19-Nov-2025

Palo Alto Networks, Inc. (PANW)

Q1 2026 Earnings Call

CORPORATE PARTICIPANTS

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

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

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

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

OTHER PARTICIPANTS

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Rob D. Owens
Analyst, Piper Sandler & Co.

Saket Kalia
Analyst, Barclays Capital, Inc.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Tal Liani
Analyst, BofA Securities, Inc.

Meta A. Marshall
Analyst, Morgan Stanley & Co. LLC

Brian Essex
Analyst, JPMorgan Securities LLC

Joseph Gallo
Analyst, Jefferies LLC

Joshua Tilton
Analyst, Wolfe Research LLC

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

Fatima Boolani
Analyst, Citigroup Global Markets, Inc.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC

MANAGEMENT DISCUSSION SECTION

Hamza Fodderwala

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

Good day, everyone, and welcome to Palo Alto Networks' First Fiscal Quarter 2026 Earnings Conference Call. I am Hamza Fodderwala, Senior Vice President of Investor Relations and Strategic Finance. Please note that this call is being recorded today, Wednesday, November 19, 2025 at 1:30 PM Pacific Time.

With me on today's call to discuss our fiscal first quarter results are Nikesh Arora, our Chairman and Chief Executive Officer; and Dipak Golechha, our Chief Financial officer. Following our prepared remarks, Lee Klarich, our Chief Product and Technology Officer and Board member, will join us for the question-and-answer portion.

You can find the press release and other key information to supplement today's discussion on our website at investors.paloaltonetworks.com. While there, please click on the link for quarterly results to find the Q1 2026 supplemental information and Q1 2026 earnings presentation.

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

This presentation contains non-GAAP financial measures and key metrics relating to the company's past and future expected performance. Non-GAAP financial 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 otherwise noted, all results and comparisons are in a fiscal year-over-year basis. We also note that management is scheduled to participate in the UBS Conference this quarter. I will now turn the call over to Nikesh.

Nikesh Arora

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

Thank you, Hamza. Good afternoon and thank you everyone for joining us for our earnings call today. As you can see, we had a strong start to the year in Q1. We exceeded expectations across every guided metric, demand across our core business remains robust, and customers continue to platformize with us. Year-over-year, RPO grew 24%, NGS ARR was up 29%, and total revenue was up 16%. We saw strength across our portfolio in SASE, XSIAM, software firewalls, and even saw early traction in our AI security platform, Prisma AIRS.

Our top line growth was complemented by continued improvement and profitability, achieving our second straight quarter of 30-plus-percent operating margin. These results are a direct outcome of our strategy, too. By delivering better security outcomes, our platform is earning more and more of the trust that used to be fragmented across dozens of point products.

At the same time, the threat landscape continues to evolve faster than we expected because of AI. As many of you saw last week with one of the major AI platforms, AI hackers aren't a future threat, they're here now. This is

the first reported case of an AI agent autonomously conducting a large-scale nation-state cyberattack. The attacker was able to manipulate an agent to take steps on its own with minimal human intervention. This is a turning point, proof that attackers are already weaponizing AI agents at scale. Even more importantly, they're able to attack fast and will be able to exfiltrate faster.

AI is exposing the cracks in our enterprise architectures, which do not have robust security. Patches are incomplete, platforms are missing, there is a plethora of point products across the enterprise. This gap is exactly where attackers thrive. They're testing how far they can exploit a model. They're running prompt injections, jailbreaks, model manipulation, and now we're seeing the next phase, autonomous AI agents being leveraged into the attack chain.

AI is here, and with it, AI attackers are here, too. Our message is – to customers is clear: rea-time visibility and security are essential for infrastructure. This reality necessitates a paradigm shift in the industry. We must move away from today's fragmented security landscape and towards platformization.

AI requires a seamless cyber data strategy. This platform approach allows security agents to be utilized effectively by the good guys to detect attacks, protect customers, and remediate security concerns. Fragmentation creates friction, which, in turn, causes latency. Latency is a critical enemy of real-time cybersecurity. This is the backdrop that informs our strategy as we go forward. Now, let's get into the quarter.

In Q1, platformization once again drove large deals across multiple industry verticals. This included US federal, where we had a strong quarter and notable competitive wins. One example was a $33 million SASE deal with a US cabinet agency securing 60,000 seats. This agency displaced a major SASE incumbent as they needed a platform to provide unified visibility across both their firewall estate and remote endpoints. Another example was a $100 million deal with a large US telecom provider. This included an $85 million commitment to XSIAM, which is our largest XSIAM deal ever.

This customer chose us to consolidate their disparate point products based on the ability of our platform to deliver materially faster mean time to respond. The common theme across these large transactions is clear: customers are moving from managing vendor sprawl to demanding superior, demonstrable security outcomes through platformization. The natural place for customers to start their journey is network security, which remains our largest business.

In Q1, we continue to see strength in our next-generation software form factors. SASE had a phenomenal quarter. ARR grew 34% year-over-year and surpassed $1.3 billion in Q1, making us the fastest-growing SASE provider at scale. We now have approximately 6,800 SASE customers, including one-third of the Fortune 500 including leading technology companies like IBM and Oracle. Even though it's early days, we continue to see strong momentum with secure browsers. The arrival of AI and agentic browsers will expose security cracks in them and focus the enterprise on ensuring widespread adoption of secure browsers. In Q1, we crossed 7.5 million browsers sold, while our bookings nearly quadrupled year-over-year.

One more product which I'm getting more and more excited about recently is a shift I'm observing in our customers to deploy more and more software firewalls, and it's beginning to show in our results. Product revenues grew 23% year-over-year. Today, nearly half of our product revenues are driven by the software form factor. We now have over 12,500 customers and maintained our leading market position in software firewalls. As the AI transformation accelerates, growth in cloud workloads, the software firewall provides essential runtime protection with a new AI data center, and with its recent ability to step up and protect AI, we expect continued momentum.

Talking about protecting AI, let's talk for a bit about Prisma AIRS. As I mentioned earlier, AI is moving faster than expected. This creates a critical moment for enterprise innovation. The reality is that while 78% of organizations are embracing AI transformation, a staggering 94% still lack the necessary security guardrails, presenting a massive risk. With our acquisition of Protect AI now fully integrated, we introduced Prisma AIRS 2.0 in Q1, the industry's most comprehensive end-to-end platform to secure AI, protecting everything from autonomous agents to models that power them.

And I predict here that AI agents will become a problematic insider threat if not secured. Prisma AIRS is the essential circuit breaker layer to stop them. It unites deep model inspection, real-time agent defense against threats like prompt injection and continuous autonomous AI red teaming in one platform. And once our acquisition of CyberArk closes, the addition of identity security will be critical to this mission, providing the essential privileged controls to govern these new autonomous insider threats and prevent agent identity impersonation.

Our commitment to add security is driving new high-value partnerships, including a collaboration with NVIDIA to secure the AI factory with Prisma AIRS on BlueField and tight integrations with platforms like Glean, IBM, Factory and ServiceNow in securing the exploding number of agentic AI workflows. Early customer attraction is strong, reflecting the general market need. The number of AIRS deals in Q1 more than doubled versus last quarter. We believe we are the furthest ahead in AI security with marquee customers signing up with Palo Alto Networks. As they move from traditional to AI workloads, we believe we are going to continue to be in the pole position.

In the same way AI surprised the world with its pace, I want to talk about something else that is going to become relevant from a technology shift and security perspective, quantum. Quantum computing has seen significant innovation over the last year. We're getting more and more optimistic on the arrival of quantum and expect it to be commercialized by 2029. As is widely known, quantum computing has the ability to break current encryption across technology stacks. Enterprises have less than five years to get their estates to quantum readiness.

There is a fear that some nation-states will have quantum compute capability sooner than 2029. Just last month, our partner, IBM, announced they were able to run a key quantum error correction algorithm on commonly available chips. The US government and many other nations are emphasizing PQC or post-quantum cryptography to drive new cryptographic standards that are resistant to attacks from future large-scale quantum computers.

To address this, we have launched and are going to be delivering a complete quantum-safe strategy. First, we help you discover. In August, we launched our new version of PAN-OS 12.1 Orion, which provides a quantum readiness solution to give customers an automated inventory of their cryptographic risk. Second, we help you protect. We launched our new fifth-generation firewalls which are optimized for quantum security. Third, we help you accelerate. Our platform's unique cipher translation capability can make legacy systems quantum-safe immediately even if the application itself cannot be upgraded.

Beyond this, we have just announced that we're deepening our partnership with IBM to deliver the quantum-safe readiness and remediation service, a complete end-to-end solution for PQC migration.

Now moving to Cortex, which is a pillar of our security operations center strategy, XSIAM continued its incredible trajectory in Q1. We now have approximately 470 customers, with the average customer paying over $1 million in ARR. This includes large, referenceable customers in every major industry. The success is no coincidence. XSIAM was built for large-scale data processing, organizing it, normalizing it, and making sense of it in real time. Today, we're processing 15 petabytes of telemetry on a daily basis. The result is demonstrable security

outcomes. Over 60% of our deployed XSIAM customers have reduced their MTTR or median time to respond from days or weeks down to minutes.

I am also thrilled to announce the launch of AgentiX this quarter. AgentiX brings powerful AI agents directly to the core of enterprise security challenges. In the future, the only effective countermeasure against hacker AI will be our own AI agents, purpose-built for advanced security detection and remediation. For years, the industry has struggled with two defining issues: overwhelming alert fatigue and a massive global talent shortage. AgentiX is our definitive answer. This is a leap beyond mere automation, this is true autonomy.

The ability to use predefined agents or build custom agents to secure enterprise is a step change in how security will work in the future. We are fundamentally transforming security operations and optimization by deploying autonomous AI agents that deliver enhanced speed, superior efficiency, and greater control for security practitioners.

Right out of the box, AgentiX leverages a broad integration ecosystem, connecting with thousands of existing security and IT tools and third-party environments. It provides customers with an intelligent, fully governed and completely transparent teammate across the enterprise. Ready to operate on day one, AgentiX accelerates response, elevates quality, and frees up scarce human talent to focus on higher order strategic work.

Now shifting gears, I am pleased to announce our CyberArk integration plans remain fully on track and we're proud to have received overwhelming shareholder support for the acquisition, which is now expected to close in fiscal Q3. Since our announcements in July, we have spent more time with the CyberArk team. We are even more excited about the growth opportunity in future product road map. This includes our vision of democratizing identity security across the enterprise and making identity the next platform for Palo Alto Networks.

Anecdotally, our customers share in our enthusiasm and the early feedback has been encouraging. As many of you saw, CyberArk's business continues to execute, achieving record net new ARR in the most recent quarter. And even as we invest ahead of the curve, our long-term financial model remains intact. The scale of our platforms and operating leverage in our business reinforces our confidence in achieving 40-plus-percent free cash flow margins by FY 2028, inclusive of both the pending CyberArk and Chronosphere acquisitions. We are executing from a position of strength and we see a clear path to drive both innovation and financial discipline.

Now let's talk about our new announcement. I'm sure all of you are wondering why Palo Alto Networks, who is in the midst of a large acquisition of CyberArk, would engage in an acquisition at the same time of Chronosphere. I think it's important to understand where we are in the AI cycle. The AI cycle is moving fast. There's never a day that goes by without significant announcements on investments in AI data centers, AI infrastructure. This large surge towards building AI compute is causing a lot of the AI players to think about newer models for software stacks and infrastructure stacks in the future.

The 17-year old observability industry was not designed for the AI era. AI requires always on comprehensive observability at gigawatt scale. The challenge so far has been that full observability is cost prohibitive for the customer. Chronosphere is one of the fastest growing software companies in history. The observability solution from Chronosphere has already been deployed and has demonstrated scale at a large frontier model, where they continue to move workloads across, leading born-in-the-cloud consumer platforms [ph] deploying (00:15:03) full, comprehensive observability offering 99.9%-plus percent availability to their customers. Chronosphere is able to deliver this capability at a third of the cost of other industry leading solutions. Yes, a third.

With $1.5 trillion of compute coming online over the next few years, there will be continued demand for next generation observability led by Chronosphere. We're really excited about the possibility of delivering remediation to the observability category by bringing together capabilities of Chronosphere and our newly announced AgentiX platform. Chronosphere also recently had acquired a company called Calyptia, a data pipeline provider. That was complementing their focus on observability and ensuring the right data got onto their observability platform. Calyptia, integrated with XSIAM, will enable us to offer our XSIAM customers comprehensive security data pipelining capabilities in line with current industry trends.

This acquisition perfectly aligns with our strategic playbook. We acquire the best technology at an inflection point in industry, we invest in its development, utilize our go to market scale to quickly deliver this game changing innovation to our customers. Remember, this is barely 2.5% of our market cap, which is consistent with our tuck-in strategy over the last seven years of acquiring companies.

To summarize, we had a strong start of the year. Our core business is firing on all cylinders. Platformization continues to take hold and overall demand is strong. Over the last years, we have shown our ability to scale billion dollar plus ARR business in SASE and Cortex. Looking ahead, we think software firewalls is our hidden gem and possibly the next billion dollar opportunity. We maintain a relentless focus on innovation by tackling new challenges in AI, security and quantum.

Finally, our ambitions continue to grow. This year, we'll be significantly expanding our opportunity in new markets as we close the acquisition of CyberArk and Chronosphere in both categories of identity and observability, which we believe are in the midst of inflection due to AI. We are less than 5% penetrated into a TAM, reaching nearly $300 billion in the next three years. As such, we are raising our expectations from $15 billion to $20 billion in ARR for FY 2030.

With that, I will hand over the call to Dipak to review the quarterly results in detail.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you, Nikesh, and good afternoon, everybody. We have an exciting opportunity ahead of us. We continue to execute with excellence, and our TAM is expanding through the pending acquisitions with two category leaders in CyberArk and Chronosphere. Given that, I would like to provide some additional color around our announced acquisition of Chronosphere, as well as an update on the CyberArk integration planning, before moving into detail on our Q1 financial results and guidance.

As Nikesh mentioned, we announced our intent to acquire Chronosphere for a total consideration of $3.35 billion in cash and replacement equity awards. Chronosphere's Co-Founders Martin Mao and Rob Skillington and their employees will join Palo Alto Networks post-close. While Chronosphere does have significant ARR relative to most of our other acquisitions, we view this transaction to be more in line with the tuck-in acquisitions that we have done over the past eight years. The business has just over 250 employees, with a customer base focused on large AI and born-in-the-cloud enterprises. The momentum Chronosphere has achieved to reach over $160 million in ARR with triple digit growth has been impressive. For that reason, we expect Chronosphere to remain largely standalone post-close and, in the near-term, enabling us to balance integration timelines with the pending CyberArk acquisitions. We expect this transaction to close in the second half of our fiscal year 2026.

On CyberArk, our integration planning is proceeding exceptionally well, reflecting the strong collaborative spirit between our teams. We've had excellent cross-functional collaborations at multiple levels, including dozens of integration planning workshops across various functions. We are firmly on track to hit the ground running post

deal close, which we expect in fiscal Q3 subject to customary closing conditions. As you can tell from our Q1 results, we're pursuing these acquisitions from a position of strength. With that, let's dive deeper into the quarter.

Remaining performance obligation or RPO grew 24% to $15.5 billion. This metric is a key indicator of long-term revenue predictability and the scale of our committed business. Note that our RPO from Q1 last year included $68 million acquired from our QRadar acquisition, which took place in that period. Our current RPO, which reflects near-term revenue realization, stood at $6.9 billion, representing 16% growth. Reflecting stability in both the quality of our RPO and customer commitments, the average new contract duration remained consistent at approximately three years. NGS ARR ended the quarter at $5.85 billion, achieving 29% growth and exceeding the high end of our guidance. Adjusting for the $74 million contribution from the QRadar acquisition in the comparable prior period, our net new ARR in Q1 grew over 20%, [ph] and then (00:20:26) the momentum was broad-based with strength from software firewalls, SASE and XSIAM.

It is important to note that our NGS offerings drive all of our revenue line items, including product revenue, nearly half of which is from software over the last year, subscription revenue and the growing portion of our support revenue. Total revenue reached $2.47 billion, representing 16% growth, which exceeded the high end of our guided range. Product revenue grew 23% year-over-year. 44% of our trailing 12-month product revenue came from software form factors, and increased from 38% in the trailing 12 months and in Q1 2025. This acceleration is fueled by growth in our software firewalls and PAN-OS SD-WAN within product revenue. We continue to see stability in hardware appliances and early interest in our newly launched Gen 5 firewalls. Total services revenue grew 14%. Within this, both subscription and support revenues grew 14%. Geographically, we saw broad-based strength across all major theaters, with Americas growing 14%, EMEA up 18% and JPAC growing 22%.

Having discussed our top line strength, I'd like to take a moment to give an update on our platformizations in Q1. As Nikesh highlighted, platformization continues to take hold as customers look for a strategic security partner that can continually adapt and innovate with shifts in the cybersecurity threat landscape. Our ability to deliver best-in-class products through our unified platforms, Prisma AIRS and Quantum Security in Q1, for example, is a critical motivation for customers to platformize with us.

We completed approximately 60 net new platformizations this quarter. This momentum was driven by strength in XSIAM, where platformizations more than doubled year-over-year, affirming that customers are actively moving towards simplicity and integration to have real time outcomes. We now have nearly 170 customers with NGS ARR over $5 million, and 50 customers with NGS ARR over $10 million, both growing about 50% year-over-year. These result will enforce our target of $20 billion in NGS ARR by fiscal year 2030, inclusive of the pending CyberArk and Chronosphere acquisitions.

Moving down the income statement, our discipline focus on profitability and operational leverage is clearly visible in the performance metrics we delivered. Total gross margin for the quarter was 76.9%. We delivered product gross margins of 80.2%, an increase of 50 basis points year-over-year, and reflected a significant sequential improvement of 340 basis points compared to Q4 2025. The services segment also demonstrated positive margin trajectory, reaching 76.2%, which constitutes a sequential increase of 70 basis points.

We continue to be pleased by the continued growth of our SaaS offerings and remain actively engaged in executing cloud cost efficiencies. We delivered an operating margin of 30.2%, achieved an expansion of 140 basis points year-over-year, and our second consecutive quarter above 30%. This strong expansion reflects not only improvements in gross margin, but critically, our ability to drive sustained scale and efficiency across all of the OpEx line items.

We continue to apply an AI-first lens to all of our processes and functions. Notably, we have been able to deploy AI in our global customer support organization to drive three consecutive quarters of case volume reduction and reduce time to resolve for 11 consecutive quarters. As a direct outcome of this disciplined leverage, our diluted non-GAAP EPS reached $0.93, which exceeded the high end of our guidance. This execution provides the basis for strong adjusted free cash flow, which came in at $1.7 billion, up 17%. Our cash and cash equivalents at the end of the first quarter is now over $10 billion.

Finally, regarding capital allocation, our approach remains prudent. We do not repurchase any shares in Q1. Our buyback strategy remains opportunistic. We have $1 billion in share repurchase authorization remaining through December 2026. Ultimately, we remain focused on leveraging this efficiency to maximize long-term shareholder value.

With that, I will move on to Q2 and fiscal 2026 guidance. For the second fiscal quarter 2026, we expect NGS ARR to be in the range of $6.11 billion to $6.14 billion, an increase of 28%. Remaining performance obligation of $15.75 billion to $15.85 billion, an increase of 21% to 22%. Revenue to be in the range of $2.57 billion to $2.59 billion, an increase of 14% to 15%, and diluted non-GAAP EPS to be in the range of $0.93 to $0.95, an increase of 15% to 17%. For the fiscal year 2026, we expect NGS ARR in the range of $7 billion to $7.1 billion, an increase of 26% to 27%, remaining performance obligation of $18.6 billion to $18.7 billion, an increase of 17% to 18%. Revenue to be in the range of $10.50 billion to $10.54 billion, an increase of 14%. Operating margins to be in the range of 29.5% to 30%. Diluted non-GAAP EPS to be in the range of $3.80 to $3.90, an increase of 14% to 17%, and adjusted free cash flow margin in the range of 38% to 39%.

As Nikesh mentioned earlier, we are also reiterating our 40% plus adjusted free cash flow margin target for fiscal year 2028, inclusive of both CyberArk and Chronosphere. Furthermore, whilst we will provide more detailed guidance after closing the transaction, we expect to maintain an adjusted free cash flow margin of at least 37% for fiscal year 2026, inclusive of both CyberArk and Chronosphere, depending upon timing of close.

We've included our typical modeling points in the presentation for your review, but I would like to highlight a few now. One, as we noted last quarter, we continue to expect our net new NGS ARR and revenue to be second half and Q4 weighted as we continue to platformize with our customers. Two, we expect product revenue growth for Q2 to be approximately 17% to 18%. And finally, we expect $130 million to $140 million in CapEx in Q2 2026, which is inclusive of a $90 million non-recurring real estate CapEx. This $90 million will be removed from adjusted free cash flow in accordance with our typical treatment for these non-recurring items.

With that, I will turn it over to Hamza for Q&A.

QUESTION AND ANSWER SECTION

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

A

Okay, great. To allow for broad participation, I would ask that each analyst ask one question. With that, we'll start with Brad Zelnick from Deutsche Bank, followed by Rob Owens from Piper Sandler.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Great. Thanks, Hamza. And it's great to see vintage Nikesh coming out strong in Q1, even after a blowout Q4. So congrats to you and the team.

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

A

[ph] Hold (00:28:19) position, Brad. First question.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

I love it, I love it. Nikesh, 2026 is setting up as a perfect AI storm where every vendor has a story to tell, and it seems all roads lead back to identity, where you clearly are in process of acquiring the best asset out there. But stepping back, it's rare that the winner in one technology generation remains the winner and the next. So what is it that you're doing outside of smart M&A to disrupt yesterday's Palo Alto to ensure success into an AI and quantum future? Thank you.

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

A

Thank you, Brad. Well, I think there are enough examples in history of technology companies which have sustained multiple technology waves and continue to win. And I think you're seeing some of the multi-trillion dollar companies out there have been around for four, five, six, seven decades. So we hope we're one of those evergreen companies that persists and is able to execute on a similar trajectory. We are – as you can see, we are very, very aware of the two biggest technology trends ahead of us, both AI and quantum. What's fascinating is the need for network inspection does not go away.

From our perspective, AI and quantum are going to drive, A, lots more volume. So as the more bits that fly around, the more they need to be inspected, which means the need for bit inspection technologies is not going to go away, just the way the need for server hasn't gone away since the time servers were created. So I think we don't have a threat to our core business of bit inspection, which is how I broadly describe our network security business. And AI is driving more volumes.

I was just talking to the CEO of a large cloud service provider earlier today, and the conversation was about how they go deploy gigawatts of capacity in short order, given that large sort of thrust towards building AI compute, and how do we make sure those bits are secured. So I guess we are going to see sustained demand over time from a network security perspective. If you couple that with the trend that AI is driving, is the idea that now data can be sensed real time and actions can be taken quickly as we discussed the recent cyber attack, that was an attack which was based purely on online availability of data and the ability of persistent access.

From that perspective, we think the solution on the other side has to be a data driven problem – solution. And if you look at what we've been doing from an XSIAM perspective, we have 470 customers. Three years ago, I remember you and I talking about XSIAM as new product categories in the SOC space, and your question to me was, what makes you think you will succeed in a space you've never played in before? Well, Brad, we proved that we can get to close to 500 customers with $1 million ARR. I don't think I know any company in recent history in cybersecurity, which has an average ARR per customer of $1 million on a product category. So I think we've proven that we are able to execute on the back [ph] half (00:31:07). So last but not the least, and I give [ph] way to others and say (00:31:11) don't underestimate quantum. Quantum is going to break every key, which means every piece of infrastructure that hasn't been upgraded, has to be upgraded.

And I just learned of something the other day, which Lee taught me is, you don't even have to have a quantum computer to start breaking keys. You can actually start storing data today and break it later. So you can imagine nation states getting forward and saying, let's just ingest the data, hold on to it. Nobody's paying attention and I've got the data, we'll crack it later. So I just think all these technology trends are in the right direction. We have products positioned in each category. And I'll tell you what, in three years from now, we'll look back and say, damn, that Chronosphere acquisition was a very smart move because you need observability. If you want your stuff to work 99.9% of the time, you need to know if something goes down ASAP. You can't know that if you don't have the data.

And if you go back historically, the question has been the two largest category of data are security and observability, and that's where Splunk started by the way. All we've done is we are now the new platform for security and observability once we close Chronosphere. But thanks, Brad, for the question.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Thank you.

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

A

All right. Next, we have Rob Owens from Piper Sandler, followed by Saket Kalia from Barclays.

Rob D. Owens
Analyst, Piper Sandler & Co.

Q

Great. Thanks, Hamza, and good afternoon, everybody. Nikesh, just building on those comments, want to touch on Chronosphere. And it has been challenging I think for a lot of vendors in security to get into observability. So I'd love to see or hear from you your perspective on, number one, that convergence happening right now. And number two, I think Chronosphere has shown success with some of the largest AI native companies out there, having two of the top five frontier models. Are there elements behind their product sets that are applicable to some of these other large AI natives that are growing rapidly that you think you can have success with? Thanks.

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

A

So, Rob, me and the team – actually, here is my story. We actually found Chronosphere because we were looking around to see, oh my God, everybody is going in abstracting data pipelining, and everybody is going to have to have a data pipelining capability in the future in the SIEM. And honestly, as a category, we think data pipelining is sort of an interim category, which is there because of data inefficiency, but we don't think it has a

sustainable future. So we kind of like walked away from data pipelining vendors, which I know that some of the industry has tried to ingest as part of their SIEM solutions. But when we looked harder and we ran into Chronosphere, we discovered, and it's very rarely when your engineering team comes back and says, these guys are good. Generally, engineers have too much pride to tell you that somebody else is good. But our team came back and said, these guys are the best engineers we've run into.

Now to be able to scale observability, when you're ingesting petabytes of data at LLM model scale and be able to not create latency, provide observability in that kind of environment at a cost, which is a third. But look – but right now, if you go talk to every customer, even we, turn down our observability vendor because it's too expensive at Palo Alto, like we can't afford to have real-time observability on this platform because it's too expensive. The problem is you can't run financial services apps, you can't run large e-commerce businesses, you can't run large food delivery businesses without persistent observability.

So, what Chronosphere has done has changed the observability model by a combination of open source and techniques where they can do scale sort of data observability at the right price. So, we think every born-in-the-cloud company, every company that has a platform that requires customers to really access it 7 by 24 is a potential customer. And I think, again, it's going to be another business like XSIAM which we have an average ARR of $1 million at some point in time.

Rob D. Owens
Analyst, Piper Sandler & Co.

Q

All right. Thank you.

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

A

Great. Next, we have Saket Kalia from Barclays, followed by Matt Hedberg from RBC.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Okay, great. Hey, guys, thanks for taking my question here. Nikesh, it's interesting to see you sign larger and larger XSIAM deals. I think you called out an $85 million deal in the quarter, while at the same time, incumbents in this space are really struggling to grow. And in the past, you've talked about how XSIAM...

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

A

Saket, it makes sense. Incumbents don't grow. We take market share, which means we grow and they decline, that's how it works.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Totally understood. But maybe from a spending perspective, maybe the question is, do you find that XSIAM is able to capture at least what those customers were spending on incumbents or is there an opportunity to capture more because of that faster mean time to respond? Does that make sense?

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

A

It makes sense, Saket. I think the way to think about it differently is we do capture at least what the incumbent is – the customer is spending on the incumbent. But in the process of delivering XSIAM, we're able to consolidate multiple products. So not only do we get the incumbent spend of the SIEM provider, but you have UEBA, you have other carriers. Maybe, Lee, it's a good time for you to say something.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.
A

SOAR, ITDR, recent launches around email security, exposure management. So, we're able to consolidate these sort of surrounding product categories back onto a single platform. So, customer saves money, but we expand the overall footprint that we can deliver.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Very helpful. Thanks.

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

You bet.

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

Okay. Next, we have Matt Hedberg from RBC, followed by Tal Liani from Bank of America.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Thanks, Hamza. Congrats from me as well on the results. Obviously, a lot of really positive developments here. The $20 billion fiscal 2030 NGS ARR target is obviously super impressive relative to the prior target that you had outlined. Obviously, there are some tuck-in sort of M&A assumptions in there, but I guess I'm curious, like from a high level, Nikesh, what are some of the biggest moving pieces that give you the confidence since you talked about the prior target just last quarter to raise it [ph] which is (00:37:14) a significant margin?

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

Well, that's a good question, Matt. So first of all, as I said, our core business continues to show strength. And as every time we're doing forecasting, somebody says, oh, [ph] no (00:37:24), large numbers is going to start making these growth rates go down. But as I mentioned, SASE continues to be strong at $1.3 billion in ARR. We're growing faster than independent public companies which run SASE. So we feel that's a strong part of our business. Software firewalls I think is our hidden gem. 50% of the product, or 44-plus percent of our product there is coming from software. I don't think software firewalls is going to stop.

As you put more and more cloud workloads out there, people are discovering they need a software firewall. We've been waiting for that trend. It's arrived. We are probably outside of the CSPs, the only large vendor in the software firewall space. So we feel strong that our core business will keep performing, which allows us to sustain our $7 billion target in FY 2026 forward. If you take CyberArk, what we intend to do with it, we hope that business continues to transform from where they are to absorb more and more identity categories that we intend to do with them. And I think Chronosphere, if you add all three of them up, that gets us very close. Will there be tuck-in

between now and FY 2030? Sure, we will have tuck-ins, but as you've seen in the past, tuck-ins don't move the needle by billions of dollars. Tuck-ins move the needle by sustaining growth rates and giving you $300 million. But I think the lion's share is going to come from the three categories you've just outlined, in our core business, in identity and in observability.

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

A

Great. Next, we have Tal Liani from Bank of America, followed by Meta Marshall from Morgan Stanley.

Tal Liani
Analyst, BofA Securities, Inc.

Q

Hey, guys, two great acquisitions. Long-term, very promising. The question is the transitory period, what's the impact on dilution on margins or free cash flow margins? And then how long does it take to see the synergies so the sum of parts is greater than two?

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

A

Yeah. I'm going to let Dipak answer the precise questions, the numbers. As I said, Chronosphere, we will run independently. Martin and teams have done a great job. We will provide obviously the services from the HR, finance, marketing people, which is great because they don't have a large team in doing that. They are basically a bunch of really smart engineers and forward deployed engineers, as well as a few sales people. So, we're going to give them some support by introducing the right customers in very targeted fashion. But Martin is very capable, he will run the business with his team. We trust him to do that. We're just going to provide the sort of the rocket fuel in him to go out and meet customers and execute it as plan. So it's kind of – it's a low because – for us, it's very important because all of our focus from an integration perspective is on CyberArk.

From a CyberArk perspective, as I said, we've had some great meetings. We understand where it is. There will be some rational synergies on day one because we don't need certain things in duplicate. We think by the time we get to the end of this fiscal year, our fiscal year, FY 2026, we have a much better handle. We'll be able to align their sales quotas and their teams and territories around our plans. So that's where I think a little bit of reshaping will happen. But I will let Dipak about specific dilution and free cash flow margin.

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

A

Yeah. So, I think, Tal, like the key part, just what I said in my prepared remarks is like with both acquisitions, we believe that we'll be able to get back to the 40% free cash flow by 2028. Your question is really about what in the interim, and I specifically mentioned that we should be able to maintain at least 37% plus free cash flow margin even in the interim, like barring the one-time costs, which I think just highlights the bottom of the floor. So, we're pretty deep into – at our scale, we're pretty deep into understanding how much we can do, how fast. And it doesn't really move the needle as much as you think it might.

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

A

So between 37% to 40% over the next two years and 40-plus percent by 2028.

Tal Liani
Analyst, BofA Securities, Inc.

Q

Thank you.

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

A

Thank you, Tal. All right. Next, we have Meta Marshall from Morgan Stanley, followed by Brian Essex from JPMorgan.

Meta A. Marshall
Analyst, Morgan Stanley & Co. LLC

Q

Great. Thanks, and apologize for the voice. Great traction with XSIAM and Prisma this quarter. Just what inning are you seeing customers in, in terms of AI adoption? And is it different on AI for security versus kind of security for AI? Thanks.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Look, it's still early innings on AI adoption. I mean, there is – on one hand, what you see is this massive build-out of AI data centers and models and everything else. That's the leading indicator. But then when you start to look at enterprise adoption, there's huge scale of production pilots and early deployments and things like that. And that's really just the tip of the spear of what we think is coming. Having said that, though, the security of that tends to be trailing that. And so, the recent attacks that we're seeing both of AI as well as AI launching attacks is obviously going to start driving more and more awareness of the importance, really, of trying to do both of those things at the same time.

What I see when I talk to customers is a growing desire for the production pilots of AI to be run in parallel to the production pilots of AI security so that they're moving in lockstep. And so that's going to require a bit more urgency, I think, on the security side to be up in lockstep with the IT deployment side. And that's starting to happen, but it's still early.

Meta A. Marshall
Analyst, Morgan Stanley & Co. LLC

Q

Thanks.

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

A

All right. Thank you. And feel better, Meta. Next, we have Brian Essex from JPMorgan, followed by Joseph Gallo from Jefferies.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Thanks, Hamza. And congrats on the results, team. Yeah, I wanted to circle back on quantum. I saw the partnership with IBM on quantum-safe readiness. I guess question for Nikesh, are customers focused on this yet? Is this going to require some evangelism on your part, or will this be kind of like a Y2K event where they wait till the end, till the last minute to address their exposure? And then maybe for Lee, how do we think about the technology advantage that you have that gives you maybe a superior right to win for post-quantum readiness? Is

it the depth of visibility that you have and observability into networks, is it data protection, all the above? How do you frame that out?

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

A

Maybe you start [indiscernible] (00:43:40).

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Let's start with your question on timing. So, there is a couple of things that are driving a level of urgency. One is, as Nikesh was mentioning, this notion of harvest now, decrypt later is one of the concerns. So probably more nation state level type attack. But collecting encrypted data and then waiting for quantum to be unreal in order to decrypt it later. And so, there are certain types of data that will still be valuable years into the future. And so, that's one reason for urgency now. Second is it's not clear yet when quantum computers will be viable, and it's possible that they'll be viable before people are currently expecting. And so, there is a certain – that that variability is also factored in.

And I'd say third is this is likely for a lot of organizations a multiyear effort. And so if they don't start now, they won't be ready two, three, four years from now. And so, all of that is adding up to what I've noticed over the last, let's say, six, nine months is a pretty significant inflection in the number of customers are starting to talk about this and plan for this from an urgency perspective.

On the technical side, the – look, part of this is really just related to we started working on post-quantum several years ago. So, we did not wait to start working on this, we've had capabilities rolling out in the last few years, with the biggest launch being a few months ago with Orion. And that has put us in a very good position simply in terms of being ahead of many of the people out there.

Two, the – our ability to sort of see across hardware stack, software stack, SASE stacks, browser stacks now gives us, I think, probably the – one of the largest footprints where we can leverage existing deployments to get that visibility and to provide remediation versus having it all be net new. And the partnerships we announced is really pretty powerful because it allows us to work with others that can complement the pieces that we already have.

[indiscernible] (00:45:48)

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

A

And the only thing I will say to that, Brian, is, look, I understand you're – I used to be on your side of the world when I was at Y2K. We were all trying to figure out which stocks to buy, which ones not to buy. But the good news is in the Y2K, they're like you had to go and reset everything, there was no quick fix across the enterprise. And in this case, yes, the long-term solution is to strengthen everything and make it more robust. In the short term, we actually have a solution where, using techniques, we can actually take existing legacy enterprise infrastructure and secure for quantum.

So as a customer's CIO, would you rather take the risk or just rather spend a few million dollars and say, I am quantum secure until I can upgrade my infrastructure? The answer is cybersecurity is insurance anyway, so buy a little more insurance.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Are you seeing a compliance push yet or is that still on the horizon?

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Early stages of that, Brian.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Okay.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Early stages. It's coming.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Yeah. Very helpful. Thank you. I appreciate it.

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

A

Thank you, Brian. Next, we have Joe Gallo from Jefferies followed by Patrick Colville from Scotiabank.

Joseph Gallo
Analyst, Jefferies LLC

Q

Hey, guys. Thanks for the question. You made some architectural changes to the cloud security product earlier this year. Can you just update us on that? How has that been received by customers and any sense of how cloud security grew in 1Q versus 4Q?

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Yeah, the – so we made some changes, Joe, as you noted, with the launch of Cortex Cloud early in the year. This was made for a number of reasons. In large part, we were seeing a increased need from customers to be able to secure the full life cycle of their cloud deployments, from code to cloud deployments to runtime, even connected all the way into the SOC. And so the – that was the impetus behind this, and we've seen a lot of very positive feedback from customers in terms of aligning to their strategies as well, and then since then, we've been able to continue to drive further capabilities on that.

Earlier this year, we announced ASPM. So this is basically allowing us to prevent application security issues from working their way into production. And then most recently, we announced the new cloud security agent, so our CDR agent. We're able to be 50% more efficient in protecting cloud workloads with that. And so we continue to drive more and more innovation. Actually, the last one was with the launch of AgentiX, that is now natively available as part of Cortex Cloud as well. So we're even bringing agents to the cloud security mix to help automate customer workflows in the cloud.

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

All right. Thank you, Joe.

Joseph Gallo
Analyst, Jefferies LLC
Q

Yeah.

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

Next, we have Josh Tilton from Wolfe Research followed by Patrick Colville from Scotiabank.

Joshua Tilton
Analyst, Wolfe Research LLC
Q

Hey, guys, can you hear me? Not sure if it's supposed to be me or Patrick.

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.
A

Hey, Josh.

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

Go ahead. Josh.

Joshua Tilton
Analyst, Wolfe Research LLC
Q

Hey, guys. I just want to follow up on the first question from Brad. I do think that today, the current investor view is that identity security is the market that is best positioned to benefit in a agentic future. But, Nikesh...

[indiscernible] (00:49:01)

Joshua Tilton
Analyst, Wolfe Research LLC
Q

...I think in response to his question, you did mention that AI is increasing volume and inspection.

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

Yes.

Joshua Tilton
Analyst, Wolfe Research LLC
Q

So what I'm trying to understand is how should investors expect the volume of network traffic to change in a agentic future and what does that mean for the traditional firewall business and the SASE business?

Lee Klarich
Chief Product and Technology Officer & Director, Palo Alto Networks, Inc.

A

Look, I think the way to maybe think about it, Josh, is the advent of AI is just creating an extraordinary increase in the amount of data, both data concentration but also movement of data, right? So, we're seeing environments now that are beyond any scale that we've ever seen before just in terms of the amount of data that's moving around.

For example, you think about how much training data has to be brought to bear to entrain one of these models, let alone all the different models that are being built in different versions of models. And so that by itself is creating a noticeable influx in the amount of network traffic, but somewhat concentrated, concentrated toward the AI platforms themselves.

The second part that comes with that though is as AI becomes more and more deployed across the enterprises, that will also drive a similar pattern, albeit maybe at a slightly smaller scale. And that's the – part of what Nikesh was talking about both in terms of amount of data, but then that translates then to the observability needs, the application criticality needs and, of course, security on top of all of that.

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

A

Yeah, I think just – so I think you probably are alluding to the fact that we didn't explain the identity thing well enough. Look, identity is a market that products were designed 15, 20 years ago. And with all respect, in our view, IAM is not identity security, its hygiene and IT – its' IT capabilities. Like the fact that you have a badge doesn't make me secure. I have a badge to enter Palo Alto. That's not security, that keeps track of the fact that I'm in the building. It doesn't stop me from doing anything bad that I want to.

So we believe true security in the world of identity happens when you start enacting privileged access-type controls across identities. And our view with CyberArk is that the fact that – why are only 500,000 people in the enterprise privileged when pretty much the remaining 15,000 people at Palo Alto could cause equal amount of damage through other ways using systems? So our view is in the future, almost every identity will get some version of privileged access management, and CyberArk is the best platform, from our perspective, and asset in the industry to be able to leverage those capabilities.

Now we have to do some joint product work, which is not unlike the fact that when I came to Palo Alto, we had a network security company with 4 subscriptions, today, we have 10. We possibly will have 15 by the time the next five years come out. So, can I have identity platform with 15 different capabilities with the underpinnings of what is a CyberArk privileged access management platform? Yes, but that requires some degree of innovation, some degree of consolidation in the enterprise.

And the more we look into what CyberArk has, the more excited we get that there is an opportunity here, but yes, there's a bunch of work that needs to be done. As Lee and I were joking yesterday...

[indiscernible] (00:52:13)

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

A

...we called it back to the future.

Joshua Tilton
Analyst, Wolfe Research LLC

Q

Very helpful, guys. Thank you.

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

A

Thank you, Josh. Next, we have Patrick Colville from Scotiabank followed by Fatima Boolani from Citi.

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

Q

All right. Cheers, Hamza. My question is for Nikesh on Chronosphere. I mean, we know many of the VC backers – and I totally agree with your comments earlier that you're acquiring a top quality asset with a toehold in a tier 1 foundation model vendor, but my question is...

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

A

[indiscernible] (00:52:47) get there, Patrick.

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

Q

Okay. Nice.

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

A

There's more than a toe already, but we're working on getting the whole foot in there.

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

Q

Well, we're looking forward to seeing that.

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

A

Okay.

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

Q

So, I mean, maybe that – like I guess why has the advent of AI driven you to pull the trigger right now on the Chronosphere deal? And then also, if I think about Chronosphere, the buyer is typically a dev or maybe a CIO...

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

A

Yeah. Yeah.

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

Q

...which is quite different to your current buyer profile, so just talk me through your thinking of how you're going to penetrate those new buyers.

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

A

So, Patrick, what's interesting is that – let me ask in three different ways. One, the actual buyer for Chromosphere is very often the CIO or even the CEO. I had a conversation, as part of our diligence, with the CEO of a financial – fintech company. I said, hey, have you heard of Chromosphere? He's like, yes. I said, are they good? He's like, yes. I said how do you know them? He looked at me, stared me in the eye and said, you think I don't know my tech stack? So, I mean, these guys understand.

Remember, if your restaurant app goes down, your ride hailing app goes down, every second is lost revenue. What observability does is make sure it keeps track of whether any element of that stack is decaying, is any element showing latency, is there any performance issues across that stack? So you need constant, persistent observability. The problem is it's expensive. The current vendors charge a lot of money for it. Now Chronosphere is able to figure it out, is how to do the same thing at a third of the cost. So it's a combination of open source stack, it's a combination of enterprise-grade features, but they're pumping large amounts of data.

So the two biggest problems are scalability and cost. They solve both problems. Now, the cherry on the cake or the icing on the cake is we plan to take what you find in observability, marry that with the AgentiX genetics and provide remediation agents which haven't been done before. So, if you can take that entire life cycle and say, found the problem, solved the problem, built an agent, fixed the problem, right?

Now, these agents will be built in partnership with customers because no customer should allow us to independently reset their infrastructure, but they can now write capability on top of the platform saying, I found a problem, I'm going to automate it, I'm going to build an SRE agent, fix the problem. So, I think this is a huge opportunity.

And I'd say in the last year, 75% of my customer conversations are CIOs and 10% are CEOs. So I know the buyer, and that's why Martin's going to run the company. Listen, there are 173 companies in the world which all need persistent observability. We know all of the names. We know exactly who's deployed, this is what Martin does for a living, we'll go one at a time and convince them this is a platform to have. Each of those guys spends $5 million or $10 million a year with us, we're home.

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

A

Thank you, Patrick. Next, we have Fatima Boolani from Citi followed by Gregg Moskowitz from Mizuho.

Fatima Boolani
Analyst, Citigroup Global Markets, Inc.

Q

Thank you – excuse me, thank you for taking my questions. Nikesh, I was going to ask you an out of the box question in accordance with how out of the box your thoughts around Chronosphere...

[indiscernible] (00:56:02)

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

A

I would never expect anything else from you.

Fatima Boolani
Analyst, Citigroup Global Markets, Inc.

Q

It's my brand now. So what I wanted to ask you, you really have kept hitting home the point around TCO scalability, cost efficiency as a conduit for this convergence of security and observability, right? So in terms of the Chronosphere rationale, I wanted to ask you, how much of the rationale there was for you to effectively modernize, insource – whatever terminology you want to use, to modernize or insource the underlying fabric of your Cortex and XSIAM technology, right?

So in the context of everything you and Lee have talked about, an absolute explosion of data, an explosion of telemetry that's going to be hitting your iron, basically, for all your appliances, how much of the rationale for Chromosphere was that versus wanting to enter outright into a brand new market where you're going to try to win budgets?

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

A

I think about the latter, not the former. And if you go back, and I'm sure you've asked the question and many of you guys have asked me the question, there's always been this sort of fantasy that observability and security will come together at some level. And I think this is what started when Splunk, half the data is used for observability, half the data is used for security. So it started there, but it never progressed past that.

Most of the observability vendors were so caught up in trying to solve the observability problem that they dipped their toes in security. And I always say, if it was so easy to build security with 20 more engineers, then God bless you, why do we exist? And the same thing applies to observability. Like if you don't – these guys have spent – they have like 200-plus engineers, they've spent the last three years doing this and have proven scale in the market. So, yes, it's a phenomenal adjacent TAM which is going to grow in double digits for the next 5 to 10 years, and yes, we want a part of that.

And if you look at it from our ambition to get to $20 billion ARR, we're not going to get there if customers are not spending a lot of their IT and cybersecurity spend with us. Now, there is a connective tissue between data across enterprises, right? Over time, the best enterprises will have seamless data access across many of their data lakes, whether it's the observability data lake, it's their security data lake, their IT data lake because eventually, you want agents to go and go figure it out what's going on across multiple data lakes and solve your problem and sometimes problems cross across multiple data lakes, right?

If something's down in an application, maybe the firewall shut it down, so firewall's in the security data lake. So if you want this agentic capability across data lakes, all we're trying to do is we're trying to build the enterprise fabric with our customers so over time, we can provide more and more capability. I mean, think of what Lee said on XSIAM, we're building more and more modules on top because we can write more software on top of the existing data.

Why does my firewall have 15 subscriptions in 2030? What does it have 10 today? Same data, same data. How do I get quantum cryptography visibility? I watch network data. I watch network data from malware, I watch for URLs, I watch it for quantum keys. So once you get the data right, you can build tremendous amount of software

capability and one at a time take out slivers of the industry. This is the third data platform of the enterprise, which is observability. Once we get that data, imagine the amount of SRE activities and agents we can build over time.

So, I just think this is foundational to our ambition to be a very large tech company. And three to five years from now, we'll be sitting back and saying, oh my God, we get it, now you put a foray into the observability space, you got access to production data from enterprises that allows you to keep them running at 99.9% of time. You can see I'm excited about this.

[indiscernible] (00:59:42)

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

Thank you, Fatima. And as promised, our last question will be Gregg Moskowitz from Mizuho.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC
Q

All right. Thanks, Hamza. Nikesh, we continue to hear more and more adoption for your secure browser. Certainly, the data points you provided today back that up. But how pervasive can this become amongst your NetSec install base and how strong is the monetization opportunity associated with that?

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

So I think, Gregg, this – connecting it back to what I was talking to Fatima about, I think browsers are going to get more and more prevalent in the enterprise. And if you look historically, browsers have been a threat vector and they're not secure, right? Pretty much companies use the browsers that come out of the box with the OSs and there's a bunch of things, like we did a test POC with a customer, 500 of their – 5,000 of their browsers were tested, we found 167 were compromised, right? So there's – it's a wild, wild west of browsers out there and I think it's going to get worse when AI browsers come out with agentic capability, so you have much more of a flood of all kinds of browsers in the enterprise.

But browser has become, I'd say, 80% to 90% of the work space for most white-collar workers, even developers. Exclude the legacy guys, but 80% or 90% of the work is being done in the browser, so the browser does become a very strong entry point from a security threat perspective. It has both opportunities and challenges. The opportunities are far higher from a security perspective of the browser, so we just think the browser becomes an important part of the foundational fabric for us to deliver services in the future, right?

But we need to wait for its pervasiveness or its ubiquitousness in time, and that's why again it's one of those foundational things. If I can get 100 million browsers out there which are secure, I can deliver all kinds of security capabilities, but way higher than that. So to that extent, I think the monetization opportunity is sort of in the future at scale. Of course, there is monetization today. We don't give the browser away for free, and effectively, it's fungible as an endpoint agent from a SASE perspective.

So, right now, we're very keen on deployment and adoption and ubiquity of the browser. It has, obviously, financial impact on our SASE numbers, so you'll see it at $1.3 billion. But I think from a strategic perspective, the more we can get out there, the better security outcomes it can give them in the future.

Gregg Moskowitz

Analyst, Mizuho Securities USA LLC

Q

Great. Thank you.

Hamza Fodderwala

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

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

Nikesh Arora

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

Thank you again, everyone, for joining us today to discuss our results and the opportunities ahead. I also want to thank our partners, our employees, and everybody who contributed to these great outcomes for us in Q1. We continue to plot along for Q2 and beyond. And I just want to reiterate, really excited that we are now able to establish a toehold or perhaps a footprint in the spaces of identity and observability in the future.