

22-Feb-2021

Palo Alto Networks, Inc. (PANW)

Q2 2021 Earnings Call

CORPORATE PARTICIPANTS

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

Nikesh Arora

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

Luis Visoso

Chief Financial Officer, Palo Alto Networks, Inc.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

OTHER PARTICIPANTS

Keith Eric Weiss

Analyst, Morgan Stanley & Co. LLC

Philip Winslow

Analyst, Wells Fargo Securities LLC

Sterling Auty

Analyst, JPMorgan Securities LLC

Saket Kalia

Analyst, Barclays Capital, Inc.

Fatima Boolani

Analyst, UBS Securities LLC

Brian Essex

Analyst, Goldman Sachs & Co. LLC

Gray Powell

Analyst, BTIG LLC

Patrick Colville

Analyst, Deutsche Bank

Tal Liani

Analyst, BofA Securities, Inc.

Brent Thill

Analyst, Jefferies LLC

Michael Turits

Analyst, KeyBanc Capital Markets

Jonathan Ho

Analyst, William Blair & Co. LLC

Andrew James Nowinski

Analyst, D.A. Davidson & Co.

MANAGEMENT DISCUSSION SECTION

[Video Presentation] (00:00:17-00:01:32)

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

Good afternoon and thank you for joining us on today's conference call to discuss Palo Alto Networks' Fiscal Second Quarter 2021 Financial Results. I am Karen Fung, Senior Director of Investor Relations.

This call is being broadcast live over the web and can be accessed on the Investors section of our website at investors.paloaltonetworks.com. With me on today's call are Nikesh Arora, our Chairman and Chief Executive Officer; Luis Visoso, our Chief Financial Officer; and Lee Klarich, our Chief Product Officer.

This afternoon, we issued our press release announcing our results for the fiscal second quarter ended January 31, 2021. If you would like a copy of the release, you can access it online on our website.

We would like to remind you that during the course of this conference call, management will be making forward-looking statements, including statements regarding the impact of COVID-19 and the SolarStorm attack on our business, our customers, the enterprise and cybersecurity industry, and global economic conditions; our expectations related to financial guidance, operating metrics, and modeling points for the fiscal third quarter, fiscal year 2021, and 2022; our intent to acquire Bridgecrew; our intent to be carbon-neutral by 2030; our expectations regarding our business strategies, speedboats, and equity structure for the ClaiSec business, and a vehicle for employees to invest in such equity; our competitive position and the demand and market opportunity for our products and subscriptions, benefits and timing of new products, features, and subscription offerings, as well as other financial and operating trends.

These forward-looking statements involve a number of risks and uncertainties, some of which are beyond our control, which could cause actual results to differ materially from those anticipated by these statements. These forward-looking statements apply as of today. You should not rely on them as representing our views in the future, and we undertake no obligation to update these statements after this call.

For a more detailed description of factors that could cause actual results to differ, please refer to our quarterly report on Form 10-Q filed with the SEC on November 19, 2020, and our earnings release posted a few minutes ago on our website and filed with the SEC on Form 8-K.

Also please note that certain financial measures we use on this call are expressed on a non-GAAP basis and have been adjusted to exclude certain charges. For historical periods, we have provided reconciliations of these non-GAAP financial measures to GAAP financial measures in the supplemental financial information that can be found in the Investors section of our website located at investors.paloaltonetworks.com.

And finally, once we have completed our formal remarks, we will be posting them to our Investor Relations website under the Quarterly Results section. We'd also like to inform you that we will be virtually participating in

the Morgan Stanley 2021 TMT Conference on March 2. Please also see the Investors section of our website for additional information about conferences we may be participating in.

And with that, I will turn the call over to Nikesh.

Nikesh Arora

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

Thank you, Karen. Hello, everyone. I know Walter Pritchard, you're listening in. Enjoy your last earnings call from the other side. Next quarter, Walter will join us at this end as our new Senior Vice President of Investor Relations and M&A Finance.

Well, moving on to the quarter, let me start with SolarStorm, which many of you are describing as one of the most serious and sophisticated cyber-attacks in history. The SolarStorm attack highlighted that enterprises need a comprehensive, up-to-date map of their full IT infrastructure environments, including understanding their own networks as well as external attack surfaces and supply chains.

In order for security teams to have an edge over the adverse adversaries, they need to embrace next-generation technologies that leverage AI, machine learning, and automation. To help our customers, we set up a Rapid Response Program. And when I say rapid, it was rapid. Our acquisitions of Expanse and Crypsis almost felt prescient. The teams swung into action. We updated XDR for all the new threat vectors. We offered free assessments from our Crypsis team. We also evaluated the attack surfaces from the outside in for Expanse and discovered that there were dozens of affected customers, including major government agencies and large companies, many of which were actively communicating with SolarStorm malware command and control infrastructure.

So far, we've received over 1,000 assessment requests and have completed over 500. We believe that the SolarStorm attack raises the mid and long-term criticality of the cybersecurity industry as a whole. This will result in more awareness and focus on cybersecurity, which in all candor, is the need of the hour given the complete reliance in technology in these times. We expect that this attack will be a wake-up call to all enterprises to modernize cybersecurity and will serve as a net incremental tailwind, not just for us but also for the industry.

Before I turn to our fiscal Q2 2021 results, I have an admission to make. Perhaps I was too cautious at the outset of the pandemic. The current sustained performance, resilience of our teams and execution has been turning more optimistic. We had a great second quarter with strong business momentum, as the organization executed across all platforms and strategies.

As a result, we beat Q2 guidance and consensus. Here are some highlights. We delivered billings of \$1.2 billion, up 22% year-over-year, with strong growth across the board. Let me give you some additional context. Due to COVID, we have provided billing plans to a select number of impacted customers. When adjusting for these billing plans, our billings momentum would have been several percentage points stronger in Q2 than the reported 22% year-over-year growth. This trend has been in place and has been growing over the last few quarters. Consequently, our revenue growth is higher than billings growth and accelerated to 25%, reaching \$1 billion for the first time ever, yes, our first \$1 billion revenue quarter, with accelerating revenue growth. The strength has been across the board. And as we continue down the path of more and more of a subscription-based model, the revenue predictability will continue to rise.

Non-GAAP EPS was \$1.55, up \$0.36 from last year. The EPS expansion was driven by revenue growth and operating expense leverage. While there continues to be beneficial impacts due to lower travel due to COVID, we do continue to hire resources to support our product expansion, which we expect to continue.

Free cash flow margin for the quarter was 32.7%. In the first half of fiscal year 2021, we generated \$838 million in free cash at a margin of 42.7%. We still expect free cash flow to normalize for the year around our full-year guidance due to some seasonality you see in the second half.

Last quarter, we started the dialogue around Network Security and Cloud & AI, and shared the P&L for both businesses. We received great feedback on the additional transparency, and we want to continue to drive more transparency to unlock shareholder value.

Let's first take a deep dive into the Network Security business, which we are calling NetSec. Our NetSec business is undergoing a transformation towards software and SaaS, making it more predictable and sustainable. Starting with our hardware firewall business and associated services, rather than building solutions only as hardware, we have chosen to offer security services and software subscriptions. Over the last two years, we have doubled our security subscriptions from four to eight, with the introduction of DNS, SD-WAN, IoT, and DLP. We're seeing great progress with DNS, which has acquired nearly 5,000 customers since launch.

These new subscriptions, along with the introduction of a higher tier support, Platinum Support, has allowed us to increase our next-generation firewall support and security subscription revenue as a percentage of next-generation firewall hardware revenue over the last few years. As you can see, we have sustained a 15% CAGR in hardware, subs and support. And our hardware contribution has gone from 39% to 29% in that time. To continue to drive software growth, we have made these subscriptions available across all form factors, Firewall FLEX and Prisma Access 2.0. We just recently completed the process of making it available on our product Prisma Access 2.0, which is our firewall in the cloud.

Turning to our software firewalls, we continue to see a transformation to software form factors. With the introduction of advanced features, cloud-native integrations, and the development of the industry's first containerized next-generation firewall, we continue to see product/market fit. As a result, VM and CN-Series grew over 60% in the first half of FY 2021. We recently launched Firewall FLEX, another industry-first, a unique approach on how we offer virtual firewalls and CN Series to increase customer flexibility and enable a consumption model to drive additional growth. This new flexible consumption model features credit-based licensing that lets you consume VM and CN-Series firewalls, choose the number of CPUs needed, and add any or all of our eight security subscriptions, which is previously limited to five. We believe that by providing greater flexibility to our customers, we will continue to drive growth and achieve greater subscription attach rates.

To highlight how our software firewalls are transforming how customers approach security, we closed a deal with a leading telecommunications company to secure their 5G network. The transition to 5G is driving a number of very important architectural changes, including a highly distributed design, containers as a foundation, and security for enterprise customers as a critical business driver. We were first to deliver enterprise and service provider clouds 5G and container security. In doing so, we empower our customers to provide a secure 5G service to their customers and provide managed security offerings to their enterprise end customers.

Now let's talk about Prisma Access. When COVID dramatically changed how work gets done at companies across industries around the world, the needs for securing remote workforce have also changed. No longer is it sufficient to have partial access to applications, or what is sometimes called good-enough security. Overnight,

connectivity to every application was needed, security became business-critical, and user experience determined the difference between maintaining productivity or falling behind.

Even before COVID accelerated this change, we were already working on turning Prisma Access into an industry-leading solution for enabling a secure remote workforce. What initially started as a GlobalProtect cloud service started to transform in 2019 with the launch of Prisma Access. In the last year and a half, we've built out industry-leading capabilities. In that timeframe, Prisma Access has gone from less than 150 customers to now nearly 1,000 customers and 30% of the Fortune 100.

Last week, we announced Prisma Access 2.0, the biggest update since introducing this service. Prisma Access is a full security platform in the cloud, with machine learning-based security, preventing unknown threats in line at light speed, a full firewall delivered as a service, and includes features like Zero Trust Network Access, Secure Web Gateway, CASB, DLP, and IoT security.

Prisma Access secures both web and non-web apps. As an example, conventional web security approach to cloud-delivered security misses 53% of all remote workforce threats that ride over non-web apps. Those threats cannot be ignored. And unlike alternative solutions in the market, we prevent them with Prisma Access. We have completely reimaged the way customers manage Prisma Access with an entirely new cloud-based UI that delivers better security outcomes through built-in security assessments. A new Digital Experience Management add-on provides native end-to-end visibility and insights to SASE and the ability to self-heal when digital experiences problems occur.

Prisma Access is built on a low latency and highly scalable infrastructure with Google Cloud as a backbone. Lastly, Prisma Access, along with the Prisma SD-WAN, our rebranded product from CloudGenix, delivers a complete SASE offering. With the recent addition of CloudBlades, we now have a SASE platform which allows for an API platform for seamless third-party service integration. Prisma Access securely enables access to all applications, delivers best-in-class security to meet enterprise security needs without compromise, and enables user experience that maintains or even improves worker productivity.

In Q2, we closed an eight-figure deal with a leading technology company with over 100,000 employees, with businesses in over 100 countries. As part of their digital transformation, the company was launching a new remote work initiative. In order to realize their vision, they needed a secure and optimized network that will support a flexible remote work environment. Palo Alto Networks was ultimately chosen ahead of several of our security peers, as the customer saw us as the only vendor that was offering a true SASE solution. Ultimately, Prisma Access was a key product given their goal to rapidly enable remote work, but the customer also purchased next-generation firewalls. VM-Series firewalls enhanced their SOAR capabilities through Cortex XDR and XSOAR. This was definitely a cross-platform deal to be proud of, and we look forward to a great partnership with the customer going forward.

Lastly, several of you have asked in the past about a software transition the associated economics. While the first phase of VM and Prisma Access purchases have mostly been incremental use cases, we've put together a few key examples on what we see in the market when a customer does choose to replace a hardware-based security solution with software or SaaS.

For use cases where VMs replace hardware firewalls, like this example of a local retail store running software firewalls and third-party hardware, along with other software applications, the estimate that the five-year revenue of this VM-Series deal is roughly equal with that of deals deploying a separate physical next-generation firewall.

For use cases where Prisma Access replaces hardware firewalls, we took a typical branch office use case and estimated that the five-year revenue of a Prisma Access deal is two times larger than a next-generation firewall deal. From a customer perspective, we estimate that the customer's total cost of ownership is generally reduced, as they move to virtual and cloud-delivered form factors. As you know, Prisma Access is only a year old, so our gross margins aren't as favorable as hardware, but we expect them to improve over time.

Now moving over and looking at our Cloud & AI business. We started this call by discussing SolarStorm, but didn't talk about our own experience with an attempted SolarStorm attack. Back in December, we shared with the broader security community that Cortex XDR instantly blocked a SolarStorm attempt on Palo Alto Networks, thanks to its behavioral threat protection capability. We continue to be bullish around the rapid pace of innovation that is going into our Cortex XDR product. In fact, Cortex XDR was recently recognized by AV-Comparatives as a strategic leader in their latest Endpoint Prevention and Response Evaluation, while still delivering lower total cost of ownership than several endpoint security peers.

Importantly last month, Cortex XDR and Data Lake achieved FedRAMP Moderate Authorization, which should make it a key piece of technology in the federal space. As further validation of our vision, we see more and more players in the endpoint security space rushing to jump on the XDR wave that we have established two years ago.

Overall, we continue to see the Cortex portfolio developing into the industry's first proactive security platform, and we see penetration into the largest companies continue to grow. 35% of Global 2000 and 66% of the Fortune 100 are now Cortex customers, indicating that automation and advanced threat detection are top of mind for these customers.

In Q2, we closed a deal with a retailer. The company chose Cortex XDR to increase visibility, control and protection of the endpoints by adopting a more complete solution with XDR rather than using EDR. With Cortex XDR support for mobile, the customer is also able to easily extend Cortex XDR to additional devices leveraged on-site of their stores, signify the endpoint security policy across the entire enterprise. We then expanded the conversation to address their SOC's operational challenges by demonstrating how Cortex XSOAR's out-of-the-box preprocessing rules and alert deduping could reduce the alert volumes dramatically. With the combination of enhanced visibility, protection and control for their entire endpoint estate, coupled with automating and orchestrating alert volumes, the Cortex platform will have an immediate impact on this new customer.

Switching to Prisma Cloud. Prisma Cloud is building the most comprehensive and best-of-breed cloud-native security platform, and we continue to see strong customer interest. Prisma Cloud has now acquired over 2,000 customers with 74% of the Fortune 100 and secures 2.5 billion cloud workloads. We also continue to see an increase in Prisma Cloud customers who are using both Cloud Security Posture Management and Cloud Workload Protection for containers and services applications now at 50%.

Additionally, last month, Prisma Cloud also achieved FedRAMP Moderate Authorization along with Cortex XDR and Data Lake, as we said. This allows US government customers to leverage our visibility, compliance and governance capabilities for securing multi-cloud and GovCloud deployments.

The last deal I'd like to highlight is the largest Prisma Cloud deal that we've ever closed, an eight-figure deal with a leading SaaS company. Like many in the industry, they're moving from a private cloud environment to the public cloud. As part of this shift, they're moving to a containerized application architecture. The customer had unique scalability, availability, and vulnerability requirements for securing their containers across AWS, GCP and Azure clouds.

The maturity, the superior vulnerability detection of the container security capabilities, and the scalability of runtime protection of Prisma Cloud helped convince the customer to choose Prisma Cloud as their container security platform of choice. Last week, we announced our intent to acquire Bridgecrew, an early pioneer of security for the development community.

The next big challenge we're taking on in cloud security is what is known as shift left security. Developers are playing an increasingly important role in cloud security, both in terms of what products are used and how they're operationalized.

Today, a single error in development can be replicated hundreds of times over, resulting in thousands of security alerts to be fixed. This drags down productivity and increases the likelihood of security issues in production applications. Shift left integrates security into the DevOps process to catch these issues upfront where they're easy and quick to fix. It's a win for developers and a win for security. Bridgecrew recognized the need for shift left security, and pioneered an approach to infrastructure as code designed for developers.

To engage the developer community, they released an open-source product called Checkov that was downloaded over 1 million times last year and have paid for product gaining early traction. When we bring Network Security and cloud AI together, we see tremendous synergies to power the platform of the Palo Alto Networks. When looking at our Global 2000 customers, we see that these customers are increasingly adopting Strata, Prisma and Cortex. 68% of our Global 2000 customers have purchased more than one platform, up from 62% a year ago and 56% two years ago.

Given the momentum that we're seeing, we're raising guidance for the full fiscal year. For fiscal 2021 and at the midpoint of guide, we expect total revenue growth of 22%, up 200 basis points from our prior guide. Total billings rose at 20%, up 100 basis points from our prior guide, slightly lower than our revenue raise due to the impact of billings plans as we discussed earlier.

We continue to expect next-generation security ARR at \$1.15 billion, up 77% year-over-year. Product revenue flat year-over-year, unchanged from our prior guidance. Lastly, non-GAAP operating margin of 50 basis points. Adjusted free cash flow of 29%, unchanged from our prior guidance, as we continue to invest to capture the opportunities in the market.

Now, let's review our fiscal year projections for NetSec and ClaiSec. Overall, we are confirming our ClaiSec projections, while raising NetSec billing for 100 basis points and revenue by 200 basis points given the strong performance of SASE and VM-Series. Moving on to adjusted free cash flows, we expect Network Security will deliver a free cash flow margin of 41% in FY 2021, up from 38% in FY 2020. We expect Cloud and AI free cash flow margin of negative 43% in FY 2021, an improvement from negative 59% in 2020. As mentioned last quarter, for the next few years, we expect Cloud and AI to achieve gross, operating and free cash flow margins in line with industry benchmarks as we gain scale and our customer base matures and becomes more efficient.

As you can see, we have been able to dig deeper and align our resources further with our business areas of ClaiSec and NetSec. And as I noted earlier, there are tremendous synergies in the power of the platform at Palo Alto Networks. At the same time, we've also been increasing our focus on our software transformation and hardware firewalls, while building a new cloud and AI business. To continue this transformation and strengthen our financial profile, we feel that we can create more focus by aligning the teams around NetSec and ClaiSec. So, we're officially going from three speedboats of aligning our efforts around these two business areas with six focused efforts as speedboats in our next fiscal year.

NetSec. We're focused on driving this transformation from hardware to software, and delivering a best-of-breed hardware solution as required. As you saw, this transformation is actually financially neutral to net positive for us and always beneficial to our customers. The speedboats here will be firewalls, including virtual firewalls, SASE, and our growing security subscriptions.

ClaiSec, the business area where we drive cloud security, and our Cortex efforts have proven that with focus and an opportunistic, organic and inorganic strategy, we can create an industry-leading set of solutions for cloud security and solutions like XSOAR and XDR driven by AI and ML. Here, we need continued investment for us to drive customer scale and for us to continue to invest in both continued product development and customer adoption.

We'll do so by continuing our focus on Cortex, Prisma Cloud and Palo Alto Networks' Incident Response Services, a newly formed team combining Crypsis' Unit 42, which Wendi Whitmore has joined to help lead. We're also excited to announce that with the board's consent, we are finalizing the filing needed for an equity structure for the ClaiSec business. Our goal is to make sure the value of the ClaiSec business is more transparent.

In addition, the board approved the development of a vehicle for employees to invest in such ClaiSec equity, strengthening the alignment of shareholders and the interest of employees regarding the success for our ClaiSec business. Lastly, I'm also proud to say that Palo Alto Networks recently made a commitment to address climate change, which Luis will go over in more detail around how we will be carbon neutral by 2030.

With that, let me turn the call over to Luis.

Luis Visoso

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you, Nikesh. Climate change is an existential threat, and at Palo Alto Networks, we're all in to do our part to address this crisis. We have done some important work up to this point, including LEED certifications, recycling and community involvement. We plan to step up our efforts and contribute even more. I'm proud of our commitment to be carbon neutral by 2030. We have already activated renewable energy and high-quality carbon offset strategies. We will be reducing our emissions aligned to science-based targets, and we will work across our value chain to have lasting impact and advocate stewardship.

The Paris Agreement calls on all of us to limit global warming below 2 degrees Celsius by 2050. We plan to reach our commitments by 2030. We will keep you informed of progress along the way. We will continue to participate in the Carbon Disclosure Project, and start sharing plans and progress using protocols set by the Task Force on Climate-related Financial Disclosures.

During the World Economic Forum's Davos Agenda last month, we committed to increase transparency by reporting on the International Business Council's Stakeholders Capitalism Metrics over time. It will take creativity, collaboration and visionary thinking to protect our planet, and we're up for the challenge. We call on others to join us, consider aligning to the Paris Agreement, and make your commitment to do your part.

Now turning to our financials. As Nikesh indicated, we had a great second quarter, and we continue to deliver winning innovation and adding new customers at a fast pace. This strength gives us confidence to raise our guidance for the year.

I would like to start with our performance in Firewall as a Platform, or FwaaP, which had a great quarter as we continue to grow faster than the market. FwaaP billings grew 21% in Q2, as we continue to transition from

hardware to software and SaaS form factors. As you can see, FwaaP billings declined 3% in Q2 2020. And over the last four quarters, we've been able to drive sustained execution and growth in this area to 21% in Q2 2021.

Next-Generation Security, or NGS, continues to expand and now represents a quarter of our total billings at \$309 million, growing 59% year-over-year. In Q2, we added over \$120 million in new NGS ARR, reaching \$840 million. Let me remind you, at our last Analyst Day in September of 2019, NGS was a gleam in our eye, and we called for \$1.75 billion in billings by 2022. We're on track to beat those numbers.

In Q2, total revenue grew 25% to \$1.0 billion. Looking at growth by geography, the Americas grew 27%, EMEA grew 24%, and APAC grew 14%. Q2 product revenue of \$255 million increased 3% compared to the prior year. Q2 subscription revenue of \$462 million increased 35%. Support revenue of \$300 million increased 32%. In total, subscription and support revenue of \$762 million increased 34% and accounted for 75% of total revenue. Excluding revenue from Crypsis and Expanse, subscription and support revenue increased 31%.

Turning to billings. Q2 total billings of \$1.2 billion, net of acquired deferred revenue, increased 22%. Strength was broad-based as we continue to see strong execution across the company. The dollar-weighted contract duration for new subscriptions and support billings in the quarter were slightly down year-over-year, but remained at approximately three years. For the first half of fiscal 2021, billings of \$2.3 billion increased 21% year-over-year. Product billings were \$495 million, up 3% and accounted for 22% of total billings. Subscription billings were \$1.2 billion, up 23%. Support billings were \$733 million, up 34%.

Total deferred revenue at the end of Q2 was \$4.2 billion, an increase of 30% year-over-year. Remaining performance obligation or RPO was \$4.6 billion, an increase of 41% year-over-year.

In addition to adding approximately 2,400 new customers in the quarter, we continue to increase our wallet share of existing customers. Our top 25 customers, all of whom made a purchase this quarter, spent a minimum of \$59 million in lifetime value through the end of fiscal Q2 2021, a 27% increase over the \$46 million in the comparable prior year period.

Q2 gross margin was 75.3%, which was down 110 basis points compared to last year, mainly driven by a higher mix of our NGS products which are less mature. Q2 operating margin was 19.8%, an increase of 190 basis points year-over-year. The operating margin expansion is driven by operating expense leverage behind operational efficiencies, lower travel and event expenses due to COVID, which more than offset the incremental investment in headcounts. We ended the second quarter with 9,038 employees, including 176 from Expanse at the close of the acquisition.

On a GAAP basis, for the second quarter, net loss increased to \$142 million, or \$1.48 per basic and diluted share. Non-GAAP net income for the second quarter increased 28% to \$154 million, or \$1.55 per diluted share. Our non-GAAP effective tax rate for Q2 was 22%.

Turning to cash flow and balance sheet items. We finished January with cash, cash equivalents and investments of \$4 billion. On December 4, 2020, our board of directors authorized an increase to our share repurchase program and extended the expiration date to December 31, 2021. As of January 31, 2021, \$1 billion remained available for repurchases. Q2 cash flow from operations of \$365 million increased by 19% year-over-year. Free cash flow was \$332 million, up 29% at a margin of 32.7%. DSO was 60 days, an increase of three days from prior year period.

Turning now to guidance and modeling points. For the third quarter of 2021, we expect billings to be in the range of \$1.22 to \$1.24 billion, an increase of 20% to 22% year-over-year. We expect revenue to be in the range of \$1.05 to \$1.06 billion, an increase of 21% to 22% year-over-year. We expect non-GAAP EPS to be in the range of \$1.27 to \$1.29, which incorporates net expenses related to the proposed acquisition of Bridgecrew, using 100 million to 102 million shares.

Additionally, I'd like to provide some modeling points. We expect our Q3 non-GAAP effective tax rate to remain at 22%. CapEx in Q3 will be approximately \$30 million to \$35 million.

As Nikesh reviewed earlier, for the full fiscal year, we're again raising our guidance across most metrics. We expect billings to be in the range of \$5.13 billion to \$5.18 billion, an increase of 19% to 20% year-over-year. We expect Next-Generation Security ARR to be approximately \$1.15 billion, an increase of 77% year-over-year. We expect revenue to be in the range of \$4.15 billion to \$4.20 billion, an increase of 22% to 23% year-over-year. We expect product revenue to be flat year-over-year. We expect operating margins to improve by 50 basis points year-over-year. We expect non-GAAP EPS to be in the range of \$5.80 to \$5.90, which incorporates net expenses related to the proposed acquisition of Bridgecrew using 99 million to 101 million shares. Regarding free cash flow for the full year, we expect an adjusted free cash flow margin of approximately 29%.

With that, I'd like to open the call for questions.

QUESTION AND ANSWER SECTION

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

In the interest of time, please limit Q&A to one question. Our first question comes from Keith Weiss of Morgan Stanley.

Keith Eric Weiss

Analyst, Morgan Stanley & Co. LLC

Q

Excellent. Thank you, guys, for taking the question. And very nice quarter. I just wanted to dig in a little bit into SolarStorm and if you could talk to us about any impacts that you saw in this quarter. And more expansively, how do you expect the impacts of that event to play out as we go through the year? Is there more on the comm? And what parts of the product portfolio do you think are going to get most impacted by that event?

Nikesh Arora

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

A

Hey, Keith. Thanks. Look, as we said in the call, we launched a series of initiatives to make sure that our customers are protected vis-à-vis SolarStorm. That was a sustained attack, which was planned over a series of quarters, if not years. And what we realized that once you get in the supply chain and start being able to spawn to 18,000 customers, the impact is going to be far-reaching. What's happened is people were first reacting to that and starting to make sure, for an emergency basis, there's nothing in their infrastructure which is already infected and they have not effectively been compromised.

Now, with that slowly and steadily behind us, what's happening is we're noticing people doing cybersecurity assessment. Every board is out there saying, take a look at what we've got, make sure that there's no breaches, make sure that we won't be breached. First question was, are we breached? The answer was, no, we're fine.

Suddenly, [indiscernible] (00:33:37) wait a minute. Could we have been breached if we had SolarStorm? The answer is yes. So, what we're noticing is they're noticing a rethinking of the cybersecurity architectures.

In that context, our Crypsis acquisition was very helpful because that's where we had the field force to be able to go out and address these situations which kind of sort of came to light. And I don't know if you know Wendi Whitmore, ran IBM X-Force until now, and she's going to come join us. She's had a stint at CrowdStrike and FireEye and Mandiant as well. So, she's going to come drive that effort even more aggressively for us.

We also saw that in our own case, XDR protected us, which again becomes an important distinction for us because it was a zero-day attack and we found it because of behavior anomalies that were happening on the endpoint, which is effectively a key feature of XDR. So, we're seeing a lot more conversations around that. And Expanse's ability to be able to look at what assets are exposed to the outside which, in this case, with SolarStorm servers, were also useful, when Expanse went out and looked and saw that there were hundreds of customers with open SolarStorm server sitting on their network. So, it's generally been useful for us in the XDR part, the XSOAR part, the Crypsis part; but more importantly, from a board focused on cybersecurity hygiene, it's been critical.

Keith Eric Weiss

Analyst, Morgan Stanley & Co. LLC

Q

Excellent. Thank you.

Nikesh Arora

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

A

Excellent.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Our next question comes from Philip Winslow of Wells Fargo.

Philip Winslow

Analyst, Wells Fargo Securities LLC

Q

Great. Thanks for taking my question, and congrats on another fabulous quarter. Really want to focus in on Prisma Cloud and the VM and CN-Series. Obviously, you saw a massive uptick in the number of workloads that you protect in the cloud with Prisma Cloud and then obviously a massive uptake year-over-year, I think, more than 4x in terms of the number of firewall software customers. So, I guess kind of two related questions on here.

First, Nikesh, why are you hearing that customers are choosing Prisma Cloud? Obviously, signed the largest deal in that product's history this quarter. And then the follow-up to that, when we think about Prisma Cloud plus the success you're seeing in the VM and CN-Series, are those two combined kind of changing the customer dialogue that you're having as you're seeing these customers accelerate their shift to cloud?

Nikesh Arora

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

A

Yeah. Phil, thank you. Look, if you look at it, if you abstract yourself, we grew our firewall as a platform 21%, right? And we've been talking about trying to get that to the 15% range. You can see all that growth has come from firewall in the cloud, i.e. Prisma Access 2.0, and has come from our VM-Series, CN-Series firewalls. And it's kind of – it's hard to understand if you're not sitting with the customer. We have seen a few deals flip from

hardware to software in the last week, literally. Customers aim to buy a bunch of hardware and said, wait, hold on. You guys launched this Firewall FLEX, why don't we just go into this flexible credit program where we can spin up as many firewalls we want and spin them down if we don't need them, and they can carry those credits to the cloud? So, what do you – I think what is something very important to understand, we are going through a hardware-to-cloud transition now in the industry. It does not mean it's the demise of the hardware industry. It just means that the incremental shift is beginning to happen. It's gathering momentum. You can't keep posting tens of billions of dollars on billings for AWS, GCP and Azure and not see a decline in data center over time. It's going to happen.

So, if you look past the quarters, and in that transition, it becomes very important, how are you going to protect yourself in the future? So, we are beginning to see customers go from hardware to software. And honestly, we're encouraging it to the extent the customer wants our opinion. We have the ability to sell them hardware, the best in the industry, and the ability to sell them software firewalls, and the ability to sell them Prisma Access 2.0 in the cloud.

We're sitting now, as I'm saying, you pick the best architecture you want, we'll service it. You ask us, we'd rather you went down the software route. And that's when all of you guys start asking us, wait a minute, if you go to software, do you lose money? So, we put up a slide saying, look, we don't lose money. We make more money. We want to say that not that loudly because that's not a good thing to say loudly. It's better security solution for the customer, reduce total cost of ownership, but we're seeing that transition. And I think that's the most important part of the story.

And as we highlighted, we did a big deal in the telecom space where suddenly security matters in 5G, right? Because in – no offense, when you and I walk around with our iPhones and Android devices, you got malware on them, tough luck, buddy. But if you're a car driving down the highway, and that can be infected malware, that's a problem. So, the 5G enterprise networks have to be secure. All 5G networks are being built in the cloud.

Philip Winslow

Analyst, Wells Fargo Securities LLC

Q

Right. Great. Thank you very much.

Nikesh Arora

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

A

Thanks, Phil.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Our next question comes from Sterling Auty of JPMorgan.

Sterling Auty

Analyst, JPMorgan Securities LLC

Q

Yeah. Thanks. Hi, guys. So, in the context of the guidance increase, I did notice that the Next-Generation Security ARR is staying the same despite what looked like good results in the quarter. Was there any pull-forward? Or what additional commentary can you give us around that NGS ARR outlook for the year?

Nikesh Arora

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

A

Honestly, there's no hidden meaning in there. We're not trying to tweak it in such a way that – look, we've seen strength in cloud firewall. We've seen phenomenal strength in Prisma Access. I have to tell you that this pandemic has forced the network conversation about how do I make sure Sterling can access every application at home, not just the ones that I let him access?

It's gone from a it's good to have remote access to you have to have remote access. And then the security suddenly start paying attention to network architecture. And then as – and Lee and his team have delivered this phenomenal next upgrade where we can look at both web-based and non-web-based apps. So, we're seeing phenomenal success. So, there's no tempering of our expectation and ambition on NGS. It's just how the math works right now.

Sterling Auty

Analyst, JPMorgan Securities LLC



Understood. Thank you.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.



Next question comes from Saket Kalia of Barclays.

Saket Kalia

Analyst, Barclays Capital, Inc.



Okay. Great. Hey, thanks for taking my question here, guys. Nikesh, maybe for you. You touched on this in your prepared comments. Can you talk about the cloud and AI equity structure? What's the reason for setting up that structure now? And how is it going to work mechanically?

Nikesh Arora

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



So, you know what, Saket, two-and-a-half years ago when I came here, we talked about building a cloud security business and we talked about building an AI-ML-based business. Last quarter, we started showing you the two pieces of NetSec and ClaiSec. You've seen that we're aspiring to get \$735 million of ARR in cloud AI security. We also shared, on the left-hand side, our Network Security business actually has phenomenal cash flow margin, 38% going to 41%. So, that's a cash-generative part of our business whilst we go through a hardware-to-software transformation.

On the right-hand side, we're competing with behemoths out there today, like the CrowdStrikes of the world and – in the XDR space and a bunch of start-ups in the cloud space. That's an area for investment. We think that the market inherently values both those business fundamentally differently. It values the Network Security business and cash flow. It values the cloud AI business and ARR. So, we want to be able to create the opportunity for the market to value our businesses differently to create more transparency for the shareholders. And it also allows us to keep investing in the cloud AI business and in the interest of driving more ARR.

So, what we've done is, as you saw, we've separated our financials, showed you both NetSec and ClaiSec. Luis and team have worked hard to get them audited and make sure that we could keep reporting them on a more regular basis going into next fiscal year. And we are looking at various equity structures that allow us to create incentive plans, as well as potentially in the future monetize the ClaiSec business for a different set of investors compared to the old Palo Alto investor.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Your next question comes from Fatima Boolani of UBS.

Fatima Boolani

Analyst, UBS Securities LLC

Q

Good afternoon. Thank you for taking the questions. My question is around the Firewall as a Platform business and the metrics there. Appreciate that deals sort of changed flavor in the eleventh hour, to your point, Nikesh. So, what are some of the core assumptions we should leave with around the installed base refresh opportunity as well as the R&D pipeline for hardware and appliance refreshes within the product portfolio on the Strata side?

Nikesh Arora

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

A

Well, Lee, do you want to talk about the hardware refresh plans? All I'm going to say is that we're not taking our pedal off the metal. We are going aggressively trying to continue to build the next generation of hardware and focus on refresh. I will tell you, in absolute dollars, we still sell the largest number of hardware firewalls in the industry. We get lost in percentages. It doesn't matter if other vendors are out there generating 18% growth, we still sell more absolute dollars of product in a quarter than everybody else. But Lee, can you talk about the hardware?

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.



Yeah. Yeah. Look, we're always working on the next generation of hardware since the beginning of the company until now. And we have some amazing new platforms coming. I won't tell you too much until they're out, but we're always working on that, really exciting stuff there, the software side as well with PAN-OS and new security capabilities, another set of amazing things we're working on.

One thing I'll point out in that, though, is the leverage we get across hardware, software and cloud delivered. Part of what really resonates with our customers is not that they get to pick which one they use from us, but their ability to actually use hardware where they need hardware, software form factors when they need software, cloud delivered where they need that with a set of consistent security capabilities, easy to manage and operationalize. That's something that only we can deliver to our customers.

Fatima Boolani

Analyst, UBS Securities LLC

Q

Thank you.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

[audio gap] (43:06) comes from Brian Essex of Goldman Sachs.

Brian Essex

Analyst, Goldman Sachs & Co. LLC

Q

All right. Great. Hi. Thank you. Thank you for taking our question. I was wondering, Nikesh, if you could dig into a little bit Firewall FLEX and your credit-based licensing model for next-gen firewall. What was the timing of that

rollout? How long has it been in market? And how much adoption is that in terms of the way it's impacting your model?

Nikesh Arora

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

A

I'll give you the preface of it, and Lee can jump in and give you the details. But look, when – we hadn't refreshed our VM pricing policy. It was set up more like a hardware business, where you had to tell us which particular model of software you wanted and you were basically stuck to that model. And if you think about software deployment, it's a key. I can give you a key with more capacity or key with lower capacity.

So, we just felt that we were being too pedantic in our approach and selling software in a very hardware-centric model, where you can only buy five subscriptions out of eight. So, we worked hard over the last 18 months to get this all done into a new credit-based model where you can right-size your requirements, so you can spin them up and spin them down. But if I say everything, then Lee doesn't get to say much.

So, Lee, explain [indiscernible] (00:44:17), Lee was saying, why do you say you're going to help – have me answer the second half of it when you don't stop. So, Lee, I've stopped.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.



In my defense, like the – when we came up with the model, that was sort of, I call it, the normal model, and that's what others were doing. I'm actually – and our customers are very excited about this new Firewall FLEX model because it is the first of its kind in the industry, giving your customers the flexibilities, Nikesh was saying, to choose how many CPUs do they need, what subscriptions do they want, where they want to deploy it, cloud, on-prem, et cetera? That level of flexibility and to do it in a credit model where each individual deployment can actually be different. So, we've actually – it's one of those unique cases where we've given the customer a lot more flexibility and options, yet made it simpler at the same time.

The last piece I'd address was in the old model, it was getting too cumbersome on how to offer all different security subscriptions. This model allowed us to easily scale up to all of the current security subs plus any future subscriptions we come out with.

Brian Essex

Analyst, Goldman Sachs & Co. LLC

Q

How long have you been working on this?

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

A

Sorry. We just launched the beginning of February. So, it's only been out for a few weeks. We're already having customers respond incredibly positive to it.

Brian Essex

Analyst, Goldman Sachs & Co. LLC

Q

All right. Very helpful. Thank you.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Thanks, Brian.

A

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

[audio gap] (00:45:37) comes from Gray Powell of BTIG.

A

Nikesh Arora

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

Hey, Gray.

A

Gray Powell

Analyst, BTIG LLC

Thanks. Can you guys here me okay?

Q

Nikesh Arora

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

Yeah.

A

Gray Powell

Analyst, BTIG LLC

All right. Congratulations on the good numbers. So, yeah, last week, you all announced cloud secure web gateway features in Prisma Access. How important is that functionality to your customer base? And do you think it creates an opportunity to gain incremental share from legacy players like Symantec or even some of the higher growth companies like Zscaler?

Q

Nikesh Arora

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

Oh, sorry, okay. Now he changed his definition of legacy [indiscernible] (00:46:14) never mind, so, sorry, I'm just kidding. We get punchy after too much coffee in our earnings call day. So, Lee, go ahead. This one's yours.

A

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Look, as I think all of you have seen and heard from us before, we used to set up this sort of either or approach; either it was next-gen firewall approach to security or is a proxy approach. And you've heard us talk a lot about the challenges associated with the proxy approach, limited application support, some of the challenges with applications and breakage and performance.

A

But at the same time, we recognized is there are certain use cases out there, where there is a right way to do it, and it is a – could be very complementary to what we do from a next-gen firewall perspective. And so with this release, we basically integrated that into Prisma Access, such that we can now give our customers the ultimate in flexibility on how they connect to the cloud through both a Secure Web Gateway model plus our next-gen firewall natively integrated, and provide all the great security capabilities we have.

Nikesh Arora

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

A

So I think, Gray, what Lee is saying is we can [indiscernible] (00:47:27) proxies, now we also support proxies as part of our product. And we also support the app-based approach. So now you can go after web-based apps and non-web-based apps. And we said 53% of your breaches come from non-web-based apps, and proxies are used less than non-web-based apps. But we cover both – we cover both opportunities by doing it the proxy way or the non-proxy way.

Gray Powell

Analyst, BTIG LLC

Q

Got it. Okay. Thank you very much.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Next question comes from Patrick Colville of Deutsche Bank.

Patrick Colville

Analyst, Deutsche Bank

Q

Hey there. Thank you for taking my question. Really appreciate it. Just want to ask about Bridgecrew. So, is that deployed on-prem, in the cloud? Who buys it? Is it the kind of developer buying it with the kind of credit card-type payment model? Or just help us understand that product better, please?

Nikesh Arora

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

A

Yeah. Look, again, I'll do the 1-2 punch here. But we've been making bets for the last 2.5 years where security is going in the cloud space especially, went from workflows, went to containers, went to microsegmentation, went to DLP, went to IAM. And what we kind of the realization is what's happening is there's a bunch of – so what happens is you do – you build an application as a developer and you give it to your IT team and they deploy it and say, hey, you silly guy, you've got a bunch of security bugs in it, go fix it, okay? So what's my security bugs? Why didn't you tell me before? They started going to open source and trying to find security monitoring software to see, let me just make sure I don't build stuff with security bugs in it.

So, what happens is what Bridgecrew has is such a – it's a open-source, free, no credit card needed, piece of software that starts tracking the security bugs in your development site, CI/CD site. So it tells the developer, you're making a mistake, fix it. Now what happens is you fix it, then you give it to the guy in security, the guy says, wait a minute, you still have bugs, so wait a minute. I checked it. So what we've done is we bought Bridgecrew. We'll take the open-source tools that they have. We'll look at the policies there. We'll map them with the policies in the enterprise side to make sure that if you need to find – if they're going to check for it in real time and in production, you get to check for it for free as a developer.

So, there's 26 million developers developing their seamless security structure. If we can get 26 million people to start checking it while they're building the application, building the software, then...

Patrick Colville

Analyst, Deutsche Bank

(

Yeah.

Nikesh Arora

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

A

...it's consistent with what they're going to be checked out in the enterprise side. That's the muscle we didn't have. That's a DevOps muscle. Most DevOps companies don't have security muscle. We have security muscle, we don't have DevOps muscle. We just bought DevOps muscle.

Patrick Colville

Analyst, Deutsche Bank

Q

Okay.

Nikesh Arora

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

A

That's what we did.

Patrick Colville

Analyst, Deutsche Bank

Q

Right.

Nikesh Arora

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

A

And so the monetization is via – so what will happen is they have a enterprise version of the free software to give away to developers. It's kind of like Dropbox. If a lot of people started using it, you want that to be in the enterprise section, because you don't want it being checked against a different product set of policies. So we're going to merge that enterprise capability in Prisma Cloud because we already checked it, and we'll say, whatever your developers checked for free is what we're going to check in production, they're consistent, so if they didn't find a bug when they were writing the code, we're unlikely to find it when we're running it.

Patrick Colville

Analyst, Deutsche Bank

Q

Good. Thank you.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Question comes from Tal Liani of BofA.

Tal Liani

Analyst, BofA Securities, Inc.

Q

Hi, guys. I want to go back and ask about the legacy or the hardware piece. I'm trying to understand the competitive landscape now and trying to understand the customers' reaction to the fact the market is migrating somewhere else. Are there still competitive replacements, or is this a case where customers just keep the status quo, whatever they have today, because if they take a decision, it's going to be a decision to migrate out of hardware into more modern solutions? So, I'm trying to understand the dynamics, the underlying dynamics in the market, and from it to understand what's the competitive landscape like.

Nikesh Arora

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

A

Yeah, Tal, thanks for the question. Look, what's going to happen in my version of the world is you will still have 40% to 50% of the customers who will still stick to a data center and a hardware-based strategy.

I think what the market has not fully embraced and understood is when you move to the cloud, the cloud can be expensive. And many companies will say, wait a minute, I don't need to do all this stuff in the cloud. I'm going to still keep a data center and do some of the less expensive stuff here, why do I want to take everything and make it real-time bleeding edge in the cloud? So you're going to end up in a hybrid world, where people are going to maintain data centers and maintain the cloud. So, I don't think every customer in the world is moving to the cloud, but I think that on the margin, yes, you're seeing a bigger shift to the cloud than you are [ph] people sticking out now (00:52:10).

So, with that fact in mind, we do see competitive replacements when customers have end-of-life for existing hardware installs, right? They're sitting there and saying, I'm coming to end-of-life for legacy vendor A, B, C, D, or E. Should I go replace this with new versions of legacy A, B, or C, or should I look at a new network architecture, which allows me flexibility of having hardware and software into more access. So the example we gave, we did a \$20 million deal with a customer, who built – who bought Prisma Access for half of their employees, who bought hardware firewalls to the data centers, and who bought virtual firewalls to their cloud. And they make sure they were all consistent.

So, we do see customers end-of-life-ing legacy hardware, which is dead-ended, which doesn't have a software form factor or a firewall in the cloud capability, and we do see them transitioning to a hardware and software model. So it's not zero sum. It's not either or. It sometimes ends up being this and that.

Tal Liani

Analyst, BofA Securities, Inc.

Q

Got it. Thank you.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Next question comes from Brent Thill of Jefferies.

Brent Thill

Analyst, Jefferies LLC

Q

Thanks. And Nikesh, there's a lot of questions from investors about this proposed equity structure and the timing and what this means.

Nikesh Arora

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

A

Pretty quick.

Brent Thill

Analyst, Jefferies LLC

Q

And I'm curious if you could just double-click on what you think this looks like, and why you're doing this right now?

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

A

Thanks for the question. Look, it's not – first of all, we have spent the last six to eight months preparing for the financials visibility or transparency of ClaiSec and NetSec. It requires a lot of work on our accounting side, lots of rules to make sure how we do transfer pricing between the entities and how do we leverage our common sales force in Palo Alto Networks.

So – and again, we're not doing anything yet, all we'd have is we've presented to the board, and they have agreed that this is an area for us to go ahead and work further on, which means we are looking at seeing how can we make the ClaiSec equity more transparent, if we believe the market values that differently than Palo Alto equity. Now the market can say, this is great, we'll just love your Palo Alto equity, and we will help it achieve all the price targets, some of the more enthusiastic and optimistic ones that you have, in which case we may not have to do anything.

If not, we may actually go take a look at the ClaiSec equity and see how do we create more transparency, because fundamentally, if you look at it, you've got one business [indiscernible] (00:54:28) generating \$1.5 billion of free cash flow, which is fantastic. We like it, 38% margin going to 41% whilst we're going through a hardware to software transition.

On the other hand, we have a \$735 million ARR business growing at 77%. That business has negative cash flows. And the market looks at them together and values us one certain way, maybe the market will value us differently if we look at it differently. So we're just exploring the opportunity of being able to make that value more transparent. We're not going to change the operating structure of the company. We're going to still run it as one company with two basically agile business units, if that makes sense.

Karen Fung*Senior Director-Investor Relations, Palo Alto Networks, Inc.*

A

Our next question comes from Michael Turits of KeyBanc.

Michael Turits*Analyst, KeyBanc Capital Markets*

Q

Hey. Good afternoon, everybody, and nice quarter. It was a really good quarter on firewall platform-as-a-service and you raised Network Security, but the product itself was just [indiscernible] (00:55:17) didn't raise it. So, what's the delta? What really raised that guidance on network for the year and drove the outperformance?

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

A

Software.

Michael Turits*Analyst, KeyBanc Capital Markets*

Q

What was the biggest piece? VM-Series, Prisma Access, subscription attach, how would you rank those?

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

A

Access, VMs, and subscriptions. Not because subscriptions aren't doing well, it's just a very large number. So, sustaining a large number growing at 30% is a good thing.

Michael Turits

Analyst, KeyBanc Capital Markets

Q

Great. So it's really – Prisma Access was the big driver.

Nikesh Arora

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

A

Yeah. I mean, look at Access, it's gone to a – when I joined, it was called GlobalProtect Cloud Service, we barely did \$10 million in a quarter. Now it's going gangbusters. Now I just said we did \$20 million deal across a customer's entire enterprise, which included Cortex and Prisma Access in there. So we can get to a 10-plus million dollar deals in Access in one deal, where we were doing \$10 million in one quarter three years ago. So, that makes it interesting.

Michael Turits

Analyst, KeyBanc Capital Markets

Q

Great. Thanks, Nikesh.

Karen Fung

Senior Director-Investor Relations, Palo Alto Networks, Inc.

A

Next question comes from Jonathan Ho of William Blair.

Jonathan Ho

Analyst, William Blair & Co. LLC

Q

Hi there. I just wanted to get some additional color in terms of the subscriptions that you've been, I guess, selling with the firewalls. Is there any way that you can maybe provide some additional perspective on maybe which ones are doing well, what the average number of subscriptions being taken are? And, yeah, that would be great. Thank you.

Nikesh Arora

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

A

Yeah, Jonathan, obviously, we had four when I joined, and they're all – had over 50% attach rates even before, the one which has gone from 0 to 500 is DNS Security in the last two years. As we just announced, we crossed the 5,000-customer mark. Many of the newer subscriptions were just launched as part of 10.0 with our software. So they're all very recent, which includes IoT, SD-WAN, DLP, those three...

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

A

Yeah, yeah.

Nikesh Arora

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

A

[indiscernible] (00:57:18), right. And, sorry, I got Lee sitting next to me socially distant, so I keep nodding, asking him if I forgot anything. But SD-WAN, you can see, is combined with our CloudGenix efforts, so we see SD-WAN traction between the two of them. We're seeing a lot of interest in DLP, which is very early. It's only a few weeks

old. And IoT, we see situations, but that's more of an architectural sale it's not just an add subscription, people want to look at the IoT architecture for the enterprise. But we launched healthcare IoT, so it's part of the IoT efforts.

So, I have expectations from DLP, I have expectations from SD-WAN obviously, with combination of CloudGenix and IoT, but I think we'll see different approaches and different sort of trajectories in terms of adoption. IoT is a bigger ticket when we sell it. DLP is a simple attach and is easy to deploy, like DNS Security is. So, they take different trajectories and different pricing.

Operator: Our last question comes from Andy Nowinski of D.A. Davidson.

Andrew James Nowinski

Analyst, D.A. Davidson & Co.

Q

Great. Thank you for squeezing me in. So, you mentioned a number of eight-figure deals for both Prisma Access and Prisma Cloud, which were record deals for the company. Just wondering if you could provide any more color with regard to your overall large deal activity for the quarter, was the activity up year-over-year? And if you did see an increase in the overall activity, kind of what drove the growth? Thanks.

Nikesh Arora

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

A

Yeah, Andy, I think purely math – I'm waiting for Luis to go look, but purely mathematically, we added the same number of customers we did this year than we did last year, and our billings grew 20%. So we got – definitely got to have more bigger deals in there. Hurry up, Luis, what are you doing? So yes, we are seeing strength. But I would say, it's kind of interesting. If you look at the landscape, the higher end of cloud sales see bigger deals, because you're comparing them to large GCP, AWS, Azure spend. So even if you get 2% to 5% of the GCP, Azure, AWS commitment, you end up with a large deal, which is typically the seven-plus figure range. And you see a similar activity in Prisma Access, because it ends up being a three-year TCV-style deal with – if you get the top end, like 100,000-plus users, you end up with a 7.5-figure deal.

XDR in the market typically ends up in the \$1 million to \$2 million range because of competitive pressures and competitive activity. So you just need to do a lot more XDR deals to get there. So, it's different depending obviously, firewall, again, depends on the installed base of the estate and the end of life. And ELAs have their own characteristics depending on, again, how much estate is there and how much people are re-upping and how much software they're buying. But Luis?

Luis Visoso

Chief Financial Officer, Palo Alto Networks, Inc.

A

So here is how I look at it. If you add up the billings of the last largest deals that we did this quarter and you compare that to a year ago, the total is 35% higher. So it just gives you a magnitude of how significant those large deals are for us.

Andrew James Nowinski

Analyst, D.A. Davidson & Co.

Q

Thanks, guys. That's really helpful.

Nikesh Arora

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

All right. Well, I see Brad Zelnick, if you change your mind about us, you don't even get to ask a question.

All right. Thank you, everyone. Thank you for joining us and thank you very much for all your questions. We look forward to seeing many of you in our upcoming investor events. I also want to thank our customers, partners, and of course, our employees at Palo Alto Networks. Have a great day.

Luis Visoso

Chief Financial Officer, Palo Alto Networks, Inc.

Thank you.

Disclaimer

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

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

The contents and appearance of this report are Copyrighted FactSet CallStreet, LLC 2021 CallStreet and FactSet CallStreet, LLC are trademarks and service marks of FactSet CallStreet, LLC. All other trademarks mentioned are trademarks of their respective companies. All rights reserved.