Corrected Transcript

11-Nov-2020

Palo Alto Networks, Inc. (PANW)

Acquisition of Expanse Inc by Palo Alto Networks, Inc Call

CORPORATE PARTICIPANTS

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

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

OTHER PARTICIPANTS

Sterling Auty
Analyst, JPMorgan Securities LLC

Keith Eric Weiss
Analyst, Morgan Stanley & Co. LLC

Fatima Boolani
Analyst, UBS Securities LLC

Philip Winslow
Analyst, Wells Fargo Securities LLC

Brian Essex
Analyst, Goldman Sachs & Co. LLC

Andrew James Nowinski
Analyst, D. A. Davidson & Co.

Jonathan Ho
Analyst, William Blair & Co. LLC

Gray Powell
Analyst, BTIG LLC

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Catharine Trebnick
Analyst, Colliers

Erik Suppiger
Analyst, JMP Securities LLC

MANAGEMENT DISCUSSION SECTION

Operator: Good morning and thank you for joining us on short notice. As you've seen, this morning we announced the proposed acquisition of Expanse. Joining us today to discuss the transaction are Nikesh Arora, Chairman and CEO of Palo Alto Networks; and Lee Klarich, Chief Product Officer.

Please note that we are still in our quiet period and we'll be reporting on our fiscal first quarter results on Monday November 16. We will not be commenting on our fiscal first quarter results or our fiscal second quarter guidance during today's call.

We'd like to remind you that during the course of this conference call, management will make forward-looking statements including statements regarding our competitive position and the demand and market opportunity for our products and subscriptions including our beliefs about the anticipated benefits at the proposed acquisition of Expanse for us and our customers; the anticipated timing of close and our integration approach and our continued execution and focus on providing new products to our customers. All statements other than historical facts including statements regarding the expected benefits of the proposed transaction and forward-looking statements. These statements are based on management's current expectations, assumptions, estimates and beliefs. While we believe these expectations, assumptions, estimates, and beliefs are reasonable such forward looking statements are only predictions and are subject to a number of risks and uncertainties which are beyond our control and which could cause actual results to differ materially from those anticipated by these statements. These forward looking statements apply as of today and should not rely on them as representing our views in the future.

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

Nikesh Arora

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

Thank you, Karen, and thank you everyone for joining us at a short notice. First and foremost, today is November 11. It is Veteran's Day. Before I begin, I would like to recognize and thank all of our veterans for their service and particularly those in our Palo Alto Networks family. We're grateful for everything you do for our nation and feel tremendous benefit of your public service. Thank you.

Now turning to our news this morning. We're delighted to share more about our proposed acquisition of Expanse which will significantly enrich our Cortex product suite to proactively address all security threats faced by an enterprise. Let me first give you an idea of why we're excited about Expanse and their unique technology before turning it over to our Chief Product Officer, Lee Klarich, who is here to dive in further. Since releasing their first product four years ago, Expanse has become a leader in attack surface management. Expanse has dedicated themselves to developing an Internet collection and attribution platform that constantly monitors the global Internet, mapping the exposed and untracked assets of an enterprise that comprise its attack surface. This data gives organizations a crucial picture from the outside in, that is to say, the same view that an attacker sees when hunting for potential weaknesses. It's because of the insight that their technology is trusted by some of the world's largest and most complex organization from members of the Fortune 500 to the US military.

While this category of attack surface management has been important on its own, we think it has more powerful implications for customers and combined with Palo Alto Networks' Cortex product suite. Once integrated after closing, Cortex will stitch together internal and threat data with Expanse's external view of exposed assets. This will give customers a complete picture and eliminate vulnerabilities across an enterprise. Together with Expanse, ours will be the first solution that combines the outside view of an organization's attack surface with an inside view to proactively address all security threats. We believe that no security solution is complete without this. As you can see with past acquisitions, we were early to support and invest in the best companies in emerging technology areas and competitors have validated our strategy by following us and investing in the same areas. Our intent to acquire Expanse will likely continue this trend.

Let me cover the details of the transactions. Under the terms of the agreement, the total purchase price includes approximately $670 million of cash and stock, approximately $130 million in replacement equity awards with each amount subject to adjustment at close. We expect Expanse to contribute $67 million of ARR in our current fiscal year ending July 2021 continuing its 100% growth momentum. Expanse transaction multiples are very favorable compared to other companies of equivalent size and even more so when adjusting for growth. As you've likely read already, Expanse co-founders Dr. Tim Junio and Dr. Matt Kraning will join Palo Alto Networks once closed and we're excited to join forces.

With that, I'll turn it over to Lee.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Thank you, Nikesh, and thank you for joining us today. I'm excited to share how Expanse fits into our broader Cortex strategy. So let me start by telling you more about Expanse. As Nikesh mentioned, Expanse was founded about eight years ago and built up an incredible team of experts across many technical disciplines including data science and machine learning, security and distributed systems. They figured out that there is a tremendous amount of information you can find simply by scanning the Internet, but to do so in an accurate, scalable and complete manner is extremely difficult. It requires a large dynamic and global infrastructure that continuously scans the Internet for any new or modified assets. To give you an indication of the scale, Expanse makes 10 trillion decisions every day with their analytics.

With their Internet collection and attribution platform, they constantly monitor the global Internet to map exposed and untracked assets that comprise the customer's attack surface. This includes all exposed cloud resources, remote workers and on-premise assets. Every asset is attributed to an owner. Security exposure is identified and presented to the customer as an X-ray of their enterprise from the outside in, the same view that attacker sees as they probe for points of weakness. As an example, when we first activated Expanse at Palo Alto Networks, we found cloud workloads that we didn't know existed and remote workers with services exposed that shouldn't be. We were able to remediate this very quickly with XSOAR but Expanse quickly became ingrained in our stock processes and we're very buttoned up security organization. Imagine what other companies would find. Expanse packages its data in a very intuitive UI as well as an exact level report that can gain immediate attention within enterprise. For example, the report will show cloud workloads that were deployed outside of enterprise security controls, something that happens all the time. It will show assets with remote access such as SSH accidentally left open to the Internet and exposed to attackers; something that happens far too often or in the case of one of Expanse's customers, it showed an unsecured military operation in a remote part of the world. Definitely not something you want to find out the wrong way.

Now, let's talk about how Expanse accelerates our broader Cortex vision, but first some context. We've spoken in previous calls and our analyst event in 2019 about the challenges facing security operations as they are constantly overwhelmed with alerts that often go ignored. The underlying reasons for this are first and foremost, data is collected into disconnected data lakes or not collected at all. Without the right data in the right place, analytics is difficult, limited and often left to static correlation rules. This then results in massive alert volume that requires an overly manual and reactive approach. It's simply not sustainable.

Our vision for Cortex is to build the industry's first proactive security platform for security operations, one that focuses on collecting a rich set of data into a robust and growing data lake applying AI-based analytics for detection and leveraging automation throughout to dramatically to reduce the number of alerts and amount of manual work needed. With this combination, we believe we can proactively detect and remediate all security issues.

At the foundation of our Cortex vision is rich security data and deep knowledge and understanding of that data. When we look at data, we see three key types. Enterprise data, including endpoint, network and cloud, threat data and attack surface data. The Cortex XDR Data Lake now holds close to 120 petabytes of enterprise and threat data and Expanse will accelerate our goal to collect all relevant security data by providing the best attack surface data. This combination will provide for the first time a true 360 degree view of an enterprise. This integrated data will drive a rich set of analytics that will be a game changer for proactively addressing security issues.

And with automation, we've seen an acceleration of XSOAR automation where we've now crossed the 400 million mark of actions that can be automated, up 100% in just the last four months. This exponential growth is a result of increased automation playbook adoption where we now have customers that automate more than 1 million alerts per day and achieve up to 20x alert reduction using automation. With the proposed acquisition of Expanse, we will take the great data and analytics from Expanse and combine it with the automation power of XSOAR enabling full security remediation via automation.

This is a great example amongst several of how the integration of Expanse can drive incremental value for our customers. This combination of Expanse, XDR and XSOAR will accelerate our path to achieving our vision with Cortex. Expanse will provide a unique outside in view of an enterprise that will become a must have data source for enterprises. This data will enable the first 360 degree view of an enterprise and at the same time provide a unique and valuable data and analytics source to Cortex. As we expand Cortex to collect data from any relevant data source, we are setting our sights on building the most robust data lake to enable greater levels of analytics and automation.

With that, let's open the call up for questions.

QUESTION AND ANSWER SECTION

Operator: [Operator Instructions] Our first question comes from Sterling Auty of JPMorgan.

Sterling Auty
Analyst, JPMorgan Securities LLC

Q

Hey, again. Thanks for letting me unmute. So just maybe to start off, I think it's very interesting technology, but can you help us understand exactly how have they monetized this capability? So what is the contract structure for the company? Is that going to change underneath Palo Alto Networks? And who do they compete with on a heads-up basis?

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

A

Hi, Sterling. Good morning.

Sterling Auty
Analyst, JPMorgan Securities LLC

Q

Good morning.

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

A

They've been able to monetize their ability by sharing the data with their customers and giving them a vulnerability assessment as part of their – they scan the Internet multiple times a day, almost on an hourly basis and they're able to see any new assets that are exposed or created in any customer's enterprise. And then they're able to take that data and check that off against existing known vulnerabilities and they're able to show the exposed assets which should not be exposed to Internet, which basically allows the customers to take that and remediate that with whatever remediation that they have in place.

Now, the benefit we have is we have two incremental capabilities. One, we already have an inside-out view of the customer. So we know which assets are being created; being able to marry that data with the data which looks at it from the outside-in, coupling that with playbooks that we have in XSOAR allows us to automate that remediation. So basically, customers over time will not have to do much effort other than just be able to subscribe to the data feeds both from them as well as use XDR. They can also use them without using XDR. So, in the future, you will see a notion from us which is an independent notion where Expanse sells which they do today. And as we saw on the datasheet, they do $600,000 of ACV per customer, which again if you look at security, this is a big number. It's hard to find companies out there in the space which can generate that amount of dollar value on an annualized basis for each customer. So I find that particularly exciting. It is a product which is targeted to larger enterprises that given we have 1600 out of Global 2000, we find that's a very sweet spot for us for where they operate. We don't anticipate changing their contract structures as much as we anticipate the ability as we integrate that into our Cortex Data Lake with XDR and XSOAR of creating new product offerings that allow us to not only sell them independently but also sell them as part of our overall Cortex capability.

[ph] You want to add something? All right (00:12:36). He's about 10-feet away from me.

Sterling Auty
Analyst, JPMorgan Securities LLC

Q

Thank you. That makes sense.

Operator: Our next question comes from Keith Weiss of Morgan Stanley.

Keith Eric Weiss
Analyst, Morgan Stanley & Co. LLC

Q

Excellent. So I thank you guys for taking the question. Maybe one for Nikesh and one for Lee. For Nikesh, it sounds like these guys have a considerable government business. Can you talk to us about sort of who their customers tend to be? They seems very large enterprise-focused. Is there a considerable government exposure here as well? And then one for Lee. Can you help us understand like post the acquisition you have Expanse, you have XSOAR, is there also a need for like the traditional VM perspective? Do you already have tools that are going to be competitive with what like a Rapid7 or a Qualys is giving you from that inside out perspective or is that like additional functionality that will be vis-à-vis partnership or whatnot be incorporated into this inside out view of vulnerabilities?

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

A

Okay. Well first of all, Keith, you look wonderful. I'm just trying to figure out which movie I've seen you in.

Keith Eric Weiss
Analyst, Morgan Stanley & Co. LLC

Q

It's pretty early in the morning for this conference call. Let's just admit that, okay?

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

A

Trust me, you and me both. I found my first malfunctioning railway track traffic light this morning. I just hung out over there for 10 minutes and what the hell's going on. Anyway, sorry, back to business. You know the vulnerability question [indiscernible] (00:14:07). On the exposure – I don't know – having customers in the government is, you call it, exposure. I call it phenomenal because they've been able to go take a technology which they developed and have been able to convince that this is critical to national security infrastructure. Now unfortunately I can't tell you who their customers are in the government. Otherwise, they will kill me. So, they have customers in the government. I think they have applicability not just to one government. They have applicability to many governments around the world because every government, they scan the entire global Internet. They watch 10% of the traffic on the Internet on a daily basis. That's a lot because really there's like 4 million IP addresses out there. So they do watch a lot of the Internet. We think there's tremendous opportunity where they already have created capability. They've only had a very few go-to-market people and we have the opportunity of applying Palo Alto Networks' marketing capabilities behind them. In fact, we're doing a commercial relationship with them to allow us to do some marketing with them in short order. So, we think the opportunity is huge. We think most enterprises should have this data. We think without this data, it's impossible for enterprises to be able to understand what the attackers are seeing. That's all really excited about it, but I'm going to let Lee talk about Qualys and Rapid7 et cetera.

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

A

Yeah. So look the data that Expanse finds by scanning the Internet is we haven't found any substitute for it. So unlike more traditional vulnerability scanning where you specifically scan the things you know about, what Expanse is doing is finding all of the assets, workloads, et cetera that you didn't know you had. So, it's a very unique data source from that perspective. Now, we'll be able to combine that with the data that we're collecting already within Cortex and recently Cortex XDR added vulnerability information from all endpoints. And as Cortex opens up to additional data sources including up to any data source in the future, yes we'll pull in other data whether that's from Qualys, Rapid7 et cetera to combine with this other view that we have with Expanse, XDR et cetera. Makes sense?

Keith Eric Weiss
Analyst, Morgan Stanley & Co. LLC

Q

Okay. Excellent. Thank you, guys.

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

A

Thank you.

Operator: Our next question comes from Fatima Boolani from UBS.

Fatima Boolani
Analyst, UBS Securities LLC

Q

Good morning.

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

A

Good morning, Fatima.

Fatima Boolani
Analyst, UBS Securities LLC

Q

How are you? As explained...

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

A

How can I be at 5:30 in the morning?

Fatima Boolani
Analyst, UBS Securities LLC

Q

Early bird gets the worm. I wanted to dig in to the competitive differentiation and the technological barrier to entry with Expanse. So my sense is there's elements of threat intelligence here. Security validation and certainly traditional VA feature functionality. So, I really wanted to drill in on the approach Expanse has from a data collection standpoint. And to what extent is the data that Expanse generates proprietary versus partnerships with other third-party threat intelligence platforms to really reinforce the quality of the data that's coming throughout the platform?

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

Thanks, Fatima. I'm going to have Lee answer most of the questions, but I will tell you I was amazed at what these people have created. They have taken eight years. This is a non-trivial engineering problem, trying to scan the global Internet because most things do not like you to be scanned a regular basis. So, they'd have to build all kinds of technologies and servers sitting in different parts of the world trying to scan everything and make sure they can, I would use the word circumvent but make sure that they are considered a valid scanner when they go and look at stuff. But with that I'm going to pass it over to Lee to answer all the threat intel and security validation questions you have.

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

Yeah. As Nikesh said, it is a hard problem to solve. On the surface, it seems easy. You just scan stuff. But getting accurate results, being able to constantly update those results as assets change, being able to make sure you have a comprehensive view is actually a very difficult data problem, machine learning problem, et cetera. The vast majority of what they do is homegrown. It's what they do versus coming from partners. They do have a number of partners in order to help extend what they do, but the vast majority is from within their own team and own technology stack.

Fatima Boolani
Analyst, UBS Securities LLC
Q

That's very helpful. Thank you.

Operator: Our next question comes from Philip Winslow from Wells Fargo.

Philip Winslow
Analyst, Wells Fargo Securities LLC
Q

Great. Thanks guys for taking my question. Obviously, this deal makes sense in your thesis of sort of security as a data problem, but I did want to focus on sort of the IT operations side of this, because obviously when you think about asset, inventory management, governance, there is an IT operations angle to this. So how do you think about sort of the blurring of lines between sort of security and IT ops and also just call it different buying centers for Palo Alto Networks and Expanse?

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

Well, Phil, first and foremost, you're 100% right. The data has applicability both in the security domain and the IT asset management domain. Interestingly, our teams once we've put it in the [ph] SOC (00:19:40) and did the security solve, they've come with a shadow IT use case where they found people spinning up stuff that shouldn't be spun up and we can go out. So maybe just [ph] found this spun this up, this will work, (00:19:50) click here to accept. If it is, we'll move it into the work domain. So yes, 100%. There is an IP asset domain capability that the data allows us to have. And I'll tell you what's interesting is over time as you get into a world where you have more and more enterprise data and large data lake, it'll have more applicability outside of security. It's kind of interesting. There are some companies out there as you know who started with collection of all data and they realized 80% of use case is security. We start with 80% of the use case, i.e., security, and then said there is a 20% use case which also is outside of security. So for now we're very focused on the ability to take this data and run all the security capabilities around it.

As we've talked in the past, two and a half years we had a thesis. We expressed a point of view. We think all security is a data problem in the future. We think security is not a hygiene problem. It's not a policy problem. It's a data problem that requires you to collect a lot of data both inside and outside the firm. And in the past, historically, whether it's healthcare or it's education or it's security, it's been hard to collect and store. It's been expensive. As you see, the world is going to a place where data is easier to store, collect and analyze. And we think we've got to stay two steps ahead of making sure all the data that's available for an enterprise that helps make them more secure is available and normalized by us in one data lake. So, as Lee mentioned earlier, we have Cortex XDR. We added firewall capability to it, we've added our e-mail capability, we have identity capability to it, we're going to add external points of view to it. So we're slowly and steadily normalizing all security data that's available to allow us to provide a sort of an auto remediation capability to our customers because we believe security both as the data problem and also needs to become more proactive in real-time. Does anyone...

Philip Winslow
Analyst, Wells Fargo Securities LLC
Q

Great. Thank you.

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

Okay.

Operator: Our next question comes from Brian Essex of Goldman Sachs.

Brian Essex
Analyst, Goldman Sachs & Co. LLC
Q

Hey, good morning. Thanks for getting up early and giving us a highlight of the acquisition. Just want to ask about the history behind the two companies, and Nikesh, how long have you been working with them and what might you expect in terms of integration? And then finally, in terms of the sales force's familiarity, how fast can this kind of go-to-market? What are the synergies across your platform from a go-to-market perspective? You guys have a lot of tools in your bag at this point; so just want to understand how quickly we might be able to anticipate integration with the platform and then impact in terms of revenue contribution with your sales force?

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

Yeah. Thanks, Brian. Look, first and foremost, we looked at them and a bunch of other people who claimed to collect data from the outside-in, I want to say about nine months ago approximately, and our CISO actually was the first one who took this, deployed it. He did the analytics on many such companies and data out there and came back and said this is by far, 3x to 4x better than any data I've ever seen. And we have a CISO as you can imagine for our cybersecurity company. We have somebody who's been around the block and seen most things out there. And that was kind of like the first aha moment. We looked at it. Our teams looked at it. And then we said, oh, wow, they don't do remediation. They do basically vulnerability assessment. They're going to like tell you what the problem is and then we're on our own.

So, our XSOAR team got involved and built a bunch of playbooks and said, wow, this is cool. Now we can find this and we can remediate it on the fly. As you know, our SOC has less than 500 alerts a week which was come down from tens of thousands. And we said, wow, what is the larger applicability of this and we sat down with the founding team. Lee, Nir and I talked about this and it's very hard to get down Nir's technical diligence. Nir is a firm believer and that everything is a simple matter of programming. When Nir tells you that this is hard, then you have to pay attention. And Nir got excited about the data they were collecting because it's a hard technical problem to go collect data from everything in the world and monitor, attempts on the traffic on a daily basis on multiple times a day. So when we got to that realization that they're collecting something unique, there's nothing out there, we looked at the viability as part of our platform. Now what's fascinating Brian is, for example, we're about to have our customer conference in 10 days, we've been working before this idea of it because Expanse with the notion that, hey what if we give our customers their vulnerability map? So we can actually, if the customer wants, you tell us the name of your company, you say yes I would like it. We can build a map, we don't need anything. Remember, I'm looking outside in. I don't need to be in your infrastructure. I'm looking outside in so I can actually build the vulnerability map for you and tell you how many assets you have exposed tomorrow. So I think that's the best sales tool our salespeople are going to have is we don't need to deploy anything in infrastructure. We don't need to do the POC. We don't need to put a censor in the infrastructure. We know.

Now we can work with you. And in about a week, we can make that deal even a lot better because you can tell us what's what and why it's open and why it's not. So, from a sales perspective, I think our team should be easy to understand, like we're telling you, this is the vulnerability map. Here's where the vulnerabilities are. And it's typically something a CISO or CIO at that senior level is interested in. So we think that will act as a huge lead generation for us. And then after that question I mean it's kind of like if I'm a CISO or CIO and I see this, I shouldn't – I can't un-see it. It's like okay I don't have a problem. It's hard to un-see. You know what. I don't need it. Thanks. Thanks for letting me know that five of my things are busted and I'll come back to you.

Brian Essex
Analyst, Goldman Sachs & Co. LLC

Q

Thank you.

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

Andrew James Nowinski
Analyst, D. A. Davidson & Co.

Q

Great. Thank you. Good morning, everyone. So is the $67 million in revenue that Expanse, is that something that Expanse may have already booked or does that assume some cross-sell contribution into your own installed base? And then second, how much customer overlap does Expanse have with your current installed base of 72,000 customers?

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

A

So first and foremost Andrew, I want to thank you very much. I spend lots and lots of time with Luis, our CFO on those two slides with numbers, and I was like holy shit, nobody wants to ask me a question about those two slides I worked hard on. Why we're early in technology on M&A and why this is a very, very attractive acquisition. So as you can imagine, we are in a quiet period. $67 million is their forecast for our fiscal year from an ARR perspective. It's a standalone number. It is to show the asset we acquired and what value we paid relative to their forecast and their growth rate for this fiscal year. We're not making any projections as to the incremental capabilities we can build and deploy in this fiscal year or next with the combination of Palo Alto Networks and Expanse. We will leave that conversation for our earnings call which is next Monday at a similar time. So, we're not commenting on that. In terms of number of customers, as I said earlier we have 1,600 of Global 2000s, not counting many governments around the world. Expanse has approximately in the vicinity of 50 customers. So there's 80 times more customers we had just at the top end of the funnel. I don't think it's applicable to 72,000 customers just yet but I think it definitely has applicability to the 1,600 customers we have, as well as to many governments around the world which have not seen this capability yet.

Andrew James Nowinski
Analyst, D. A. Davidson & Co.

Q

Great. Thanks, Nikesh.

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

A

Thank you, Andrew.

Operator: Our next question comes from Jonathan Ho from William Blair.

Jonathan Ho
Analyst, William Blair & Co. LLC

Q

Hi. Good morning. I just wanted to ask in terms of Expanse's ability to collect data from assets globally. Is this easier in some regions than others? Are there dark spots out there that maybe require more CapEx investment? I just wanted to get a sense of the need to potentially expand their coverage over time. Thank you.

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

A

Hi, Jonathan. It's a good question. The Internet assets react differently depending on where you're coming from. And so in order to get a true global view of the world, you actually have to be global in the scanning infrastructure itself. And this is part of what I was saying before in terms of just needing to build out that global infrastructure for scanning, for scale, for speed, et cetera. And they figured out how to do that. They significantly leverage the cloud to be able to do this which obviously gives them benefits in terms of how dynamic and agile it can be in terms of where they're running it around the world. And it can combine it with additional data sources and additional probing locations to augment that where needed. But this is proving to be a key piece to how they're able to achieve the level of accuracy that they do and that we saw when we did the testing versus others in this space.

Operator: Our next question comes from Gray Powell of BTIG.

Gray Powell
Analyst, BTIG LLC

Q

Okay, great. Can you hear me?

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

A

Yeah.

Gray Powell
Analyst, BTIG LLC

Q

Hi. Thank you very much. So yeah Expanse sounds very much like a high end enterprise grade product. How should we think about the potential to move the product set more into the middle market? Are there pricing changes or anything that you would need to tweak?

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

A

Not particularly that I think from our perspective getting it down to middle market, the more we can package it as a set of solutions. So, for example, our SOC has already prepared the playbooks needed to remediate. What do you find when you get from enterprise down to the mid-market that there's not as many security people around who want to go solve every security problem, learn every tool that's out there. So the more we can auto-remediate things, the happier people are. So we already have automated playbooks. If you can step into a mid-market company and say, look, if you turn this data on, we get the data, we look at the vulnerability and this playbook will remediate that problem for you and solve. So you don't have to get involved in solving the problem. The more we can do that, the more applicability it has, the lower the enterprise tier. So we think that's very well in the realm of capability and possibility for us to go ahead and do and obviously we have plans to do that. So, as and when we – first, we got to acquire the company, get it closed. Once we have closed it, we've got to go put the packaging in place around some of these automation capabilities which we think we should be able to do.

Gray Powell
Analyst, BTIG LLC

Q

Got it. Okay. Thank you.

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

A

[ph] Sure (00:30:52).

Operator: Our next question comes from Shaul Eyal from Oppenheimer.

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Q

Thank you. Hi. Very early good morning to you guys. On Expanse, do they collect structured or unstructured data or both? And do they have sensors in the dark web?

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

A

So they're collecting both structured and unstructured data and as you would expect they're constantly scanning for everything they can find. The dark web, I'd say, for the most part, no. And that tends to be more of a threat intel kind of feed that can be interesting but it is distinct and different from the outside-in view that Expanse is collecting and analyzing.

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Q

Thanks.

Operator: Our next question comes from Matthew Hedberg of RBC.

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Q

Oh hey, guys, thanks for taking my question.

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

Famous words of 2020. You are on mute.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

There we go. Sorry about that. It's the unmute and mute on phone and in Zoom. $650,000 ARR per customer is impressive. Can you guys talk about how did a customer start and get to that level, because with four years of history these are some really, really big customers. I'm just kind of curious that land and expand with the customer.

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

Yeah. So mostly what we've been talking about today is what they call their expanded product which is that outside-in view, understanding all of the assets, understanding what security risks are exposed. And even that can start off with a subset of a large enterprise or a large government organization and then expand to include the entire enterprise. They then can also come in with a product they call Link which is how they can then start to apply the same level of visibility and scanning to critical suppliers. Supply chain integrity has become a very important part of organization's security posture as more and more companies realize the importance of their suppliers to their overall security capability.

And third, they can expand into a behavior module that actually looks more at the traffic leaving an enterprise and analyzing that against potential risky behavior. And so they sort of take those things together, they can land in a portion of enterprise in Expanse. From there, they can expand into supplier security and from there they can expand into the behavior analysis as well.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

That's great. Thanks a lot.

Operator: Our next question comes from Catharine Trebnick of Colliers.

Catharine Trebnick
Analyst, Colliers
Q

Hi, there. Yeah. Just to net this out, it seems like you're adding a solution on to give you better visibility because you don't really have all the capabilities to look at what you don't know to protect the surface. So, I'm just trying to simplify what seems to be pretty complicated. Is that simplified messaging or not? So, it's not really a question.

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

Catharine, if you think about most security products in the world, they're installed inside the enterprise and they're looking from the inside and say, well there's doors; let's shut them down. When you open this door, let's make sure that our guardrails around opening this door what it opens for and whether you set the right rules or not. And when you're done, it's like bringing in a security expert who walks on the outside and say, we'll let windows open and that doors open and why is that door open, it doesn't have the right things that need to be in place for that door to be open. So, yes, you have a website which is open to customers who can access your data, but why is the other website open because it's not supposed to be open externally. Why is it open? So, you can find the errors from the other side when we're scanning from the outside. And we can also say, oh, I know I see that. That's a known malware or that's a known security vulnerability. Why is that exposed to the Internet? So you're just basically looking from the outside in to see what do I see when you believe you've done all your work on the inside out.

Catharine Trebnick
Analyst, Colliers

Q

All right. Thank you very much.

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

A

No problem. I have to dumb it down for myself. So don't worry. I won't let Lee answer it because if he does it, he'll tell you the exact answer.

Catharine Trebnick
Analyst, Colliers

Q

Thank you.

Operator: Our last question comes from Joel Fishbein from Truist Securities.

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

A

This must be the second most exciting thing on Zoom. He's no longer there.

Operator: Joel, can you please unmute yourself?

Operator: Okay. Last question will be from Erik Suppiger from JMP Securities.

Erik Suppiger
Analyst, JMP Securities LLC

Q

My questions have been answered. Thank you.

Operator: Great. That concludes the Q&A portion of our call. Thank you for all of your questions. I'm going to turn it back to Nikesh for closing remarks.

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

Thank you very much, guys. Appreciate your quick turnaround and dialing-in early in the morning for some of us. Can't wait to be with you again in less than a week at same time, same place. See you next week.

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.