02-Jun-2026

Palo Alto Networks, Inc. (PANW)

Q3 2026 Earnings Call

CORPORATE PARTICIPANTS

Hamza Fodderwala
Senior Vice President-Investor Relations and 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

Saket Kalia
Analyst, Barclays Capital, Inc.

Brian Essex
Analyst, JPMorgan Securities LLC

Matthew Hedberg
Analyst, RBC Capital Markets LLC

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

Shaul Eyal
Analyst, TD Cowen

Fatima Boolani
Analyst, Citigroup Global Markets, Inc.

Michael Turrin
Analyst, Wells Fargo Securities LLC

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

John DiFucci
Analyst, Guggenheim Securities LLC

MANAGEMENT DISCUSSION SECTION

Hamza Fodderwala

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

Good day, everyone, and welcome to Palo Alto Networks Fiscal Third 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, June 2, 2026 at 1:30 PM Pacific Time.

With me on today's call to discuss our fiscal third quarter results are Nikesh Arora, our Chairman and Chief Executive Officer; and Dipak Golechha, our Chief Financial Officer. Following our prepared remarks, Lee Klarich, our Chief Product 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 Q3 2026 Supplemental Financials Information and Q3 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 today's presentation.

Our presentation also 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 as substitute for financial measures made 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 otherwise noted, all results and 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. As you can see, our Q3 performance was exceptional as we delivered a record quarter. Our results surpassed every guided metric, fueled by an acceleration in organic bookings momentum, the sustained tailwinds from our platformization strategy, and surging cybersecurity needs as AI transitions from experimental stages to enterprise-wide production.

Within our core portfolio, we achieved significant traction in Network Security in XSIAM, while Prisma AIRS continues to establish itself as the fastest-scaling product in our history. Altogether, we delivered $8.13 billion in

NGS ARR during the third quarter, representing 60% ARR growth. This is our most significant quarterly outperformance to-date and surpassed our guidance.

Our RPO reached $18.4 billion, up 36% compared to last year. When adjusting for our recent CyberArk and Chronosphere acquisitions, both of which are exceeding expectations in their first quarter post close. Our organic NGS ARR and RPO rose 28% and 22%, respectively. These results are materializing as AI fundamentally redefines the enterprise tech stack, elevating cybersecurity to mission-critical priority for every organization.

Much has been said about Mythos over the last many months. Over the past quarter, frontier AI development reached a critical inflection point. We have entered the era of truly cyber capable systems, where models like Mythos possess the autonomous capability to execute comprehensive attack campaigns from start to finish.

This represents a fundamental paradigm shift for the cybersecurity industry. The most critical factor in this transition is speed. When weaponized by adversaries, these frontier models can identify and weaponize vulnerabilities in mere minutes, a process that previously required months of manual effort.

Earlier this year, our Unit 42 researchers demonstrated the acceleration by simulating a comprehensive ransomware campaign from initial entry to data exfiltration in just 25 minutes. In contrast, the typical enterprise still requires days to identify a breach.

These existing latency gaps are already a concern, but the emergence of these latest models makes them completely unsustainable. We believe this is merely the opening act. As Frontier AI development continues to accelerate, we anticipate a three to six-month window before these systems evolve into more sophisticated [ph] hacking capable (00:04:50) entities globally.

Within a few years, we expect agentic AI to reach a level of autonomous execution that is truly unprecedented, scanning environments, generating bespoke exploits, and orchestrating end-to-end campaigns at machine speed without human intervention. That is the trajectory [ph] as a (00:05:09) modern threat landscape.

However, the same technological leap provides a powerful defensive advantage. We validated this potential during the quarter, leveraging our strategic partnerships with leading frontier labs. We utilized early access to their most advanced models to complete the equivalent of a year's worth of pen testing in less than three weeks. This unique vantage point allowed us to introduce Unit 42 frontier AI defense, enabling our customers to fortify their environments against AI-driven attacks.

Market reception has been exceptional. With north of 1,200 customers asking to meet us, we have already completed 800 meetings the last six weeks to help our customers think through their cybersecurity future. These meetings are driving conversations across the platform. In fact, we're already seeing strong interest in our agentic endpoint security offering since the acquisition of Koi and have already generated interest for over 150 customers. This is critical for securing rise in AI coding tools [ph] and (00:06:03) agents as they proliferate our endpoints.

While identifying vulnerability is a critical first step, true mission-critical protection is achieved at runtime. Real-time inline defense is the only way to shield even unpatched infrastructure as an attack sequence unfolds. This is where the cybersecurity battle will be won or lost.

Countering the next generation of adversaries requires a comprehensive architectural vision that goes far beyond simple large-language models. While the capabilities of these frontier systems are impressive, they are not a silver bullet for cybersecurity.

We currently see two major structural challenges. First, the prevalence of false positives, with error rates often reaching 25%, forcing manual intervention that destroys the speed advantage of automation. Second, these models always fail at the last mile of complexity, leaving critical gaps in remediation and vulnerability management.

In today's threat landscape, the most subtle 1% of novel attack techniques are what lead to the most devastating breaches. For every enterprise, the defensive bar must be perfect, while an attacker only needs to succeed once.

The probabilistic nature of even the most advanced systems leads to inaccuracies, and in a mission-critical environment, the cost of a false positive is simply too high. One wrong enforcement decision can take down a global production network.

Just as autonomous vehicles require constant real-time validation, an automated defense must be built on high-fidelity telemetry and battle-tested against every edge case to be mission-ready.

An AI model is only as effective as the data it can see. As frontier models become available to everyone, the real competitive advantage shifts one model to the data fuel. That is why having sensors that sit in line with live traffic is so vital. They provide the telemetry and context needed to outmaneuver bad actors while serving as a critical enforcement point.

The logic is simple, the more you integrate, the more you see, the more data you unify. The better the AI performs, the more you inspect at runtime, the faster you can stop an attack. Our global footprint now exceeds 125 million sensors across network, endpoint, and cloud, ingesting over 17 petabytes of daily telemetry. This scale creates a powerful flywheel.

Every new sensor makes our entire platform more intelligent, which leads to more deployments, more data, and even stronger real-time protection. This reality is why platformization is the only sustainable answer. The legacy approach of query-based tools that wait for human reaction cannot keep up with machine speed threats.

We're transforming the industry by consolidating data onto a single platform, reducing breach response times from days to minutes through AI-driven pre-analysis. Point products that silo data and increase latency are becoming obsolete. As the battle moves to fighting AI with AI, we believe Palo Alto Networks is in pole position, and our Q3 results prove that momentum.

As AI compresses attack timelines, only a platform that gets smarter with scale can respond fast enough. During third quarter, we secured 110 net new platformizations, a figure that includes 20 from our CyberArk and Chronosphere integrations.

These strategic additions expand our reach into large addressable markets within identity and observability. Given the fragmented nature of these sectors, they're perfectly aligned with our overarching platformization vision.

We concluded Q3 with roughly 2,280 total platformized customers, bolstered by the inclusion of our latest acquisitions. These engagements represent deep architectural commitments rather than simple transactions.

When organizations reach this integration milestone, they standardize their infrastructure on our platform, yielding superior long-term retention and expansion. This is reflected in our 120% net retention and single-digit churn rates amongst this cohort.

Moving forward, we remain confident in surpassing 4,000 platformizations by fiscal 2030, providing the primary momentum towards our $20 billion target for NGS ARR. The scale and quality of our customer wins this quarter reflect how strategic these platform commitments have become and how customers are increasingly bringing us in to secure their production AI deployments at scale.

Let me share a few examples. In Q3, we surpassed $200 million in ARR with the leading frontier AI lab that relies on us for observability across its most demanding training and inference clusters. We expect that to continue to grow again next quarter as they complete their migration to Chronosphere.

One of our largest Q3 deals was the $80 million transaction with a leading power producer in the United States, an organization at the center of the AI infrastructure expansion. They selected our next-generation firewalls and also adopted SASE to secure distributed workforce over 25,000 employees.

A global consulting leader signed a deal for over $20 million, selecting Prisma AIRS, our AI security platform, to secure its rapidly growing fleet of AI apps and agents, now running more than 2 trillion tokens per month on our platform. This was an existing platformized customer who spent several months working closely with us to secure this entirely new frontier. It was also a record Prisma AIRS win and speaks to how customers partners with us for their AI transformation journey.

As AI raises the stake, these deals further validate our position as the cybersecurity partner of choice. That was particularly notable in our Network Security business, where we had our strongest Q3 in several years. Our largest business unit, Network Security, delivered its most robust third quarter performance in years. This momentum underscores the mission-critical role of real-time network traffic inspection, as enterprise-wide AI initiatives continue to transition to production. We saw strong growth in hardware, SASE, and software firewalls during the period.

While we're in the early innings, we anticipate that AI will serve as a structural catalyst for deeper traffic inspection requirements. The initial phase of AI adoption was primarily conversational, but the shift towards agenetic AI represents a fundamental change. Unlike simple chatbots, autonomous agents trigger a massive volume of secondary machine-to-machine interactions, consistently accessing tools and data to complete complex workflows. This creates a surge in nonstop high-volume traffic that must be secured at runtime.

This evolution directly translates into heightened demand for high-throughput hardware, expanded cloud-based software capacity, and the necessity for unified policy enforcement across the entire platform. Our Q3 results featured the strongest hardware performance in a decade, with next-generation firewall booking rising nearly 40% year-over-year. This was supported by our latest Gen 5 appliances in early access and AI data center buildouts. We're seeing early adoption from a new class of buyers, including sovereign infrastructure providers and AI labs, representing a significant new market as deployments move beyond traditional hyperscalers.

A key differentiator for hardware portfolio remains the strength of our [ph] subscription attached (00:12:41), illustrating how our customers are standardizing security stack on our platform. Within our installed base, we currently average more than four subscriptions per device. Our innovation engine continues to expand this opportunity. We now provide 11 advanced subscriptions, including our Next-Generation Trust Security, which utilizes CyberArk's certificate management to address emerging compliance standards for shorter certificate lifestyles – lifespans.

[indiscernible] (00:13:06) Palo Alto Networks remains the fastest-growing provider in the SASE market. In Q3, SASE ARR reached $1.6 billion, growing 40% year-over-year as customers prioritize unified protection across hybrid workforces and AI applications. Competitive momentum remains high, with nearly 50 displacement wins totaling $200 million in contract value year-to-date.

Secure browser also achieved a major milestone, scaling to 11 million licenses, a fourfold increase that cements its status as a critical control point for the AI enterprise.

Furthermore, software firewalls remain a high growth pillar of our strategy. ARR rose 25% in Q3, accelerating as organizations expand their capacity to inspect growing traffic between cloud and AI workloads. As these environments scale, the requirements for high-fidelity telemetry only increases.

The common architectural approach [ph] that's (00:13:56) also increasing is driving increased customer growth in Prisma AIRS, which continues to be the fastest-growing product in our history. Organizations are aggressively moving beyond the experimental phase, deploying AI agents and applications into production. This transition creates entirely new mission-critical security demands. We believe we are the first in the industry to embrace AI security platformization, yes, AI security platformization capable of securing and monitoring AI end to end. We have effectively doubled our capabilities in this space in just over nine months.

Our journey began with securing models in runtime defense. We then integrated identity security to govern agent access and observability to trace agent behavior across complex infrastructure. Most recently, we expanded to agentic endpoint security as AI tools proliferate across the edge.

Our recent acquisition of Portkey marks yet another strategic milestone. As a leading AI gateway processing trillions of tokens monthly, Portkey provides a critical enforcement point to monitor every request to apply real-time policy to agent-to-agent interactions at scale.

This relentless innovation has established Prisma AIRS as our fastest-growing product ever. Reached over 300 customers in Q3, tripling our Q2 count, and have clear visibility towards $100 million in ARR with the next couple of quarters for a product that was not in the market one year ago.

Ultimately, securing the AI enterprise generates a massive volume of runtime telemetry. The data is only actionable if processed at machine speed, which is the core mission of our Cortex platform. XSIAM remains our primary response to the emerging frontier model threat. As attack cycles compress to machine speed, organizations can no longer rely on legacy query-based architectures or manual dashboards. Effectively, countering AI necessitates a defensive strategy powered by AI.

Upon the introduction of XSIAM 42 months ago, we entered the sector as a disruptive innovator, engineering our platforms to ground up to redefine security ops centers. Today, our platform processes more than 17 petabytes of daily telemetry, volume unmatched by any other pure-play security vendor.

We ended third quarter with more than $600 million in ARR, representing 100% year-over-year increase across a growing base of 740 customers. The most significant metric, however, is the outcome. The majority of our customers are now responding to threats in under 10 minutes. This is a dramatic reduction from the days or weeks previously required and serves as a blueprint for the modern SOC.

In observability, our Q3 performance was well above our initial expectations. As AI initiatives generate a surge in telemetry, Chronosphere is a purpose-built capability to scale alongside these workloads. Our observability ARR surpassed $300 million this quarter, nearly doubling since our acquisition announcement last autumn.

Furthermore, 80% of our net new customer acquisition this year adopted multiple products, reinforcing our platformization momentum. The world's leading AI natives, including two of the top five frontier labs, have adopted Chronosphere, validating our ability to provide observability at AI scale.

Beyond our early investments in markets where AI would drive a positive inflection, we also recognized early where AI would overhaul existing security categories. Consider Posture Management. Traditional periodic scanning is insufficient when attack timelines are measured in minutes. As a result, we proactively transitioned our cloud portfolio from static posture to real-time detection through Cortex Cloud. We're making steady progress and anticipate most Prisma customers will be migrated to Cortex Cloud by the end of the fiscal year.

Now, as these agents proliferate, every autonomous entity represents a new identity that must be managed, what leads directly to our progress with CyberArk. In our inaugural quarter post close, CyberArk has surpassed our internal benchmarks as we move to execute our unified vision for identity security. Last month, we launched Idira, our next-generation identity platform for the AI-driven enterprise.

For years, the industry operated under the IAM fallacy, the belief that you only needed to secure a handful of privileged administrators. In the era of agentic AI, that distinction has vanished. Every identity, whether human, machine or software agent, now possesses the potential to access the sensitive systems at machine speed. Idira addresses this shift by democratizing modern PAM controls across all users and extending protection to agentic identities, which represent the primary attack vector of the future.

Our execution in Q3 was strong. Joint go-to-market efforts have already initiated approximately 1,000 cross-org engagements. We have sustained CyberArk's growth trajectory while improving its profitability profile through our integration initiatives. Given our rapid progress, we're now three to six months ahead of our original timeline for converging CyberArk's profitability with our own, a milestone we expect to reach within the next 12 to 18 months. This acceleration reinforces our path towards a 40% free cash flow margin in fiscal 2028, which Dipak will talk about more.

The events of the third quarter represent a watershed moment for cybersecurity and has elevated our category even higher on the CIO priority list. Mark my words, Mythos has increased the terminal value of the entire cybersecurity industry. We are identifying several structural catalysts from the AI cycle, driving growth across our platform. First, AI creates a massive surge in traffic and connection points, requiring real-time inspection. As agents trigger hundreds of second actions, network security becomes indispensable foundation for safe AI adoption.

Second, countering machine-speed adversaries requires real-time automated defense. This is a core mission of XSIAM, consolidating data onto a single platform so AI can respond to threats in minutes rather than days. And third, in an environment populated by both human and agents, identity serves as a primary defensive layer. When autonomous entities can execute actions independently, securing access via Idira becomes mission-critical.

The convergence of these trends validates our platformization strategy. Managing fragmented data and siloed point products is no longer viable in an AI-driven landscape. A unified platform that gains intelligence with scale is the only path forward. While we're still in the early stages of this shift, we remain committed to innovating ahead of the threat landscape and earning our customers' trust every day.

I will now turn the call over to Dipak to discuss our financial results in greater detail.

Dipak Golechha

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you, Nikesh, and good afternoon, everyone. We delivered a record Q3 with broad-based demand across our platforms and geographies. We exceeded our guidance ranges across the board, driven by an acceleration in organic bookings growth and outperformance from our recent acquisitions as we made early progress on our integration efforts.

Please note that during my remarks, I will discuss results with and without the impact of Chronosphere and CyberArk. The financial impact of our acquisition of Koi, which closed later in the quarter, was immaterial to our Q3 results.

Starting with next-generation security ARR, we delivered 60% year-over-year growth in Q3, reaching $8.13 billion. This included $1.63 billion from CyberArk and Chronosphere. We surpassed $300 million in ARR for Chronosphere, our next-generation observability platform. That was an over 50% increase from Q2 and far exceeded our expectations, driven by an existing LLM customer increasing consumption as they continue to migrate from an incumbent vendor.

Excluding the impact of CyberArk and Chronosphere, NGS ARR was $6.5 billion, up 28% year-over-year, and net new NGS ARR was $370 million, up 18% year-over-year. Please note that this excludes ARR attached to our hardware backlog that also reached record levels for a Q3 quarter. We saw notable strength in Network Security, which is our largest segment and accounts for approximately 70% of our total revenue. All NetSec form factors delivered sustained or accelerating growth in Q3.

In SASE, ARR reached $1.6 billion, up 40% year-over-year, more than two times the overall market growth rate. We have seen a nearly 50% increase in SASE net new NGS ARR over the trailing 12 months, driven by continued scale, strong performance in net new logos, and displacement wins.

Software firewall showed strength once again this quarter, with ARR up 25% year-over-year, driven in part by the increase in Prisma AIRS and firewall Flex deals. As Nikesh highlighted, Prisma AIRS continues to be our fastest-growing product ever. We have over 300 Prisma AIRS as customers as of Q3, up from just 100 at the end of Q2. As AI adoption grows in the enterprise, we believe AIRS is becoming a foundational infrastructure for secure AI deployment.

Turning to remaining performance obligation, or RPO, we ended the quarter at $18.4 billion, growing 36% year-over-year. Excluding $1.8 billion from CyberArk and Chronosphere, RPO grew 22% year-over-year, which we believe is a direct result of our platformization strategy, driving deeper customer commitments across our platforms. Current RPO was $8.3 billion, up 34% year-over-year. Excluding the impact from CyberArk and Chronosphere, current RPO was $7.2 billion and grew 17% year-over-year, an acceleration versus 15% in Q2.

Total revenue for the quarter was $3 billion, growing 31% year-over-year. Product revenue was $594 million and total services revenue was $2.4 billion, both growing 31% year-over-year. As I've highlighted in previous quarters, software and recurring revenue now represent a large and growing portion of this line item.

Today, product revenue includes major growth drivers, including software firewalls and Prisma AIRS, SD-WAN, and self-hosted identity security subscriptions. As a result, 46% of our trailing 12-month product revenue in Q3 included recurring software revenue, a significant increase from just 22% three years ago.

Hardware, which is approximately 10% of our total revenue, delivered its best quarter in a decade, fueled by strong demand for our next-generation firewalls, and we saw early AI data center wins contributing to record Q3 backlog. Our next-generation firewall bookings grew nearly 40% year-over-year in Q3 as we continue to gain share. AI data centers and AI-driven enterprise networking needs are driving a new market opportunity for us, which could potentially be additive to our long-term growth for firewall appliances.

From a geographic perspective, we saw broad-based growth across all of our major theaters, with the Americas growing 32% year-over-year, EMEA up 32% year-over-year, and JPAC growing 26% year-over-year.

Moving down the P&L, our Q3 strength was not confined simply to our top line metrics as we continue to drive profitable growth across the P&L and executed against our M&A integration strategy. Total gross margin for the quarter was 75.8%. This included services gross margin of 75.1%. We continue to balance services gross margins by driving efficiencies in cloud hosting, while the shift – whilst the mix shift of our high-growth SaaS offerings increases. Within this, product gross margin was at 78.8%, which was a 40-basis-point improvement year-over-year.

Turning to the supply chain, we are closely monitoring rising component costs, particularly in memory and storage. Please note that we have approximately 1 million firewalls in the field and our required component volumes are not as significant as some of our peers. Furthermore, we remain well-positioned to navigate these dynamics for the following reasons.

First, our higher recurring revenue mix acts as a natural hedge. Hardware today accounts for approximately 10% of our total revenue compared to 20% in fiscal year 2021. Second, our vendors view us as critical infrastructure provider, and we have a track record of leveraging our prior supply chain experience and expertise to mitigate these impacts. This includes evaluating alternative sources of supply, extending purchase commitments with our suppliers.

Thirdly, we continue to evaluate further pricing actions. As a reminder, we implemented a 10% price increase on hardware in early April. The impact of pricing and rising component costs are reflected in our Q4 and fiscal 2026 outlook. These dynamics paired with the continued operating efficiency resulted in non-GAAP operating margin of 21.3% (sic) [27.1%] in Q3, flat versus Q3 of 2025. Looking forward, we expect to drive operating leverage as we scale and continue to make progress against our M&A integration plans.

In Q3, we made a lot of progress on our integration plans. This was driven by strong execution and collaboration by our teams across every function, including our new colleagues from our recent acquisitions who have truly risen to the occasion. This is already driving tangible results.

Our integration philosophy starts with product and our relentless focus on driving innovation. Just months after closing the CyberArk transaction, we introduced Idira, our next-generation identity security platform. This includes the key innovations Nikesh highlighted, including modern PAM and agentic identity security integrated with Prisma AIRS, as well as deeper integration of identity signals with our core NetSec and Cortex platforms. Early go-to-market collaboration has also been encouraging, with more than 1,000 cross-organization engagements initiated between the core and identity sales organizations to date.

On the expense side, we're leveraging our combined scale to drive improved cloud hosting economics for the acquired CyberArk business. Post close, we're optimizing our organizations to deliver a unified, one team culture that is future-ready. We are carefully reviewing every single line item across each of our financial statements to drive operating leverage across vendors and functions. This includes streamlining our combined real estate footprint, which includes over 40 new facilities from our acquisitions, to enhancing and fostering collaboration post close.

Additionally, we're optimizing our marketing and our IT vendor footprint. To date, we have identified more than 300 IT vendors to streamline and have already dispositioned approximately 20%. All of these factors combined will enable us to hit our CyberArk synergy targets about three to six months earlier than we initially anticipated. This visibility paired with our continued operating leverage across the overall company reinforces our confidence in reaching 40% free cash flow margin in fiscal 2028.

In Q3, we generated adjusted free cash flow of $910 million, a 57% increase year-over-year. On a trailing 12-month basis, we generated $4.08 billion in adjusted non-GAAP free cash flow. This represents a margin of 38.5%, a 430-basis-point improvement year-over-year, even with the inclusion of CyberArk and Chronosphere. We will, of course, have a full year of CyberArk and Chronosphere expenses next year, but these results solidify our continued ability to deliver best-in-class free cash flow margin and enabled us to raise our fiscal 2026 guidance.

The strong cash flow generation supports our opportunistic share repurchase program. During Q3, we utilized $1 billion to buy back 6.8 million shares at an average cost of $147.69 million. We currently maintain $1 billion of remaining capacity on our existing repurchase authorization.

Moving to the non-GAAP items, stock-based compensation increased sequentially to 17% of revenue in Q3, primarily driven by SBC related to our recent acquisitions. While M&A-related SBC will continue to be amortized in future quarters, we expect stock-based compensation as a percentage of revenue to return to pre-acquisition levels on a run rate basis in approximately 12 to 18 months.

Beyond stock-based compensation, our GAAP results are – also reflect transaction and integration costs from these acquisitions, further detailed in our SFI. These non-recurring charges resulted in the GAAP net loss per share of $0.22 for the quarter. Our diluted non-GAAP EPS, which adjusts for SBC and one-time items, reached $0.85, which came in $0.05 above the high end of our Q3 guidance.

Reflecting on my five years in the seat, I've always maintained that our business model scales well across every line item of our P&L. This financial framework is precisely what allows us to execute our broader corporate strategy from a position of strength. When you look at our M&A trajectory, we initially proved this execution capability by integrating over 20 tuck-in acquisitions to build out our platforms. Today, we are successfully integrating larger, highly strategic acquisitions, all while driving durable growth and balancing against our profitability commitments.

Now turning to guidance, given the acceleration in our Q3 organic bookings growth, our early progress on M&A integration and the strong Q4 pipeline, we are raising our full-year fiscal 2026 guidance across all metrics for both our core and acquired businesses. This quarter and last, we provided a breakout of performance for both our core business and our recent acquisitions. Our intention was always to make this a one-time in nature and move our disclosures closer in line to how we run the business, therefore, we'll be moving to total company guidance moving forward.

Beginning in fiscal 2027, we intend to provide segment-level revenue disclosures across Network Security, Cortex, and Identity. This will align our reporting with how we run the business and our platform strategy post integration.

Now let me take you through guidance in detail. For the fourth quarter 2026, we expect NGS ARR of $8.9 billion to $8.95 billion, or 59% to 60% growth; we expect RPO of $20.9 billion to $21 billion, or 32% to 33% growth; and we expect revenue of $3.345 billion to $3.355 billion, or 32% growth; fully diluted share count of 830 million to 840 million shares; diluted non-GAAP EPS to be in the range of $0.96 to $0.98.

For the fiscal year 2026, we expect NGS ARR of $8.9 billion to $8.95 billion, or 59% to 60% growth; we expect RPO of $20.9 billion to $21 billion, or 32% to 33% growth; we expect revenue of $11.415 billion to $11.425 billion, or 24% growth; operating margins to be in the range of 28.9% to 29.2%; diluted non-GAAP EPS to be in the range of $3.77 to $3.79; fully diluted share count of 763 million to 766 million shares; and adjusted free cash flow margin of 37.5%. We've included our typical modeling points in the presentation for your review.

And with that, I will turn it back over to Hamza for Q&A.

QUESTION AND ANSWER SECTION

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

Okay. Thank you, Dipak. To allow for broader participation, I would ask each analyst, ask only one question. First question goes to Saket Kalia from Barclays, followed by Brian Essex from JPMorgan.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Okay. Can you guys hear me?

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

Yes, we can hear you.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Okay. Excellent. Having a little trouble with the video but I'll ask the question. Guys, thank you so much for taking my question here and congrats to the team on the results and the guide. Nikesh, maybe for you, there's tons to talk about, but I'd love to dig into your Network Security business just a little bit more since you mentioned a potential multiyear tailwind there.

Maybe the question is, can you talk about how much AI data center demand is contributing to that? And outside of AI data center builds, how are your other customers thinking about their network security needs as AI traffic grows?

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

Thanks, Saket. First of all, I thought you were going to ask me about the 40% free cash flow question you mentioned on CNBC, but anyway, we'll save that one for Dipak.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

That speaks for itself.

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

Okay. Look, you saw across the board we've always maintained that as more traffic traverses networks, more inspection is needed. When more inspection is needed, hardware is the cheapest and fastest throughput mechanism to inspect the data. I think the multiyear tailwind will come from the fact that more and more data needs to be stored, both by organizations, needs to be used for training all these frontier labs out there. And you can see the explosion of data centers being built, whether it's by hyperscalers, frontier labs, or neoclouds out there, and you're seeing that demand fall through to some of the hardware vendors in the space.

I think couple that with the – sort of the scarcity and component pricing, you're seeing some price increases, you're seeing some of that mixture of price uplift as well as demand uplift. But I think – maybe the number's gone from 5% to 8% to 10% to 12%, so that's a 50% increase in demand for the industry I think. I think you'll see that and I think you'll tell me before I can tell you, when you see – when data center growth starts to taper off or plateau, this thing is going to come to roost. But I expect that this trend should continue for the next few quarters, if not few years. Lee, did you want to answer? No, Lee thinks I gave a good answer.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Very helpful. Thank you.

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

All right. Thank you, Saket. Next, we'll go to...

[indiscernible] (00:36:51)

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

...Brian Essex from JPMorgan, followed by Matthew Hedberg from RBC.

Brian Essex
Analyst, JPMorgan Securities LLC
Q

Yeah, thanks, Hamza, and congrats on the results, guys. Thank you for taking the question. Hey, Nikesh, I'd love to ask you about Prisma AIRS. Great to see the traction there, and would love to understand from a customer perspective, one of the things I thought was very important that you mentioned was the ability for a platform to have more effective speed or meantime to detection and response, how are your customers evaluating that as they look at kind of the elevated threat environment they have following the emergence of like Mythos and GPT and Glasswing, Project Glasswing announcement?

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

A

So let's do a double-team with this. I'm going to start off then – and have Lee talk about some of the capabilities that are needed in the AI future. Look, one of the things which we have done, as many of you know, over the last many years, we actually built native VM capability in many of the hyperscalers. Now you're seeing that is where a lot of the models are being hosted, a lot of the AI artifacts are sitting for customers, because AI is not an on-prem event, it's typically a cloud event, hyperscaler event, and the fact that we have native firewalls sitting in those hyperscalers allow us to inspect traffic, not just regular cloud traffic but also AI traffic.

I'm going to have Lee talk about all the capabilities we've built in Prisma AIRS the last 12 months, which have allowed us to provide all the security capabilities that AI needs.

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

A

Yeah. So there's – like every cybersecurity sort of space, I'll call it, there's – it – there's an end-to-end component. There's what sort of shift left, which is even before you deploy AI and what you do in terms of model scanning and AI red teaming and validating the application itself and the AI usage of that, all the way through the runtime components, which are sort of very focused on real-time threats, how to detect and prevent them.

And then all of that also becomes a feed into the SOC and the SOC has to be able to ingest data from all of these different sensors, analyze it in real time using AI, and then apply automation in order to achieve the meantime to remediation that Nikesh was talking about earlier in prepared remarks, where we can't be operating in a model where – sort of legacy model of meantime to detection of days when attackers, particularly with these new models, are able to carry out attacks start to finish in tens of minutes.

And so there the, the feed into XSIAM, the amount of data that XSIAM can ingest, speed of processing, AI automation and response, that ability to prove to customers of all the rest that have already been deployed that we can achieve MTTR in minutes is a very powerful proof point for them of believing that they'll be able to achieve the same outcomes as well.

Brian Essex
Analyst, JPMorgan Securities LLC

Q

Great. Thank you. I'll leave my follow-up for later, but thank you.

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

A

All right. Thank you, Brian. Next, we'll go to Matt Hedberg from RBC, followed by Meta Marshall from Morgan Stanley.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Q

Great, guys. Very impressive results, to say the least. I guess within your observability platform, the $200 million AI frontier lab customer, $100 million of net new ARR added this quarter, super impressive. Yeah, I guess can you talk about how observability and security is converging and how that positions you really to take share versus competitors that primarily start with an observability-first solution?

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

Yeah, Matt, I think first of all, it's important to note that these are each specialized environments, so meaning, you have to be really, really good at observability regardless of any potential integration with security, and the same is true with security. And I start there because if you look at all of the previous attempts to try to expand from one to the other, what you saw was perhaps a strength in one, but then trying to apply the same logic to the other. You can't take an observability platform, just add a little bit, and all of a sudden, say that it's a good security platform and vice versa.

And so I say that because it's very important. XSIAM is best-in-class in what it does, and we've proven that. Chronosphere, from observability perspective, is best-in-class and we've proven that, and in both cases, we have very strong road maps of capabilities that we'll continue to add to them.

What you'll see overtime going forward is data collected for the observability use case will be valuable as a sensor to the security use case, meaning XSIAM will start to leverage that data to expand the data it can analyze for security purposes. And importantly, vice versa, data collected for the security use case will be valuable to having additional context, broader context for the observability use case. So the first part is the data that is collected for each of these independent use cases starts to cross-pollinate to the other.

The second part is really related to agentics. And what you're seeing across these spaces is a need for AI-driven automated response, and agentics, we believe, is that foundation that will be leveraged across all of our platforms, obviously, starting with Cortex and expanding to Chronosphere. And so agentics becomes the other key point where you'll start to see increased integration across the observability and security space from us, but again, in both cases, this is starting from a position of strength independently and the cross-pollination adds to those capabilities.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Super helpful. Thanks, Lee.

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

Yeah.

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

Thank you, Matt. Next, we'll go to Meta Marshall from Morgan Stanley, followed by Shaul Eyal from Cowen.

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

Great. Thanks. Maybe – the question for me is just building on the $200 million opportunity that you guys hade with the frontier lab. How does that change how you're thinking about the opportunity with the AI native, and just can you give a sense of the breadth of the platform that they were kind of buying within that deal? Thanks.

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

Well, look, each of the models has a different approach in terms of how they deal with observability. Some have their own approach on a DIY basis, some of them are using third-party vendors like us, so I don't think it's one size fits all. What we are seeing, that Chronosphere is particularly good at AI-native platforms, whether it be frontier AI labs or whether it's – be SaaS Software. I'd call them modern SaaS software companies and not older SaaS software companies.

Typically, what's happening is the observability market is maturing. Companies are beginning to realize as volume scales, it's not okay to be DIY. I think the general reluctance in the observability industry historically has been cost. I mean, even at Palo Alto, when we were deploying a third-party vendor, we chose to turn it off because it was prohibitively expensive. And what Chronosphere has done has been able to deliver that same capability at approximately half the cost of what the industry charges. So it starts to meet the number at which you're better off not building your own or using open source with some enterprise capabilities, you're better off using platforms like Chronosphere.

So it's early days and Lee said we have a road map, it requires us to bolster a few more capabilities on the platform to make sure it's competitive in its space, but the – I call it the advanced practitioners already see the capability and the ability and are happy to use it, and we continue to make progress in the road map to make sure that it becomes a full comprehensive platform, and hopefully it becomes another mainstay platform for us in the future.

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

All right. Thank you, Meta. Next, we'll go to Shaul Eyal from Cowen, followed by Fatima Boolani from Citi.

Shaul Eyal
Analyst, TD Cowen
Q

Hey, good afternoon, guys. Congrats on results and guidance. Nikesh, I know most are focused on the ongoing progress of CyberArk and Chronosphere, great results on that front. I actually want to ask and double-click on Koi and agentic endpoint and progress and interest that you guys are seeing on that angle. There's definitely some sort of a renaissance taking place at endpoint. Can you tell us what's driving that?

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

Sure. I feel like it's been maybe a little while since the endpoint really changed. The types of application deploys seem to be pretty similar, the types of attacks seem to be kind of similar. They evolve, but what's happened really, and it's very quick in the last 12 months, is the – all of the activity now in the endpoint – I shouldn't say all, but most of it now is becoming agentic.

And so you think about some of these vibe coding tools, think about things like OpenClaw in the – its brief sort of history. It's not just a new application that gets deployed there. It's the application and it brings a whole ecosystem with it, right? So you look at these vibe coding tools, it's not just a vibe coding application. You have skills and hooks and scripts and MCP servers and all sorts of other stuff that come with it, and so it's almost like you have a whole new endpoint ecosystem on top of the one that already existed.

And that requires specialized functionality. It's not as simple as just adding a couple features and claiming to be able to secure the new agentic endpoint. And that's what we observed. We observed this starting last fall, and as we started to look around, we identified that Koi was very unique in their ability to provide this type of security

capability. That is what got us excited about it enough to actually deploy it at Palo Alto Networks. That is what led to, obviously, acquisition.

And now with the advent of what we're seeing with these new AI frontier models, that is adding to the already high level of interest because it's very clear that vibe coding and AI development and agentic endpoints in general are going to be critical to the success of every organization and it has to be secured.

Shaul Eyal
Analyst, TD Cowen

Q

Thank you.

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

A

Yeah. Thank you, Shaul. Next, we have Fatima Boolani from Citi, followed by Michael Turrin from Wells Fargo.

Fatima Boolani
Analyst, Citigroup Global Markets, Inc.

Q

Oh, good afternoon. Thank you for taking my questions. Nikesh, this one is for you. There is a voracious appetite for any large company that's basically had the rug pulled under them as it relates to the risk of novel AI attacks. So, in the context of Unit 42, I wanted to get a sense of how much incremental investment do you expect to put behind that franchise? How capacity constrained are you?

And maybe to take it up another level, this whole notion of the agentic SOC and agentic remediation, if you will, how much of that are you dogfooding or champagne drinking, you can choose your flavor, inside Unit 42, whereby you can drive both scale and efficiency and a strong product feedback loop into the portfolio?

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

A

Well, Fatima, thank you for the question. Look, we have repurposed our Unit 42 team to focus primarily on frontier AI defense. As I mentioned, we've had north of 1,200 outreaches from customers, both directions where we reached out to our customers and they have to us. Both Lee and I and a lot of people in my team have personally done tons of meetings. I've done close to 100, Lee's done close to 100. We're doing these meetings to talk to our customers how they want to strategize, not just about how to react to models like Mythos, because we believe it's real, but also to prepare for something that can get better and better and how does the infrastructure need to change in 6 to 12 months from now.

We are firmly of the belief that people will have to deploy the near endpoint capability, like Koi, go to Prisma Access Browser or secure browsers. They will have to go put virtual patching capability in their firewalls and fundamentally reimagine their SOC and use XSIAM.

So, all of that is true. But the conversation usually start with Unit 42, trying to help them test their code, make sure their code is safe, their code is robust, test their configurations and help them with some form of, I'd say, managed patching for their environment because every vendor is going to show up with lots of patches that need to be done this time. So, that's probably where Unit 42 is focused short-term. Long-term, they're focused on transforming architectures where, again, [ph] Palo Alto (00:49:38) is focused on delivering that capability.

As it relates to agentic dogfooding or champagne drinking or dogs drinking champagne, I think we have, and I don't want to say it, just sometimes better to be lucky than good. We did design XSIAM with the idea of pre-analyzing everything before we ingest the data. So, XSIAM is turning out to be a great tool in this regard in terms of reducing the median time to detect and remediate for our customers, and it has agents running in it to give you that capability.

I think that capability will increase and we can have a long conversation on what exactly an agent is. I think there's a lot of deterministic workflows that run to reduce the task of a SOC analyst, a lot of automation that exists in XSIAM. And over time, perhaps our customers will trust those agents to act independently. For now, the customers want to sort of see, observe, and approve, which is where it's set up. I think as customers get comfortable with deployment, they'll [ph] get – they'll (00:50:40) give it agency.

So, we're not seeing the rush demanding agency. I think right now customers are in phase zero where they're saying, [obscenity] (00:50:47), I better collect all my data because if I don't have all the data, I don't have all the context. If I don't have all the context, I can't actually react to an AI attack.

Fatima Boolani
Analyst, Citigroup Global Markets, Inc.

Q

Thank you.

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

A

Okay, great. Thank you, Fatima. Next question is Michael Turrin from Wells Fargo, followed by Adam Borg from Stifel.

Michael Turrin
Analyst, Wells Fargo Securities LLC

Q

Hey, great. Thanks and congrats on the strong results here. Nikesh, you had some useful details throughout the prepared remarks, but hoping you could expand on some of what you're seeing in terms of AI-driven demand, specifically how some of the larger customer conversations you [ph] had to account (00:51:20) in terms of customer conversations you're having have evolved since Mythos and if there's a greater sense of urgency there heading into fiscal Q4.

And in terms of the metrics, is it RPO platform wins or what are the key metrics you'd point us to to help us gauge progress as you continue to work towards those opportunities?

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

A

So, Michael, I want to make sure all of you understand. Six months ago, cybersecurity stocks were doomed because AI was going to protect every one of us and we were all out of a job, right? And suddenly, we're hiring more people. AI is not taking jobs away. And suddenly, you can't execute a cyber protection scenario without using a platform cybersecurity vendor.

I mean, think about it. I think the part which you must pay attention to, Michael, is I said there's a 25% false positive rate, which means an AI model can say, oh my god, I see a vulnerability. And one times out of four, it's not seeing the right vulnerability, which means if you let AI do the job, it could try and patch something that was working perfectly fine. And if you let AI go protect that, you might have screwed up something else.

So, I think you got to take this with a grain of salt and understand that the big takeaway, if I was in your shoes, I would take from this is if you thought that the terminal value of cybersecurity was gone, like many SaaS companies, this terminal value is here to stay. You actually just created a longer term G in your model for long-term growth rate for cybersecurity. I think to the extent you felt that demand was going to get weak in Q4 or Q1 or Q2 for someone, it's not going to get weak.

Now, I wouldn't get ahead of my skis and start throwing the kitchen sink at numbers for cybersecurity companies because there is still a process, a mechanism, a cycle that people buy in and there's execution and deployment. So, to the extent that do I see good demand? Yes. To the extent do I believe that this demand will continue for longer? Yes. To the extent do I expect a windfall next quarter, the following quarter? No. I expect robust growth.

Michael Turrin
Analyst, Wells Fargo Securities LLC

Q

That's great. Thank you.

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

A

Thank you, Michael. Next, we'll go to Adam Borg from Stifel. And we'll end with John DiFucci from Guggenheim.

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

Q

Awesome. Thanks so much for taking the question. Great to see the continued traction. Nikesh, maybe go deeper into SASE, I mean, these results have been great, outpacing the market. Talk more about the traction you're seeing overall and maybe help us just rank order, is that traction across SSE, SD-WAN, Prisma browser, et cetera. Any more color there would be really helpful. Thanks.

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

A

Look, I think, Adam, we are what I think I like to call the second wave of SASE, right? The first wave of SASE was internet access or VPNs, and that's what you could call them SASE, but they were effectively feature capabilities in that market. And you saw the VPN people, like the firewall guys, win the VPN battles. You saw the internet access companies, which are the early SASE players, win the SASE battle.

I think as we evolve from there, what we're seeing is the desire for a comprehensive network stack. What I mean by desire for a comprehensive network stack, people call it zero trust. People [ph] call it (00:54:19) single policy across multiple network capabilities. People call it a network re-architecture. People are figuring out that if you want to secure your traffic, you want to dynamically route your traffic, there's a lot of contention between SD-WAN and security. You need to have [ph] this common (00:54:34) platform.

Now, we've got SD-WAN many years ago, and we only sell it as part of the SASE platform because we don't believe we should be in the [indiscernible] (00:54:42) SD-WAN business for the most part. And that was the strategy. Now, we're seeing network architecture projects show up and people say, oh my god, I already understand Palo Alto's security framework because we use Palo Alto firewalls. Amazing, you're telling me I can just replicate those policies across my entire network stack and not have to go learn a new stack, right, new set of policies? That's cool. Oh, wait, I can do that in software firewalls in Prisma AIRS now as well. So, I think what we're seeing is the benefit of consolidation.

Now, I think one more thing has changed in the mind of the customer. This is my eighth year, [ph] eighth week (00:55:14) anniversary, in four days, I'll hit eight years at Palo Alto, surprise, surprise. And I'll tell you, there was a lot more willingness to take best of breed eight years ago. I think that willingness has slowly subsided where the customers see the value. Perhaps the products have normalized, perhaps the companies have matured, but customers are much more comfortable talking about a consolidated strategy with hardware, software, and SASE.

And I think what you're seeing is our ability to present that capability as a platform. We are taking share from some of the, I'd say, SASE-only customers. And unfortunately, to their chagrin, firewalls are not dead. Just the way hardware is not dead and PCs aren't dead, the storage isn't dead, firewalls aren't dead either. So, having a firewall leader who has the ability to deploy world-class SASE is helping in the market and that's what you're seeing.

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

Q

Excellent. Thanks, again.

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

A

Thank you. Adam. And our last question will go to John DiFucci from Guggenheim.

John DiFucci
Analyst, Guggenheim Securities LLC

Q

Thanks, Hamza. Nikesh, everything looked pretty good this quarter, like everything. Like you had some – one of your competitors on the hardware side did well. So, I think people kind of expected that. But everything looks good. So, the one I wanted that wasn't asked here is CyberArk. I mean, we all modeled CyberArk before and we had models. And I know it's a month off, but geez, that looked like better than I had modeled it before. And CyberArk was one of the...

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

A

You just don't trust me, John.

John DiFucci
Analyst, Guggenheim Securities LLC

Q

I trust you. I do. I do, I trust you.

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

A

Okay.

John DiFucci
Analyst, Guggenheim Securities LLC

Q

And I wish I was not where I am right now.

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

[indiscernible] (00:56:53)

John DiFucci
Analyst, Guggenheim Securities LLC
Q

I guess if you think about CyberArk, is that something – is it just like, okay, this first quarter that you have your all go-to-market behind it or have you even done that yet? And is it – are we seeing – is it really the core PAM from CyberArk? Are you seeing any machine identity actually taking hold yet or can you talk a little bit about CyberArk and how come it was so strong?

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

Look, the one which I think we talked about fleetingly, John, and I'll tell you, a lot of things are going well, and we continue to toil through migrating our Prisma Cloud customers to Cortex Cloud. I wish that was behind us, but that is still ahead of us for the next six months, so we'll keep grinding through that.

That one's not contributing as well as some of the other products are. So, that's fine. That's why you have a portfolio of platforms and some do amazingly well and they cover up for their slightly slower brethren. And the slower brethren come from behind and go in after that. So, I think we feel not everything's perfect, John, but a lot of things are doing well. So, thank you for that part.

As far as CyberArk is concerned, I think we have a very, very measured strategy around CyberArk. Remember, this is our first large acquisition. The biggest fear in large acquisitions people think is that we will break it. And I think the most important part is we did not break it.

Look, mommy, I didn't break it. It's working. Okay? We worked with the company. We made sure that we talked to every one of their leaders. In fact, the entire CyberArk product team is in Palo Alto right now in our offices. We spent most of yesterday and this morning with them, and we'll continue to spend the next two days with them.

The plan was just the way when I found Palo Alto eight years ago. It was a great company. It is a great company. So, CyberArk, we have to make sure that that product gets more modern and more innovative, and that's what the team's very focused on. And what you're seeing is commitments, we're out going out to customers, showing them the roadmap, promising them that the PAM product is going to even get better than compared to what it already is. And we're going to show them great outcomes. There are Palo Alto customers who are asking to meet CyberArk. There are CyberArk customers asking to meet Palo Alto.

We said we've done 1,000 meetings, where Palo Alto and CyberArk people are talking to each other and going to the customer together, two independent sales teams, but they are connected in 1,000 different places, which is already creating some degree of momentum.

So, our plan is don't hurt the top line. Make sure that the existing customers still love us, want to buy, want to upgrade, and they're going to see better product. That's phase zero. Take out all the places where there could be friction or overlap, which allowed us to streamline and get better operating margins. I just got an email this morning. We have migrated one of our critical systems from CyberArk independent system to Palo Alto and CyberArk on the same system. We have four more major systems to get through in the next four months. We

think we'll get there before the end of this calendar year. If we can integrate their backend systems to the common systems, we're using AI to write a whole bunch of new coding capabilities, sales capability.

So, topic number one, trim the fat or trim the overlap and don't break the top line. We think we're on track not to break the top line, improve the profitability, which we've done. As we said, we think we're going to be six months ahead on profitability because we found ways to get there faster. Our job is then to make sure that if we can deliver the next capability of products, which is incremental to what they already had, that allows us to look at the following fiscal year and say, how do we go out, hit the ground running in the following fiscal year to deliver better top line.

So, CyberArk is our chance at Palo Alto to prove that we are capable of doing amazing large acquisitions. We're capable of integrating large teams. And if I can prove that, the market will give me the license to go win again. So this is existential for me. It's existential for my team, and they know it. So, we're going to work hard to make sure CyberArk succeeds, allowing us to do more and more of that in the future at Palo Alto Networks. Thank you for that question, John.

John DiFucci

Analyst, Guggenheim Securities LLC

Q

That makes a lot of sense. Thanks, Nikesh.

Hamza Fodderwala

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

Thank you, John. This concludes the Q&A portion of the call. I'll pass it back to Nikesh for any closing remarks.

Nikesh Arora

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

I just want to say thank you. We officially declare [ph] SAS Eclipse for cybersecurity dead (01:00:44). I want to thank our partners and employees and all of you guys for supporting us. See you guys next quarter.