18-Aug-2023

Palo Alto Networks, Inc. (PANW)

Q4 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.

Anand Oswal
Senior Vice President & General Manager, Palo Alto Networks, Inc.

Ankur Shah
Senior Vice President & General Manager-Prisma Cloud, Palo Alto Networks, Inc.

Gonen Fink
Senior Vice President-Cortex & Head of Israel R&D Center, Palo Alto Networks, Inc.

William D. Jenkins
President, Palo Alto Networks, Inc.

OTHER PARTICIPANTS

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Saket Kalia
Analyst, Barclays Capital, Inc.

Rob D. Owens
Analyst, Piper Sandler & Co.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC

Brian Essex
Analyst, JPMorgan

Jonathan Ho
Analyst, William Blair & Co. LLC

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Roger Boyd
Analyst, UBS Securities LLC

Michael Turits
Analyst, KeyBanc Capital Markets, Inc.

Patrick Colville
Analyst, Scotia Capital (USA), Inc.

Tal Liani
Analyst, BofA Securities, Inc.

Joseph Gallo
Analyst, Jefferies LLC

Adam C. Borg
Analyst, Stifel, Nicolaus & Co., Inc.

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 Fourth Quarter 2023 Earnings Conference Call. I'm Walter Pritchard, Senior Vice President of Investor Relations and Corporate Development. Please note that this call is being recorded today, Friday, August 18, 2023, at 1:30 Pacific Time.

With me on today's call to discuss fourth quarter results are Nikesh Arora, our Chairman and Chief Executive Officer; and Dipak Golechha, our Chief Financial Officer. Following the Q4 session, we will take questions on our results and the 2024 guidance, with Lee Klarich, our Chief Product Officer, also joining us. We will then continue with the forward-looking portion of our program. For this, Lee, along with several of his product leaders, and BJ Jenkins, our President, will present along with Dipak and Nikesh, with additional Q&A session to follow.

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 to find the fourth quarter 2023 earnings presentation and supplemental information. Following the event, we will post the full set of slides, including the forward-looking portion of our program.

During the course of today's call, we will make forward-looking statements and projections regarding the company's business operations and financial performance. These statements made today are subject to a number of risks and uncertainties that could cause our actual results to differ from these forward-looking statements. Please review our press release and recent SEC filings for a description of these risks and uncertainties. We assume no obligation to update any forward-looking statements made in the presentations today.

We will also refer to non-GAAP financial measures. These measures should not be considered as 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 in the Goldman Sachs Conference on September 7.

With that, I'll now turn the call over to Nikesh.

Nikesh Arora

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

Thank you, Walter, and good afternoon, everyone. Thank you for spending your Friday afternoon, or perhaps, some part of your Friday evening with us. Our choice of Friday has definitely made us the topic du jour these past two weeks and has made for some very interesting reading of all the analyst notes. We apologize to people who are inconvenienced, but as we had mentioned in our press release, we wanted to give ample time to analysts to have one-on-one calls with us over the weekend, and we have a sales conference that kicks off on Sunday, and we want to make sure all of our information was disclosed out there. So again, we apologize for the unique Friday afternoon earnings call, but clearly, we have enjoyed the attention.

Well, let me go and just straightaway dive into our Q4 results. We started off the year focusing on excellence and execution. We've stayed true to that and delivered strong results in Q4, capping off a strong fiscal year 2023, where we met or exceeded our original top line guidance and significantly exceeded our profitability and cash flow guidance. This year indeed required clear focus across our company and we're all proud that our team have delivered throughout the year and especially in Q4.

Our Q4 revenue grew 26%, making our – marking our 12th consecutive quarter of revenue growth north of 20%. Our billings grew 18%, off a very strong 44% growth in Q4 a year ago, and RPO grew 30% ahead of our revenue growth. Our Q4 operating margins expanded by 760 basis points, driving $1.44 in non-GAAP earnings per share, and we achieved 39% adjusted free cash flow margins for the year.

Our performance in Q4 did not come as a surprise to us. We've been investing in our next-generation security portfolio for some time now to position ourselves in a leadership position for the future of the cybersecurity market. It is this next-gen portfolio driving that is our growth transformation and enabling our leverage. Lee and his team will expand on this in the forward-looking portion of our program.

We achieved several important milestones in this quarter, especially in our software and cloud-based businesses this year. Our combined SASE, Cortex and cloud bookings were north of $1 billion in Q4. Our Cortex platform surpassed $1 billion in annual bookings last quarter, and we achieved the same milestone with SASE this quarter. We also exceeded $500 million in Prisma Cloud ARR. These product performances have all contributed to strong growth we continue to enjoy in NGS ARR. Remember that our NGS business is largely a capability new to us in the last five years and is primarily cloud-delivered. This quarter, we added more net new ARR than any other pure play cybersecurity company.

Our platformization is continuing to drive large deal momentum. One way to illustrate the traction of our next-generation security capability across network security, cloud security and SOC automation is to look at the makeup of some of our largest deals. When we deliver best-of-breed products that are also integrated into platforms, we help customers simplify their architectures, lower their cost of ownership and benefit from differentiated cross-platform capabilities. This is a win-win scenario.

8 out of our top 10 deals saw significant contribution from our next-generation security capabilities. Five were essentially next-generation security deals. Here are some examples. One, a large industrial manufacturer signed a transaction with a total value of $45 million. A Prisma Access expansion led the transaction, but the deal also included significant commitments to Prisma Cloud, XSOAR and our IoT security offerings. The customer's success with Prisma Access and our executive level engagement were keys to winning this additional opportunity.

A large professional services firm standardized on Prisma Access in a transaction exceeding $40 million, securing their hundreds of thousands of users. The completeness of our offering, particularly our strong capabilities in private access, differentiated us from the competition. By standardizing on Prisma Access, the customer consolidated legacy security offerings from many competitors to a single solution.

A large retailer also signed a landmark transaction for more than $40 million, led by XSIAM. In this deal, we displaced the incumbent SIEM offering and also added our threat intelligence and attack surface management capabilities.

Rounding out the examples, a large technology service provider chose our XDR and XSIAM capabilities in a transaction worth over $30 million. This deal started as an independent evaluation of replacement for both endpoint security and their SIEM. This is the second quarter in a row where we signed an eight-figure deal that

was driven by our unique capability to provide both XDR and XSIAM, competing against separate competitors in each of these categories. This sample represents the success we see across industries and regions.

As I mentioned, a critical part of our profitable growth formula is selling more to our largest customers. In Q4, we saw larger deals grow faster than our overall business. Notably, we saw the number of deals greater than $20 million grow faster than our deals over $10 million, as our go-to-market motion becomes more and more increasingly successful in selling the platform and building the sort of trusted relationships required to close this quantum of business.

Now for the surprise of this quarter, starting with Cortex, there are a number of things I'm excited about in this business as we ended this year. We launched XSIAM to general availability last October and set an aggressive goal of booking north of $100 million in our first year. The year is not over yet. We have closed out the year achieving $200 million in XSIAM. This is strong validation that our outcome-based value proposition in XSIAM is resonating well with security organizations and also a sign that interest in applying AI to transform security operations is very high. Lee will talk extensively about this in our forward-looking section.

Our customers have told us loud and clear that the legacy products powering their SOCs are no longer working and they need to reduce their mean time to remediation by an order of magnitude. This becomes increasingly important with the new SEC rules detailing that all public companies will be required to report material breaches within four business days.

XSIAM is shaping up to be our fastest-growing offering outside our original next-generation firewall releases. XSIAM transactions are large and long term, which help to further our goal of evolving our customer relationships from vendor to partner.

As excited as we are about the early success of XSIAM, we are also seeing strong growth across the entire family of Cortex products, namely XDR, XSOAR and Xpanse. We crossed the 5,000-customer milestone in Cortex as we continue to gain share in the market and see the opportunities for upsell to the platform. Our average Cortex deal size grew over 50% year-over-year, reflecting our success in cross-Cortex adoption.

Moving on to the next star of the quarter, SASE, SASE continues to become our standout offering. We're seeing strong customer awareness and momentum following our new leadership position in the Gartner SSE Magic Quadrant last quarter. We were recognized this quarter with a leadership position in the Forrester Zero Trust Edge Wave that was published earlier in the week, establishing Palo Alto Networks as a clear industry leader in SASE.

We also have some breaking news on industry recognition. Very excited that Palo Alto Networks has been recognized as the only, I repeat, the only leader in Gartner's first Single Vendor SASE Magic Quadrant just published on Wednesday.

Our recent acceleration in external industry recognition has contributed to customer momentum, and we saw many new customer and large expansion transactions in Q4. This included four transactions over $10 million and many seven-figure deals that span numerous industries and regions.

Not to be left behind, Prisma Cloud went past $500 million in ARR. Our cloud security platform, where we believe all companies will eventually lead to manage security across multiple cloud applications and provide a [indiscernible] (00:09:56) platform, continues to show strength.

Ensuring customers consume our capabilities after committing to the platform is vital. In Q4, we saw steady consumption growth, where credits consumed up by 45%. We're also seeing strong growth in customer adoption of multiple modules. This quarter, we are showing our growth in customers with five modules or more, as it's starting to become a meaningful trend, with customers up 179% year-over-year.

We continue to make significant organic investments in Prisma Cloud and grow the platform through acquisitions. We launched the CI/CD security module last week based on technology from the Cider Security acquisition. This is our 11th module and we continue to have the broadest cloud native application protection platform in the industry, with capabilities spanning our customers' entire code-to-cloud needs. Later on our call, you will get a chance to see our exciting developments and glimpse into our plans for the future.

Finishing where I started, I couldn't be more proud of our performance in Q4 and the year. Our teams helped drive steady performance, enabling us to maintain a strong outlook through macro challenges by focusing on crisply executing our differentiated strategy. We continue to drive platformization and capitalize on the opportunity that changing landscape presents through products like XSIAM. We continue with our go-to-market transformation, for example. We consolidate our SASE sales team into our core a year ago, and we have seen a strong outcome, as you saw, with some large transaction and opportunities across the pipeline. We have continued to not hold back on investing in innovation to ensure we can capture share in a market that constantly presents new opportunities. Lastly, we successfully accelerated some of our efficiency initiatives in the fiscal year as we saw the environment change.

I'll now pass the floor to Dipak to cover the detailed financial results and our 2024 guidance.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you, Nikesh, and good afternoon, everyone. Beyond providing the detailed results this quarter, I also wanted to highlight some additional business insights through the Q4 numbers to help you understand our results and provide context for our go-forward plans.

As Nikesh mentioned, we saw strength across our various metrics, starting with the top line. This was especially true in our NGS ARR and RPO. NGS ARR grew 56%, driven by strength across our portfolio. RPO grew 30%, well ahead of our revenue growth. Broadly, the industry has experienced an increase in deal scrutiny, as well as deal pushouts. The environment has become more challenging this year, and we started telling you about that at the beginning of our fiscal year.

We got ahead of this changing environment by frontloading our sales hiring for the year, training our teams to address the tougher procurement processes, and by having our sales management teams apply additional scrutiny to the pipeline earlier in the quarter. As a result of these efforts, we did not see a significant impact in Q4 from unexpected deal delays.

We did see, however, see two impacts on the top line from the changing environment. First, the rising cost of money has caused customers to hold on to their cash and more frequently seek deferred payments – payment terms. These deferred payment terms are delivered in the form of annual billing plans and through our PANFS financing capability. The percent of bookings that included deferred payments increased approximately 45% year-over-year.

Additionally, the proportion of our bookings that included billing plans more than doubled from Q3 to Q4. This quarter-to-quarter increase negatively impacted our billings as compared to what we forecasted 90 days ago in our guidance.

As we see the shift in billing terms, RPO is becoming a more important leading indicator for our business and it – as it's not impacted by billing terms. As a reminder, RPO represents the booked business we expect to recognize as revenue in future periods. Also, all customers' purchases included in RPO are non-cancelable.

Second, we have seen the market return to a more normalized growth rate in hardware-based firewalls, and I wanted to help further the collective understanding of this. As many of you are aware, there have been several factors that have impacted industry hardware revenue. These include the COVID pandemic, the reopening-related hardware demand catchup, post-COVID supply chain challenges, price changes and backlog release following supply chain easing. Despite these positive and negative fluctuation, there's a relatively consistent level of underlying hardware growth that is in the low to mid-single-digits and we see the industry returning to those levels.

This return to normalized appliance growth is also happening on the backdrop of a broader transition from hardware to software in network security and growth in new security markets. We are unique in being recognized as a leader across different network security form factors, including our software-based VMs and our cloud-delivered SASE. Our firewalls of platform billings growth captures our business across these form factors and grew north of 20% the last three years.

Within this business, we've seen the mix of software increase substantially. Over the medium term, this mix transition to software and cloud and network security, as well as the growth we are seeing in the rest of our next-generation security portfolio, are driving an increase in our recurring revenue mix.

Our platform business model and our focus on efficiency drove significant improvements in operating margin in fiscal year 2023, including 760 basis points of margin expansion in Q4. This higher operating profitability, strong bookings growth and interest income form the baseline for our free cash flow at higher levels, as we achieved 39% adjusted free cash flow margins in fiscal year 2023.

The same dynamic of higher deferred payments plans not only have an impact on our top line but also on our free cash flow. As I mentioned in my discussion of RPO, it is noteworthy that we absorb the impact of the higher mix of bookings with deferred payment terms in Q4 and fiscal year 2023, and we were still able to exceed our cash flow margin target for the year.

If you look on a multiyear basis, we've seen the proportion of our bookings that occur with deferred payment plans increase over four times in the last three years while we grew our free cash flow margins over the same period. As I will talk about when I come back in the second half of the program, this gives us confidence we can maintain our free cash flow margins at a high baseline.

Moving on to the rest of the results, product revenue grew 24% in Q4, driven by the impact we noted last quarter from new go-to-market motions and SKUs that contributed more renewable software revenue to product than in the past. Total subscription and support revenue grew 27%, with subscription revenue of $918 million, growing 31%, and support revenue of $528 million, growing 20%. We saw consistent revenue growth across all our theaters, with the Americas growing 26%, EMEA was also up 26% and JPAC growing 24%.

Gross margin for Q4 of 77.3% increased over 400 basis points year-over-year. This caps off a year where gross margin is expanded by 230 basis points, as we saw our benefit from higher software mix and some scale synergies on a customer support spending. Our operating margin expanded well over 700 basis points in Q4 and over 500 basis points for the year. We saw the higher gross margins and efficiency across our three operating expense lines as we accelerated some of our efficiency initiatives.

As happy as we are about the outcomes here, we're only part of the way through executing on these multi-year efforts. The result of all of this is that we continue to see strong non-GAAP EPS growth due to substantial operating leverage, which also translated to strength in GAAP EPS, which more than doubled quarter-to-quarter. We are now firmly GAAP profitable, with GAAP net income of over $200 million in the quarter.

Turning to the balance sheet and cash flow statement, we ended Q4 with cash equivalents and investments of $5.4 billion. We had our 2023 convertible note mature on July 1, 2023, and we settled the principal obligation with cash of $1.7 billion. We settled the excess in shares and had previously accounted for these in our non-GAAP diluted shares outstanding. Q4 cash flow from operations was $414 million, with total adjusted free cash flow of $388 million this quarter.

Stock-based compensation expense declined by 310 basis points as a percent of revenue sequentially. On a year-over-year basis, stock-based compensation expense was down 220 basis point as a percent of revenue.

I'd like to provide the details of our fiscal year 2024 guidance, as well as guidance for Q1, before we move on to the broader forward-looking section of the presentation, where we will provide context for this guidance and talk about our medium-term targets. Overall, we are pleased we capped a strong year of growth and margins and look forward for more to come.

For the fiscal year 2024, we expect billings to be in the range of $10.9 billion to $11 billion, an increase of 19% to 20%. We expect NGS ARR to be in the range of $3.95 billion to $4 billion, an increase of 34% to 36%. We expect revenue to be in the range of $8.15 billion to $8.2 billion, an increase of 18% to 19%. For fiscal 2024, we expect operating margins to be in the range of 25% to 25.5%. We expect non-GAAP EPS to be in the range of $5.27 to $5.40, an increase of 19% to 22%, and we expect adjusted free cash flow margin to be 37% to 38%.

For the first fiscal quarter of 2024, we expect billings to be in the range of $2.05 billion to $2.08 billion, an increase of 17% to 19%. We expect revenue to be in the range of $1.82 billion to $1.85 billion, an increase of 16% to 18%. We expect non-GAAP EPS to be in the range of $1.15 to $1.17, an increase of 39% to 41%.

Additionally, please consider the following modeling points. First, we expect our non-GAAP tax rate to remain at 22% for the first quarter in fiscal year 2024, subject to the outcome of future tax legislation. We also expect cash taxes in the range of $230 million to $280 million. This is an increase as compared to the $150 million in cash taxes in fiscal year 2023.

For the first quarter, we expect net interest and other income of $50 million to $55 million. We expect first quarter diluted shares outstanding of 336 million to 339 million shares. We expect fiscal year 2024 diluted shares outstanding of 338 million to 343 million shares, and we expect fiscal year 2024 capital expenditures of $160 million to $170 million.

With that, I'd pass it back to Walter to start a short Q&A, covering what we have discussed up to this point. Walter?

QUESTION AND ANSWER SECTION

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

Thanks, Dipak. We'll take about 15 minutes now and we'll have a few questions. We ask that each analyst only ask one question and we ask that we cover the topics that we've focused on thus far. For the first question, we'll go to Matt Hedberg from RBC, with Rob Owens from Piper Sandler on deck. Please go ahead, Matt.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Great. Guys, thanks for taking my questions. Maybe, Nikesh, with you, the macro, good results in the quarter. Wondering if you can just talk a bit more broadly about some of the broader trends that you're seeing. There's been some other – obviously some comments from some competitors that [indiscernible] (00:21:59) go a bit different. But just broad brush strokes on high-level demand trends.

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

I think as I said and as Dipak elaborated, look, it's – interest rates are higher. CFOs are scrutinizing deals, which means you have to be better prepared to answer their question and show the business value that you bring to them with your cybersecurity products. We are lucky that we've been focusing on a platform strategy, so we can usually walk in and say, here, you can consolidate the following five, it doesn't cost you any more but you get a better outcome and you get a modernized security infrastructure. So from that perspective, that strategy of ours is resonating but there is more scrutiny. There are deals that go through multiple levels. There are some that get pushed. There are some that get canceled. And again, you just have to get more at the top of the funnel.

And as Dipak very clearly highlighted that eventually, you end up and there's a conversation about saying, wait, I used to pay you upfront. Now, you need to understand the cost of money and is there a way, either my cost has to be lower from you so I can sort of account for the cost of money, or you got to allow me to pay you later from a deferred plan perspective. So, those are really the two effects.

And I think the biggest – and if I summarize Q4 for us, great execution, there's a lot of demand out there. And the two things which are sort of more different is, one, we saw the hardware sort of cycle start to normalize much faster, and not like we told you so, but we've been very consistent. I think one of you guys actually was kind enough to cut and paste every time we talked about hardware into their note. We've been very consistent that we think underlying hardware growth is at single digits – low-single – low to mid-single digits. So, we've seen that mean reversion. Other than that, honestly, we just got to go out there and get more stricter on execution. That's the outcome from a macro perspective.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Great. [ph] Thanks for answering (00:23:51).

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

Thanks, Matt. Next question [ph] here (00:23:53) from Saket Kalia of Barclays, with Brad Zelnick from Deutsche Bank on deck. Go ahead, Saket.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Okay. Great. Thanks for taking my question here and nice end to the year to the team. Dipak, maybe for you, great to see the free cash flow margin for next year. I think a couple things that we were all thinking about as we model next year were cash taxes and the deferred payment plans that you referenced in your prepared commentary. Of course, the profitability here is well ahead also. But maybe you could just talk us through some of the puts and takes you thought about within that free cash flow margin guide for next year.

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

Yeah. So, I think – thanks for the question, Saket. I think the primary driver really is the stronger profitability, right? So, that's really what underpins a lot of the cash flow confidence. We've also seen benefits of higher interest rates on the cash that we have, right, and that also helps. That's another put and take. But I would say you're right. We've absorbed the additional headwinds from deferred payment terms. We've modeled in the cash taxes. And when you put all the different puts and takes, we feel pretty confident of where we are.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Great. [ph] Thanks (00:25:12).

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

Thank you. Sorry to skip the order there. We're going to go back to Rob Owens at Piper Sandler, and then go to Brad Zelnick at Deutsche Bank. Go ahead, Rob.

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

Thanks, Walter, and Saket's much more interesting than I am. But wanted to build on that question just a little bit relative to deferred payments. And is there discounting when you're doing these multi-year deals? And will we actually see a longer-term economic benefit as people start to move towards annual payments? And I guess given the shift in the portfolio and what you guys are selling, this should be no surprise. So, if you could just comment on if there is a broader economic benefit to kind of moving to annual terms and understand that we'll probably address the mid-term guidance on the next portion of the call.

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

Rob, I'm going to give you a little macro flavor and then Dipak can jump in as well. First of all, your shirts are way better than Saket's. So, don't worry about that.

Look, on the macro front, the part I'm really excited about, that Dipak and his team have basically navigated a significant part of our business into annual billings effectively through these deferred payment plans, right? And we're able to hold our free cash flow in spite of those downward sort of pressure. And we think we're going to keep absorbing some of that as it goes.

In the end, it's an economic argument. It's like there's a cost of money. I can take the money upfront and let the customers get a discount and I can go try and get a return on that cash, or I can let them pay when they're ready to pay and I can extract a better economic outcome in that context.

And I think it's important to understand. Given our portfolio-based approach, our customers, different products lend themselves to different discussion. On cloud, we see a lot more of these shorter duration discussions because cloud is more of a consumptive event. On XSIAM, they want longer deals. They don't want even three-year deals. They don't want five-year deals. They want price locks. So, there also is a counter effect they're worried about inflation.

So if you put it all together, as Dipak said, we're very comfortable with the way we've modeled it. There's definitely levers that go in different directions. And our sort of aspiration and desire and hope is that we keep transitioning seamlessly into more and more annual billings over time while being able to hold these metrics and these outcomes for ourselves.

Dipak?

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

Yeah. No, I think Nikesh mentioned it well. The only comment that I would say is we're probably more focused on the economics of the actual deferred payments versus the upfront. I understand the argument that if you're more of a SaaS business, then you don't have to make as much like discounts to pull the deal through. We haven't really built that in, right? At this stage, we'll see how that goes. We're still going through the transformation.

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

And don't forget, there's still a reasonable part of our business that still has to be paid up front, which is the hardware business.

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

Right. Thank you.

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

Thanks, Rob. We're going to take our last question in this segment from Brad Zelnick at Deutsche Bank. The IR team is available to take questions offline, and we will return at the end of this program to take more questions from you all. Go ahead, Brad.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.
Q

Great. Thank you so much, Walter, and – so many questions to ask, but I'm going to keep it high level. Nikesh, heading next week into Sales Kick-Off, you're going to once again rally the troops to perform even better next year, topping a fantastic fiscal 2023. What are the highest level messages that you're going to focus on to ensure that they really step up their game and can overachieve and do even better next year?

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

A

Brad, So I've worked in sales and interacted with salespeople majority of my life. Salespeople like to win. And I think what has become apparent in fiscal 2023 for our teams is that can – that we can win in each of these categories. They were used to winning in firewalls. I will tell you, our win rates have gone up tremendously in SASE. I mean, we did $1 billion in SASE this past year.

Winning XSIAM has been a phenomenal surprise and a delight to all of us, and literally, I'm telling you what's going to happen on Sunday, every salesperson is going to say I want to be able to sell that product. This product is selling with an average ACV of $1 million. Hasn't happened in security before.

So, I think the – just generating enthusiasm towards all these capabilities and solutions is kind of a key message for our team. There are some structural changes. Like last year, we took the SASE team and merged that with the core team, and you saw the outcome and we managed to do that seamlessly without an impact to our business, in fact, grew faster. We're doing that next year with Cortex. We're taking our Cortex team and making them part of core. That's why Dipak talks about the constant ability to improve operating margins. We've hit sort of scale economics in our business. We've hit scale. Everybody has to do these deals. It's no longer a firewall business. So, our teams want to do cross-product deals.

So the message really is we're winning in major categories, [ph] guard and (00:29:52) win those deals. The message is cross-platform is working for us. The message is you are now empowered and trained to sell everything. And every opportunity, we use the opportunity to tweak certain things which will work better than the other. So I mean honestly, like sorry to drag you out on a Friday afternoon, but I think it's important for a few thousand people next week that we shared all these results with them and we just got caught in the trap of trying to get a board meeting done and do that on Sunday. So here we are on Friday.

But [indiscernible] (00:30:20) if it gives you any comfort, Dipak and me and the team are going to be working all Saturday and Sunday as well.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Awesome. Thank you.

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

A

Thanks, Brad.

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

Thanks, Brad. Thanks, everybody, for your questions. We will come back at the end to do more. We're now going to move to the forward-looking portion of our program and talk about our medium term update.

And with that, I'll pass it back over to Nikesh.

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

Well, that's a wrap on our Q4 results. The reason we wanted to make sure you had the opportunity to enjoy our Friday evening celebrations in the context of a long-term or midterm outlook from us was we wanted make sure that you'd see our FY 2024 guidance in the context of where we believe we are in the next three- to five-year journey.

I think what's important to understand is that over the last five years, the cybersecurity TAM has continued to rise. It's grown at approximately 14% and [indiscernible] (00:31:16) twice the pace at which the IT market has grown. Now, the reasons for that are as we get down these transformations that are going on in the world where we get more and more reliant on e-commerce, as we get more and more reliant on digital transformation movement to the cloud and possibly now with the sort of arrival of AI as a mainstream opportunity, every one of us is trying to make sure we grab that with both hands so we will continue to see the pace of technology spend go sort of up or forward.

Similarly, we're going to see that cybersecurity is going to get more than its fair share of growth. So from an opportunity perspective, from what's going on in the market, we believe the cybersecurity market is robust and will continue to be so in the next three to five years.

Having said that, if you look deeper, there are actually three things going on in that market. One, there are new markets being created. If you look at the last five years, we saw a sort of a surge in this concept called SASE. You saw SASE come on mainstream. Everybody's out there trying to build a SASE business. That's kind of been a big thing.

As we had anticipated and talked about five years ago, cloud continues to become bigger and bigger. As companies go sign up with cloud service providers, they are beginning to go move their applications from on-prem or their hybrid clouds to the public cloud.

Now, what's important to understand is that approximately 80% of the applications in the world are actually homegrown applications which are working in on-prem data centers. As we go forward, we're seeing enterprises take those applications, reimagine them, rewrite them, rearchitect them, and move them to the public cloud.

Now, that work has to be done by 33 million developers around the world which work for these companies. As they write new code, as they put together code by looking at open-source and grabbing stuff from here and there, there is this real opportunity to make sure that that code that is written is written in such a way that is secure, secured by design. So we will continue to see that cloud security part of their market grow. That's a market that's effectively been created the last five years.

Couple that with the arrival of IoT and OT as mainstream opportunities, we've seen even that market has been sort of a new market. Approximately, it's a $30 billion market between those categories which has been built the last five years, driving some of the cybersecurity opportunity.

Outside of that, in the underlying cybersecurity market, we have also noticed that some markets have undergone transformation. We're seeing a large transformation in network security as people try and figure out how much to go in the public cloud, how much to leave on the data center, how much hardware to deploy, how much software to deploy. We're seeing that network security is beginning to evolve from a hardware-only market to effectively a faster growing software part of the network security market. Not just that but we're also seeing is things like SD-WAN, which are part of the networking TAM, are moving into cybersecurity because people want an integrated solution, as a SASE solution between SD-WAN and your security protocol.

So it's interesting. There are markets undergoing inflection like network security. The market of endpoint has gone through huge inflection the last five years. You've seen people go from endpoint protection to EDR and XDR. And you see an explosion. There are about 14 vendors at last count in the EDR/XDR space, but you can see clear leaders emerging, which are down to two or three players in that space and there's a huge inflection going on there.

We think not just there. You're going to see a large inflection in effectively what is a 15-year-old market called SIEM and SOC. That market's been technology that has not been evolved the last 15 years. It's primarily been a reactive technology where if I am breached, I need to figure out what to do and we collect a lot of data and analyze it. That's no longer going to work. The arrival of AI, the need for automation, the need for normalized data is actually going to force that market to inflect. And that's something we'll talk about more, and you saw already in our Q4 results that something like XSIAM, which is targeted to that market, is where the real opportunity is for that inflection to continue for that market to go through its own transformation. Outside of that, there are still about $30-plus billion in sort of steady cybersecurity segments as well as about $80 billion of service which we think will also continue to evolve in the next three to five years.

So with that in mind, I think it's important to think about where we were when we thought about the transformation of Palo Alto Networks five years ago where we said cloud is going to be big, AI is going to be big, and the networks are going to have to start getting reimagined as we go towards the cloud. So effectively, cloud was going to drive the cloud security market and the network transformation and AI and machine learning would have to start helping us do this transformation in the SIEM and SOC market.

Now, what we saw over the last three to five years is we at Palo Alto Networks as well as, to some degree, different players in the industry started to look at the various piece parts of these markets and say, look, these things need to start getting integrated because you can't deliver great security outcomes without these things getting integrated.

So this is a thing. We talked about this. We were told that the market does not need platforms. We were told that integration is not key. Customers can deal with the integration. What we want is best-of-breed products. So we decided we're going to do both. We're going to have phenomenal success of best-of-breed categories. In addition, we're going to make sure our best-of-breed products were integrated.

So in these three TAMs, these three markets of network, cloud, and SOC operation, what happened is you saw these point products which started to get integrated into the larger platform vision we had and we saw the TAM continue to grow because these are all markets which are undergoing transformation or rapid growth. Now, where we are today, we believe this is about $100 billion opportunity across these three platforms. So for us, the opportunity's grown. It's almost gone up two times from five years ago where we believe it's $100 billion market today which allows us to deliver the superior growth you've seen and the continued consolidation of the market that we've had at Palo Alto Networks.

What's even more exciting but in these markets, we'll continue to drive future growth. And you will see that because of the arrival of AI, the need for more real-time autonomous security, these markets will continue to drive opportunity.

In the same [indiscernible] (00:37:20) the last five years, as I said, we have been able to transform Palo Alto Networks to get it to where it is today. A, we actually proved that platforms are relevant and important in the space of cybersecurity. Just imagine, it seems obvious now possibly to many of us but five years ago, we had customers

who had more cybersecurity vendors than they had IT vendors. And was the customer's responsibility to take these vendors, deploy them across their infrastructure, make them work together to deliver security outcomes.

You're expecting 2,000 customers out there in the Global 2000 or possibly tens of thousands of customers having security experts trying to stitch together products made by fast-growth cybersecurity companies which are deeply technical and trying to figure out how to correlate what one vendor saw or one set of alerts is telling you is another. It just seemed like a problem that could not be solved.

But over the last five years, you've seen that starting to stitch these together, starting to take these disparate solutions for security, trying to provide them in a common fabric has actually allowed us to deliver better security outcomes. And we've proven that by doing that in a way that each of those pieces work in a best-of-breed fashion are leading in their own category. However, they are kind of better together in the platform.

So the last three years, the last five years, as we just shared in our Q4 results, we have been able to build a $1 billion business in security operations under Cortex which was zero. We have been able to build $1 billion SASE business in the last 12 months to be able to show that integration across this remote and hybrid network space is actually working. Not only that. We actually built a $500 million ARR cloud security business proving that, again, the ability to stitch across the entire cloud development lifecycle is useful for our customers.

So we think that we've established these platforms are going to be around, are important, and necessary and that is the way of doing security in the future. Not only that. We've also proven that in the last five years that you can teach an old dog new tricks. Palo Alto Networks, which was a single product in one lane, we had the best firewall technology in the world as well as had amazing services that work as a firewall, we have been able to take that and build multiple products across multiple security swim lanes and make them work better together.

And the only way you can do that in security is you have to keep driving innovation. You have to stay at the bleeding edge because you don't need your customers to be at the bleeding edge. It is our responsibility as a security company to make sure we take all the innovation, we distill it, we make it work in an integrated fashion, and deliver it to our customers at the fastest pace possible because the bad actors are not waiting. They're constantly looking for ways to get to our customers, to get to penetrate their infrastructure, and try and figure out how to go extract data from our customers or possibly hold them with ransomware.

So we have taken what was an amazing company in one category and actually built what we like to say is an innovation engine that allows us to stay at the bleeding edge. We've also done that, to be honest, not just by doing it ourselves because the fact that the cybersecurity industry has 3,000 startups out there, which are constantly funded because they're all working in a specialist way to solve a problem which they believe is important for the end customer, we have to be vigilant and make sure that we don't have any issues in either building it for our customers or partnering or acquiring something that's out there that is important as part of the security fabric that we need to build to deliver to our customers.

So as a team, we're really excited that where we are in our sort of juncture today allows us to go forward and build an even better, larger, and a more compelling business for our shareholders. Not only that, to deliver phenomenal security outcomes for our customers across all these categories that we see inflecting as well as categories that we believe will be created the next three to five years.

So with that in mind, if you think about what's our view going forward for the next three to five years or possibly the next decade, I'd say the last five years, we saw that huge sort of technology trends underlying it of cloud and

AI allowed us to create the stitching to build what I would say the building blocks of building world's largest cybersecurity company actually prepares us phenomenally well for what we think lies ahead.

What we think lies ahead is the need for security to stop bad actors mid-flight real-time as it's happening. If you think about security today, the industry is only 30% or 40% real-time. You know a bad URL. You know bad DNS. You know how to stop your customers from something that is bad that we know. What we still aren't good at as an industry is being able to figure out unknowns and stop them before they happen.

To do that requires a fundamentally different way of thinking about security, something we have been sort of leading, having a point of view on. And that is the idea of having stitched products that work from end-to-end. The idea that as something is happening, you're able to analyze it real-time on the fly and understand that's good or bad. It is reducing the noise of security in the industry by eliminating all these superfluous alerts or bad signal to noise ratio. So to get that right or to get security right, we will have to be more and more real-time as an industry.

Now, we sit at a point where everybody's talking about AI and actually that is the solution. The solution is to make sure you ingest large amounts of data, you analyze them on the fly, and you're able to deliver superior security outcomes, something we talked about just in our Q4 earnings call right before this. You saw that everything we're doing in XSIAM is driving us to that vision, but that's not enough. You have to make sure every platform that we have continues to grow and continues to get more and more ubiquitous with our customers, at the same time also stitches these things together.

So we believe in the next 5 to 10 years, we're going to see this shift, which is going to be palpable. It is going to be big. It's going to be understandable where we have to become more and more real-time. It'll no longer be about putting a bunch of sensors and thinking about hygiene and security policies. It'll be about how do you stop a bad act and we'll talk more about this because today, the mean time to fix a bad act, as we've talked to you about in our earnings, is four to six days. That's not acceptable. This thing will have to go down to minutes and near real-time. So that's a big shift we see that's going to drive a lot of the innovation in our industry, that's going to drive a lot of our strategy and our vision because we think we're on our way to be able to deliver that future to our customers as the world's largest cybersecurity company.

In that context, we talked about those three categories. We think those three categories are going to continue to become bigger and if you look at it, the biggest opportunity is that big green circle of security operations and automation because we think the current paradigm is broken. The current paradigm is a reactive security paradigm. It's a paradigm which says let's hire 3 more million people to solve security problems. No, I don't think that's going to solve the problem. What's going to solve the problem is let's collect good data. Let's analyze good data. Let's find out the anomalous behavior. Let's block it while it's happening so our customers have a better security outcome.

I think that's where we're going to be going and we're going to have a phenomenal opportunity at Palo Alto Networks to go ahead and address a $200 billion market which is primarily going to be a software-based market which has its own benefits across the board because it's a lower cost of ownership for our customers, lower cost of integration for our customers, it's easy for us to go deploy and keep our customers all at what is the best and current sort of best-in-class capability so a future that is driven by software capability, a future that's driven by software solutions and security, and a future which has integration as part of it as a key tenet with the objective of delivering a real-time autonomous security outcome.

So that's where we think the world is going. That's where we'd like to be and we think we're best positioned in the industry to be able to deliver that future. Not only that, to deliver great security outcomes to our customers.

So with that in mind, how are we going to do this? What are we going to do in the next three years? How is that going to translate into numbers that are loved by our shareholders? So it is really the five things. Part of it's something which we've been doing and some things we're going to have to keep pivoting harder.

For example, one, we want to maintain this notion of being an evergreen innovation company. Our biggest insight is that if you want to lead in cybersecurity, you always have to be on the bleeding edge because the bad actors are. You always have to be scanning the market, understanding where the world is going where technology is going to see what potential security risks are going to get created in the adoption of that technology, in the deployment of that technology to make sure we're ahead of the curve. And we start delivering security by design as in we're not going to come in and try and bolt it on afterwards as our customers have been through the transformation is to work with them and better our architectures with our customers. As they go through their innovation journey, we're in lockstep with them delivering security innovation.

I think the second part which we talked about is we want to make sure that our platforms which are now deployed in sort of different stages or different amount of sort of capacities of customers, they become ubiquitous. We want to make sure that our customers have wall-to-wall platforms that allow them to look at it as a data problem, as an AI problem, not have to stitch our platform with five other security solutions out there and trying to build their own outcome because it's impossible for every customer to go to a secure integration by themselves.

I think the best analogy I can come up with, I think in the next decade, we will see sort of a standard platform for security out there, just the way we've seen platforms in CRM or we've seen platforms in HR, as you've seen platforms in financial sort of software. We think it's time that in the next decade, we will see a security platform in our future which just works for our customers and the customers are not spending time integrating multiple vendors trying to stitch their own. I just think that's the only way we're going to get to the future that we need for real-time and AI-based security.

Third, the topic du jour, everybody's talking about AI. We're talking about AI. We're not only talking about it. We will demonstrate that we could deliver security outcomes and the vision and the future that security needs using AI across Palo Alto Networks. And we'll talk more about that.

That's great. We can build amazing products but also as a company for our shareholders, we have to make sure that we can deliver all this innovation to our customers both effectively and, two, we have to make sure that it's easy to consume and deploy for our customers. And we're going to have to make changes as we go forward on how we actually go deliver all the wonderful capability to all of our customers not just by ourself but actually working together with some of the bleeding edge partners in the world who are, in this journey, our partners are delivering these great security outcomes for our customers.

Last but not the least and one of the key things is we cannot do this unless and until our employees are fully bought into our strategy, our vision, feel excited every day to come to work and deliver a better security outcome for our customers to make them secure and be their cybersecurity partner of choice. So with that, let's take a quick look into each of these categories, see how we're going to get there.

It now sort of boils down to these five key strategic sort of requirements or directions from our perspective: innovation, continued platformization, leveraging AI, continue to transform our go-to-market capabilities, and last but not the least again is to make sure our team is along with us every step of the way.

So getting into the topic of innovation, I think very proud of the track record we have so far. We've gone from 13 products/acquisition that we've integrated in 2019 to delivering 74 in 2023. It sounds like a lot but actually, these 74 are delivered in an integrated fashion. So it actually improves the efficiency of security for our customer. It actually makes usability better. It actually makes it much easier for us to deliver security outcomes, so really excited about that.

I think this whole AI revolution that we're undergoing or we're looking at, witnessing, is going to require us to keep investing, looking once again as to what capability AI is going to deliver across all of our products because we do collect the world's most amount of security data so we will keep driving innovation by underpinning more and more machine learning and AI under our platforms. We'll keep looking at how to deliver more capability with the sensors that we have out there with our customers from innovation perspective.

We've talked about this. We are happy to make sure that we deliver innovation and security outcomes to our customers. It does not all have to be invented at Palo Alto. We will constantly keep scanning the market to make sure that there's something out there that our customers need to get and somebody else is doing really well. It's our job to make sure we partner, collaborate, integrate or acquire to deliver the outcome that the customer needs from an innovation perspective.

And last but not the least, being at the bleeding edge of security, being one of the largest players, it is our responsibility to make sure we're looking at all-new technologies to see how they're going to impact our customers and their estates, whether it's quantum, whether it's AI because there is a dark side to AI. It's our job working with our partners and the industry to make sure we deliver innovation in how to protect against AI getting abused or misused in the market. So I strongly believe for us to deliver on the next three- to five-year vision at Palo Alto Networks, we are going to have to continue to be an evergreen innovation company, which I think will give this company longevity and sustainability forever in the future in being the leader in cybersecurity.

We talked about platformization or you've heard that word. You will keep hearing it for the next sort of 45 minutes from our team because we believe that's the way to deliver security. It's resonating with our customers. Our customers are seeing it. My team's going to show you some amazing UI. I think you're going to start seeing not only just we're talking about this sort of the next level of platformization. You will start seeing right after me how we're actually bringing it to life.

So I cannot be more excited about some of the work we're doing on the product side, stuff that we haven't shown anybody yet. You are going to see it today because it's important for us not just to talk about it, be able to show you how we're going to deliver. So you will see a next level of integration and how we can deliver security outcomes. You'll see sneak peaks into how we're going to leverage AI Copilot in each of our products to create the simplicity and usability that security has not had, to be honest, so far.

So I couldn't be more excited about how our teams are going to keep driving more and more platformization, more and more integration where things of integrating best-of-breed vendors as sort of DIY or do-it-yourself or do it at home is going to be a thing of the past.

So moving on to leveraging AI, I talked about this. But again, clearly, there's no Analyst Day out there today that you cannot – you must talk about AI. So I think the reason's different for us. As a security company, we have always focused on figuring out how to leverage data. We have north of 100 machine learning models that run today at Palo Alto Networks across our products, so this is not new news.

But the way I think about it is let's call all of that precision AI. That's AI where I cannot afford for it to be wrong. If it's wrong, lives matter. If it's wrong, ransomware happens. If it's wrong, bad actors get in. So we have to be right 100% of the time and to me, that's the definition of precision AI. And to deliver that future, we have to build a lot of our own models, we have to train them, we have to collect first-party data, we have to understand the data.

Today, we collect approximately 5 petabytes of data. Yes, 5 petabytes of data on behalf of our customers and analyze it for them to make sure we can separate signal from noise and take that signal and go create security outcomes for our customers. We stop 1.5 million net new attacks every day across our 60,000 customers so we know how to use AI and we believe we're uniquely positioned in the industry given our presence in endpoints, our presence in firewalls, our presence in the cloud, our presence across the entire network security stack to be able to deliver those AI-based outcomes to our customers.

And we're doubling down. We're quadrupling down to make sure that precision AI is deployed across every product at Palo Alto and we open up the flood gates of collecting good data with our customers for them to give them better security because we think that is the way we're going to solve this problem to get to real-time security.

But let's not underestimate the opportunity generative AI puts in front of us. On a very personal basis, I believe generative AI is amazing for data summarization, for natural language interaction, for doing all the things where there was an information decay between our products and our customers. We build great products. By the time they get to our customers, there's a lot of translation that happens between our product developers and the customer and sometimes, the breaches happen because the customers don't fully understand our product because they cannot configure them right.

All those things can be eliminated if we can implement generative AI effectively through our products. So our customers can interact with our products in natural language. They don't have to have complex security understanding to operate our products. They don't have to have complex security understanding to fix a problem. We can fix all of that if we, in our company, learn how to deliver generative AI-based interfaces, generative AI-based outcomes through our products. And you know what? Our teams are going to show you a glimpse of that. We have been working diligently over the last five months across the board at Palo Alto Networks and I couldn't be more excited about some of the stuff that you're going to see just after this from our product teams to give you a sneak peak.

At the same time, we're going to do it in a deliberate fashion. We're going to crawl, walk, run. We think we are on the right path. We're going to work in lockstep with the industry. We have people analyzing and working with almost everybody out there. We understand where the best-in-class LLM activity is. We understand where technology is. We also understand where it might be going the next three to six months.

So all I can say is that I think the combination of precision AI and generative AI is going to fundamentally change the way security outcomes are delivered to our customers because it'll take away the complexity. It'll take away the confusion, the sort of usability problems that you have with security and it'll start helping deliver great outcomes to our customers. I think it's just going to make our platforms amazing as we go forward.

On the go-to-market side, in the last five years, we have done a phenomenal job, I think, of building the products that our customers need yet we have to make sure that every customer understands our capability, every customer has a roadmap with us where we can take them to deliver real-time security outcomes. For that, we need to upscale our team in some areas, which we have been doing very effectively. As you saw, our team was able to deliver some amazing results for Q4, and I think we're going to keep doing that.

We are going to go from being just a security vendor to being a solution partner. For that, we have to work harder with many players out there which is something we've geared up to do and we're having some amazing early success. We've got to figure out how to institutionalize that capability at Palo Alto Networks, and that's something BJ and his team are going to focus very effectively on in the next three to five years.

Not just that. As I said, we need to figure out how to deliver architectural outcomes to our customers. Our customers are tired of spending too much money on cybersecurity and ending up with the same mess and saying, wait, my security outcomes aren't getting much better but I seem to be spending more money. It's important for us to work with every one of them to deliver those capabilities in an architectural way so they understand the long-term roadmap because I think it's fair to say that where we are today is not where we were five years ago. I think we have enough confidence in our customers to partner with us for the long-term because they believe we're going to be around. We're going to be an evergreen cybersecurity company.

And last but not the least, I think it's very important. As part of our go-to-market efforts, we have a large team that delivers customer delight. Well, I just think we're about to see a step change in customer delight with the application of generative AI. Again, we've been working really hard. You'll see a bit of a glimpse of that in some of the things the teams are going to show you and over the next possibly three, six, nine months, you will see more and more capability delivered to our customers using that generative AI framework or predictive AI or precision AI framework. I think in the next three to five years, that is going to fundamentally change what Palo Alto is able to do out there in the market.

And, as I said, you cannot do this without the best people. Our employer brand has become phenomenal in the last five years. As we continue to deliver great innovation, great outcomes, people want to come work at Palo Alto Networks. People want to be part of the success of being the cybersecurity partner of choice for our customers.

So we can only do this, we can only deliver our strategy if you have the best team. We continue to track the best. We continue to empower them. We continue to make sure that they can deliver great outcomes for our customers. We plan to keep doing that over the next three to five years because we believe this is a mission-driven opportunity. It's an opportunity that allows us to make the world a better place by making sure that our customers can be secure.

So, as I said, you will notice the next three to five years we will continue to transform Palo Alto Networks from where we are to where we would like to be. We will continue to focus on the demand function at the top. We believe the market is continuing to inflect, as I said, in the area of security operations. It's highly likely that some of the other steady areas are going to see some inflection as well.

We're going to continue to relentlessly innovate and keep making our platforms more ubiquitous. We're going to make sure that we can deliver the amplification from our go-to-market teams and also we're going to make sure that we have the best team in the industry to deliver solutions to our customers.

I couldn't be more excited about the prospects of Palo Alto Networks. I couldn't be more excited that we are seeing tremendous success in our software-driven capabilities. I think we are going to continue to be able to transform this company from where we started as a hardware vendor to a software-delivered security with real-time security outcomes. And I believe we will continue to be the best cybersecurity partner of choice for our customers.

With that, I'm going to hand over to Lee because he's going to show you some really cool stuff which is hopefully going to excite you about our ability to deliver the future we've talked about.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Thank you, Nikesh. Now, in a second, we're going to go into more detail on our three leading platforms. But first, I want to share some context. After all, we're a cybersecurity company. What's happening in the threat landscape? And I'll just give you the really obvious answer. It's bad. The threat landscape is intensifying, $8 trillion of cost due to cybercrime. Attackers are becoming very sophisticated with the tools they use, whether that's automation, attacking the supply chain, et cetera. And just the sheer volume is off the charts, growing about 20x since 2011 to over 1 billion new malicious programs. This is incredible. So clearly, that is a challenge but it's even more challenging than that.

It wasn't that long ago when it took an attacker on average about 44 days from initial compromise to exfiltration. Now, 44 days is basically the time period that a organization would have to detect, disrupt, and potentially prevent the breach from happening. So when 44 days goes down to hours, which is what we're now starting to see, that is a huge problem. That requires a very different approach but on average, the industry is able to respond and remediate attacks in about six days. That doesn't work and even more challenging now with the SEC new rules of being able to disclose within four days, none of the math adds up.

Now, before we get comfortable in just solving these problems, there's one more challenge coming. Attackers have recognized the power of AI just as much as everyone else has recognized the power of AI to do good things, whether it's FraudGPT or WormGPT or other uses of AI, it is clear this is going to become the next major tool used by attackers to launch more attacks, more sophisticated attacks, and faster attacks.

So we have to innovate and we recognize that. Palo Alto Networks was built for innovation from day one and today, we have over 4,400 product engineering and other experts that are building and driving innovation. And you see just how fast we've ramped that over the last several years, in part by being able to scale our organization across three main R&D centers in the world.

In addition to this organic innovation engine we've built, we look at about 250 private companies every year to identify the absolute best teams, the absolute best technology that could become part of Palo Alto Networks in order to further drive our innovation engine. And we combine these two together and we'll continue to combine them together to have the best innovation capability.

And then we combine that with AI. We recognized early how important AI would be to our innovation and over the last several years, we have been infusing AI into our products in very unique ways to solve very challenging problems that only AI can. And from this foundation, we're only going to do more and better. We're going to accelerate our pace of innovation even further. We're going to leverage our proven playbook around M&A to be able to augment what we do organically. And we are going to take our capabilities in AI and turn that into an AI-first company.

And why I'm so confident in our ability to leverage AI is we've built the right data foundation. We've combined that with the right architecture and we've leveraged an amazing set of expertise across all of that. We collect more data per customer than anyone else, security data, relevant data for AI. We combine that with an architecture that over the last several years, we've been migrating every product into a cloud-based architecture because we know that that sets us up to use AI in everything we do. And today, I have a team of over 150 AI experts that I can leverage across all three of our platforms to identify and drive even more AI capabilities and innovation. That's how we do innovation.

How the industry does innovation is very different. The industry tends to look at this in the context of point products. Every time there's a new need, there is a new point product. This leads to incredible complexity for end customers. Think about having to stitch all of this together.

Now, it does create a large security market of about $210 billion but it means that there's an incredible opportunity for disruption and for a disruptive and innovative approach, which is why we've taken our platform-oriented approach because we recognize that the only way to achieve the real-time security outcomes that our customers need is by integrating natively all of those capabilities into a set of very focused platforms around zero trust, code-to-cloud, and security operations.

In a moment, we'll go into detail on that. But last and certainly not least point, not all platforms are created equally. I shared with you how we think about innovation because that is so fundamental to the outcomes of our platforms. In addition to that, our platforms are designed to be as comprehensive as possible. It doesn't mean we do everything, but it means that we do all of the core set of capabilities necessary such that we can then selectively integrate and enable third-party technology to complement the platforms.

Everything we do is integrated. It's designed to solve hard problems through integration that cannot otherwise be solved with point products and that combination enables our platforms to be real-time and enable real-time security outcomes for our customers.

So with that, let's start our first deep dive with our Zero Trust Platform. It's very clear in the network security market what's happening. The point product approach that we've been fighting for so long as a company is getting harder and harder to sustain. There's more technologies, more capabilities needed. Those capabilities are needed across a broader attack surface with the advent of hybrid cloud and hybrid work. The only way to solve this is with a platform and we're going to share that in a second.

In addition, the next set of trends is going to further propel the need for platformization. As passwordless becomes common, as quantum becomes common, as BYOD becomes enabled across enterprises, all of these, there's going to be a decision. Do you want to try to enable them across 25 and 30 different stand-alone point products or do you want to enable them in a single platform? The answer is obvious and clear. And that is why we are well-positioned to take advantage of the opportunity in front of us across all of network security with our Zero Trust Platform.

And to go into more detail is Anand Oswal, leader of our network security Zero Trust Platform team. Anand?

Anand Oswal

Senior Vice President & General Manager, Palo Alto Networks, Inc.

Thank you, Lee. Before I talk about network security, let me first talk about the evolution of network security. Today, network security has become increasingly complex. In the past, when users were predominantly in the office and applications in the data center, network security was delivered by a centralized firewall. Data center virtualization and migration to the cloud required inspection of traffic moving to the cloud and many organizations had software firewalls. And with the hybrid workforce and protecting remote branches, many enterprises deployed a cloud-delivered stack, SASE.

As you can see, many organizations today have three distinct and disparate stacks. This leads to complexity of architecture, poor operational experience, inconsistent security, and poor user experience. What if you could take a radically different and new approach, ensuring that any user across any location accessing any application and data is secured by unified security stack, which means we are one platform with a set of security services that

ensure that users across all locations have consistent user experience and administrators can now author policies in a centralized manner?

This is enterprise-wide zero trust. Over the last five years, we've developed a Zero Trust Platform with best-in-class products and has three key components. First, network security [ph] enforcing (01:09:04) points: hardware firewalls, software firewalls, and cloud-delivered SASE. Second, cloud-delivered security services that run consistently across all form factors of network security; and management that provides configuration, writing of policies, monitoring and analytics. And each of these three components ensure that we can provide our customers near real-time security, better operational outcomes, and a simplified and consistent user experience.

Let's now talk about the components of the platform. First, the network security [ph] enforcing (01:09:41) points, the foundations: hardware firewalls, software firewalls, and SASE. We're the leader in next generation firewall now for over a decade, a Gartner Magic Quadrant leader 11 times, and we're the only vendor that's a leader in both SSE and SD-WAN that make up the SASE market. We're also a leader in Zero Trust.

Next, let's talk about cloud-delivered security services. Over the years, as Lee mentioned, the attackers have become more and more sophisticated. The old approach of signatures and databases is not working. We're working on using AI and the power of machine-learning to ensure that we can provide our customers with protections against attacks that they have never seen before and ensuring that we can provide near real-time security. We've also expanded from three services five years ago to seven, ensuring our customers can consolidate point products onto the platform.

In addition, we've developed new services like ADEM and AIOps. ADEM, or autonomous digital experience management, provides customers segment-by-segment visibility from user to application, helping them understand exactly what's going on at every segment along the way. And with AI operations, we can automate many of the complex tasks for customers, ensure that they're using security with best practices, configuration with best practices, and ensuring that we are able to predict things that [ph] they may not have (01:11:10) seen before.

Now, as you can see, we've had some great success with different capabilities of our platform. However, if you think about the market, hardware firewalls to secure data centers and campuses, software firewalls to secure cloud networks, and SASE to secure hybrid works and remote branches, these for the most part have acted as three distinct markets, and customers for the most part have made independent decisions. I believe we're now at an inflection point. With unified management across the entire network security estate, we will change the way how customers buy, how customers deploy, and how customers operate network security.

Let me now show you a glimpse of our unified management, which I'm really excited about. As you can see, we have unprecedented visibility here. Users can be anywhere, in campuses, in branches, remote workers on the go, and applications that are sitting everywhere, data centers, public cloud, SaaS, and traffic flowing to all the enforcement points, hardware firewalls, software firewalls and SASE. And we have a complete comprehensive view of all the threats in the entire network security estate, the data risks, the posture and the experience.

Now, the tech landscape is constantly changing, and we always have new vulnerabilities that show up and are published often. And many times, network administrators want to know exactly what happens for a particular vulnerability. Is the enterprise affected by it or not? Now with this unified management, we can easily search for a given vulnerability. And once we understand, like in this case, [ph] that we have compromise (01:12:54) by this vulnerability, with a single click, we can get remediations of best practices and make sure that we can apply these best practices across the entire network security estate, which means our hardware firewalls, our software firewalls and Prisma SASE. That's the power of having complete end-to-end visibility of an entire estate.

Now, let me talk to you about our network security copilot. With the power of generative AI, we're ensuring that customers can use our platform to the best of its capabilities, optimizing security, optimizing configuration and optimizing their operations. This is what you'll see when you come to the copilot. As you can see, it'll tell you all the activity that happened in the last 24 hours.

And now, as you can see, we have 140,000 users that have a good experience, but over 10,000 users have a degraded experience. Now rather than point and click to understand what's going on, we can engage with the copilot with natural language and ask the copilot exactly what's happening for those 10,000 users.

And behind the scenes, the power of AI and ML and getting data from all sources, endpoint, cloud identity engine, applications, network enforcement points, we can tell the customer that the users are having degraded experience accessing a [ph] Jira (01:14:15) application. Not only that, we can also give root cause which is because their authorization failures, open [ph] an ITSM ticket (01:14:22) on their behalf with all the relevant information.

Let's take an example next about a network administrator wanting to know exactly what are the risky applications being accessed in the organization. Again, you're going through all the enforcement points, hardware firewalls, software firewall, and SASE. We can give a summarized view of all the six risky applications in this case.

Now once you know those applications, the next step would be what is the policy I need to apply to block access to this key application? And using best practices, we're able to give them the right policy configuration, as the customer deliver the policy changes or apply them. And once they apply them, it's applied across all the enforcement points, making sure the customer is now protected.

As you can see with the power of the unified management, with the power of the copilot, we're changing the way network security is deployed, operated, on a managed, on an ongoing basis. Super exciting.

To wrap things up, we have over 1,700 customers today using our platform. And over the next few years we expect many more customers to use the platform to get the power of Zero Trust, to get the power of ensuring that they have consistency across the entire security estate, to get unprecedented visibility.

At the same time, we've seen customers use and adopt more of our security services. In the last two years, that number has increased and we continue to see a trend, customers consolidating their point products onto the platform, to make sure that they get the network effect of data and simplify their operations.

In summary, Zero Trust can only be delivered through a platform-centric approach. It's very hard to do it with point products and disparate solutions. Customers will continue to integrate more and more of the services onto the platform, and we'll continue to give a delightful experience to our customers, the power of AI.

With that back over to you, Lee.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Thank you, Anand. So clearly, huge opportunity in network security with the Zero Trust platform. Now turning your attention to the cloud.

Cloud is just absolutely gone through an incredible transformation. Today, there's over 500 million cloud-native applications deployed. There's 33 million developers that are constantly pushing new capabilities and new applications. Nearly all enterprises are multi-cloud. That is just an amazing starting point when you think about what is going on.

And at the same time, there's a tremendous amount of innovation happening because of the cloud and a lot of it's being driven through the ability to leverage open-source, that's being combined with custom code, that's being combined with infrastructures code. All of that just enables this speed, this dynamic nature of the cloud, and it all needs to be secured.

And very much like the rest of enterprise cybersecurity, the industry approach has been a whole bunch of point products that customers are somehow expected to stitch together. We have a different approach. We believe that all of these capabilities should be modules natively integrated and delivered in a platform. And when we get this right, we can not only secure in real-time but we can then fix at-source so the issue doesn't happen again.

And to go into more details on how we're able to achieve that is Ankur Shah, leader of our Prisma Cloud code-to-cloud platform. Ankur?

Ankur Shah

Senior Vice President & General Manager-Prisma Cloud, Palo Alto Networks, Inc.

Thanks, Lee. Like Lee mentioned, we live in an app economy. The average enterprise today uses over 100 application, some for commercial and some for internal use. With AI-led code development, I expect this trend to continue.

Before we talk about securing the apps, first let's talk about how these applications are assembled. In the code phase, some custom code, a whole bunch of open-source code gets deployed using infrastructure as code. And ultimately, it moves through the pipeline, goes into the run time and construct what we call the application.

The key thing to note here is that everything that happens in code phase gets multiplied in cloud, a single infrastructure [ph] that's coded on open-source (01:18:39) component can get deployed across hundreds of thousands of workloads and application component.

What is true for infrastructure in the application layer is also true for the security risk. A risk like an open-source vulnerability, secret, pipeline risk introduced in the code phase gets multiplied in the run time where now you have hundreds of thousands of containers and application components running that risk. The attackers has more ways than ever before to exploit this risk and cause a data breach.

Now there are two approaches to solving this problem. One approach is what the industry has always done, which is to have a point product per problem. In the code phase, there are about half a dozen different tools to scan security posture. In the infrastructure layer, you have yet another set of tools. And finally, in the run time, you have tools for cloud worker protection, network security, and application security.

Now, this is not the right approach to solving this problem for two reasons. Number one, each of those tools lack the context so the customers have to stitch all of that together. And the second thing is, like Lee described, there are 33 million developers and a really few security professionals who understand code and cloud.

This is a battle that the security team simply can't win with this specific approach. We believe there's a better approach, and that's the approach that we have been steadfast in executing over the last four years, and that is

an integrated code-to-cloud platform approach that can help customers prevent risks and breaches in near-real-time. Prisma Cloud does that today by scanning security vulnerabilities at each phase of the application lifecycle and also have run time protection to prevent breaches in run time.

Our strategy is resonating well with the customers and analyst community across different component parts, as well as the entirety of the platform. Typical customers start their journey in the infrastructure layer, where we have now today 68% of the customers where we're securing over 4 billion cloud assets.

Then, they shift left where they want to prevent the risk from happening to begin with, where we have today 20% of our customers, and we're today scanning millions of code assets. And finally, customers want [ph] defense in depth (01:21:03) and they want active prevention and protection technology in the cloud run time should a bad actor cause a data breach, where today we have 54% of the customers where we're scanning 13 million-plus containers.

Let's see the entirety of the Prisma Cloud platform with a quick demo. What you see here is a code-to-cloud dashboard that gives the security practitioners visibility across the entire application pipeline. What you see here is, as the code assets and the cloud assets are growing, so are the security risk. For example, in the code phase, you're seeing a whole bunch of security risk that Prisma Cloud has already scanned. The typical enterprise uses multiple tools just to do the security of the code. And on the cloud phase, you're seeing a whole bunch of security scans that Prisma Cloud has done should things fall through the crack and go into production.

The key thing to remember here is that a risk introduced in the code phase gets multiplied in the cloud, 20 risk in the code got to be 2,000 in cloud. Now, typically, the security practitioner, it takes months and months to resolve these 2,000 issues because they don't have the context, don't have the traceability to fix the root cause of the problem. Let me show you how Prisma Cloud does that.

So I clicked on the 2,000 security risk. What you see here is a code-to-cloud security graph where we're tracing the 2,000 security risk back to the two problems in the code phase. More specifically, these are the two Log4j components that the developers introduced that has the security risk that lead to those 2,000 problems. You can see that those 2,000 risks belong to a single application. And like I described, a customer is using multiple application, so now the customer has tens of thousands of different risk.

With a single click of a button, Prisma Cloud is able to fix the root cause of the issue, as you will see that momentarily. We're able to upgrade the latest version of the Log4j, invoke the pipeline, reduce the risk at each stage of the application lifecycle, and now you see that the 2,000 risk got reduced to zero with a single-click option.

So that was the first demo. The key thing to remember here is any time there's a risk in the cloud, you have to trace it back to the [ph] code (01:23:17), and we're the only platform that can do that today.

The second demo I want to show, and that's something we have been working on, which – was with the AI copilot. So let me show you how our AI copilot experience is going to look like. It's going to show you all the things that it has done for you since you last logged in. The user, this time around, is going to ask the question around how many Log4Shell vulnerabilities do I have in my environment. Through a simple natural language processing, it was able to understand the question, was able to render a similar graph, as you can see, there are 1,000 cloud risks for Log4Shell, trace it back to the one source problem.

The user is able to interact with the copilot, get a little bit more definition of these problems, and finally, just like you saw in the first demo, ask the copilot to go ahead and fix all this problem with a single click.

The key thing I want you to remember about the security copilot is that it's a resource multiplier for you. There are not enough security professionals, and the copilot is going to help you burn down the risk and prevent breaches in cloud.

As I wrap this, let me tell you the opportunity ahead of us. The average customer today doubled their credit consumption within a year and quadrupled in two years by growing from two to five to eight modules. We have a natural land-and-expand motion with our existing customers. When you add that with the new customers that we're going to be adding, and enough headroom that we have at the installed base, the opportunity in front of us is massive.

The last thing I'll leave you with is the market in front of us is huge. Prisma Cloud is the clear leader in the space, and we have the right strategy and the vision to win this market.

Thank you, all.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

All right. Thank you, Ankur. Again, clearly, huge opportunity in cloud security with our unique approach and what we're driving. Really excited with where we are and what we're working on.

And now for our third platform, our AI-driven SecOps platform. This is a market that I believe is ready for a fundamental transformation. Most of the technologies that companies use are or were developed 15, in some cases, 20 years ago. That clearly does not work. They were not designed for an attacker sophistication that we see today. They were not designed for real-time detection and automation remediation. These tools were not designed for supply chain attacks. These tools were not designed for the advent of attack AI being used by our adversaries.

We have to reimagine security operations from the ground up. And in doing this, leveraging data, leveraging AI, leveraging automation, as core, tightly integrated foundational aspects to how an entire SecOps platform functions within the SOC. And this is the journey that we've been on for the last several years, building this platform, refining it, developing the capabilities necessary, and then refining it again, until we reach the point where we are today, where we have a set of leading products and an incredible platform delivering incredible outcomes to take advantage of this entire security operations market in front of us.

And to share more details, I'm joined from our Tel Aviv R&D center by Gonen Fink who leads our entire Cortex product organization. Gonen?

Gonen Fink

Senior Vice President-Cortex & Head of Israel R&D Center, Palo Alto Networks, Inc.

Thank you, Lee. Let's take a deeper look at why existing SOC architecture doesn't work. With the growth of sophisticated alerts, multiple tools were created, each one designed to solve a specific problem. This leads to an extremely fragmented SOC. Very hard to manage. It is the customer's responsibility to integrate those tools into a human-driven workflow. The result of that is bad security outcome, low-confidence alert, analyst shortage, unable to resolve those incidents in real-time.

So what is required to deliver real-time security operation? We need to replace this fragmented architecture with a unified, single-flow architecture. We need to replace multiple products that collect data with a single-data platform, and silo detection tools with an AI engine that is trained on a full dataset. And then automation should be natively integrated into the flow rather than being placed as an afterthought.

Five years ago, we recognized the criticality of data, AI, and automation for the future of cybersecurity. We built three amazing products, each of them became a leader in its respective category. And we continue to innovate in each of those categories to maintain our leadership. This drove Cortex to become $1 billion business for us, and it also brought us into [ph] thousands (01:28:39) of customers' security operation centers.

Cortex XDR extended the EDR market, and it is the best AI tool for endpoint prevention and real-time detection of all security threats. Cortex XSOAR is the best-in-class security tool for automated threat response, and Cortex Xpanse proactively manage your attack surface and reduce that.

But to harness the full potential of AI and automation in order to build a real-time SOC requires more than that. We need an integrated AI-driven architecture that reimagine the legacy, 20-years-old SOC architecture from the ground up, and this is what we brought to the market with XSIAM last year.

So, what happens is legacy SOC and how it has changed with XSIAM. Let's look at that. In order to detect attacks, siloed tools just get alerts. But we are living in dynamic world. Unfortunately, looking at anomalies or alert in isolation might be suspicious, but there are many of them. Each of them look at the world from a very narrow standpoint, and the result is that high volume of alerts that overwhelm the SOC. This means that SOC gives up on reviewing all of those alerts, and eventually, the SOC is missing the important ones.

With XSIAM, customer no longer needs to review low-confidence alert and try to connect the dots themselves. XSIAM collect large amounts of data and uses AI to analyze low-confidence signals, stitch them together with raw data, and get enough context to resolve most of them automatically, presenting the user only with [ph] what's relevant need to them (01:30:35) and with the full context for each of those incidents. By grouping this into incidents, prioritize them, [ph] risk-score (01:30:44) them, XSIAM provides a full picture of view to the analyst, allow the analyst to respond very quickly to the events.

How do we do this magic? Let me use new [ph] product UI (01:30:57) to explain the key elements that differentiate XSIAM on the rest of the products in the market. It starts with the data. We ingest normalized, stitched-together petabytes of data from dozens and hundreds of data sources to recreate the full story of each and every event in your environment.

This stitched rich dataset and sophisticated AI engine with [ph] over 3,000 model (01:31:27) that produce high-confidence alerts, that groups those alerts into incidents, assign a risk score to each and every incident, and then integrate natively built automation to resolve most of the incidents, leaving only a small number of incident for human review and resolution.

Like the copilots you saw for both network security and cloud security, our new [ph] Cortex UI (01:31:54) we incorporate to copilot, with an early alpha testing starting next month. We started working with Palo Alto Networks SOC as our first partner as we design and build Cortex and XSIAM.

Palo Alto is the largest security vendor, and as such, we have a lot of assets that we need to protect. And in order to do proper job, we collect a lot of data. Over 1 trillion events are collected every month, or 75 terabytes every

day. With Cortex, Palo Alto Networks SOC can protect its network with a small team working on standard shifts, resulting with less than one minute incident resolution. This is not [indiscernible] (01:32:35). This is relying on technology and AI and automation to achieve the right security outcomes.

So when we launch XSIAM, we wanted to see how this plays with customers, and the early indications are remarkable. Our customers are able to ingest a lot more data than before which provides them with broader coverage for their attack surface. Even though they ingest a lot more data, product generate a lot loss false positive, and those true positive alerts are being grouped together, prioritized by AI, delivering much, much superior security outcomes, better coverage, shifting the median time to response from day to hours.

As we look forward, and we see a tremendous opportunity in growing Cortex and XSIAM. We continue to win and gain market shares with our best-of-breed products XDR, XSOAR and Xpanse, [indiscernible] (01:33:38) a basis to upsell our customers to the full XSIAM solution. Each of those customers is a candidate, is becoming a prospect to move to the full platform XSIAM. And we demonstrate these over the past 12 months in being able to convert [ph] a lot (01:33:57) of the customer that use part of the platform to become a full-platform users.

But the most exciting part is when we look at where we can expand XSIAM. We believe the era of AI and automation is just beginning, and XSIAM is quickly becoming the largest security data platforms, and the technology we build with AI and automation could be the basis to expand what we can deliver with XSIAM, to new modules within the SOC and across the entire security landscape.

Thank you, all, and back to you, Lee.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Awesome. Thank you, Gonen. Clearly, an incredible opportunity in Cortex, and specifically with XSIAM, as we think about the journey ahead where we are going to transform security operations in just absolutely incredible and amazing ways.

And with that context across our three platforms, let me now turn it over to BJ to share with you how we take all of this wonderful stuff to market. BJ?

William D. Jenkins

President, Palo Alto Networks, Inc.

Thanks, Lee, and it's great to be here with all of you.

I couldn't be more excited to talk about our go-to-market transformation that will allow us to take full advantage of the product innovation you heard about. I just had my two-year anniversary at Palo Alto Networks, and the evolution of this go-to-market organization, in step with our customer needs and product innovation has been incredible.

To understand how we can best serve our customers, we need to understand how organizations are tackling cybersecurity challenges today. On average, large companies have 75-plus security solutions. This leads to fragmentation and growing complexity as customers try to stitch together all these individual products and data. To add to this, they are dealing with overlapping vendor solutions that don't talk to each other. Many customers are buying cybersecurity in this way. They recognize how unwieldy and ineffective it is, and they need our help.

This is a call to action for our industry to do a better job at helping our customers, and at Palo Alto Networks, we will do this through three key go-to-market transformations.

First, we are transitioning from a transactional vendor to a true strategic partner, guiding customers on their transformation journey. Customers are looking to us for direction on how to secure their enterprises and keep their employees and end-user customers safe.

Second, we are transforming from selling point products to architecting outcomes in partnership with our customers' most trusted ecosystem solution providers. Our customers' ecosystem partners will become even more important as we work with them to create more value through new services and joint offerings.

Third, we are moving from a reactive help model where customers only call us when they need us to a more collaborative model where we are proactively driving success for every customer with an in it together mentality.

Palo Alto Networks is well-positioned to help our customers through these three key shifts, and we have made significant headway on each of these fronts.

In the past, our go-to-market motion focused on technical domain expertise, solving very specific product requirements. These conversations often revolved around price, and they were transactional in nature. Today, C-suite executives are engaging us more and more. They are looking to transform their entire business, understand security strategy, and deliver better security outcomes. We now have a seat at the table for key architectural decisions and ongoing multi-year roadmap engagement. Our 3,000 integrated sellers are set up to scale, and have these strategic conversations with our customers.

Our ecosystem is also playing a critical role as we move from selling products to architecting outcomes. Five years ago, we sold a single product, primarily hardware firewalls, as part of a larger partner-delivered motion. Most of our partners were focused on transactional fulfillment of customer orders. Today, we are deeply embedded with strategic partners across all routes to market and are co-leading the sales motions with our partners to deliver joint solutions.

We have 150 $10 million-plus strategic partners today in our ecosystem. In the future, we're going to continue to strengthen our sell-together motion by building integrated offerings with a shared focus on improving client outcomes. Our top 30 partners will become even more important, and we're looking to drive $10 billion-plus of business with them.

Delivering the best security outcomes means that our customers' post-sales experience must also undergo a shift, as I said, to an in it together model, allowing them to be successful faster and get the most value from our solutions. Although we have consistently achieved a 90-plus percent CSAT score, we aren't stopping there. Continuous improvement is the goal.

As part of our strategic focus on AI, we will leverage AI to resolve customer issues more quickly. With AI-enabled in-product support, we plan to reduce our mean time to resolve for calls by over 65%. We also plan to scale our global network of 300-plus fully certified professional service partners in order to further expand our ability to deploy our products with speed and agility. And last but not least, we'll increase adoption by staying with our customers throughout their entire journey. We have a 600-plus-person customer success team with deep expertise helping to build customers for life.

You've heard this from others today, but it bears repeating. We see massive opportunity ahead for Palo Alto Networks, and our go-to-market model is transforming to meet it head-on. As you can see in the chart, we are already well on our way with our Global 2000 customers, with 54% of our customers on the journey across all three platforms, and we have great potential to extend our breadth by selling the full portfolio across our install base and our platform depth by covering our customers full estate.

I'll end where I started, with a reflection on the opportunity and unprecedented ability to help our customers secure and transform their business. Palo Alto Networks platforms are the best in the industry, and we have a world-class go-to-market organization uniquely positioned to bring them to our customers and partners. Our go-to-market model is ready to scale and deliver real-time security outcomes for every customer through the power of our platforms.

Thank you, everyone. And back over to you, Dipak.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

As you heard from Nikesh about our strategy, Lee and his team on products, and BJ around go-to-market, we have the entire company pointed in the same direction. I now wanted to bring this all together to help you understand why we are confident that we can capitalize on our opportunity and translate it into financial results that will drive superior total shareholder return.

I will go through all four of the primary drivers of TSR, including revenue growth, profitability, cash conversion and capital structure.

First, on the top line. You heard about our TAM from Nikesh. We have proven, over the last five years, that we target the largest and most attractive parts of the market. We've been able to capitalize on an expanding opportunity, taking share from within existing markets and positioning ourselves in new markets to drive further growth potential.

Our share today stands at just 7% of our addressable market, which is lower than the share of leaders in many other markets outside of the cybersecurity industry. As we plot the course to the larger TAM that Nikesh outlined over the next five years, we continue to see the opportunity to gain share in our existing markets and continue to fuel above-market growth for Palo Alto Networks.

Looking at this through the product lens, Lee and his team outlined our platform leadership in our three areas, and showed you the innovation plans their teams have to continue to lead our markets. From my seat at the company, innovation is our lifeblood, and we will continue to spend aggressively on R&D. We do not focus on driving leverage to the bottom line, but rather we redeploy any savings we identify to invest in additional innovation.

Our customers expect us to continue innovating, and we have consistently shown a strong return from these innovation investments. This includes recognition of our innovations, such as the Gartner single vendor SASE leadership position that we mentioned today.

We expect our innovation to show through in financial outcomes in each platform and the company overall. In network security, our investments across form factors, especially software-based and cloud-delivered, enable us to further our market position and sustain our growth in FWaaP billings. Our market share in our software-based VM business, is approximately two times what it is in hardware. In SASE, we believe that we are the number two player in this fast-growing market. In cloud security, the growth algorithm is leveraging product and go-to-market

capabilities to drive credit consumption ahead of the growth rate customers are deploying public cloud. Along the way, we are confident we can increase multi-module consumption to solidify our position as the definitive code-to-cloud leader.

In Cortex, we have a solid business with XDR, XSOAR and Xpanse, competing in attractive individual product markets. We've seen a shrinking number of players in the XDR market, and have steadily added several hundred customers per quarter. Adding customers across Cortex is important to allow us to drive larger, more strategic fields in the future where we can further cross-sell our products including XSIAM. XSIAM is truly game-changing innovation where we are selling outcomes, and I'm confident the momentum will beget momentum here after a very strong launch of the product in the first year.

It should be clear from BJ's presentation that we've invested in building a large dedicated go-to-market organization and are transforming how we engage with the market. Transformation here has been a non-stop effort and has driven growth in the number of large deals each quarter. On the back of the core tenets BJ covered, we see the opportunity to continue to drive more strategic relationships with customers that can result in eight and even nine-figure relationships.

At the same time that we have seen these large deal outcomes, we've consistently improved the productivity of our core apps as they collectively become better at selling the broader portfolio. As Nikesh mentioned, SASE has been a big success here. Additionally, we have seen standout growth from new ecosystem partners, including the cloud service providers and global system integrators. Not only has our business transacted through these channels increased, but more importantly, so has our success leveraging these partners as influencers. We have the product portfolio that makes us an attractive partner to these players, along with the scale to make the investments to support the success of these partners.

Bringing this together on the top line. As Nikesh noted, we're targeting growth of 17% to 19% in revenue and billings over the next three years, which is ahead of the cybersecurity market growth rate. We see hardware as a percentage of our total revenue decreasing to approximately 10% with NGS ARR exiting fiscal year 2026 above 55% of our fiscal year 2026 revenue.

RPO remains an important metric as it captures the full value of our customer contracts independent of payment terms, and we expect growth of 25% annually through fiscal year 2026. Additionally, we see about two-thirds of our revenue in fiscal year 2026 driven by current RPO entering the year highlighting the increase in predictability of our revenue profile.

Now, moving to the cost side, and first with gross margin. As I hope Lee and BJ have impressed upon you, we have significant advantages inherent in building and delivering platforms. There are characteristics of our platform business model that benefit gross margins. A higher software mix in our network security business helps contribute to a higher gross margin, something we saw in fiscal year 2023. On the cloud-delivered side, most notably in SASE and Cortex, we've aligned with public service providers to enable us to instantly leverage their scale and delivery capability, as well as take advantage of their ongoing innovations and efficiencies. As we grow, we see improvements in our unit economics.

Lastly, in customer support with multiple scale products in each of our platforms and common customer support needs, we see leverage within our platforms and across the company. Above and beyond these platform benefits, as we talked about earlier in fiscal year 2023, we accelerated some efficiency initiatives that contributed to higher gross margins. We also saw a normalization of the supply chain during fiscal year 2023.

Starting in 2023, we have increased our investments around generative AI to leverage this technology in customer support for efficiency and better medium-term customer outcomes. While we see these platform leverage and efficiency opportunities in gross margins, we also leave room to invest in new cloud-based offerings, which generally have sub-scale gross margins in their initial phases. For this reason, we expect a relatively steady gross margin in fiscal year 2026 as compared to fiscal year 2023.

Moving on to operating expenses. We see similar benefits from being a platform company across our major functional areas. At the top of this list is the sales productivity improvements already discussed. It's important to reinforce my point around the platform benefits in R&D. We choose to redeploy those resources to ensure we are leaning into innovation instead of driving overall financial leverage in R&D.

Our fiscal year 2023 focus on accelerated efficiency did yield benefits in terms of leverage in OpEx, and we expect to continue many of these initiatives. One to highlight is the consolidation of sales specialists. Similar to customer support, we also have generative AI initiatives to both improve outcomes across sales and marketing and our G&A functions that we expect will contribute to efficiency in fiscal year 2024 and beyond.

Translating this to operating margins. While some may see a 500-basis-point improvement in one year as a milestone achievement from our 2021 Analyst Day, we simply see this as a new beginning, as we see many opportunities to drive this higher. We look for non-GAAP operating margins in the range of 28% to 29% in fiscal year 2026 with a long-term opportunity for those to be in the low-to-mid 30s as we further scale our platforms and gain confidence in the power of AI and other business transformations. We're also committed to growing non-GAAP EPS on a compounded rate greater than 20% from fiscal year 2023 to 2026.

Moving on to cash flow. Recall that in fiscal year 2021, we guided to 33% free cash flow margins. In front of that guidance, we spent considerable effort looking at our entire business end-to-end from the point of view of cash flow and understanding all the drivers. We have now had two years operating in this manner. We're confident we can sustain our high cash conversion, focusing on areas such as best-in-class working capital management and low CapEx business models. Our top line growth and underlying improvement in operating margin form the foundation of our strong cash generation. There are other factors impacting cash flow that I want to highlight and that we have already included in our forward-looking guidance.

First, with the rising cost of money, we have seen more customers asking for deferred payments over the last three years, but especially in last 12 months, as we previously talked about. Also, our rise in GAAP profitability and some changes in US tax law, we see rising tax cash taxes. This has all been included in our forward-looking guidance.

I wanted to double click on the impact of deferred payments for a moment. We've already seen this have a significant effect on our cash flow. In the second half of fiscal year 2020, along with the pandemic, we launched Palo Alto Networks Financial Services or PANFS to ease customers' challenges with short-term cash flow issues. As I mentioned, with the rising cost of money in the last year, we've seen this trend broaden. PANFS and deferred payments allow us to drive success partnering with our customers on long-term transformation of their security architectures while working with their cash flow constraints.

The amount of bookings with deferred payments was up 4x in the fourth quarter as compared to three years ago. This impacted our reported cash flow in the last three years, yet we have maintained our strong cash generation. As we look to the next three years, we expect this impact to continue and have accounted for this in our medium-term targets. A by-product of the rise in deferred payments is greater predictability of our cash flow over time. For example, we now expect about $1 billion in cash flow from deals entered into in prior years where payments will

now come in fiscal year 2024. This $1 billion is twice what it was in contributions to our fiscal year 2023 cash flow when we entered the year.

Summarizing cash flow. I'm confident we can maintain a baseline of 37% free cash flow margins over the next three years after accounting for the factors I noted. This and the revenue growth targets I covered should keep us on the aspirational path to Rule of 60 economics in our business. This combination of top line and cash generation puts us in a rare peer group, and allows us the flexibility to navigate the changing environment.

Finally, I'll cover the capital structure as the last tenet in TSR. With all the opportunities ahead of us, organic investment in our business to drive growth will remain our number one priority. We have ample cash generation to make these investments. From here, we have three capital allocation priorities. As we've done previously, we will continue to balance these.

Our first capital allocation priority is our M&A strategy. We have successfully acquired companies that are early leaders in adjacent and emerging cybersecurity markets. Many times, these are markets in which we've had an early organic effort, but we see external innovation that can significantly accelerate our time-to-market. We target companies that have achieved product market fit, with teams that can accelerate their innovation inside Palo Alto Networks. Revenue is not a focus for us, but we do ensure that we have a solid plan to accelerate the trajectory of our business. We've used $2.5 billion in cash over the last five years, pursuing the strategy successfully.

Secondly, we manage a capital structure that gives us flexibility. For example, we use our balance sheet as a competitive advantage with PANFS and deferred payments. We repaid our 2023 convertible debt in July, and have another convert coming due in about two years, which we also plan to settle for cash. Beyond enabling reasonable flexibility in our capital structure, we're also focused on minimizing dilution and reducing our organic stock-based compensation expense as a percent of revenue by at least 300 basis points over the next three years.

Lastly, we will use share buybacks opportunistically, something that you have seen from us over the last five years, as we have repurchased nearly $4 billion cumulatively.

In concluding my section on bringing it all together, I wanted to bring together the financial targets I've covered. As Nikesh mentioned at the outset, we're focused on an evergreen innovation-led approach that will continue to fuel our transformation into a software- and AI-driven cybersecurity company. I am more excited than ever about our growth prospects over the next several years, and our plan is to continue to do this profitably, benefiting from our platform business model.

I hope my excitement comes through today, and you can clearly see the drivers of our confidence in these targets from the various presentation.

With that, we'll now transition to taking your questions, and I will hand the call back to Walter to manage this. Walter?

QUESTION AND ANSWER SECTION

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

A

We'll now take questions on the entire program. We're going to start first with Hamza Fodderwala from Morgan Stanley and go next to Andrew Nowinski from Wells Fargo. Hamza, please go ahead.

Q

Hi. Apologies. Can you guys [ph] see me (01:56:14)? Hi. I'm [indiscernible] (01:56:16) Morgan Stanley, dialing in for Hamza. Thank you guys so much for taking my question today and really congrats on the great quarter.

You did mention that AI is a very large opportunity for the company going forward. And I know that you've broke down some of the gross margins, as well as potential operating margins impact. But could you just let us know how we should think about the company's investment for AI going forward? Are there any upfront CapEx or margin that we should consider a little bit more? Thank you so much.

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

A

Hi, yeah, thank you very much for your question. Look, it's early days in AI as I mentioned. On the precision AI side, we have been using it. We have been using it across our products. There's no incremental costs. It's embedded in our current product development capabilities.

On the generative AI side, I'd say you saw a sneak peak of all the copilots. The good news is all of those things should generate positive outcomes for us either in terms of incremental modules that customers would like to buy to enable certain functionality, or possibly reduce costs from our capabilities to deliver much superior customer support.

So I think at this point in time, I would not bake in any incremental sort of spend expectations in our forecast as it relates to the implementation of AI. Dipak has given you guidance that we can continue to see operating leverage and operating margin. Clearly, some of that is driven by expectations in AI, but I'd say we're being normal about it. We're not overtly aggressive, nor are we overtly conservative around it. And hopefully, there will be upside in that if and when we start to see the fruits of deploying it effectively across Palo Alto Networks.

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

A

Great. Thank you. Next, we're going to go to Andrew Nowinski from Wells Fargo, with Brian Essex from JPMorgan after that. Go ahead, Andrew.

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC

Q

Thanks, Walter, and congrats on the nice quarter as well. So, I wanted to ask about Zero Trust. That's clearly a top priority, and really, it seems like it's the only architecture that's capable of stopping a sophisticated attack. And you showed how it requires hardware, software and SASE components. So if we think about Zero Trust demand

continuing to ramp going forward, why would firewall demand drop, I think you said, to 10% of total revenue in fiscal 2026 if it's such a critical component of your Zero Trust offering?

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

It's important to understand. We didn't say it will drop to 10% of revenue. Everything else is growing really fast. I think it's important to understand, like, it's not growing as fast as everything else. Look, for the last five years, I've always been asked that hardware question. I've been trying to avoid it for five years unsuccessfully. So thanks again, Andrew. Only took one question to get to it.

I think it's important to understand, as we started moving to the cloud, people started coming to the notion of software firewalls. And then with this whole pandemic thing, remote work and sort of distributed network became a real thing. So what you're seeing is that there are different form factors which are really good in different circumstances. Against the public cloud, you put a software firewall. You use VMs in various scenarios.

When throughput becomes really important, hardware is still the best option, and I don't think the whole world is going to end up only in the public cloud. By the way, we also sell firewalls to the cloud providers. Believe it or not, they need firewalls in their data centers because eventually the public cloud also runs in our data center.

So I think in that context, the demand for hardware is not going to go away. I think what Anand showed you beautifully that you're going to end up with all the form factors at most of our customers. And the key is these things need to work better together. I think if you go today, there are many customers will have a Palo Alto firewall and a firewall of some other vendor.

Now if we can give them SASE, we can give them software firewalls, there is no reason that they should be on two hardware vendors when they're a single software vendor and a single SASE vendor. So I think the point we want to highlight here is there is a further consolidation opportunity in the firewall space driven by the Zero Trust needs, as well as the UI that Anand gave you a sneak peek into. So I think that's the way to think about it. We like hardware. It's great.

Andrew James Nowinski
Analyst, Wells Fargo Securities LLC
Q

Thanks.

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

Great. Thanks, Andy. Next question's going to be from Brian Essex at JPMorgan, followed by Jonathan Ho at William Blair. Go ahead, Brian.

Brian Essex
Analyst, JPMorgan
Q

Great. Thank you, Walter, and thank you for taking the question. And, Nikesh, thank you for making this a better Friday night than some of those conspiracy theories floating around imply.

[indiscernible] (02:00:50)

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

...we have [ph] 5,500 (02:00:51) people dialed in, Brian, that makes up like the last six earnings calls we've had. So, I don't know, maybe there's [indiscernible] (02:00:57).

Brian Essex
Analyst, JPMorgan
Q

Yeah. So I just want to touch on the security copilot, Prisma Cloud copilot XSIAM. I would imagine these work best with your platform products. But to what extent will you partner with other vendors? How will you incentivize the use of Palo Alto's platform with these products in mind? And will we get metrics to help us assess any improvement attach rate with these copilots and AI tools may drive? And when we might expect general availability? I know that's a lot, [indiscernible] (02:01:29).

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

Yeah. Now, let me tell you. I think, look, we all heard of this concept called hallucination or the idea that it doesn't give you the perfect answer all the time, right? And I'd say we are working really hard to see how do we reduce the error rate in the answers that the copilot comes up with because, in security, we can't afford wrong answers. So I think our teams are working really hard. What we've discovered in the process is that, irrespective of which LLM you deploy, you need better knowledge articles, you need better integration of the UI. So our teams are busy doing a lot of [indiscernible] (02:02:00) work, and you saw them give you some sort of glimpse into what the [indiscernible] (02:02:05) could be.

I would say, sometime before the end of the year, we will start testing it with a bunch of customers to get real feedback from customers. I think the best way to think about it is like the examples you saw, it's like security is complicated. UI on security is also complicated. If you don't know where to look, sometimes it's right there, you just don't know where to look. If you can ask that question and view the answer, that improves the productivity of all of our customers. It improves the configuration capability of all of our customers. It improves our ability to provide real-time customer support to our customers.

So, I think there's lots of advantages if done right. And I'd say it's always like people often overestimate the short-term and underestimate the long-term, that's why we give you a three-year forecast. I think we may get the three-month or six-month wrong, but we'll not get the three-year or five-year wrong. Three to five years from now, the world will be different. UI will be 50% natural language. We'll be generating tons of efficiency from people using AI-driven tools. I think that's the opportunity. And you don't get there if you don't work hard now.

Brian Essex
Analyst, JPMorgan
Q

Fair enough. Thank you very much.

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

Thanks, Brian. Next is Jonathan Ho from William Blair, and after that we're going to have Gabriela Borges from Goldman Sachs. Go ahead, Jonathan.

Jonathan Ho
Analyst, William Blair & Co. LLC

Q

Thank you and let me echo my congratulations as well. Just in terms of your comments around reducing vendor sprawl and platform consolidation, this has been a significant goal for the industry for some time. So why do you think it will be different this time? And how can you sort of sustain innovation across such a large set of products? Thank you.

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

A

Jonathan, I think you saw, I think, Dipak, Lee, myself, all of us have made this point, so did BJ, around the fact that without innovation, we're out of the game. We launched 74 different capabilities last year, and I think we'll probably do more next year than 74.

But I think what's interesting, what you're seeing is these 74, many of these are existing point products in the industry which we are relaunching by adapting them to our platforms. And the reason it's going to work this time, Jonathan, because it's working.

One of the deals we talked about, the SASE deal with a large professional services organization, we consolidated seven vendors, right? Our XSIAM deals, which totaled $200 million, consolidate on average three to seven vendors in the SOC. So, it's working.

Now the question, I'm already in the SOC, I've consolidated seven, I go to my customers [indiscernible] (02:04:32) listen, you got these other five things hanging around. Look, I've got these five new modules in XSIAM. Why do you want to do five new vendors and solutions which don't talk to each other? Right? So I think what we have in our opportunity is once – it's kind of like, I think you like to call it, land and expand. I think we're landing with our platforms. We used to land with SASE. We used to land with firewalls. Now we're going and saying, listen, you have our hardware firewall, we have our SASE, with this beautiful UI, it brings it all together, why don't you clean up the rest of the infrastructure?

I think it's an evolution in the industry. I think five years ago it was an idea. We're seeing it actually happen. You're seeing us put distance between ourselves and single-product vendors in many categories because people are seeing the power of the platform. That's just the opportunity, and that's something BJ, Lee, Dipak, me and the gang have to execute on. And it's just relentless execution that's needed.

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

A

[indiscernible] (02:05:25)

Jonathan Ho
Analyst, William Blair & Co. LLC

Q

Great.

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

A

One is prior attempts to do this generally required a trade-off for the customer. It was the capabilities that were delivered on their attempts to do a platform were not industry-leading. And so, the customer had to make a trade-

off between worse capabilities but in one place, or best-in-class capabilities. And that's a hard trade-off in cybersecurity. That is one thing that we're not asking our customers to do. We're making sure that everything we do is industry-leading on its own.

The second thing we're doing is making sure that when we integrate it, they're actually integrated together in solving hard problems that can't be solved as standalone capabilities. So it's not just about consolidation, although that's a clear value. It's about delivering technical outcomes through the integration that cannot be achieved otherwise.

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

Great. Thank you, Jonathan. Next, we're going to go to Gabriela Borges from Goldman Sachs, and after that, Roger Boyd from UBS. Go ahead, Gabriela, with your question.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC
Q

Good afternoon. Thank you. My question is for BJ on the go-to-market. And I'm looking to understand to what extent NGS cross-sell is or isn't still tied to the firewall refresh cycle. And as you think about the conversations you're having with customers on platformization, I'm curious to what extent Microsoft is coming up on those conversations as a potential security platform and how you help customers think through the advantages of standardizing on Palo Alto Networks instead of potentially Microsoft at some point in the future for security.

William D. Jenkins
President, Palo Alto Networks, Inc.
A

Thanks. Good question. Look, I think all of this starts with what Lee ended with is we get to sell, I think, the best products in the industry and we deliver better customer outcomes. We have three primary consolidation motions. One has been around network security services on the firewall but also in the SASE. And actually, we have within that now, [ph] we've landed (02:07:32) customers with SASE and are going back and getting the network firewall business. So our core reps tend to focus on that. They are the account owner and represent the whole portfolio.

The second motion is we talked about code-to-cloud and we usually land with workload protection or posture management and then branch out into other modules off of that to either shift left or get a complete platform for the customer on cloud security.

With Cortex, we have three outstanding solutions that we land with. We either win with XDR [ph] or for customers (02:08:13) focused on automation, XSOAR is a great starting place for us, attack surface management with Xpanse. And many of our first wins with XSIAM have been leveraging that installed base to deliver a full SOC transformation.

Again, on the surprising side though, many of our XSIAM wins, we also didn't have an installed base in Cortex and the customer jumped completely in. We have specialists in those areas, in both code-to-cloud and in Cortex, and so the core team works with those specialists to run those consolidation plays also.

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

Great. Thanks. Next question's going to come from Roger Boyd at UBS, followed by Patrick Colville from Scotiabank. Roger, go ahead with your question.

Roger Boyd
Analyst, UBS Securities LLC

Q

Great. Thanks for the question and happy Friday. Nikesh, you mentioned you're now extending the Cortex to the core sales force. And I'm wondering how you think about the repeatability of the success you've seen with SASE. I think you mentioned last quarter 80% pipeline contribution from the core reps within a year of selling that product.

But if I think about SASE versus Cortex and SASE maybe benefiting by being a little closer to the core network operation function that's behind firewalls, how do you think about that as a challenge with the core reps selling Cortex? Any thoughts there would be great. Thanks.

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

A

Look, the whole idea originally was to have sales specialists because we were in the early stages of our products, we were trying to build them out. We had lots of changes, we wanted to make sure they were trained and available as extra resources.

Now, think about it, we did a $44 million XSIAM deal. Everybody was involved. The core rep wasn't going to let that deal go. That's a lot of money of commission for the core rep if he or she can understand XSIAM.

So I'll tell you, BJ and I are going to have this wonderful sales conference starting Sunday. I promise you every one of those guys will be lined up for the XSIAM session because they want to learn more about it, because see the deal size, deal size is equal to dollars for the company, is equal to dollars for the sales person. And they're all very smart people, so they're going to go gravitate towards where the real business is.

So I think when you can get salespeople to lean in to learn something, it creates a great outcome. And also, guess what? I mean, it's not like people suddenly woke up yesterday and became Cortex specialists. They used to sell cybersecurity before. They just did a good job of embracing and getting trained.

So our products are at a point where we believe they're mature. We understand the differentiation in the market. There is [ph] reputation (02:10:37) out there in the market. We have people in the back who can stand up POCs. I think we can do this. I think we showed that with SASE we can do this. I think we can do this with Cortex.

The cloud thing is slightly different. Cloud is still early in the customer and from an adoption perspective. It's a consumptive model. It's [indiscernible] (02:10:52) model. So that it lends itself to a slightly different sales motion, and there, we're not going to be in a hurry to merge that. But I think from a Cortex perspective, it's not just merging the team. It's opening up the flood gates for 3,000 people to sell it. That's the way we think about it.

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

A

Great. Thank you, Roger. Next question from Patrick Colville at Scotiabank, followed by Michael Turits at Key. Go ahead, Patrick. Patrick, are you on? All right. We're going to go to Michael Turits at KeyBanc, and will be followed by Tal Liani at Bank of America. Go ahead, Michael.

Michael Turits
Analyst, KeyBanc Capital Markets, Inc.

Q

Hey, guys. [ph] Good evening (02:11:36). And just sort of a question for Dipak. When we have the 10% bogey for – out there for hardware in the out-year, how should we think about product which is a broader category at this point, both in terms of how that ramps over the years and what other products or categories might fold into that? [ph] It's just (02:11:58) SD-WAN has been in there, portions of VM series, so how should we think about that line in a dynamic way?

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

So, I think obviously we've got the technical side of what's in products. There's VMs, there's SD-WAN, there's all of those different things that are in there. I think a lot of it will depend on, like, what customers want in terms of their network security architecture. We believe that the software side of product continues to grow faster. We've been talking about that a lot. I think last quarter we talked about how 30% of product revenue was software. But honestly, we're not guiding to product anymore, and I think the reason for that is because it's not as relevant, right?

[indiscernible] (02:12:45)

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

I think, Michael, one of the things that I think we should tell you is that we're in the process of re-examining how to classify the revenue to make it much more easier for you guys to think about it, because product was the artifact of hardware. It comes from a 1919 or 1930 SEC...

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

1970. Yeah.

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

1970, thank you, FASB requirement that has to be physically tangible. And I think with the emergence of SaaS companies, it becomes sort of hard to do that. So I think we're going to take a look at that. And I didn't want to do it on a Friday night and add one more exciting for you guys to think about. So as the year progresses, we'll find a better way of letting you think about our revenue which is more measurable and more trackable and possibly more [ph] kind of (02:13:27) predictable for you guys.

But yeah, this is like product, and we don't have to tell you the percent of product that's not hardware every time to tell you how to split that between hardware and software. I think it suffices to say we're looking at it as a business across the board. We look at RPO. We look at revenue, obviously. We look at margin. We're looking at free cash flow which is the numbers we're guiding to. And that's what we manage on a sort of day-to-day basis to run the business.

Michael Turits
Analyst, KeyBanc Capital Markets, Inc.
Q

But just in case [indiscernible] (02:13:53) thinking about our workload, we do appreciate not having to rebuild the model tonight. Thanks, Nikesh.

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

All right.

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

[ph] Oh, my gosh (02:14:00). I was hoping one of you guys was going to show up with a glass of wine at least, but.

Michael Turits
Analyst, KeyBanc Capital Markets, Inc.
Q

I got my T-shirt on. This is as close as I'm going to get.

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

All right. That's good.

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

All right. Thanks, Michael, for your question. We're actually going to go back to Patrick Colville, who I understand is now connected from Scotiabank, and then we'll go to Tal Liani from Bank of America. Patrick, go ahead.

Patrick Colville
Analyst, Scotia Capital (USA), Inc.
Q

Thanks, Walter. I never thought I was going to hear The Cure, Friday I'm in Love on an earnings call, so a really quality way to start a Friday evening.

Dipak, another one for you. I mean, you've said lots of quite juicy metrics with us. The standout metric, to me at least, was Palo Alto guiding to, was it 17% to 19% billings CAGR to fiscal 2026? I mean, clearly implicit in that is the firm's consolidation message, you see resonating with customers, which we see as well. But what I wanted to ask is in that billings target, you mentioned new M&A philosophy, but I just want to double click. Does that billings target need a steady stream of tuck-in acquisitions to hit it? And then also, would Palo Alto ever do a transformative deal? What would kind of change your mind there to do a transformative deal?

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

Let me start with the second question first. If you don't think we've transformed the company in the last five years, I don't know, man. I don't know what else to do to make you happy, okay? I'm sorry, it's Friday night, I'm going home. So, I think we've been doing transformative for the last five years, and what we've shown you is transformative in itself, and I'm just in part just – I don't – look, you don't need me to buy businesses for you. You guys, you're shareholders, you're smart, you can do it yourself. Unless there's a huge leverage that we can prove that something we can take one plus one and make that two possibly two-and-a-half for you guys, it's not sensible for us to do.

And so far, we looked at everything. We look at everything every day. We see how things operate. So far, we haven't felt compelled because we have a lot of work to do ourselves. I mean, if you'd been busy integrating a

transformative acquisition, we'll miss the next five trends because we're busy. So, that's how we think about it, gives you some insights to how we think about it.

As it relates to tuck-in acquisition, I think the better way to see it goes back to what I said. Look, there are technologies out there that other people are working on, but we are not the only security company in the world. We're not working on everything. And if something becomes relevant, something becomes an important feature that we think is needed by our customers, and we haven't been working on it, it behooves us to go out and partner acquire, which is what I said.

So, should you expect us to maintain a rhythm around how we acquire companies? Yes. But you should understand, we have a five-year track record of doing that responsibly, doing it judiciously, doing it in a way that we integrate the acquisition, doing it in a way that we generate more ARR, and pretty much most of the ones we bought in the last five years have really not contributed on day one to the ARR or revenue because they have been mostly tech acquisitions. So, I think that's the way to think about it, if that helps.

Patrick Colville
Analyst, Scotia Capital (USA), Inc.

Q

Very clear.

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

A

Thank you, Patrick. Next question from Tal Liani at Bank of America, followed by Joe Gallo at Jefferies. Tal, go ahead with your question.

Tal Liani
Analyst, BofA Securities, Inc.

Q

Hi. I want to ask about the synergy between the various components of next-generation security. When you talk about Prisma Cloud and Prisma Access and Cortex and even firewalls, talk about the synergy to a customer. Are these the same customers that have benefits of buying multiple solutions from you or are you addressing conceptually different customers with different products and kind of addressing the entire market? Thank you.

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

A

Tal, you got the question of the evening award. In the last five years, we went out and we used our various products to do the land. We sold SASE where it was needed, we sold hardware firewalls that were needed, we sold software firewalls that are needed. 1,700 of our customers in some way, shape, or form have all of these things. I think the next step in our evolution is going back to them saying, listen, you have the hardware firewalls. It works way better with SASE. You want to integrate this across as a network security platform? That's where we have to show value, and you started to see glimpses of that of what Anand showed you.

Cloud, XDR is a combination of endpoint and firewall data. That has been now expanded to all the data that you have in XSIAM across your entire state, so now we're offering capabilities that Splunk has, we're offering capability that QRadar has, we're offering capability that Chronicle and Sentinel have in XSIAM, right? So, we're doing that.

To your question, you should expect us to say, listen, you have XSIAM. If you had Prisma Cloud, it will work a lot better. If you have XDR, the Prisma Cloud host protection and XDR host protection should work a lot better. So,

you'll start to see us selectively start to create, demonstrate value across our platforms. So, it's a great question, I think, but it needs to – customers need to be evolved to that because everybody has a bunch of products out there, and not everybody is lined up at the same-day for end-of-life, so I think you're right, you should see more of that from us in the next three to five years.

William D. Jenkins
President, Palo Alto Networks, Inc.
A

I'll just add one, Tal. So, for many of the large deals that you saw in the presentations, it's not just looked at as a solution acquisition cost. We put together for that customer not only the solution acquisition costs and the better security outcome you get. We talk about their operating costs, how they have to train their people, how many people do they need to operate these solutions and the environment, and the savings they get, so that when they go to justify an eight-figure deal with their CFO, they're talking about reducing capital and operating costs with better security outcomes, and I think Lee hit on this in his earlier answer. There hasn't been a company that's really been able to do that before in this industry. And when you combine those two, I think it's what's helped us in a tough economic environment to continue to close larger and larger deals with those customers.

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

Great. Thank you. Next up, we have Joe Gallo from Jefferies, and our final question will come from Adam Borg at Stifel. Go ahead, Joe.

Joseph Gallo
Analyst, Jefferies LLC
Q

Hey, guys. Thanks for the question, and great results, and appreciate the long-term framework. Just wanted to drill into the visibility into fiscal 2024 guidance. You guys just put up 18% billings growth, which is incredible on a 40% comp. I imagine that had some backlog benefit though. Now, you're guiding to an acceleration in billings next year relative to our 4Q which, as an opening guide, we would presume to be conservative. So, what underpins the confidence in that, especially if you have hardware and duration headwinds? Thanks.

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

So, first of all, Joe, great job at CNBC today navigating the question about our SOC, so thank you very much. On your question, look, we have conviction in some of the platforms. Like, let's start with our favorite one today. It's like XSIAM came out of left field. It did [indiscernible] (02:21:09) for us. We would have been happy at 100 for our fiscal year. We came in at 200. So, part of what you're seeing is that there are some products where we have tailwinds, and I think the part where we're sort of normalizing for is the – not normalizing for, the part we're sort of said to you – the part that we're careful about is the hardware normalization, which we've been anticipating or always positively surprised every quarter, and finally came home in spades in Q4. So, I think the forecast we have is what we represent to our board. That's what we're saying we're going to go do, that's what we're telling you.

Now, are we going to try and work hard to go beat it? Yeah, of course, that's what we do every time. There's lots of puts and takes. So, based on the puts and takes, based on where we are in different products, based on what plans we have to launch different things, this is our best estimate as of now, and we're going to give it our best to go out and deliver it. I think that's the best way to describe how we think about our numbers. Yes, of course, there's hardware headwinds, there's SASE tailwinds. I don't know if you saw, we became the only vendor in SASE far right, a single vendor sort of SD-WAN, plus SSE. So, there's some good tailwinds we have. Customers pay attention to these kinds of things.

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

A

All right. Our last question from Adam Borg at Stifel. Go ahead, Adam.

Adam C. Borg
Analyst, Stifel, Nicolaus & Co., Inc.

Q

Awesome. Thanks, everyone, for fitting me in and all the color tonight. Maybe just for Nikesh or BJ, just on the federal vertical talk of some large deals in the quarter. Maybe just talk about the opportunity that you're seeing, especially as we head into the fiscal year-end for the government next quarter. Thanks so much.

William D. Jenkins
President, Palo Alto Networks, Inc.

A

Yeah. I think to Nikesh's credit, even before I came on board, there was large investment in our federal team and the knowledge that with many of the federal directives, the budget being put in and obviously some of the geopolitical events, there was a opportunity for the company. And so, we're seeing the benefits of many of those forward investments, and we're going to continue to invest there. There's obviously large-scale projects that are occurring. We had one last year that we announced was our largest deal of the year. Those take a long time to mature, and we're involved in many of them. So, I feel like we have a great opportunity going forward in that space. There's specific ones obviously out there that we're looking to get. We've got some first orders in and gained momentum with them, and I think we'll be talking more about that in the coming quarters.

Adam C. Borg
Analyst, Stifel, Nicolaus & Co., Inc.

Q

Great. Thanks again.

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

All right. Thanks, Adam, for your question. With that, we're going to close it out, and I'm going to pass it back to Nikesh for some closing remarks.

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

Thank you, Walter. I just want to take the opportunity one more time to thank all of you. I know this was a unique one. You'll be telling your future mentees that you're going to mentor in the analyst community, maybe talking about that one Friday afternoon call which Palo Alto hosted out of their sort of misdirected sense of trying to get you guys to go do this over the weekend for us, so we really appreciate you taking the time. We apologize for taking up some of your Friday. We will be available tomorrow and the day after for some of you who have been kind enough to schedule time to talk to us because we want to make sure you get all your questions answered.

It'd be remiss of me not to both acknowledge and thank our employees, which is what makes all this happen, all of our partners out there who help us deliver this capability. And of course, I also want to thank my entire management team for delivering a really, really good FY 2023 and what has been a yet another set of different year. I don't think I had a normal year in the last five years between the pandemic and supply chain and inflation and money and this. So, I look forward to possibly a normal year next year.

And again, once again, thank you very, very much for all your support and your indulgence.