at a – in a very good place to be able to understand the right permissioning and the security implications of that. And so we shared this in two forms: one, what we're doing on Prisma AIRS to secure agentic systems; and two, we gave a preview of agentics, which is going to be our approach to building agentic platforms for our customers, and I'm excited about both of those.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Q

Thanks guys.

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

Thank you, Matt. Next up, we have Shaul Eyal from Cowen, followed by Jonathan Ho from William Blair.

Shaul Eyal
Analyst, TD Cowen
Q

Thank you. Good afternoon guys. Congrats on solid results. Congrats to Hamza leading his first call. Nikesh, back to QRadar and Talon, and I get these are two different products at their core. Both seem to be exceeding their targets internally, both should continue to show great results. From where you sit, would you rank them as Palo Alto's probably better acquisitions over the course of the past four, five years? Where is the bigger TAM opportunity longer term?

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

I think the – if you step back and you think five years out, I think five years out, security will be delivered on top of a large security data lake by some version of machine learning and AI. I think the traditional approach to security of writing policies and writing rules and writing human set of controls at the edge is going to fail. Because AI will be incessantly banging at those edges, trying to find the loopholes and the misconfiguration in the way humans have not secured the perimeter.

So if you believe that, and you say that the way to make sure that your perimeter is secured, is look at all the data, analyze it, pattern recognize it and have your agents, the same agents that Matt was asking about. Those agents should go back and say, I found a misconfiguration at the edge, let me go fix it, right? Why should that not happen? Why should security in the future be some security analysts sitting and writing a policy pane, saying, do this for traffic and do this for HTTPS, et cetera.

So, by definition, it means you should have some version of agentic AI securing your perimeter five years from now. That requires that agentic AI to have access to all the data across all your endpoints, right? It doesn't mean you have to have the same endpoint. It doesn't mean you have to have Prisma Access Browser or SASE or Palo Alto SASE. You can have anything. You have Zscaler, Netskope, Palo Alto, whoever you want. But at the end of the day, the data has to get to one place.

Now what's happened is we've been collecting data recently in a new paradigm for the incident respond use case. Well, guess what? That same data can be used for the policy remediation use case or protect your perimeter use case. So I think the evolution of security will be people will go towards [ph] a lot (00:48:07), harmonized security data lakes, which will be used for multiple activities. And I think we're seeing the beginning of that. And I think three to five years from now, when you look back and say, that was obvious. It's not obvious today because people are still going to sell best of breed products at the perimeter protected. But how can you protect the perimeter if you only have a singular lens on the problem? If you only see what you see with your product, how can you protect the perimeter? You have to see the entire enterprise to understand where the relative opportunities, where the relative mistakes are. And I think that's where security goes in two to five years.

So in that context, I think Prisma Access Browser is a great edge device, which will actually be very interesting and useful because you have full visibility of the interactions of the endpoint or the human perhaps or the agent perhaps in that use case. But you're going to need something in the back to try and make sense of that data and be able to respond in real-time. And I think that's where the underpinning of the next-generation SIEMs of the world is going to be.

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

All right. Thank you, Shaul. Next up, we have Joel Fishbein from Truist, followed by Andy Nowinski from Wells Fargo.

Jonathan Ho
Analyst, William Blair & Co. LLC
Q

Hey, guys. Can you talk a little bit about the enterprise browser and why Talon has seen the inflection that it has? And does this perhaps help your platform approach, particularly around the AI opportunity? Thank you.

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

Yeah, absolutely. So the key if you think about this from a secure browser perspective is it's a niche sort of use case when it is disconnected from everything else, right? You have a user, they browse the Internet, you secure it. It's interesting. When we deliver it and are able to integrate it with our platform, it completely transforms that from being a sort of one-off use case to being an everything use case. We can now secure users' traffic to the Internet, we can secure their connections to SaaS, we can secure their connections to private applications. With the recent announcements where we are integrating VDI, we can even secure their connections to things that are not even browser-based.

And so the – what I just described is enabled by us delivering it as part of a comprehensive platform as opposed to a standalone solution. Now we can deliver standalone, and we have some customers that are starting there as a first step toward broader adoption, which, that's part of the flexibility and how our platforms work, but the comprehensive solution is really what's driving the inflection point as we see it.

And then to your point around how AI factors in, we're finding that through the secure browser, we're able to then deliver a differentiated solution to our customers for securely adopting AI, where they get better security and a better user experience when adopting AI because we can embed a lot of the security controls directly in the browser, which just makes it a lot easier from an adoption perspective.

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

Sorry about that, Jonathan. Next up, we have Joel Fishbein from Truist, and we'll wrap it up with Andy Nowinski from Wells Fargo.

Joel P. Fishbein
Analyst, Truist Securities, Inc.
Q

Thanks for the question, and Hamza, congrats. Nikesh, I guess, a follow-up to Shaul's question or your answer to Shaul's question. A pretty powerful statement about the data lake security. I'm curious about how you view threat intelligence and the importance of sharing threat intelligence in this AI era and protecting against the bad guys. Love to hear your thoughts on that.

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

Look, we've always had a belief that threat intelligence should be shared, for the most part. There's obviously certain exceptions. But generally speaking, we've been open. We're one of the founding members of the Cyber Threat Alliance, which is focused on doing just that, even amongst security vendors, so with our competitors.

I actually think the – to a certain extent, the advent of AI and attacker AI is going to have an interesting impact on this. A lot of threat intelligence is oriented toward the idea that if I know about a specific attack, a specific piece of malware, or a specific IOC, I can build a protection for that specific thing. And in the advent of AI, more and more attacks are going to be novel attacks. They're going to be new and different, and it becomes much more important that protections then are AI-based.

Now these AI-based protections will be informed by threat intelligence, but it will be less of a direct correlation. It will become much more important that what is being shared from the threat intelligence perspective actually becomes more about attack techniques and approaches. And that's actually going to require a bit of a change to the threat intelligence space. So that will need to happen, will need to play out. It will be interesting to see how that shift manifests itself.

Joel P. Fishbein Q
Analyst, Truist Securities, Inc.

Thank you.

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

Thank you. And our final question will be from Andy Nowinski from Wells Fargo.

Andrew Nowinski Q
Analyst, Wells Fargo Securities LLC

Okay. Thank you for squeezing me in, and I'll make it a good one here. You guys had solid growth in platformization customers. I think you now have 1,250 that have deployed a platform. That's a small percentage of your total installed base of over 70,000 customers. So I'm wondering, is there any way to look at the percentage of ARR that those platform customers account for? Because I would guess that they account for a much higher percentage of your ARR than the 2% they account for in your installed base. So I'm really trying to understand the importance of the growth in these platform customers relative to reaching your $15 billion ARR target. Thank you.

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

So let's recap, Andy. I think we had said we want to get to between 2,500 to 3,500 platformizations. And we believe when we get there, at the current trajectory of ARR per platform deals, we're going to get close to our $15 billion target. And that assumes somewhere between 60% to 70% of our NGS ARR is made up of these platform customers. Does that make sense?

Andrew Nowinski Q
Analyst, Wells Fargo Securities LLC

Yeah, certainly. Okay.

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

That's our math. So you can do the math now yourself and say, what does that mean? If – 70% of $15 billion is not hard to compute.

Andrew Nowinski
Analyst, Wells Fargo Securities LLC

Q

[indiscernible] (00:54:30). [ph] 3,500 (00:54:31)...

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

A

And then you can divide that by 2,500 to 3,500, whichever you like, and see the average ARR per deal. And then we'll tell you if you work that back 5%, 6% a year, over the next five years, you'll say, wow, that must be the average platform deal that Palo Alto has, give or take.

Andrew Nowinski
Analyst, Wells Fargo Securities LLC

Q

Got it. Thank you.

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

Okay, great. With that, we will conclude the Q&A portion of this call. I will now turn it back to Nikesh for his closing remarks.

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

Again, thank you, everyone, again for joining us for our earnings call. We look forward to seeing many of you at upcoming investor events. I also want to thank our customers, partners, and as I said, our employees for powering through what was a tumultuous April, but we think now it's business as usual, and all of us are heads down trying to execute on our big 4-plus billion dollar quarter in Q4. Thanks again.