17-Feb-2026

Palo Alto Networks, Inc. (PANW)

Q2 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

Rob D. Owens
Analyst, Piper Sandler & Co.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Saket Kalia
Analyst, Barclays Capital, Inc.

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

Joshua Tilton
Analyst, Wolfe Research LLC

John DiFucci
Analyst, Guggenheim Securities LLC

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Adam Tindle
Analyst, Raymond James & Associates, Inc.

Adam C. Borg
Analyst, Stifel, Nicolaus & Co., 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 Fiscal Second 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, Tuesday, February 17, 2026 at 1:30 PM Pacific Time.

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

You can find the press release and other information to supplement today's discussion on our website at investors.paloaltonetworks.com, while there, please click on the link for quarterly results to find the Q2 2026. Supplemental Information and Q2 2026 Earnings Presentation.

During the course of today's call, we'll be making forward-looking statements and projections regarding the company's business operations and financial performance, as well as the company's recent 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 expected future performance. Non-GAAP financial measures should not be considered a substitute for financial measures prepared in accordance with GAAP.

The most directly comparable GAAP financial measures and reconciliations are in the press release and the appendix of our investor presentation. Unless specifically noted otherwise, all results in comparisons are on a fiscal year-over-year basis.

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 today for our earnings call. We delivered a strong Q2 fueled by robust demand for cybersecurity and continued execution against our platformization strategy. This led to strong organic results in Q2 with NGS ARR up 28% and revenue growth of 15%, excluding the impact of recently closed Chronosphere.

We saw broad-based strength across our products from SASE, software firewalls and XSIAM to our emerging leadership in AI security with Prisma AIRS. We paired this growth with improving profitability, achieving a 30% plus operating margin for the third consecutive quarter.

We're excited to head into the second half of the year, having closed both the CyberArk and Chronosphere acquisitions, and I want to extend a warm welcome to both teams. Both companies continue to deliver record numbers in their most recent quarters, and we look forward to building on the momentum as we hit the ground running on our integration plans. These investments are a direct response to the inflections we see taking shape in the market. And while it's still early, the initial feedback from our customers has been very encouraging. We believe we're now entering the next phase of AI adoption.

Large enterprises are moving beyond experimentation and beginning to integrate foundational models into real workflows. As AI becomes embedded in day-to-day work, the central question that organizations face is shifting from capability to control. That shift has meaningful implications on security.

As AI becomes more pervasive across the enterprise, it expands the attack surface area, more agents, more infrastructure, more machine-to-machine activity and new classes of risk that simply did not exist before. In that environment, security cannot sit on the sidelines. Despite the current sentiment about AI and software, we firmly believe that security is enabling layer that allows innovation to move forward safely and at scale.

And as AI agents become autonomous employees, the old security playbook is not just slow, it's obsolete. Security must operate in real-time at the critical control points where decisions are made across network, endpoint, cloud, browser and identity. This is where Palo Alto Networks operates. And as AI becomes more embedded across the enterprise, those control points are converging.

A fragmented defense of disparate products is no longer a viable strategy. The risk is simply too high when adversaries are moving at machine speed. Our latest Unit 42 research confirms this, end-to-end attacks are now 4 times faster than a year ago, and in nearly a quarter of the cases attackers were able to break in and exfiltrate data in under an hour.

The good news is that 90% of those breaches were preventable, caused by basic gaps in visibility and controls across multiple attack vectors. This is why we committed to our platformization strategy a few years ago.

A platformized approach built on a real-time data-driven model that gets smarter with scale is the only way to secure the modern enterprise, and our results continue to prove that out. In Q2, we delivered approximately 110 net new platformizations, a quarterly record outside of our seasonally strong Q4.

This brings our total platformizations count approximately 1,550, up 35%. The success of this strategy is also reflected in our best-in-class net retention rate amongst platformized customers, which stands at 119% with low-single digit churn. This proves that once customers adopt our platform, they not only stay but continue to invest more with us over time.

This momentum isn't accidental, it is a result of a deliberate flywheel motion we built. When we committed to our platformization strategy years ago, we're betting on a shift that has now become an industry standard. This approach allows us to not only solve today's problems, but also provides the foundation to address new ones as they emerge. It starts by providing multiple clear landing paths.

In network security, customers can begin with SASE, hardware or software firewalls, and now AI security with Prisma AIRS. In the SOC, [ph] they can rely on (00:06:12) our Cortex platform via XDR, cloud security or directly onto XSIAM, from any starting point customer experience, the superior outcomes of an integrated platform which leads them to adopt more deeply across our ecosystem.

In a market changing this quickly, we believe our responsibility is to anticipate the next inflection and ensure our platform is ready. That philosophy guides our strategic investments, and the results give us the confidence to continue.

Our secure browser for example, was one such early investment that is now accelerating our SASE business with over 9 million licenses sold to-date. Similarly, in AI security, Prisma AIRS launched just a few quarters ago and already rapidly scaling with over 100 customers ending in Q2. This is the discipline we now plan to apply for the two large established markets poised for inflection, identity and observability.

If AI becomes a new interface for how work gets done, identity security will be required to create the permissions and boundaries that teams can trust. And as AI introduces unprecedented scale, observability is essential for building resilient systems that can operate reliably.

By bringing our platformization discipline to these new pillars, we believe we can deliver even greater value to our customers and solidify our role as a trusted partner to navigate the complex security and data challenges of AI era.

Let me share a few examples of how this strategy is translating into deeper, more strategic customer relationships. First, a global automotive leader selected us for a major security transformation. Their goal was to modernize their security architecture and dramatically improve efficacy. This resulted in an over $50 million deal, including $30 million for SASE and $20 million for XSIAM to run their global SOC.

Similarly, a global technology supplier selected us for a transformation initiative for over $40 million choosing XSIAM to modernize their security operations globally, while expanding their investment in SASE.

Finally, a transaction with leading IT service provider perfectly illustrates our flywheel. Building on existing investments, they committed for a $20 million expansion centered on XSIAM and have now platformized across network security and security operations.

These aren't just transactions. They're architectural decisions. When the stakes are highest, these wins validate that industry leaders are choosing the superior outcomes delivered by Palo Alto Networks.

With that, let's dive deeper into the individual performance of our platforms, starting with our largest segment. Our Network Security business delivered a standout quarter, demonstrating the power of a platform designed to meet customers wherever they are in their hybrid journey.

In Q2, our SASE business continued to go from strength-to-strength, surpassing the $1.5 billion ARR milestone while growing approximately 40% year-on-year, solidifying our position as the fastest growing SASE provider at scale.

[ph] What's particularly telling (00:09:03) in this shift, we are seeing in the market, many early adopters of SASE who made choices four or five years ago, during the pandemic, are now finding that those early solutions are not comprehensive enough for today's threats and complexity.

As a result, they're reconsidering their first generation point products in favor of a platform approach that provides a single, unified architecture to secure the entire hybrid environment, from the data center to the cloud and the remote workforce.

A key driver of these wins is also our secure browser, which stems from a strategic bet we made over two years ago with the acquisition of Talon. Our thesis was that the browser is the most critical, unmanaged edge where users, data, and now AI agents intersect.

The results show our customers agree. As of Q2, Prisma browser has been adopted by over 1,500 customers, 10% of which are in the Global 2000, with an additional 2 million licenses seats sold in Q2. This success has clearly not gone unnoticed. It's encouraging to see others in the industry waking up to the idea that they must secure their browser layer, validating the importance of this increasingly critical control point.

While many of these approaches simply extend existing architectures into the browser, we continue to believe the browser itself should function as a native security platform architective real-time control rather than retrofitted through extensions.

We also continue to see strong momentum in our software firewall business. Last quarter, we called it our hidden gem that was validated once again in Q2. Our ARR growth was approximately 25%, driven by the need to secure increasingly dynamic multi-cloud environments, a need that grows as AI workloads scale.

This is complemented by our strongest hardware performance in several quarters, with revenue up nearly 10%, driven in part by early adoption of our latest Gen 5 firewalls.

Finally, we remain focused on where the market is going. That includes preparing our customers for the post-quantum era. The threat is already here. Adversaries are using a harvest now, decrypt later strategy, stealing encrypted data today to break in the future. We're seeing this become a C-level priority in our early customer conversations.

And the broader interest in this topic was confirmed by nearly 5,000 attendees at our quantum Summit last month. This is a critical part of our customer's long-term roadmap, and we believe we are uniquely positioned to guide them through this coming architectural uplift and shift.

Now moving to Cortex. Customers continue to partner with us on their AI SOC modernization. In Q2, XSIAM surpassed the $0.5 billion ARR milestone. We welcome almost 150 new customers, bringing our total base to over 600, paying an average of nearly $1 million in ARR.

But the key story here remains not just the growth, it's the outcomes. Over 60% of our deployed customers now achieving, mean time remediation of less than ten minutes. The profound shift from the days or weeks they measured before. The success of XSIAM is a great example of our ability to identify a market inflection early, invest aggressively, and execute to scale.

We have made a bet on the AI-driven SOC well before it became an industry-wide theme. The results are showing its scale, in just three and a half years after GA. The same focus on what's next led us to develop AgentiX. The simplest way to think about it is we're enabling our customers to build a workforce of autonomous agents. But the key differentiator and what makes this real breakthrough is where these agents can operate.

Unlike traditional security tools confined to their own ecosystem, our agents can securely extend into first and third-party infrastructure. This means, an agent can not only detect an issue in XSIAM, but then can go out and auto-remediate it directly in a cloud console, an identity provider, or a firewall at machine speed.

This capability, already enabled by 200 XSIAM customers is key to delivering true enterprise wide automation. This is a powerful example of how we use AI to create better security outcome, but that's only one part of our AI security strategy.

Over the last couple of years, we have expanded our AI security capabilities, aligned to what our customers need as they deploy AI at scale. We're bringing those capabilities together as part of a universal AI security platform, one designed to protect AI deployments across models, agents, and the environments in which they operate.

It starts with Prisma AIRS to secure AI models and AI powered applications across their life cycle from model scanning and red teaming to runtime defense. We launched this platform just a few quarters ago, and its adoption has been remarkably strong. From Q1 to Q2, we more than tripled our customer count to over 100. While bookings also doubled during the same period, with the nine-figure pipeline already materializing, it's clear the market has been waiting for a comprehensive platform to secure AI.

At the same point, we're also seeing a new class of autonomous agents emerge. Software, that can perform tasks and interact with local systems on its own. This naturally extends security requirements to the endpoint.

This is why I'm excited to announce our intent to acquire Koi, a pioneer in securing the next major inflection point in security, the agentic endpoint. Koi will enhance our endpoint capabilities within XDR 2.0, while also becoming an integrated part of our universal AI security platform, extending security and governance to autonomous agents at the device layer.

We are witnessing a dramatic shift in how software lives on the endpoint, traditional security tools are often blind to the new AI layer of software, the massive rise of MCP servers, browser extensions, plugins, and ephemeral code that bypasses standard security controls. This represents a significant unmanaged attack surface.

We identified this new threat vector early and Palo Alto Networks has been a customer of Koi, since summer of 2025. On my recent trip to Israel in December, Lee Klarich, and I met with the Koi team and were immediately impressed by their foresight into the next generation of endpoint threats.

Since then, we've seen this risk pattern intensify, including security concerns that have been recently popularized by the widespread adoption of OpenClaw. We believe this is the latest example of what the future of AI attack surface will look like, and that Koi will help our XDR platform, remain well positioned to provide the most innovative security solutions to our customers.

After closing, Koi will also be able to provide unique extensions to Prisma AIRS and Prisma browser to ensure that our customers have visibility to any AI software and browser that are only present on the endpoint, resulting in the most comprehensive visibility to the AI attack surface. Overtime, this will help ensure that the endpoint becomes more agentic. Our customers will remain fully protected.

Now this focus on visibility is critical, but to act with precision, you first need to see with clarity. This is why a new level of observability is so essential, which brings me to Chronosphere. In the age of AI, Chronosphere offers a unique value proposition, deliver observability at a massive scale, proven in production today by many of the world's leading, born in the cloud and AI native companies.

During Q2 and after we closed the Chronosphere acquisition, we signed a multi-year, nine-figure expansion deal with a leading AI model provider, a testament of Chronosphere's ability to scale in the largest and most complex environments.

The momentum is clear in the numbers with the company generating approximately $200 million in ARR as of Q2, well above our expectations. The internal observability platform is also getting traction with over 80% of new logos last year landing with multiple products such as metrics, logs, and traces.

By combining Chronosphere's deep visibility with the automated action of AgentiX, we are enabling our customers to build a self-healing, autonomous enterprises of the future.

So we have prevention, we have visibility and we have automation. But every action, whether by a human or an AI agent, is governed by an identity, which brings me to our next newest major pillar.

We're delighted to have closed the acquisition of CyberArk early in Q3 and are ready to execute on what I believe is a massive opportunity in identity security. As many of you noticed earlier this month, CyberArk is coming off an exceptional December quarter, the record net new ARR and 30% of subscription ARR growth at scale. We've been rigorously building and refining our integration plans and we're moving fast to put these plans into execution. This includes aligning our go to market engines, we're already well underway on detailed account planning and aligned sales incentives to ensure our teams are collaborating from day 1.

From a product perspective, the innovation roadmap here is massive. We aren't just looking at legacy IAM, which in our view is basic hygiene. We're building a next generation identity security platform that protects across humans, machines and AI agents.

We also look forward to delivering machine identity and certificate lifecycle management to our 65,000 plus firewall customers. Longer term, we remain excited by the opportunity to address the growing needs of identity to secure AI agents. We bought CyberArk because when AI agents start logging in at machine speed, logging in becomes the primary attack factor. We believe we are now the only company that can verify the Who and secure the What simultaneously.

Given the momentum in the business currently and our innovation roadmap, we believe we are well positioned to become the largest identity security player over time.

In summary, we continue to execute against our platformization strategy in Q2 with momentum building across multiple areas of business. Our core innovation engine remains strong, with great traction and new products like AIRS and AgentiX, and ready to put our integration plans into action with CyberArk and Chronosphere.

Before I hand over to Dipak, I want to take a few minutes to reflect on the recent advancements in AI. We're seeing significant innovation in new agentic platforms targeting the enterprise. And while it's still early, it is causing some companies to reassess how the applications are built, how workflows are automated and how decisions are made.

Long standing assumptions about systems of record are being revisited, and perhaps even more so, the analytics layer built on top of that. In many enterprise applications, data reflects structured business processes within defined workflows. Security data is different, in our case, it is real-time threat activity generated at the control point where our platforms operate and continuously refined through more than 30 billion attacks blocked daily and 15 petabytes of telemetry processed in our AI SOC. That distinction matters when we say precision AI, it's not AI layered onto a feature set, it is AI trained on our proprietary dataset and embedded directly at those critical control points.

As AI begins interacting autonomously across application's infrastructure, fragmented security [ph] introduces delay, precisely (00:19:26) the wrong moment. Security must operate as a coordinated system, unified, consistent, and real-time. Because our platform sits at these control points, with these shifts, we see these shifts as they happen. The data generated across the network, cloud, identity, endpoint and browser continually informs our models, creating a feedback loop that compounds the scale.

But scale is not enough, sustaining leadership requires a willingness to adapt and challenge our own assumptions. Technology cycles change. Architectures evolve. Over the past seven and a half years, we've consistently aimed to invest ahead of inflection points in technology even when the path is not fully defined. Maintaining this discipline is vital to ensuring that we remain the digital guardian for our consumers. However, the technology stack could evolve.

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 everyone. As Nikesh noted, our strong Q2 results reflect the consistent execution of our platformization strategy coupled with a robust demand environment. The increasing adoption of our platforms is most evident in our next-generation security ARR, which grew 33% to $6.33 billion. This includes a $200 million contribution from our recent acquisition of Chronosphere.

On an organic basis, NGS ARR was up 28% year-over-year, and net new ARR was up 11% year-over-year. This performance was driven by an acceleration in SASE and software firewall ARR, alongside continued momentum in XSIAM. A key contributor to our software firewall growth in recent quarters is Prisma AIRS. As customers increase their AI deployments, they're looking for a trusted partner to secure this critical transformation. Prisma AIRS directly addresses this need and as Nikesh mentioned, it is scaling rapidly with over 100 customers ending Q2.

Our remaining performance obligation, or RPO, grew 23% to $16.0 billion. This includes approximately $150 million of RPO from our Chronosphere acquisition. It's important to note that RPO balances for Chronosphere can fluctuate from period-to-period given usage based pricing with ARR and revenue being more representative of business performance. Our current RPO, which represents the near-term revenue realization, was $7.1 billion, representing 18% growth.

Total revenue was $2.59 billion and grew 15%. Given the close of our Chronosphere acquisition came near the end of fiscal Q2, the revenue contribution was immaterial during the quarter.

Product revenue was up 22%, with 45% of the product revenue coming from software form factors over the trailing 12 months, which was up from 38% in the trailing 12 months ending Q2 2025. This was driven in part by strong demand for software firewalls as noted earlier.

Our software growth was complemented by improving hardware demand led by the adoption of our latest Gen 5 firewall appliances and SD-WAN.

Total services revenue grew slightly above 13%. Within this, subscription revenue was up 14%, while support revenue grew 12%. From a geographical perspective, we saw broad-based strength across all of our major theatres with the Americas growing 14%, EMEA growing 17%, and JPAC growing 17%.

Moving further down the income statement, our disciplined focus on profitability and operational leverage continue to deliver strong results in Q2. Given the timing of the Chronosphere acquisition, the impact of this transaction to our P&L financials was immaterial.

Our total gross margin for the quarter was 76.1%. Within this product gross margin was 78.2%, an increase of 150 basis points year-over-year, driven by a higher software mix compared to last year. As noted earlier, we did see improvement in our hardware business during Q2. Therefore, on a sequential basis, the higher mix of hardware and product revenue resulted in a 180-basis-point decrease to product gross margin versus Q1.

The services segment delivered gross margin of 75.6%, down 100 basis points year-over-year. The year-over-year change in services gross margin reflects a positive mix shift towards our high-growth SaaS offerings, which remain in the earlier part of their scaling curve. We continue to be pleased by the growth of our SaaS offerings and remain focused on driving efficiencies here.

Now turning to the supply chain. We observed a marginal impact on product COGS this quarter from higher memory and storage pricing, but we believe we are well-positioned to manage through these dynamics. First, our high and growing software mix provides a natural hedge.

Second, we will leverage our scale, deep supply chain expertise and lessons learned through COVID and prior supply chain constraints. And third, pricing actions taking effect later this fiscal year will help offset corresponding cost increases.

We have proactively factored these considerations into our Q3 and full year outlook. We delivered our third consecutive quarter of 30% plus operating margins with Q2 operating margin of 30.3%, a 190-basis-point expansion versus Q2 of last year. The strong expansion reflects our ability to drive consistent scale and efficiency across all OpEx line items.

Our diluted non-GAAP EPS reached $1.03, which once again came in above the high-end of our guidance. Q2 adjusted free cash flow was $502 million. On a trailing 12-month basis, we generated $3.75 billion in adjusted non-GAAP free cash flow, representing a margin of 37.9%.

Our cash and cash equivalents for the period was $7.9 billion, reflecting a $2.6 billion cash consideration for the Chronosphere acquisition. Given the recent close of our CyberArk acquisition, we expect a $2.3 billion cash outlay in Q3. This results in total combined cash outlay of $4.9 billion.

In connection with our acquisition of CyberArk, we guaranteed the payment obligations under CyberArk's convertible senior notes due 2030. The acquisition resulted in a make-whole fundamental change under the notes, and we will be making an offer to repurchase the notes in the coming days. We also issued 112 million shares in consideration for the CyberArk acquisition.

Before I turn to guidance, I also want to extend a warm welcome to the over 4,000 talented individuals from CyberArk and Chronosphere. We're thrilled to have them on-board and excited to execute on our integration plans to unlock the full value of these acquisitions. Our focus is on a frictionless onboarding experience for our new colleagues. And within just the first few days, we've provided access to collaboration tools for every individual to work as one cohesive team. We remain confident in our ability to deliver significant scale and leverage across every line of each of our financial statements.

From an operational standpoint, integration is being executed with the same rigor that we apply to running our core business. We've established clear governance, defined work streams across all functions, including IT – finance, IT, HR, product and go-to-market and implemented measures to ensure continuity for customers, partners and employees. Our priority is maintaining business momentum, while methodically bringing platforms, reporting structures and operating rhythms together. Taken together, we believe this disciplined approach to integration reinforces our confidence in delivering sustained growth and operating leverage, enabling us to achieve our target of 40% free cash flow margin by fiscal 2028 and our longer term goal of $20 billion in NGS ARR by fiscal 2030.

Now, let me take you through the guidance. Please note that our Q3 and full year 2026 guidance is inclusive of both the CyberArk and Chronosphere acquisitions, which have been aligned to our fiscal year and our definitions of certain non-GAAP metrics. This includes NGS ARR, which reflects only the subscription portion of CyberArk's ARR and has been conformed to our standard revenue based definition.

Our Q3 and full year 2026 guidance assumes reported NGS ARR, the CyberArk will be approximately 2% to 3% lower than the equivalent under CyberArk's previous bookings based ARR definition. Please see the appendix of our earnings presentation for more detail on the comparison of the two ARR definitions.

For the fiscal third quarter 2026, we expect NGS ARR to be in the range of $7.94 billion to $7.96 billion, an increase of 56%. This includes a $1.47 billion contribution from M&A. Remaining performance obligation of $17.85 billion to $17.95 billion, an increase of 32% to 33%. This includes a $1.6 billion contribution from M&A. Revenue to be in the range of $2.941 billion to $2.945 billion, an increase of 28% to 29%. This includes a $340 million contribution from M&A.

Our fully diluted share count of 812 million to 817 million shares, which accounts for the close of the CyberArk acquisition on February 11. Diluted non-GAAP EPS to be in the range of $0.78 to $0.80. For the fiscal year 2026, we expect NGS ARR to be in the range of $8.52 billion to $8.62 billion, an increase of 53% to 54%. This includes a $1.52 billion contribution from M&A. Remaining performance obligation of $20.2 billion to $20.3 billion, an increase of 28%, which includes a $1.6 billion contribution from M&A.

Revenue to be in the range of $11.28 billion to $11.31 billion, an increase of 22% to 23%. This includes a $760 million contribution from M&A. Operating margins to be in the range of 28.5% to 29%. Diluted non-GAAP EPS to be in the range of $3.65 to $3.70 per share. Our fully diluted share count of 768 million to 773 million shares, which accounts for the close of the CyberArk acquisition. And adjusted free cash flow margin of 37%.

We've included our typical modeling points in the presentation for your review, but I would like to highlight a few now. First, note that under our accounting policy, the upfront portion of term licenses and any perpetual license revenue from CyberArk will be recognized as product revenue. All of our Chronosphere revenue will be included in services. For Q3, we expect product revenue growth of 25%. And for the year, we expect product revenue growth in the low-20s.

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

QUESTION AND ANSWER SECTION

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

A

Thank you, Dipak. [Operator Instructions] First, we've got Rob Owens from Piper Sandler, followed by Brad Zelnick from Deutsche Bank.

Rob D. Owens
Analyst, Piper Sandler & Co.

Q

Great. Thank you, Hamza and good afternoon, everyone. Nikesh, looking back at 2018, 2019, there was a prevailing fear that cloud computing would render parts of the cybersecurity stack obsolete. At that time, you leaned in via M&A and repositioned the portfolio. And obviously, the business has tripled since that today. Now we enter this AI era and the narrative feels oddly similar. Could you compare that existential nature of this AI shift to what we saw in cloud? And maybe what areas you think will be obsolesced? And then specifically, is M&A the primary lever again this time around? Or does your starting position differ at Palo Alto from where you were, let's say, at the start of the cloud cycle? Thanks.

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

A

That's a long one question, Rob. Nice to see you again. So that's a good question, Rob. Look, I think when we looked at it in 2018, 2019, you were trying to manage two challenges. One challenge was how do we get customers to get off on-prem to cloud and then deliver them cloud security. And the other challenge was how do we deliver services off the cloud the customers would accept because they're being delivered from the cloud. And that's kind of where us, we had to refactor our entire security service and the firewall, delivered them from the cloud, which was a huge opportunity. We made a lot of acquisitions to deliver cloud security. And we fundamentally architected XSIAM at that point in time as a cloud-delivered SOC, which is generally not the prevailing trend.

I think this time, I'm still confused why the market is treating AI as a threat to at least cybersecurity, I can't speak for all the software because one thing we're definitely seeing that customers have figured out that they need to drive more consistency in their security stack to be able to respond faster using AI. You cannot respond fast if you've got 70 different vendors who have different data, different logs, different APIs running. So we are seeing a trend towards more consolidation, more platformization, and that's evident in what we said. We did our best number of platformizations this quarter than we have ever done, barring Q4, which is seasonally strong. So I think that's one trend we're seeing.

I think the other trend we are seeing is slow adoption on the enterprise side, slower than the consumer side of AI. But as the adoption is beginning to happen, we're beginning to hear conversations around security, which, as you see with Prisma AIRS, we delivered 100-plus customers. This is much faster than we did in cloud security. So people are adopting it faster. So from my perspective, AI is inevitable. It's going to be used by enterprises. As enterprises start putting more critical functionality in the hands of AI, they will want control of AI agents or of their AI infrastructure, and that requires more security. So I think generally, it's a positive trend towards more security adoption. I particularly believe it's a bigger trend towards platformization and consistency of data and harmonization of data on the enterprise. We're not collecting enough data right now to get good security outcomes.

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

Thank you, Rob. Next, we have Brad Zelnick from Deutsche Bank followed by Saket Kalia from Barclays.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Great. Thanks so much. Nice to see everybody. Nikesh, I pay close attention to the acquisitions you make and the things that you tell us because you've proven very astute at identifying future opportunities. As we think about XSIAM and the AI-driven SOC, I've heard investors concerned lately that LLMs are going to kill SIEM tools. How do we think about the balance of opportunity and threat of LLMs doing a lot of the things that we relied upon SIEM for. And even if you're competitive from a product standpoint, is there a risk that you now face a new strong competitor for these modernization opportunities?

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

A

So I think, Brad, the LLMs are a net positive and additive to our capability to deliver security, like, LLMs are very useful for data classification. We're doing DLP, because we've to relied on very traditional approaches towards exact matching data and try to do DLP and LLMs are much able to understand context, and this definitely looks like something that is – data that is restricted or PII.

So I think there are certain examples where generative AI and LLMs are extremely useful. All the examples you see, they're really good at looking at patterns and finding gaps that you'll see in offensive security or red teaming, LLMs are being helpful. I think the challenge that LLMs will face or do face in providing comprehensive security is, it's not the 95% of time they're right. It's the 5% of the time they're not right, you need to be right, right. This is like we're fighting bad guys who have to be right once, we have to be right 100 times, 100% of the time.

So LLMs until they get to 99%, 99.9% accuracy are not a threat to delivering security. They are tools that can be used to summarize capabilities. There will be agentic actions that can be used to get a lot of the pre-work done from a precision AI perspective and get data together. So I think AI it helps the cause. Every security company is going to have to use AI to deliver the capabilities that they deliver today.

So – and I think it's not a secret. Every one of us is working hard, almost every AI – every security product has some version of a Copilot that now runs in tandem with the product. This helps you understand the patterns, understand the capabilities, and be able to answer questions faster. I don't think it's going to replace the security product anytime soon.

And don't forget, Brad, one more thing is, in most cases, our security products sit at edges and create new data and logs that didn't exist from everything that's around them. So to the extent we are creating proprietary data and security that is not going to be replaced by an LLM. We're not a system of record. We're not a system of work. We are generating domain-specific data based on threats we see out in the environment, and then using that analytically to figure out how the customer should protect themselves.

Brad Zelnick
Analyst, Deutsche Bank Securities, Inc.

Q

Awesome. Super clear and super helpful. Thank you.

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

A

Okay. Thank you, Brad. Next we have Saket Kalia from Barclays, followed by Meta Marshall from Morgan Stanley.

Saket Kalia
Analyst, Barclays Capital, Inc.

Q

Okay. Great. Hey, thanks for taking my question here. Congrats on closing Chronosphere and CyberArk. Nikesh, maybe on that point, I'd love to dig into the joint pipeline opportunity with CyberArk a little bit.

You have a big go-to-market machine that we can leverage here. So I'm just, kind of, curious how you think that opportunity unfolds, and maybe relatedly, Dipak, for you, you gave some breadcrumbs earlier on CyberArk on inorganic, but wondered if you could help us bridge maybe how much ARR we can include for CyberArk this year as we kind of think about that buildup of organic versus inorganic?

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

A

So Saket, the good news is that CyberArk has a phenomenal team out there in the field, so does Palo Alto Networks. We have very carefully, [ph] sort of (00:38:32), been working with them after the close. Both teams have been made aware of how to pursue joint opportunities together. We understand our pipeline. We understand their pipeline. We built a roadmap for overlapping pipeline where both customer has opportunities in the fray in the next three to six months, and we've already armed the teams with plans as to how to address the joint opportunity.

But what's fascinating is just anecdotally, just as you are informing the teams, we already have had CyberArk reps come tell us they have an opportunity for Palo Alto's products in an account they're particularly strong at. And I know that BJ Jenkins, our President, was on a call over the weekend, trying to help close the customer for CyberArk reps with Palo Alto capability, and it's happening in both directions. But I think it's early days. But I think the opportunity is real. And as the teams get to know each other, as they get to know each other's processes, I think we're going to see more and more momentum with both the teams. It is going to be a bit of a crawl, walk, run, because right now both our systems are different, so we have to do this stuff manually and we have people helping us build sort of a central acceleration team, which drives both.

But as CyberArk teams understand more and more of the Palo Alto products and the capability in the platforms, and as Palo Alto teams understand the CyberArk capabilities and also as we work with CyberArk team to build the next generation of products that we've been ideating with them recently, I think we're going to see continued momentum in both those pursuits.

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

A

Yeah. And then if I can just take the breakout. So look, we're not breaking out every M&A deal that we do separately all the time. However, just as a baseline Saket, we did say that CyberArk NGS ARR was about $1.2 billion as of December 2025. And I just said that in my prepared remarks that $200 million of ARR came from

Chronosphere. And then I've also guided what the total M&A contribution is. So, I think it's hopefully you'll agree that it's a lot more than breadcrumbs to be able to allow you to do the math here.

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

[ph] Full English breakfast (00:40:24).

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

That's right.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

We'll take it. Thank you.

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

All right. Thank you, Saket. Next we have Meta Marshall from Morgan Stanley followed by Josh Tilton from Wolfe Research.

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

Great. Thanks and congrats on the quarter. Maybe just a question for me on SASE business. We saw a nice reacceleration in that business in fiscal Q2. Just any commentary about what you're kind of seeing driving some of that strength. Thanks.

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

Yeah. Good question. We're obviously very excited by seeing that business accelerate at scale. I think Nikesh said it fairly well when he talked about, sort of this notion of a first gen adoption of customers that was tended to be more sort of point product type adoption. They're trying to solve a particular problem. And the existing solution at the time, we're pretty good at solving that one problem. And now we're seeing both new customers, as well as many of those customers come back and look for a more comprehensive solve. Their employees might all in one day show up to an office and work, work from home and work while traveling and if they get three completely different experiences and application access and everything else, it doesn't work for them from a productivity perspective.

And so what we're able to do by delivering this as a platform is, we can bridge how we apply network security from a hardware perspective, software perspective, SASE perspective, and even all the way down into the browser with Prisma browser, all in a very consistent way, both for security outcomes, as well as the end user experience and the productivity they achieve. That is the overarching trend that I see, and what's driving the business right now in SASE and the customer excitement about what we do.

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

Great. Thanks.

Operator: All right. Thank you, Meta. Next we have Josh Tilton from Wolfe Research followed by John DiFucci from Guggenheim.

Joshua Tilton
Analyst, Wolfe Research LLC

Q

Thank you, guys. Maybe just a high level one for me. What are you guys seeing in regards to the volume of network traffic from your customers as they move more out of the experimentation phase and actually start to really adopt agents enterprise wide? And how, if at all, will that impact the demand for the broader network security suite, whether that's firewall or SASE?

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

A

It's too early to tell. I think if you look at the AI adoption in the enterprise, there is a surge of AI adoption in the coding space. So people using Codex, Cursor, Claude code and equivalent, you're seeing a lot of that. Those are very application-specific. And actually, that fits exactly where Koi operates because when you start doing coding and vibe coding off your desktop, you'll see MCP servers and clients spun up on edges, you'll see a whole bunch of code that is sitting at the edge, which is not visible to traditional XDR capability. That's why, that was a solution we were using Koi. And that's where we saw they had traction. They had 40, 50 customers, and we were a customer of their. And so, well, this is an unsolved problem in security, and this is kind of where all the action is from an enterprise adoption perspective.

Outside of that, there is now enterprise adoption that we're beginning to see where customers are running perhaps millions of tokens in one or two particular applications they're working with some of the LLM providers on, and that's where we see the traffic. That traffic is again more within the network. I don't think it's traffic that networks cannot handle. I think the challenge right now is consolidating that traffic. How do you get all the AI traffic to be in one place so you can understand it, provide visibility, look at the ability to control it and be able to act on it.

So I think that's going to be the next bastion as to how do we figure out the solution for all this traffic that is beginning to have a different nature in enterprise, and it needs a different set of controls and tools. But it's not really impacting the network level traffic yet. And I say yet because as adoption grows, I fully expect. I mean, you can't build $600 billion worth of data centers and not expect traffic to grow and you can't expect that not to happen. So I think that's going to happen. The data center is being built. It's early days and consumer actually is far outstripping enterprise for the moment, but we expect enterprise will surely and slowly get on that bandwagon.

Joshua Tilton
Analyst, Wolfe Research LLC

Q

Super helpful. Thank you.

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

A

Thank you, Josh. Next, we have John DiFucci from Guggenheim, followed by Gabriela Borges from Goldman Sachs.

John DiFucci
Analyst, Guggenheim Securities LLC

Q

Thank you for taking my question. Nikesh, I agree with you, everything you said.

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

Thank you, John. I'm going to sleep better tonight.

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

Next question.

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

You can stop now. It's good. Great question.

John DiFucci
Analyst, Guggenheim Securities LLC
Q

I don't always agree with you, but I really do on this.

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

Okay. Good.

John DiFucci
Analyst, Guggenheim Securities LLC
Q

I really do. I agree with you on everything you're saying about AI, its positive effects on security. I actually really like the acquisitions you've done here. But if AI is going to be good for security, and I think it will in both cases. Both you need to secure AI...

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

Yeah.

John DiFucci
Analyst, Guggenheim Securities LLC
Q

...also AI is going to – I could be a hacker if I want to be. But if that's the case, when are we going to see it? Because it doesn't show up in the number – it doesn't show – I mean, not that, it doesn't show up in your numbers yet. It doesn't show up in anybody's numbers yet, really, maybe a couple, but not really. I mean when – is this...

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

No, I think that's – look, I think, John, if you – I think the best analogy I can give you is if you look at cloud security, you didn't see cloud security numbers for a while because typically, cloud adoption in enterprises lagged the consumer. And then even then, it was literally a two-year cycle or a three-year cycle before enterprises fully got all their applications and workloads moved on to the cloud.

So I expect there – right now, if you look at it, you tell me how many enterprise AI apps are you using, which are driving tremendous amounts of throughput. And I can't think of anything but coding apps. Now coding apps are not resource intensive on your infrastructure, they're resource-intensive on your endpoint. So like endpoint capability and LLMs are where all the action is. So I think its early days. What I'm heartened by the fact is that our number of customers of Prisma AIRS is kind of following the same trajectory as XSIAM. The volume isn't there because the throughput is not coming through LLMs right now. So I think it's early days.

Look, you have to have 1 of 2 beliefs, John. You have to be in one camp or the other. Either you have to believe that the $600 billion of data centers that are being built are going to be consumed. And if you believe that, which most people seem to do, then that consumption is going to be 80/20, 80% consumer, 20% enterprise. But those data centers are yet to be built. I think what is happening is we're all laying the groundwork right now, it's a bit of a sort of an arms race to try and see who can get the AI security, sort of, platform up and running as quickly as we can.

And you can see innovations happening in every direction. That's why you see us buy protect.ai which is now well-integrated. We took the firewall, made an AI firewall. Now we're taking Koi. We see that, that's where the action is. The next is going to be how do you consolidate all the AI traffic in one place. So I think we're seeing the piece parts being built mid-flight. I think it's how to be a bit patient.

John DiFucci
Analyst, Guggenheim Securities LLC
Q

Okay. I'm not always patient, but I'm going to try. Thank you.

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

All right. Thank you, John.

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

All right, John. Thank you for the question. Next we have Gabriela Borges from Goldman Sachs, followed by Adam Tindle from Raymond James.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC
Q

Hey, good afternoon. This one is for Lee. It's a CyberArk question, but it's a product based CyberArk question. If we think about CyberArk historically being strong for privileged users at the high-end, what is the technical lift that has to be done to make that technology more accessible for every user?

And I'm curious what you've learned in the last six months or so from your customer base on the method to securing agentic identity between PAM, IGA and IAM. Any learnings from the last six months would be curious to hear? Thanks so much.

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

Yeah. Thanks, Gabriela. Good question. First let me start with your first question. The – I think, the just the general space of privileged access management has largely been a more, sort of, sophisticated category. And as such has been the more sort of security conscious enterprises have been the biggest adopters.

And there's already sort of a transformation underfoot of, sort of this notion of modern PAM and moving to just in time controls and zero standing privileges and things like that. And part of that is actually improving security, but part of it actually is also about making it easier for the end user to actually interact with these systems.

We so that's already happening. The further we have ideas for how we can leverage integrations between CyberArk and for example, Prisma browser in terms of how do we integrate capabilities in the place where the user is already doing work in order to make it even easier for them to take advantage of these capabilities.

So we – there's already a lot of progress, and we have more ideas for how we're going to continue to make that easier so we can drive broader adoption across existing customers, but also make it easier for non-customers to adopt. And then ultimately, we think that leads to the broader sort of full human identity solution that we're excited about.

Now, as that is happening, yes, there is the agentic identity, sort of market that is rapidly forming. And look, my view on agentic identity is, it's going to have, sort of aspects of machine identity and privileged users sort of wrapped into one. And this is partly why I think CyberArk is well-suited for being able to go after this because of their leadership in both of those foundational spaces. And then, it's how do we adapt, add to, and then optimize for agentic use cases. And again, some of that will be, sort of, I'll call it standalone CyberArk from an identity platform perspective and some of it will be how we think about that in concert with Prisma AIRS, where we already have hooks into the AI infrastructure, and we'll have again integration opportunities to be able to bring solutions to our customers.

Gabriela Borges
Analyst, Goldman Sachs & Co. LLC

Q

That makes sense. Thank you.

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

A

All right. Thank you, Gabriela. Next we have Adam Tindle from Raymond James, followed by Shaul Eyal from Cowen.

Adam Tindle
Analyst, Raymond James & Associates, Inc.

Q

Okay. Thanks, Hamza. Nikesh in your comments, you talked about it with Chronosphere, a nine-figure expansion deal with the leading AI provider. I just want to pick on that and just ask about the key attributes that help Chronosphere get that level of commitment where you displacing an existing vendor, the timing for that, the rationale for it, and maybe even the pipeline beyond that?

And just a quick clarification, Dipak, just because I know this is coming up in after hours after you talked about ARR in total. I think investors are stripping out the $1.47 billion from Q3 NGS ARR and looking like organic net new NGS ARR is down a lot. I think there's probably some flaws to that. But just want to toss that out there to have you clear the air? Thanks.

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

A

All right, Adam. First things first, look, Chronosphere is a highly scalable solution, and its scalability is dependent on a net new architecture design for observability, which is different from what the current incumbents in the space have.

So that's scalability allows them to deliver those capabilities at approximately half the price, if not more than – or less than some of the other players out there. So they are displacing another vendor in that space.

They have been partnering with the large language model over the last six months or so. And they have passed every technical hurdle which allowed them to make a commitment to Chronosphere. We expect the full transformation over the next 6 to 12 months or full transition from the other vendor.

Part of the $200 million ARR is from one of those large LLM vendors. We expect that to continue to grow. In addition to that, they have other customers who are significant customers, and they are going to pursue significant customers over the next three, six months in partnership with us.

But that's why we bought the company because of the scalability, because of the capability from a technical as well as a commercial perspective. And we're – Lee is going to – Lee can talk more about product capabilities that we're going to give it.

But we hope that, that will allow it to be a full, sort of, full scale replacement option for both DIY, many customers do DIY in that situation as well as being able to compete effectively with some of the big observability players out there.

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

Yeah. Look, I'll just give you a high level. [ph] Adam (00:53:06), they've built something very unique for that very high-end of the market, scalability and the economic aspects, even the start of some of the AI analytics and that will complement with the AgentiX. The next phase is going to be how do we build out a lot of sort of enterprise, sort of off-the-shelf kind of features that make it just really easy to do integrations to basically replace existing incumbent infrastructure, whether that's commercial products or open source. We think in both cases the Chronosphere will scale down into that large enterprise segment very nicely.

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

And then, Adam, just on your question on NGS ARR, just to be clear of organic NGS ARR is roughly in line with consensus for Q3 and we've reiterated the full year. So maybe folks just haven't fully appreciated that Chronosphere is closed before Q2, but we'll make sure that that's all cleared up.

Adam Tindle Q
Analyst, Raymond James & Associates, Inc.

Yeah. Thank you.

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

Okay. Looks like Shaul is not here. So next we'll go with Adam Borg at Stifel, followed by Gregg Moskowitz from Mizuho.

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

Q

Great. And thanks so much for taking the question. Maybe Nikesh, you talked about a little bit in the prepared remarks about the quantum opportunity. You talked about it a little bit last quarter. Love to hear more about kind of the early learnings from kind of the discussions with the customers from the panel a few weeks back and ultimately how you're thinking about the opportunity in coming years? Thanks so much.

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

A

Look, as part of the CyberArk deal, we've acquired Venafi. I'm going to have Lee talk about a new capability we're building called the Next Generation Trust subscription plus our quantum capability. We have been in discussion with 100 customers who are experimenting with our beta customers – product.

We have tremendous feedback for them. Our quantum capability is not just for Palo Alto firewalls. It actually looks at the enterprise capability. So we have actually integrated ten other vendors worth of quantum data into our quantum sub. But I'm going to let Lee talk about the sub.

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

A

I think – yeah, in both of these cases, whether it's cryptography and PQC or certificates and managing, the alternative is largely a very manual sort of human-centric repetitive kind of task approach.

It's either some poor person or people that have to constantly sort of manually go look at certificates, look at their renewal dates and ages and other things like that. And then redo them manually or we can do it through technology. The same is true with quantum cryptography. It's either a lot of manual consultation going through and trying to figure out what exists or we can use technology.

And so in both cases, we figured out. Obviously, Venafi, in one case that will be joining the team is and then the NetSec team is how do we use technology largely our next-gen firewalls, but not only our next-gen firewalls, other data sources as well to do that discovery, to be able to technologically discover everything that is needed.

And then through automation to then also be able to automate the process of remediation. And so this has obviously security benefits, but it also has reliability and uptime benefits as well, because you have to remember, in both of these cases these are fundamental to how production systems operate.

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

A

Okay. Thank you. We'll end it here with Gregg Moskowitz from Mizuho.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC

Q

All right, last question. Thank you, Hamza. So closing Palo Alto's, two largest ever acquisitions within a couple of weeks of each other, it's exciting, the potential is tremendous.

But it could also add an unprecedented amount of stress on the management team, engineering, go-to-market teams, et cetera. Nikesh, how do you keep everyone's eye on the ball, yourself included, and not be subject to execution or distraction issues? Thanks.

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

A

Well, Gregg, these acquisitions, at least in the case of Chronosphere, has been in the works the last two or three months. And CyberArk has been in the works the last seven months.

I've visited their Boston facility, spent days there with them. Lee and I were in Israel with the team and spent time with them. So CyberArk just didn't come upon us this week. It has been in the works over the last many six or seven months.

As you might have read, we had worked with the management team to fully understand what role every employee at CyberArk was going to have. So we were able to on the date of close, inform every employee what their role in the future joint organization was going to be, what their plans are.

Give OKRs, give targets to every one of them, so they all have that within the first 48 hours. So it's not like we've been waiting. There are some system transitions that we need to do in the case of CyberArk, which the teams are working hard, fast and furious on, we've had the opportunity to plan what they need to be.

So we have our eye on the ball. That's our job, right, from a CyberArk perspective.

And Chronosphere is honestly, [ph] in fact (00:58:14) that the price tag was big, but it's still a 250 people engineering team that does observability, which is fundamentally different from anything we've done. The only point of product interaction is they're working hard with the Cortex team to figure out how to incorporate AgentiX into their platform, so they can have agents solve the observability problem, not just sort of being an observability company.

And separate to that because they are, sort of, they are whale hunters, they go after big observability clients. We are able to selectively and surgically help them on a client-by-client basis and help them drive what they need to do. So this is our 32nd or 33rd acquisition being the two of them. We have a lot of lessons from prior acquisitions, which we have brought to bear, our teams have been working really hard over the last many months, and we have been actually adding capacity at our end to make sure we can handle some of these transitions that are required.

Gregg Moskowitz
Analyst, Mizuho Securities USA LLC

Q

Terrific. Thank you.

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

A

Thanks, Gregg.

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

Thanks, Gregg. All right, that concludes the Q&A portion of this call. I'll pass it back to Nikesh for any closing remarks.

Nikesh Arora

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

Well, I just want to say thank you to all of our customers, to all of our employees around the world. And thank you to all of you for joining us on our conference call. We will see you guys next quarter.