Corrected Transcript

23-May-2023

Palo Alto Networks, Inc. (PANW)

Q3 2023 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
Equity Analyst, Morgan Stanley & Co. LLC

Brian Essex
Analyst, JPMorgan Securities LLC

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Adam Tindle
Analyst, Raymond James & Associates, Inc.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC

Shaul Eyal
Analyst, Cowen & Co. 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' Fiscal Third Quarter 2023 Earnings Conference Call. I am Walter Pritchard, Senior Vice President of Investor Relations and Corporate Development. Please note that this call is being recorded today, Tuesday, May 23, 2023, at 1:30 PM Pacific Time.

With me on today's call are Nikesh Arora, our Chairman and Chief Executive Officer; and Dipak Golechha, our Chief Financial Officer. Following the prepared remarks, our Chief Product Officer, Lee Klarich, will join us in the Q&A session.

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 Events & Presentations where you will find the Investor presentation and supplemental information.

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 risks and uncertainties. We assume no obligation to update them. Please review the press release and our recent SEC filings to see these risks and uncertainties.

We will also refer to non-GAAP financial measures. These 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.

We also note that management is participating at the Bank of America Global Technology Conference on June 6.

I will now turn the call over to Nikesh.

Nikesh Arora

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

Thank you for joining us. Good day, everyone, and welcome to – oops. There's a bit of a little repeat AI action there. Thank you, Walter. Good afternoon, everyone, and thank you for joining us today for our earnings call.

As you can see, once again, our teams have delivered a balanced quarter between our top and bottom line performance in the current macroeconomic environment. In Q3, our billings grew 26% year-over-year and revenue grew 24% while RPO grew ahead of these at 35%. Our Q3 non-GAAP operating income and our trailing 12-month adjusted free cash flow both grew about 60% year-over-year while we achieved our fourth consecutive quarter of profitability on a GAAP basis.

Let's talk about the macro environment. The overall macro trends of cautious spending, deal scrutiny and cost and value consciousness persist. Moreover, the behavior continues to be more widespread across a larger swath of our customers.

Against this backdrop, we have been staying ahead with rigorous execution. It increased our own deal scrutiny, gotten ahead of the challenges and continue to sharpen our business value focus while demonstrating superior security outcomes to our customers.

From a technology trend perspective, there is no significant change. The teams we have seen around cloud adoption, automation and hybrid work continue with minor variations. Network transformations, albeit with long cycles, continue to be undertaken because they offer cost savings and are part of the modernization stack for most customers as they go down their cloud and network transformation journeys. This in turn continues to drive a sustained demand for SASE and hardware and software firewalls.

As we have shared before, the team of consolidating around platforms continues to come up, and we are well-positioned to offer solutions in this regard. Needless to say, in the last three months, ChatGPT and generative AI have revived interest in AI as a technology. As we have always maintained, AI is a data problem and security is a data problem and AI has an interesting role to play in security both for its ability to help deliver superior security outcomes in nearly real-time and unfortunately the potential threat associated with AI being used for generative tasks. We have and continue to work on these problems. We should talk more about this today.

On the other hand, we continue to see limited underlying growth in hardware in the industry. While the supply chain crisis and its effects are all but over, there is a shift that the crisis created. We have seen a higher appetite for software-based solutions and networking and a higher appetite for cloud-delivered form factors. This is particularly salient to the current CapEx constrained environment.

On the adversary front, there seems to be no impending recession in threats. Increased cloud activity and connectivity continues to drive the threat environment. This is best illustrated by recent findings in the seventh installment of our Unit 42 Cloud Threat Report. It still takes the average security team approximately six days to resolve a security alert. In contrast, it only takes a threat actor a few hours to exploit a newly discovered vulnerability.

While over 7,000 malicious versions of open-source software packages were circulated in 2022, less than a quarter of those packages are sourced properly to ensure a clean software version is incorporated into a typical customer's code base. Regulatory interest continues to rise and is prevalent across multiple governments. There is sustained activity around incremental regulatory mandates and executive orders to create awareness around cybersecurity. This is true not only at the government level but also as companies' Board of Directors are bringing additional oversight and driving alignment of accountability for cybersecurity. This requires incremental organizational focus and investment by our customers.

On the macro front, customers anticipate that global growth may slow. Some are grappling with rising capital costs and are watching their bottom lines more closely. This means looking for efficiencies in their business. Within cybersecurity, complex architectures and long vendor rosters have come into focus and many customers see this as an opportunity to simplify and drive consolidation.

Five years ago when I highlighted the need for platform architectures and consolidation, the idea was met with some resistance. Over the last few years, our industry-leading solutions, three-platform approach has continued to take hold and has allowed us to provide a much needed option for simplicity, a modern stack and better security outcomes for our customers.

I mentioned earlier that our customers are engaging in more scrutiny of deals and value resulting in robust discussion internally with us. We continue to work hard to stay ahead of deal cycles engaging the CFO and procurement departments. The cost of money continues to be on the topic of conversation as customers enter the larger and longer-term relationship with us; some also seek more flexible business terms. A strong balance sheet allows us to accommodate customers while we maximize our medium-term cash flow.

Let's turn to efficiency and operations. As we started this fiscal year, we pivoted our efforts and focused our effort in doing more with less. Our teams responded effectively. Coupled with the waning of the supply chain crisis, we have been able to adapt our operating model significantly. Dipak will get into specifics, but suffice it to say we have found a new rhythm and at our scale we believe we can continue to drive better margins from our business. We have achieved this through selective hiring in our customer-facing teams as well as streamlining a go-to-market efforts in addition to hiring for key innovation areas which we expect to continue to do. These efforts are self-evident in our higher Q2 operating margins and our increased operating and free cash flow margin guidance for the year be.

We continue to see platformization in cybersecurity. I talked about consolidation earlier. A key part of our thesis at Palo Alto Networks has always been to drive superior cybersecurity outcome for our customers. To do that, we need a robust portfolio that works both individually and cohesively to reduce the burden on our customers who have to stitch together disparate cybersecurity products. We had to navigate this fine line with our customers.

We continue to see the benefits of this approach and think we are in a multiyear trend. We have the opportunity to do the security what we have seen done in financial software, HR software, or CRM where customers have adapted to platforms due to the inherently superior benefits from data integrity, integration, seamlessness and outcome orientation. As they say, the proof is in the pudding. You can see our success here driving larger platform transactions. Across the board, the size of the transactions we are signing is increasing. This is evidenced by booking from transactions validated over $1 million, $5 million and $10 million in the third quarter which are up year-over-year by 29%, 62%, 136%, respectively.

We see a similar trend in cohorts of our customers. For example, when we look at the average lifetime value for our 200 largest customers, we've seen steady growth of 30%-plus over the last three years. When we look at purchases of our platforms amongst the Global 2000, we see now that 53% of our customers have bought a product in all three platforms of Strata, Prisma and Cortex, up from 48% a year ago and 33% three years ago. We see this as a continuing trend. It convinces us that the opportunity to impact outcomes for our customers is large if you can get this right. We see the paths to continued success with large customers and multiproduct expansion around installed base.

I'll now update you on our three platforms starting with network security. We are the comprehensive zero trust network security company. This quarter, we were proud to be named a new leader in Gartner's most recent Security Service Edge Magic Quadrant. This recognition is apt as our teams have been delivering significant innovation and seeing stronger customer adoption in SASE for years. This, in addition to our leadership position in SD-WAN, makes us the only SASE vendor in the industry to be named leader in the Gartner SSE and SD-WAN Magic Quadrants. Add to that our leadership position in network firewalls and our number one market share position in virtual firewalls, we are the only vendor with clear leadership across zero-trust network security. This leadership across the network security category is a testament to our ability to drive significant innovation in new markets while maintaining our leadership in core markets and offering this innovation as part of our cohesive platforms.

Let's talk about SASE. SASE remains one of the fastest-growing markets within all of cybersecurity. Our ARR is growing over 50%. At scale, we have surpassed 4,200 customers in Q3. Our success has spread across all three major geographies as highlighted by large deals in each of these territories in Q3.

Let me tell you about three of these notable wins. First, a global beverage company with US headquarters signed a transaction north of $30 million which includes $24 million of SASE for a complete SASE transformation that included Prisma Access, Prisma SD-WAN and our ADEM, or Autonomous Digital Experience Management, for tens of thousands of employees.

Second, a Japan-based technology company signed an eight-figure transaction to modernize its network and its network security after an extensive POC. Before standardizing on our SASE, the customer replaced its legacy firewalls and other network security capabilities and standardized on our next-generation firewalls, driving a full zero-trust network strategy.

Finally, a European technology company signed a high seven-figure SASE deal that was part of an overall transaction to Palo Alto Networks of once again nearly $30 million in total value. The customer bought from us because of our multiple network security form factors. In the broader transaction, we added capabilities such as IoT and fully adopted our core network security subscriptions.

You all might remember at the beginning of this fiscal year, as part of our scaling efforts, we combined our SASE sales organization into our core sales organization. Drivers here were that we saw SASE demand going mainstream, and we saw encouraging signs that our core sellers could sell the more complex SASE offering. After three quarters of executing as a combined organization, we're delighted to report that over 80% of our core reps participate in the creation of Prisma SASE pipelines as we enter Q4.

Q3 was a strong quarter of innovation, highlighted by our AI-powered SASE launch. This flagship release includes capabilities to enable organizations to automate their increasingly complex IT and network operations center functions with AIOps. It improves monitoring for networks and apps at the branch office and significantly improves integration with IoT security.

Moving over to our firewall business, broader than SASE, the future of network security is clear to us. It is centered around software. And while we have led and expect to continue to lead the hardware appliance market for many years, software and cloud-delivered form factors have been an increasing focus since I joined as CEO.

There are multiple reasons why this shift to software is accelerating. In the changing macro environment, customers are more challenged in their CapEx budgets which often fund appliance purchases. As a result, their interest in software and cloud-delivered form factors remain high. This is especially true when tied to strategic initiatives around cloud adoption.

Illustrating this, we saw significant uptick in customer requests to evaluate our virtual firewall offerings at the beginning of the pandemic. Customer interest in VMs was also sparked by supply chain challenges where we saw evaluation sustained. We continue to see primarily net new demand for software and cloud-delivered form factors. However, we are seeing more appliance replacements and planning for this trend to continue and possibly accelerate.

Beyond the strength I already covered in SASE, we saw VM-Series deals over $1 million more than double in Q3, including an eight-figure deal we signed with a government agency where they moved from a primarily appliance-centric model to VM-Series as a fully leveraged public cloud as their primary infrastructure. This year so far, our VM-Series bookings are up more than 40% year-over-year, and it grew over 55% in Q3.

Most investors have equated our product revenue with hardware. However, given the drivers I have mentioned here, this has been rapidly shifting. Software now contributes 30% of our product revenue. This is up from about 10% three years ago. We expect this trend to continue, and as Dipak would remind you, bookings from our VM-Series and SASE transactions are recognized as revenue more over time than an appliance booking.

Given the conversation about AI, as I mentioned, there is a renaissance in artificial intelligence driven by significant advances in large language models, the development of more powerful and next-gen computing, and the broad availability of large volumes of training data. As a result, we have all seen some of the fastest innovation cycles and launches of unique applications over the last several months. At Palo Alto Networks, we have been focused on this technology for many years, and our efforts have been accelerating over the last two years.

We first introduced machine-learning capabilities as part of our WildFire offering seven years ago. In the ensuing years, we added AI and machine-learning capabilities across our network security portfolio. And it has been a critical driver of our innovation and differentiation in the market. In 2020, we introduced the industry's first machine learning powered next-generation firewall where machine learning detection moved in line to prevent zero-day attacks. Since then, we have overall nearly all of our security subscriptions with advanced AI capabilities: DNS Security, advanced URL filtering, advanced threat prevention, advanced WildFire, all harness machine learning for in-line detection and prevention of zero-day attacks. This means even new attacks that have never been seen before are blocked at the very first attempted use by an attacker. Additionally, we applied AI to IoT security to discover, identify and secure IoT devices, and most recently it was expanded to cover both medical IoT and OT security needs.

We had a signature release in SASE that included AI-powered autonomous digital experience management in addition to leveraging AI for SDWAN as well as AI-powered phishing prevention. In short, we have really been accelerating the application of AI to our network security stack and is one of the most mature applications of AI in the security industry today.

We are not only ahead in investments in AI and machine learning as a differentiator in our products, but these investments have driven tangible customer benefits. In a typical day, we analyze nearly 750 million, yes, 750 million new, unique telemetry objects worldwide. This includes files, URLs, domains, DNS connections, and other signals. Our AI models analyze this data and every day, we see 1.5 million new attacks that have never been seen before. We take these new insights and add them to all the other things we have already knew about and use them to block 8.6 billion attacks across our customer base daily. This forms the foundation how we do better security across our network security platforms and this is how we continue to get better and better at detecting zero-day attacks and being in a position actually to prevent those attacks as well.

Moving on to Prisma Cloud, our early data in Prisma Cloud continues to strengthen. Most of our competitors continue to provide only point products while customer demands continues to shift towards the platform approach. Within this, connecting the left side to the right side, otherwise known as code to cloud, is becoming paramount.

As an example of our platform success, we continue to see strong usage of our cloud security posture management and cloud workload protection offerings. Customers are increasingly standardizing on these foundational modules, with 49% of Prisma Cloud customers using both CSPM and CWP. This quarter, Gartner noted that in 2022, only 25% of enterprises buy these capabilities from a common vendor. They expect this will increase to 60% of enterprise by 2025.

At the same time, we continue to stay ahead of the industry's need for new capabilities, which is core to our commitment as a platform. We are on track to launch our 11th module as we integrate Cider Security.

We're also focused on driving industry certification on Prisma Cloud and just last quarter, we were accepted by the joint advisory board and reached Ready status for FedRAMP High, a first for a cloud security platform. This comes in addition to other certification we have achieved including recently announced Prisma Access achieving Impact Level 5 or IL5 Provisional Authorization. IL5 is the highest unclassified authorization level for DOD agencies under the FedRAMP process.

We continue to see steady growth in consumption of Prisma Cloud credits, which were up 44% year-over-year in Q3. Our platform is key to this steady growth. We continue to see customers increase their consumption as they deploy workloads and strategically leverage the public cloud at the core of their IT and business strategy. This includes migrating workloads to the hyperscale clouds, building new application in the clouds, and leveraging new cloud services.

They're also deploying new Prisma Cloud modules, of which we currently have 10. The number of customers using two or more Prisma Cloud modules grew 37% year-over-year while the number using four or more modules almost doubled. We now have one in five of our Prisma Cloud customers using our Cloud Code module across our capabilities and Infrastructure as Code, SCA or software composition analysis, and [ph] sequence management (00:18:39) as they leverage the more efficient approach to detect and remediate security issues as core decision for cloud applications before it reaches production.

Now, moving on to Cortex, this has been a net new business for Palo Alto Networks, a business which has born the belief that we need to bring next-generation innovation to the SOC and all the related activities, just like we have brought firewall business years ago. We're delighted to announce that Cortex achieved $1 billion booking milestone over the last 12 months.

Cortex was born in 2019 and since then we have focused intensively on ensuring we have industry-leading capabilities across endpoints, SOC automation, and attack surface management. The last four years, we have risen to a leading player in automation, application of AI. Attack surface management continue to climb the charts of the XDR industry as one of the most technically capable solutions. We're particularly proud of the fact that XDR has consistently led in security efficacy. XDR delivered 100% prevention and 100% detection across the 19 evaluation steps conducted by MITRE and has had the highest quality detections of any part in the latest round of evaluations.

On the back of our hard work driving these capabilities, we have built Cortex business to over $1 billion in bookings the last 12 months, as I mentioned. It is up from $150 million in annual bookings when we launched Cortex as a business in 2019.

As we look forward, these three core capabilities in Cortex are precursors to leading in next-generation autonomous security operation center, which pulls this all together and was launched publicly a few months ago called XSIAM.

Our next-generation SOC platform, XSIAM, built totally on AI is on track to be our fastest-growing new offering. XSIAM represents another significant opportunity within Cortex as we fulfill our vision around autonomous security operations. Like network security a decade ago, security operations have evolved slowly. XSIAM is now paving the way for us to drive AI-driven security transformation outcomes.

After our GA launch in late Q1, our design partners made significant commercial commitments to XSIAM. We followed that up in Q2 by broadening our go-to-market and achieving early success with $30 million in bookings. This quarter, we established momentum for XSIAM with quarterly bookings more than doubling sequentially as we signed our first eight-figure deal and transactions across all three of our major geographic theaters of this product.

We remain optimistic about the prospects of XSIAM, with the product the center of customer security operation center transformation. We're seeing XSIAM give us access to a broader swath of our customers' budgets. Based on what we have achieved this quarter and what we see in the pipeline, we are confident we can achieve our goal of $100 million in bookings faster than we originally anticipated. This would make it one of the fastest-growing security platforms from Palo Alto Networks.

Not only does XSIAM bring together the core capabilities of Cortex, it also brings AI-driven outcomes to customers. This heralds a new approach to security, an outcome-based approach. The inspiration came to us from our own SOC where we were woefully slow in our own mean time remediate five years ago. Our MTTR was in days, which in today's adversarial environment isn't acceptable.

With that insight in mind, we were able to collect billions of events and then using AI reduced this down to just over 100 alerts from a handful of incidents. From here, continuing to use AI automation, we are able to investigate and respond while detecting incidents in a matter of seconds and responding to higher priority ones in under 1 minute. This is one of the most compelling outcome stories in security.

So far, in the early customers that are farthest along on this journey with us, we are seeing the benefits accrue in a similar way. We process over 3.5 petabytes of data a day across the customer estate of XDR and XSIAM. From here, we apply approximately 1,000 AI models to detect attacks. We then leverage smart scoring and use automation to accelerate investigation response. We are seeing early indications that customers are able to see reductions in mean time to respond from days or weeks down to hours or minutes, just like we did.

Circling back, we are fortunate to be focused on the part of technology market that is more resilient. Our customers depend on their partnership with us to address challenges that are only becoming more sophisticated. The market is tough, and definitely more challenging than when we started the year. I'm proud that our team has executed through this environment.

Our strategy focused on having industry-leading capabilities, helping customers simplify their architectures and consolidating vendors is working. Given our diverse portfolio of products, some of our products are growing faster in any given quarter and others are moderating. Combined, you see this portfolio benefit in the top line results we reported today.

We also see significant opportunity as we begin to embed generative AI into our products and workflows. There are three ways that our concerted investment is generative AI will benefit us. First, generative AI will help us improve our core under-the-hood detection and prevention efficacy by further advancing state-of-the-art AI and ML in our products that I spoke of today.

Second, it will manifest itself in how our customers engage with our products. We will leverage our large cybersecurity dataset and telemetry to provide a more intuitive and natural language-driven experience within our products which will improve NPS and drive efficiency benefits for our customers.

And finally, as our employees leverage generative AI, it will drive significant efficiency in our own processes and operations across the enterprise. We intend to deploy a proprietary Palo Alto Networks security LLM in the coming year and are actively pursuing multiple efforts to realize these three outcomes.

Our portfolio approach, company's overall scale, and focus on efficiency have enabled us to drive significant leverage. We are well ahead of schedule here and we're not done. As we continue to execute on our plans, we see additional opportunities for efficiency. With our visibility into incremental leverage, we continue to see the operating profit levels in our fiscal year 2023 guidance as a baseline to build upon.

With that, I will turn the call over to Dipak to discuss the details of Q3 and our guidance.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you, Nikesh, and good afternoon, everyone. For Q3, revenue was $1.72 billion and grew 24%. Product revenue grew 10%. Total service revenue grew 29%, with subscription revenue of $838 million growing 31% and support revenue of $495 million growing 25%.

Moving on to geographies, we saw revenue growth across all theaters, with the Americas growing 24%, EMEA up 23%, and JPAC growing 24%. The strength of our next-generation security capabilities continues to drive our results, with NGS ARR of $2.6 billion, growing 60%. We saw strength across all three platforms: network security, cloud security, and security operations.

We delivered total billings of $2.26 billion, up 26% and above the high end of our guidance range. Total deferred revenue in Q3 was $8.1 billion, an increase of 38%. Remaining performance obligation or RPO was $9.2 billion, increasing 35% with current RPO just under half of our RPO.

Our non-GAAP earnings per share was significantly ahead of our guidance, growing 83% year-over-year. We again delivered strong cash flow in Q3 with trailing 12-month adjusted free cash flow of $2.8 billion, growing 68% year-over-year.

Moving on to the rest of the financial highlights, non-GAAP gross margin of 76.1% was up 320 basis points year-over-year driven mainly by a higher software mix, reduced supply chain costs, and some efficiencies in customer support. Our non-GAAP operating margin of 23.6% increased 540 basis points year-over-year. In addition to improving gross margins, slower head count additions contributed to our operating leverage. Based on our performance in Q3, we are raising our fiscal year 2023 non-GAAP operating margin guidance.

Non-GAAP net income for the third quarter grew 86% to $359 million or $1.10 per diluted share. Our non-GAAP effective tax rate was 22%. We again delivered GAAP profitability in Q3, with GAAP net income of $108 million or $0.31 per diluted share.

Now, turning to the balance sheet and cash flow statement, we ended Q3 with cash equivalents and investments of $6.7 billion. It is worth reminding investors that our 2023 convertible note will mature on July 1, 2023, and we expect to settle the principal obligation with cash on our balance sheet of $1.7 billion. The excess will be settled in shares. These shares have previously been accounted for in our non-GAAP diluted shares outstanding.

Q3 cash flow from operations was $432 million with total adjusted free cash flow of $401 million this quarter. Stock-based compensation declined by 90 basis points as a percentage of revenue sequentially. On a year-over-year basis, stock-based compensation was down 220 basis points as a percent of revenue.

As we look forward, we remain focused on profitable growth. At our Analyst Day in 2021, we outlined plans to drive 50 to 100 basis points of margin expansion annually in fiscal year 2023 and fiscal year 2024. In the months leading up to this profitability commitment, we focused in-depth on optimally balancing investments in our business and opportunities to capture efficiencies and benefit from our growing scale.

As a result, we came out of this effort with significant conviction in meaningful operating leverage. In fiscal 2022, we started implementing these plans but faced supply chain challenges that unexpectedly drove higher costs. While the supply chain was uncertain as we entered fiscal year 2023, we also saw signs of a changing macroeconomic environment. As such, it was the right time to accelerate our efficiency plans. We focused our head count additions in sales and R&D to fuel our medium term growth prospects. Outside of these critical investment areas, we've leveraged our scale and employed technology to accommodate our growth in all the business areas.

Additionally, supply chain challenges have continued to abate at an increasing pace, helping to improve our gross margin. The result has been a significant acceleration in operating margin expansion through the first three quarters of fiscal year 2023 and also increases to our operating and free cash flow margin guidance through the year.

As you see with our guidance for non-GAAP operating margin in fiscal year 2023, we're nearly 300 basis points ahead of the midpoint of our fiscal year 2024 range that we implied back in 2021. We now see our fiscal year 2023 non-GAAP operating margin as a baseline to build on in the future.

Moving on to guidance, for the fourth fiscal quarter of 2023, we expect billings to be in the range of $3.15 billion to $3.20 billion, an increase of 17% to 19%. We expect revenue to be in the range of $1.937 billion to $1.967 billion, an increase of 25% to 27%. We expect non-GAAP EPS to be in the range of $1.26 to $1.30, an increase of 58% to 63%.

For the fiscal year 2023, we expect billings to be in the range of $9.18 billion to $9.23 billion, an increase of 23% to 24%. We expect NGS ARR to be in the range of $2.80 billion to $2.85 billion, an increase of 48% to 51%. We expect revenue to be in the range of $6.88 billion to $6.91 billion, an increase of 25% to 26%. We expect product revenue growth in the range of 15% to 16% of fiscal year 2023 as we see supply chain challenges normalize as we exit fiscal year 2023.

For fiscal year 2023, we expect operating margins to be in the range of 23% to 23.25%. We expect non-GAAP EPS to be in the range of $4.24 (sic) [$4.25] to $4.29, an increase of 69% to 70%. We expect our adjusted free cash flow margin to be 37.5% to 38.5%, and we expect to be GAAP profitable for fiscal year 2023, including in Q4. Additionally, please consider the following modeling points.

We expect our non-GAAP tax rate to remain at 22% for Q4 2023 and fiscal year 2023, subject to the outcome of future tax legislation. For Q4 2023, we expect net interest and other income of $50 million to $55 million. We expect Q4 diluted shares outstanding of 326 million to 332 million. We expect fiscal year diluted shares outstanding of 322 million to 324 million and we expect Q4 capital expenditures of $35 million to $40 million.

With that, I will turn the call back over to Walter for the Q&A portion of the call.

QUESTION AND ANSWER SECTION

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

Thank you, Dipak. To allow for broad participation, I would ask that each person ask only one question. Our first question will come from Saket Kalia of Barclays, with Hamza Fodderwala from Morgan Stanley on deck.

Saket, you're muted. Right. Why don't we go to Hamza...

Saket Kalia
Analyst, Barclays Capital, Inc. Q

Okay. Can you hear me now?

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

Go ahead.

Saket Kalia
Analyst, Barclays Capital, Inc. Q

Sorry. It didn't let me unmute. Thanks so much for taking the question here, and nice job to the team executing in a very challenging environment.

Nikesh, maybe a lot of good things to talk about, but I'd love to just double-click on the operating margin improvement here that you've seen and really a new baseline that the team is creating going into next year. Maybe the question is, can you and Dipak maybe talk about what areas the team is finding efficiency in and what are the opportunities for efficiency maybe going forward as well? Thanks.

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

Yeah. Look, I'll preface that. As Dipak highlighted, supply chain crisis is all but over and as you know, there was some adverse impacts to gross margins driven by hardware. I think the product mix is in our favor as we go from hardware to software. Our gross margins are way better on software than they generally are on hardware given software firewalls are much, much more profitable for us.

Coupled with that, I think what Dipak really has been driving for the last year as we flipped into the new macroeconomic environment has been a real focus on resource utilization ROI as well as making sure we are – focused our hiring only on stuff where it's important.

We also talked about streamlining sales forces. If you remember, Saket, we had the conversation around making sure our SASE team is integrated with our core, which saved us hundreds of heads in terms of efficiency as well as driving more outcome and [ph] outpour (00:34:10) from a SASE perspective. So generally, those have been some of the key drivers.

But, Dipak, did you want to add something?

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

No, I think you've covered it all. I think, Saket, we've talked this before.

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

[ph] Welcome. (00:34:18)

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

Yeah. We scale well as a company, right, and I think that's across all the different elements of our P&L. I think Nikesh has talked about the supply chain. We talked about the OpEx.

I'd just also mention cloud hosting and cloud consumption. As we get bigger and we can see more, we have the ability to go back to our service providers and try negotiate better contracts. So I think across all the areas of the P&L, we scale pretty well as a company.

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

And I think to your question in terms of where this goes, as Dipak said, this is a new baseline. We think there is continued opportunity from here and we haven't even factored in the potential impact of generative AI as you've been hearing all the conversation in the industry. We're still working on it. We're understanding it. We're really looking at processes, but we believe there is a there there. We think there will be an opportunity in the future to get more efficiency from generative AI as we go ahead and implement some of the capabilities through our organization.

So I think there's upside both in the continued efforts of what Dipak has been driving for the last nine months, and there is the sort of the icing on the top. It's the potential application of generative AI as we continue to grow business over the next few years.

Saket Kalia Q
Analyst, Barclays Capital, Inc.

Got it. Well done.

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

Great. Thanks, Saket.

Saket Kalia Q
Analyst, Barclays Capital, Inc.

Thank you.

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

Next question is from Hamza Fodderwala from Morgan Stanley with Brian Essex from JPMorgan on deck. Hamza, go ahead.

Hamza Fodderwala
Equity Analyst, Morgan Stanley & Co. LLC
Q

Hey, guys. Good evening. Hope you can hear me okay. Maybe a question for Nikesh and Lee Klarich if he's around. Nikesh, on AI, you've clearly been thinking about this a lot based on what I can tell from your Twitter. But we were at RSA last month and while there's a lot of opportunity around AI, there does seem to be a lot of risks around data security, around sort of the data that these models are trained on. So I'm curious as you had that AI-based conversation with your customers, how are you getting them comfortable around that to really leverage the full capabilities of AI to automate their SOCs.

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

Yeah. I think there's two different parts of it. I think one part is us using AI already in our products where we have been using it for a while like a pattern recognition, look at what it's telling us from a real-time analysis of data perspective. As I mentioned, we deploy over 1,000 AI models to go look at what happened the next time. This is all proprietary. It's happening. In our instance, this is not an LLM that's going out and getting trained. This is a proprietary AI model used by Palo Alto Networks, built by Palo Alto Networks being used for a specific use case and a task for security.

Now, to the extent that we intend and will deploy conversational AI in our models, we are working with every public model and open-source model out there to understand how can we build it using our own proprietary data. I don't know, Lee, can you elaborate on that, please? [indiscernible] (00:37:11)

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

Yes, of course. It's very early in the large language model adoptions that we're seeing and as you point out, there are a number of risks associated with them, particularly in enterprise use cases. We've already seen some examples where data has fed into large language models without the understanding of how the data would be used and the data has been made publicly – made public available and then it was confidential. So it's very clear that there is sensitivity there.

There's also sensitivity from a security perspective of things like prompt injection attacks, data poisoning, and things like that that have to be taken into account. And so I think what we'll see is the enterprise use cases of LLMs will evolve a little bit more. I should say need to evolve a little bit more methodically and carefully to take the security challenges into account.

At the same time, though, it's also important to recognize that they offer tremendous promise, as Nikesh mentioned earlier, in terms of being able to help guide product adoption, product usage to help enhance security capabilities and to drive greater efficiencies across the business.

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

Yeah. I think to cap it off, I think there's no doubt we will continue to deploy our proprietary AI models for XSIAM or for our network security use case, as I highlighted. We believe in our preliminary analysis the last three months and driving a lot of these work streams internally that there is a there there with generative AI. So we believe that we will be deploying generative AI over the course of the next few months, and we'll talk more about it at a later event. But we think that has an opportunity both to significantly improve our customer efficiency and the efficacy of our products at the same time also to drive efficiencies within the way we run Palo Alto Networks.

I think last but not the least, which is something you didn't ask but I'll say, separately, Lee and his team have been working hard to see and look at the adverse impact that generative AI could have in terms of adversaries using generative AI to build new malware to try and attack our customers. And there's a lot of work we're doing as well to make sure we are able to protect our customers against any such activity that is conducted using generative AI.

Hamza Fodderwala
Equity Analyst, Morgan Stanley & Co. LLC
Q

Thank you.

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

Thanks for your question, Hamza. Next question's from Brian Essex at JPMorgan followed by Brad Zelnick from Deutsche Bank. Brian, go ahead.

Brian Essex
Analyst, JPMorgan Securities LLC
Q

Yeah, hey. Good afternoon. Thank you for taking the question and to follow-up on Saket's comments, nice progression in operating margin here. And it's good to see cash flow margin guides go up as well. If I could tick down – if you could maybe peel back a couple layers on that, core drivers of that cash flow margin improvement, how sustainable it is. We noticed that CapEx looks like it's a little bit lower than you previously guided to so just wondering. As we kind of look at that as a foundational metric to lean on for valuation, how sustainable is that? And as we kind of forecast operating margins going forward, should that, I guess, gap between operating margins and cash flow margins remain relatively consistent going forward?

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

Yeah. So, Brian, thanks for the question. Let me just start off with like the biggest driver over the long-term is really just the strength in your bookings, at least your billings and then comes down. Then the foundation really is your operating margins that then makes up the base that you can do on your cash.

There are multiple other factors, but do recognize that when we came into the year, the interest rates were at a different level. We have had the benefit of higher interest rates. We've deployed a lot of our cash that we earned interest income. We're not predictors of interest rates, but fundamentally, we believe that that will continue to be a tailwind for our cash generation.

And then last but not least, we do have PANFS. We have a certain amount of our business that we do structure and financing. Frankly, that's been broadly in line with what we assumed at the beginning of the year. But those are really the drivers and we feel pretty comfortable on what we're able to do with those different drivers in delivering our numbers.

Brian Essex
Analyst, JPMorgan Securities LLC
Q

Great. Thank you.

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

A

Great. Thanks, Brian. Next question from Brad Zelnick at Deutsche Bank followed by Andrew Nowinski at Wells Fargo. Go ahead, Brad.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Great. Thanks so much for the question and nice job both to Nikesh, Dipak, and the entire team. Nikesh, my question is about M&A, which I feel like typically comes later in the call but I feel like it's such a great opportunity right now. What's the hurdle to doing a large deal and can you remind us how you think about transformative M&A?

And just related to that, your competitors naturally knock you on having grown through acquired innovation. Just to set the record straight, can you talk about how much a priority and a focus it is to have a deeply integrated product?

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

A

Yeah, Brian. I think first of all, I'm amused that you're asking for transformational M&A. I think I feel like somehow we at Palo Alto Networks have been going through a transformation already the last five years. Let me talk about the two different parts.

One, I'd like to bust the myth of the notion that we've grown our innovation through M&A because pretty much the entire XSIAM product that we've built which is now going to be one of the fastest platforms at Palo Alto Networks is homegrown. It was built by our team internally. It was designed, built, and delivered by the Cortex team. So I think it's a disservice to them to say that someone with the fastest-growing platform being built at Palo Alto Networks was acquired, similarly, our next-generation firewalls or our SASE product. Our SASE product, for the most part, is entirely homegrown, driven by the security capabilities that we built using our firewalls as well as our virtual firewall business.

I think majority of our M&A has been focused on building our cloud security portfolio where we felt where we needed to be assertive and be out there in the front. And I would say auxiliary capabilities, whether it's in automation with XSOAR or auxiliary capabilities around attack surface management.

So, bottom line, we're very comfortable with the three platforms that we have and what we need to get done. I think we've been very clear about from an acquisition perspective, we look for product capability where we can take product capability and attach that and make sure we can solve more problems for our customers that they're looking at.

So from that perspective, my view on M&A is consistent, that we find something interesting, an industry trend which is added incremental tech capability, we will do it. I think from a transformational M&A, I think we can transform this company and have continued to transform it to where it is based on our innovation and our balance of execution. I think we will continue to do that. I don't think the market is particularly cheap yet if you were to try and look for a transformation M&A and I think it's kind of a double-edge situation.

One, I think we continue to get stronger as we get execution under our belt, and we continue to grow in value as Palo Alto Networks. And if some of the large players out there end up committing missteps, then we'll go take a look at it. But for now, I feel very comfortable with the position Palo Alto has in the industry. I feel very, very comfortable with the amount of cash we have on our balance sheet and I believe it is our job to keep our heads down and keep executing because it's a tough market.

And I think one of the things which was brought up just a minute ago, I think the opportunities from AI have not been fully comprehended by most enterprise businesses. I think we are going to undergo a transformation both as Palo Alto Networks as well as generally an enterprise software industry over the next 12 to 24 months as we embrace generative AI. I think that's the real opportunity and challenge in front of us, and I think half of the people out there will get it wrong. And hopefully, we're on the right side of history.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

You're doing a great job. Keep it up. Thank you, Nikesh.

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

A

Thanks for that.

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

A

Great. Thanks for the question, Brad. Next question's from Andy Nowinski from Wells Fargo followed by Matt Hedberg from RBC. Andy, go ahead.

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC

Q

Okay. Thank you and congrats on a great quarter. So nearly every single vendor and nearly every single reseller we talk to says they're seeing an elongation of sales cycles yet you seem to defy those headwinds with massive growth in large deals and customers spending $5 million and $10 million with you. I guess would you view this as an important inflection point as it relates to sort of consolidation in that if you can drive large deals in this macro-constrained environment, you could potentially see an acceleration of those consolidation trends when the macro improves?

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

A

Are you predicting a macro improvement, Andy?

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC

Q

I certainly hope so.

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

A

Well, look. I think, first and foremost, I don't want to leave you with any impression that the macro is not hard. It is hard out there. I think everything you're hearing from resellers, from other people in the industry is true. Customers are spending more time paying attention to deals. Customers are taking longer. Some are rightsizing deals. Some are focusing things that are important. Some are looking for financing. Some want to pay annually.

So all the effects that you talked about are true in the industry, and we recognize this towards the end of our first quarter and I'll tell you what. We've been working at double-time like literally, the day Dipak sort of shut the doors on us being able to book anything this quarter, we were out there hunting for next quarter. We have a big number to hit this quarter. We're out there in the field. We're executing. Our teams are out there.

So as you probably appreciate, there's no magic in the world around the fact that our quarter end on July 31. There's no budget year-end for any part of the world on July 31. It's a date which has been created, that Palo Alto finishes the year, Q4 on July 31, which means we have to run as hard as we can to get business done by July 31.

We know that's the end of our year. We know that's the end of our quarter. Our customers know that. So all we're doing is getting ahead of it. We're hoping us getting ahead of it and continuing to rigorously execute is going to allow us to be able to improve our conversion rates.

And our conversion rates on our pipeline are down. Guess what? You drum up more pipeline, therefore your conversion rate that's down still allows you to make the number that you promised the Street. That's what we've been trying to do. And as I've said, the macro is hard, and we're going to keep trying to keep our heads down and execute.

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC

Q

Thanks, Nikesh. Keep up the good work.

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

A

Great. Thanks, Andy. Next question from Matt Hedberg at RBC followed by Gabriela Borges at Goldman. Go ahead, Matt.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Q

Thanks, Walter. My congrats again, team. Outstanding results. I guess, Nikesh or Lee, on the success you've seen thus far with XSIAM, you noted you essentially have full access to SIEM budgets right now, and I'm curious, with some of the large deals you're seeing, are these generally replacing legacy SIEM vendors? Or are you actually generating new TAM that didn't exist previously?

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

A

So, Matt, I'll let Lee jump in and talk about some of the specifics, but I'll tell you what. Every one of these deals is a replacement of a legacy SIEM or a data store. In addition, we do not sell XSIAM without our endpoint products. You have to buy Palo Alto Cortex XDR to deploy XSIAM because we believe the only way to have normalized good single source of truth data is to deploy our endpoint products, and then we use that, as I showed, in the AI funnel of how we can go cross-correlate that and go drive great security outcomes.

So in every case we are replacing an existing vendor, but I will tell you the SOC industry is upside down. It was designed so far to go understand when a breach happens, how the breach happened, and try and figure out how to remediate it. And those remediation times, as I highlighted, were six days, and now most modern attacks are in and out in under 12 hours. So if you've got a SOC infrastructure, what it allows you to come up with what happened to you after six days, the bad actors have gone in and out in 12 hours, you have a mismatch, and that is a problem.

But, Lee, can you highlight some of the key use cases where we have seen in the first 30%-plus customers that we have, what's driven some of this transformation?

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

Yeah. Look, nearly – so XSIAM is replacing the SIEM. It's also replacing other tools in the SOC as well. There's three core elements to how this is happening. The first is around data. As you saw, 3.5 petabytes a day is being ingested and analyzed. Data is the key to driving good AI, and XSIAM is specifically designed to be able to ingest large amounts of data across different data sources into an AI data lake.

Second is how we drive AI-based analytics on that data to be able to detect attacks in real-time. This is something that the traditional SIEM industry was just not well-designed to be able to do. That is driving the meantime the detection that you're seeing. And then three is the integration of automation natively into XSIAM that allows us to drive the meantime remediation down from what in the past used to be in many cases days down to hours and even minutes.

And so in all of the XSIAM deployments we're seeing, it's amazing how quickly we're seeing the outcomes that we saw in our own SOC when we deployed and operationalized XSIAM.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Thanks...

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

I think the last thing I'll add – sorry, Matt. The only thing I'll add on this is that over the last 15 years what has happened is the cost and value equation in existing SOCs has diverged tremendously. So people are spending a lot of money collecting data in large data stores and they're not getting adequate value out of it and they're not getting adequate security outcomes out of it.

So I think that is a big gap, and that gap is something we've built this product to try and fill and now it really is very early days for us. I think the fact that we'll get to $100 million in a time span that you thought was aggressive, less than that, I think tells us there's a huge potential out there which means we have to keep our heads down, again, keep building, keep executing, and keep trying to solve the problems that our customers are presenting in front of us. But I have a good feeling about this.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

It certainly seems that way. Thanks.

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

Great. Thanks, Matt. The next question is from Gabriela Borges at Goldman Sachs with Adam Tindle from Raymond James on deck. Gabriela, go ahead.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Q

Good afternoon. Thank you. Either for Lee or Nikesh, I wanted to ask about your cloud security strategy and Prisma, specifically with respect to how you think about the right balance of incentives that you give customers up front to catalyze adoption and then also how you think about the balance of top-down growth versus top-led growth given that DevSecOps, DevOps, some of those tools seem to be driven by-product-led growth as well. Thank you.

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

A

Lee, go ahead. Answer that question.

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

A

So one of the challenges that we have set out to address with Prisma Cloud was this fundamental challenge in enterprise cybersecurity of sort of the proliferation of point products. Every time there's a new security need, there's a new product, and then customers become the system integrator of all the deterrent point solutions and they spend more time trying to be the system integrator than they are actually getting the value from the products.

And so with Prisma Cloud, we've taken the unique approach of building a platform where we can deliver many different capabilities pre-integrated from the same location.

Now, at the same time we did that on the technical side, we also approached it from a sort of the adoption side, and I'll call it the procurement side of having a single Prisma Cloud credit system that makes it really easy for customers to buy a level of capacity and then simply use it to adopt as much of the platform as they need and when they need. And so it's allowed us to focus more of our attention in terms of how we engage with customers and how the product works on in-product adoption, guided adoption of additional capabilities, and enabling them to easily use more and more the services as they need them as opposed to having to go back and turn every module into a new transaction with a customer.

And as you saw from what Nikesh showed, the new credit usage year-over-year going up about 44% year-over-year, but then also the number of customers at two or more, or three or more, or four or more modules, in the case of four or more almost doubling year-over-year shows how well that is working.

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

A

Great. Thanks, Gabriela. Next up, Adam Tindle, Raymond James, followed by Gregg Moskowitz, Mizuho. Adam, go ahead.

Adam Tindle
Analyst, Raymond James & Associates, Inc.

Q

Okay. Thanks. Good afternoon. I want to start by just acknowledging the progression in operating margin is really impressive and commitment to that being a baseline is a really important point. If I'm thinking about tomorrow, some of the distracting questions that might come up would be around product revenue. I think you grew 10% year-over-year in Q3 and you had previously guided the fiscal year to 10%. But if I saw on the slides correctly, I think you're now raising that to 15% to 16%. So what's driving that increase in product revenue and the acceleration in Q4 despite the cautionary comments? And anything we can think about in terms of puts and takes to product revenue as we think about fiscal 2024 so we don't get ahead of ourselves. Thanks.

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

Adam, I think there's two parts to it. One is, as you will appreciate, we highlighted that software has become 30% of our product revenue. So whilst when you book a hardware firewall, you get a dollar-for-dollar for revenue. In software you don't get a dollar-for-dollar for revenue. There's some part of an amortized value we get from our software firewalls and some part of our SDWAN which becomes part of our product revenue. So we have to run harder on billings to be able to deliver product revenue in the context of software.

But as I mentioned, our virtual firewalls grew at 55% this quarter. They grew at 40% for the year so far. This is a tailwind we had not expected. At the same time the hardware, as I mentioned, is not as strong as we'd expected. So they balance each other out, but the balance is in favor of software for now coming off a low base of last year. So as a result, we have been able to improve our product revenue guidance. Obviously, it comes as a cost of services revenue because some of our software has now had to work triple time to be able to deliver product revenue.

So I think that's the context in which you should think about it overall where there has been a draw from one side and a partial give on the other side. On the product revenue, however, given our RPO is growing way ahead of revenue, it just means we are saving up a lot of revenue for a future rainy day. Does that sound about right financially? Savings revenue for a rainy day.

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

Yeah. No. That's quite right. The only other thing that I would maybe just add to that is simply the supply chain dynamics that Nikesh talked about in his remarks. I mean that does have some factors but we really have been able to with a world-class team get ahead of the supply chain reality. And so that may explain some of the variability you're seeing, Adam.

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

Great. Thank you, Adam. Next up, Gregg Moskowitz from Mizuho followed by Shaul Eyal from Cowen.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC
Q

Thank you. Can you hear me?

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

Yes.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC
Q

All right. I have a follow up for Lee or Nikesh on generative AI. So your comments on LLMs were helpful. But do you think gen AI will tilt the scales in favor of Palo Alto and perhaps some other security vendors over time? Or is it ultimately more likely to cause an even faster game of cat and mouse between the vendors and the attackers? How do you see this playing out?

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

Well, I think, look, first and foremost, the benefit of generative AI so far is twofold, right. One is in its ability to summarize data and give you access to information much faster. Can I imagine a sales rep at Palo Alto having access at their fingertips with about all Palo Alto information? Of course I can. Can I imagine my customer support people having access to amazing amounts of information that's at the tip of their fingers so they can answer customer questions much faster? Can I imagine showcasing that information directly to my customers as you see in the industry now suddenly, a plethora of co-pilots start to emerge in every product. So I think that is going to become an obvious benefit of generative AI.

Now don't forget, it relies on one principle called having a lot of data. It's very important that whether you're using it for sharing your own information from your customers to your customers, you need all that data. You have to clean all your data processes and have that. Secondly, if you're in the security business, it definitely helps if you have the largest data lake in the world of security data. So from that perspective, I think it favors the people who have a lot of data already as part of their strategy, and they've built a business in the back of a data-led strategy. I think not just specific to security. In any industry, especially consumer Internet, if you've been a UI company, you have something to worry about. And if you're a travel booking operator or something that just takes other people's data and makes a better UI, you have something to worry about. So I think from that perspective it favors companies which have tremendous amounts of data.

I think the second thing that's also important to understand, if I have 14,000 people and I spend thousands of billions of dollars in customer support or more, there's leverage. I can go spend $30 million, $40 million, $50 million deploying LLM and saving half my cost. If you're running a small company and your entire cost is $50 million, it probably doesn't behoove you to go out and create an LLM-based generative AI project to go out and pay and take away $20 million of cost. So I think it also benefits people of scale who are able to drive efficiencies using generative AI across their enterprise, allowing them to grow their business much faster with limited resources. Does that help?

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC
Q

It does. Thanks, Nikesh.

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

Great. Great. Thanks, Gregg. And Shaul Eyal from Cowen our last question.

Shaul Eyal
Analyst, Cowen & Co. LLC
Q

Thank you for that. Good afternoon. Congrats, team. Nikesh, I want to go back actually. Brad was asking about M&A. I want to ask about the competitive landscape but specifically with a focus maybe on the CNAPP front. So my question is, how do you think about it? Any change? Do you think that the product right now, as it stands, is comprehensive? Or anything that you might be thinking of maybe augmenting specifically on the CNAPP front? Thank you for that.

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

A

We have by far the most comprehensive Cloud Native Application Protection Platform there is. That doesn't mean that we do everything, but we do far more than any other solution out there. There is tremendous amount of focus on delivering capabilities that we've been building internally, organically amongst the team. We've seen the most recent one we delivered with Secrets Scanning just a few months ago. We've seen very good early adoption of that. At the same time, we're also delivering on the latest acquisition of Cider Security where we expect that to become a new module within the next couple months, available to all of our Prisma Cloud customers.

And so Nikesh talked about how we've leveraged M&A in the past to help build some of the key technology areas of Prisma Cloud, which is absolutely true. We have also shown an ability to deliver new cloud security capabilities organically and be very successful at that, and right now feel good about the balance of both those capabilities and how we're bringing them together and how we continue to deliver new innovations.

Shaul Eyal
Analyst, Cowen & Co. LLC

Q

Thank you.

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

Thank you for the question. With that, we'll conclude the Q&A portion of the call, and I'd like to pass it back to Nikesh for his closing remarks.

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

Well, thank you very much again, everybody, for joining us. We look forward to seeing many of you at the upcoming investor events.

I also want to once again take an opportunity to thank all of our employees who work very hard in a very dedicated fashion, as you all know, to help us achieve these results. Not only that, but a big thank you to all of our partners and our customers around the world.

Have a wonderful day. Thank you.

Disclaimer

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

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