Corrected Transcript

04-Sep-2019

Palo Alto Networks, Inc. (PANW)

Analyst Meeting - Q4 Earnings

FACTSET: callstreet
1-877-FACTSET www.callstreet.com

CORPORATE PARTICIPANTS

David Niederman
Vice President, Investor Relations, Palo Alto Networks, Inc.

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

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

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

Nir Zuk
Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Amit Singh
President, Palo Alto Networks, Inc.

OTHER PARTICIPANTS

Jonathan Ho
Analyst, William Blair & Co. LLC

Kenneth Talanian
Analyst, Evercore ISI

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Saket Kalia
Analyst, Barclays Capital, Inc.

Imtiaz Koujalgi
Analyst, Guggenheim Securities LLC

Fatima Boolani
Analyst, UBS Securities LLC

Sterling Auty
Analyst, JPMorgan Securities LLC

Matthew Hedberg
Analyst, RBC Capital Markets LLC

Philip Winslow
Analyst, Wells Fargo Securities LLC

Karl E. Keirstead
Analyst, Deutsche Bank Securities, Inc.

Pierre C. Ferragu
Global Team Head, New Street Research LLP (US)

Keith Bachman
Analyst, BMO Capital Markets (United States)

Michael Turits
Analyst, Raymond James & Associates, Inc.

Erik Suppiger
Analyst, JMP Securities LLC

Andrew James Nowinski
Analyst, Piper Jaffray & Co.

Brad Zelnick
Analyst, Credit Suisse Securities (USA) LLC

Srini Nandury
Analyst, Summit Redstone Partners LLC

MANAGEMENT DISCUSSION SECTION

Operator: Please welcome Vice President of Investor Relations, David Niederman.

David Niederman

Vice President, Investor Relations, Palo Alto Networks, Inc.

Hello. Thanks for coming. We really appreciate it. Good afternoon. I'm David Niederman, Vice President, Investor Relations at Palo Alto Networks. Thanks for joining us today to discuss our Fiscal Fourth Quarter and Full Year 2019 Results. This meeting is being broadcast live over the Web and can be accessed on our Investor Relations section of our website, investors.paloaltonetworks.com.

Earlier this afternoon, we issued a press release announcing our results for our fiscal fourth quarter and full year ended July 31, 2019. We also provided a script of certain fiscal fourth quarter and full-year 2019 financial results and operating metrics, along with applicable reconciliations as exhibits to a current report on Form 8-K filed with the SEC earlier this afternoon. Copies of these materials can also be found on the Investor section of our website.

I'd like to remind you that management will be making forward-looking statements, including statements regarding our near- and long-term financial guidance and strategy as well as modeling points for Q1 2020 and full year fiscal 2020. Please kindly take a moment to review the Safe Harbor language provided with the meeting materials. 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 provided reconciliations of these non-GAAP financial measures to GAAP financial measures in the Supplemental Financial Information that can be found at the end of the presentation and the Investors section of our website located at investors.paloaltonetworks.com.

On stage with us today will be Nikesh Arora, our Chairman and Chief Executive Officer; Kathy Bonanno, our Chief Financial Officer; Lee Klarich, our Chief Product Officer; and Nir Zuk, our Chief Technology Officer. We will have a Q&A forum at the end of the financial presentation.

And with that, I'll turn it over to Kathy.

Kathy Bonanno

Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

Hi, everyone. Thank you so much for coming today. Look, a spattering of applause, how nice. I appreciate that. Thank you. Thank you all very, very much for coming today. We appreciate your interest in Palo Alto Networks. We have a lot to cover today, and so I'm just going to get right into it.

I'm going to start by providing a quick overview of our fiscal Q4 results for the fiscal year 2019 and full year results. Nikesh will then come up and he'll walk you through our strategy and our operating framework for the next three years. And then, Lee Klarich and Nir Zuk will take you through our product strategy and I'll return to cover forward-looking guidance at the end.

So, let's turn now to fiscal fourth quarter 2019, which capped off another great year for Palo Alto Networks. In the quarter, we grew revenue 22% year-over-year to approximately $806 million. Quarterly billings crossed the $1 billion mark, a first in the company's history. And our performance in Prisma and Cortex, or as we refer to them collectively as next-gen security, was especially strong.

Our next-gen security billings were approximately $192 million in the quarter. This represents a $768 million annual run rate and accelerated our growth to approximately 180% year-over-year. For the full fiscal year, we also delivered strong top-line results, and full year free cash flow was approximately $924 million. If we adjust for the cash charges associated with our headquarters in Santa Clara and the retirement of our 2019 convertible debt, free cash flow for the year was $1.1 billion at a margin of 36.7%.

So, let's turn now to some of the product highlights for the quarter. In Q4, we completed the acquisitions of Twistlock and PureSec, and we are actively integrating them into our Prisma Cloud offering. We also released significant updates to Prisma Access, including providing over 100 network on-boarding locations around the globe and providing Clean Pipe for service providers, along with several other unique capabilities in that release. In addition, we released Traps 6.1, which included expanded support for macOS and Linux, further strengthening our endpoint and XDR offerings.

And we received FedRAMP certification for WildFire cloud, a huge milestone towards shifting government WildFire usage towards the cloud. And as you probably just saw, earlier this afternoon, we announced our intent to acquire Zingbox, an enterprise IoT security company. As Nikesh will discuss a bit later, this acquisition is yet another example of our ongoing strategy to consolidate new technologies into our next-generation firewall platform, making it easier for customers to protect their complex enterprise environment.

In addition to product releases, we had several notable wins during the quarter. We displaced Symantec and Zscaler at a Fortune 50 U.S. retailer to secure their data center and network of more than 2,000 retail outlets. We displaced Zscaler and beat Fortinet at a major European national healthcare provider in their digital transformation project. They're securing their hundreds of hospitals along with all of their patients and employees, was a great win for us in the quarter. We beat CrowdStrike and displaced Symantec with our Prisma and Cortex platforms at a global insurance company with more than 25 million policyholders. And we beat Fortinet and displaced Cisco to become the standard security platform for the government of one of the most populous regions in Asia Pacific.

In summary, there was a lot of great news in the quarter. We continue to have high win rates against our competition and add thousands of new customers every quarter. In Q4, we added nearly 3,000 new customers and are now privileged to have won nearly 65,000 customers. We're looking forward to another great year in fiscal 2020 and we'll now move on to the rest of the presentation.

Please welcome our CEO, Nikesh Arora.

Nikesh Arora

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

Good afternoon. Thank you very much for joining us. And thank you, Kathy. Normally, when I get up on stage, I usually ask the audience what can I answer so that you'll leave here happy. Now, many of you are so kind, you've written me very long notes about what you want me to tell you, which are going to make you happy. So, it's very helpful. It's like I have my marching orders. You've given me the script.

So, Keith Weiss from Morgan Stanley, yes, we will talk about product evolution M&A. Keith Bachman talks about depth and duration of depressed cash flow. Sounds very depressing, but we'll talk about that. They're not depressed. Gur, we will go down to the details of our next-generation security business and explain the financial models around here. They don't get spooked by duration issues.

And yes, Brad, no hardware company this size has made a transition like this. But hopefully, we just need to keep growing and not make the transition. You do notice that we're displacing your favorite company, Zscaler, in many situations. But I was scared, today, Brad changes the recommendation. Something is going to happen to the rest of you guys. So for now, I'm happy with Brad where he is.

So, it's been about 12-plus months I've been at Palo Alto Networks, and I know you guys have been asking for us to come about and explain how we're thinking about this company going forward. So, hopefully, in the next 75, 80 minutes, me, Nir, Lee, and many of my management colleagues will share our plan for the next three years with you in terms of where we want to take this company.

Before I go there, I thought what I would do is quickly walk you through what I've learned over the last 12 months. Now, unfortunately, there's going to be no earth-shattering secrets in what I'm going to tell you in the first section, but hopefully you'll get a sense that I've been studying this industry for a while. And the problems are obvious, right? This is $140 billion industry and we have too many vendors. I've gone to over 300 customers in the last 1 year. The winner so far is 212 cybersecurity vendors deployed in one customer. That's a lot. And what happens is when you have 212 cybersecurity vendors and cybersecurity is only 8% to 10% of your spend, it's way too many vendors for the amount of spend you do on IT compared to the rest of the vendors we have.

What that results in is people are deploying too many tools. One of these customers, not the 212 vendor customer, has nine endpoints deployed. And you don't have nine CRM systems, you don't have nine HR systems, we have nine endpoints in one financial services organization. We think that model is broken, it's wrong. It cannot be the part of securing that enterprise of the future.

If you think what we do in the industry is we give you the tools and say now, you can write policy against it, you can spin up a bunch of alerts, and we'll give you all the alerts, then you can figure out what to do with them. So, we have tremendous amounts of alerts being generated, many of our customers, and Lee and Nir will talk more about this. On average, a customer can get 175,000 alerts a week. That's a lot of alerts.

And then, you spend a lot of time and effort manually going through your issues and investigating, which can take anywhere from 4 to 57 days. So, we have an industry, where we have too many vendors, too many tools, too many alerts, and too much manual labor. We think, at the same time, while we're busy complicating the industry, our friends, the adversaries have gotten more and more sophisticated. The days of malicious software, the days of keyloggers are gone. Now, we're talking about AI-based bots, ML-based attacks, and people are really addressing an entire enterprise infrastructure trying to figure out how to get in.

So, the amount of breaches have actually gone up. Last year, was about 3,800 breaches. And most of these breaches were automated attacks. So, it's kind of an interesting situation in the industry. We have a situation where people are spending more and more money on cybersecurity and they're feeling less secure. This is the problem.

This problem needs to be fixed. So, we believe we need a new paradigm for security. And much of what we're going to talk about is what that new paradigm is going to be or needs to be. We believe we need to go towards lesser number of vendors. We believe we need to go towards more comprehensive security. We believe this has to be more of an automated industry as opposed to an industry that is full of lot of manual labor. So, a lot of what Lee and Nir are going to talk about is going to be how our products are going to enable that going forward. And we will talk specifically about some of the things we're working on, which will be unveiled over the course of next few quarters and years, and how we intend to make this happen.

At the same time, we are at an inflection point in the industry. In my [ph] travels (00:12:13) over the last 12 months and my time at Google, I haven't met a customer who's not thinking about going to the cloud. Almost every customer I've met, approximately 300 of them, is in some way, shape or form on their journey to the cloud. Some of them are evaluating the cloud. Some of them are – sort of deploy some applications in the cloud. Some of them are in a hybrid cloud environment. Some of them are going to go to multiple clouds. But there's not a customer who's not talking about the cloud.

Interestingly, we don't believe that cloud security has matured as fast as the cloud platforms have. So, the best security you can get is some cloud native security offered by an individual platform provider, but you actually don't have comprehensive cloud security that allows you to make that journey to the cloud in a more comfortable and happy fashion. So our belief is, as we see this cloud market go to potentially $1 trillion in the next five years, there is huge opportunity for cloud security to play a relevant role in allowing these customers to make that cloud journey over the next three to five years.

There's a big opportunity, and the big opportunity we have here is to make sure we don't make the same mistakes we've made in enterprise security. We need to get cloud security right. We anticipate, in cloud security, there's an opportunity for us to become a platform of choice and customers not have to deal with the problem of too many tools, too many vendors, too many alerts, and too much manual labor. And we'll talk more about that when Lee and Nir come and talk about what we've been doing in the last 12 months for cloud security.

But before I have them come up on stage and talk about the opportunity ahead of us, I want to make sure I give you a sense of what was I doing for the last 12 months. I know you guys have been all writing all these notes and trying to figure out what we've been up to as a company.

Let's take a look at where we've come from. 12 months ago, when I came to Palo Alto Networks, we had a phenomenal company, a company that had built an amazing firewall, had a great brand, tremendous amounts of trust with our customers and over 50,000 customers in the market.

There's a lag between when I click this and the slide shows up. This was Palo Alto Networks. We were primarily a firewall company. We'd made a few acquisitions and we had done a bunch of projects on the side. But despite the way we had implemented then, we had managed to get 8% of our billings from [ph] none of that (00:14:36) services, outside of our firewall business.

The worrying thing was, though, I noticed we would acquire companies and decouple them and merge them into our hardware-based business. So, that's a bad thing if you start taking software businesses and start making them work like hardware businesses. Hardware has a certain QA cycle, has a certain deployment cycle. Software has a slightly different cycle. It's very important for us to make sure we were going to get this right. So, we spent the last 12 months focusing.

Now, I may not know enough about cybersecurity, but having spent – as many of you know, I spent 10 years at Google. The one thing I did learn at Google is that, first and foremost, you have to get your product strategy right. So, poor Lee Klarich, our Head of Product; Nir, our CTO; and many of our product colleagues has spent many a night sitting with me, [ph] providing (00:15:26) and rewriting product plans, looking at competition, looking at our strategies, looking at whether we are set up to win or not, and literally re-architecting many of our products and our strategies to make sure we set ourselves up to win.

So, we spent hours there, written documents, and probably on their 15th iteration, where we went through every product category and said, why do we make this acquisition? What is the way to win in this category? How are we going to win? Do we have enough resources deployed against it? And once we get the product right, do we have the go-to-market capability to go make this happen in the market?

It wasn't simple. It wasn't easy. But some of the results are very exciting. In our firewall business, we had been selling subscriptions, four subscription against our firewalls. And we sat and talked about, why cannot the firewall become a platform? Why cannot we take what we have as a firewall and instead of having 20 different network appliances in a customer's infrastructure, why can't our firewall become the platform of the future for enterprise security?

So as Lee and Nir will talk about, we are going to go from 4 to potentially 10, maybe more subscriptions over time, because we believe once our customers trust us to be part of their enterprise infrastructure, we have the ability to go and deploy more and more capability into that infrastructure. And we will talk about our latest acquisition of Zingbox. The whole intent is to make that another subscription of firewall. We believe our customers will deploy that firewall just the way they've deployed DNS Security, which we launched a few months ago.

So on our firewall side, we've continued to build the next-generation firewall into a faster, better firewall. But really, when we went back to the drawing board, we sat back and said, Nir, if you were starting a company and building firewall today, if you wanted to, although some of you believe that firewalls are not going to be interesting, and we'll talk about why they're going to continue to be interesting. We sat down and thought how would you re-architect the firewall business and how would you build it going forward. So, what you will see as part of our Enterprise Strategy firewalls is our expectation of how this market is going to evolve and how do we need to be in the top right of that Magic Quadrant and continue to go further in that direction as opposed to not continue innovation.

Not only that, on our cloud front, we had one acquisition called Evident we'd made 12 months ago. Over the last 12 months, we've examined the cloud security space very, very carefully. We believe there needs to be a comprehensive multi-cloud, multi-technology platform available for cloud security. We have made two acquisitions in that space with Twistlock and PureSec, and we hope to be able to integrate them very swiftly, hopefully, before the end of this calendar year and be able to provide the best cloud security platform to our customers. Prisma Cloud, I'm not confusing this with VMs or any other product, has over 1,000 customers already.

We do not believe there is any cloud security company in the world today with over 1,000 customers securing the public cloud, none. And we've been able to achieve that over the last 12 months.

Not only that, we looked at our products called GPCS, which is effectively Prisma Access, which is – I shouldn't talk about competition just yet. So, it's a product with real security that helps you secure cloud native architectures, unlike some of the fakes in the market. Fake is a popular word, today's lexicon.

So, we took Prisma Access. We resourced it. We moved it to Google Cloud. We on-boarded 200-plus locations, and you saw the results. We had the biggest quarter for Prisma Access in Q4 than we ever had in the company. We have our first over $10 million deal for Prisma Access where, as we highlighted, we've displaced Zscaler. So, feel very confident in our ability to keep building Prisma Access as one of the future architecture for securing the cloud.

On securing the future, we looked hard at the SOC industry. And Lee and Nir will talk about it. We weren't comfortable with the way the industry is going. We're not comfortable where the solution needs to be that you take all your data, put it in a very large data repository, run a bunch of analytics against it and spin up more alerts. Take these alerts, give them to the SOC analyst saying, hey, you had 174,000. I've got another 100 really good alerts for you, take a look at it. That's not the right answer. We looked at the market. We acquired Demisto. Demisto has done really well for us. And we believe the future of SOCs is going to be more towards automation. And Lee and Nir will talk more about what we're able to do in that space.

We also took what was our Traps acquisition and our LightCyber and Cyvera acquisitions and looked hard at the EDR space and said, where is the endpoint industry going to evolve to? How are we going to win? We launched XDR four months ago. We've had our first full quarter of XDR. And we're delighted with the fact that 250 customers have already been acquired by the XDR team. Now, this wasn't done without our ability to run not just the product focus, but also a focus in our go-to-market capability.

Over the last 12 months, we have taken our Prisma and Cortex teams from 500 people to 1,500 people, and we did that by hiring new people and acquisitions and effectively redeploying resources from what would have been part of our core business into our new business, which is what has allowed us to accelerate our Prisma and Cortex growth rates from approximately 70-odd percent to 180%, as Kathy highlighted. And we feel very confident that that is a number or a set of numbers we can really focus on and drive further. And we'll talk more about where we expect those numbers to go over the next three years.

So what does it look like today? We've been able to grow our billings from our next-generation security service to $452 million, approximately 13% of our total billings in FY 2019. And we feel very, very confident that we have our product portfolio cleared up. And we believe we are actually in the process of delivering and deploying three different platforms in the market, one around our firewall, one around our cloud security and one around securing the future where both the firewalls and our cloud security capabilities come together in the SOC.

So, we believe our opportunity in the enterprise is to be able to simplify enterprise security, reduce the number of vendors and the reliance our customers have on vendors. And it's fascinating, as Kathy highlighted, one of our very large retail customers we acquired in Q4 has gone to a single-vendor solution, a single vendor across all forms of firewalls, firewalls in the data center, virtual firewalls against our cloud instances and Prisma Access against their network security needs.

So, we are noticing customers re-architecting the security. As they think about going to the cloud, they're rethinking do they need multiple vendors to secure them across these various form factors, across these various technologies. And many of the smarter ones, of course, I'm going to say that, are making the choice towards consolidating into a single-vendor platform.

Not only that, on the cloud front, we've had customers after we acquired Twistlock and RedLock, who were in evaluation mode, have signed multi-million-dollar, multi-year deals with us, because now they believe with Twistlock and RedLock and PureSec with Palo Alto Networks, we are going to keep building and investing in these products and continue to grow them further. And they're delighted with our vision in terms of how we plan to deliver cloud security to them.

We believe we have an opportunity to keep being ahead of the curve of cloud security. And it's funny, when we acquired RedLock, the RedLock team came to me and said, we're going to go build container security for you. I said, sounds wonderful. And I came to New York and I went to about 10 or 15 customers in the financial service and said, look, you're using our Prisma Cloud security, we're going to build you container security in nine months. They're like, we don't have time, we're going to take what's out there, the best-of-breed container security, and we're going to use it.

So, it's interesting, our customers want best-of-breed, but they don't want to wait for integrated platform to appear and be available across multiple technologies. So, we have been able to take RedLock and Twistlock and PureSec and put them together and offer best-of-breed across container, serverless and public cloud to our customers as a platform. We believe our opportunities stay ahead in that space and deliver a comprehensive multi-cloud, multi-platform, integrated security solution for our cloud. Last but not the least, in the future, we believe we have the opportunity of taking good data as opposed to all data, taking that and applying analytics to it, and being able to provide tremendous amounts of automation to allow our customers to be able to secure the future.

So, I had an option of standing up here and regaling you with my product capability and my product knowledge, but I figured one of the highlights of today could be for you guys to hear from our Founder, who's promised to give you an unfiltered version of what he thinks about the industry and how things need to go from there. And then, we'll have Lee try and moderate him to make sure he doesn't go off the rails. But before I invite them, I'm delighted to say, last night, we did an Analyst Day, we pointed you to a Palo Alto Networks TAM of about $19 billion.

We believe with all the product investment and product capability we've developed, we now have the opportunity of addressing close to $73 billion TAM in FY 2022. The magic of FY 2022 is, you will notice when I come back after Lee and Nir have talked about our product investment, I'm going to give you guidance for the next [ph] three (00:24:46) years in terms of what we expect our billings to be and what we expect our next-generation security capabilities to get to our cash flows and our operating margin. So, hold your breath – or don't hold your breath, just hang in there.

With that, let me welcome Lee and Nir up on stage.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Good afternoon.

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Good afternoon.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

I've been – [ph] We're well-behaved here (00:25:17) so far. I've been working with Nir for a very, very long time.

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Almost [ph] 15 (00:25:26) years.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

And I think this is the first time that he and I are actually sharing a stage together. So, see how it goes. No, it should be fun. So, what we like to do is share with you our product strategy and how we think about things, and we will fit that into the construct that Nikesh just walked through in terms of the three pillars, securing the enterprise, securing the cloud and securing the future.

Now, I've been in the security industry for a very long time. I've been at Palo Alto Networks for a very long time, and I can definitively say that I've never been more excited and confident in our ability to deliver these platforms in a very unique and differentiated way.

Now, to kick us off, no better person than Nir to talk about securing the enterprise. Nir?

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Thank you, Lee. So, let's talk a little bit about securing the enterprise and specifically about network security. I know that some of you would like to believe that the firewall is going away and there is no role for network security in the future. In reality, there are things that have to be done through the network, through network security, and there's just no other place to do them. And so, things like looking for command-and-control connections, things like combining access control, user identity and authorization systems. And most importantly, more than half of the devices that enterprises use today cannot be protected by running something on a device itself, have to be protected from the network.

Mobile phones with lock-down operating systems or limited battery life. Router, switches, printers, network-attached scanners, and all other kind of IoTs, like IP phones and things like that, the only way to protect them is through the network because you can't run anything on it. So, network security is here to stay. It's always been the core of cybersecurity and will continue to be the core of cybersecurity, but changes have to be made. Because over time, applications have been moving from the corporate data center into the cloud, whether SaaS or public cloud.

And users have been moving from corporate networks into smaller offices, branch offices. They've been moving off the network completely in the form of being mobile users. And network security has to follow them, and network security has to follow them wherever they go because, again, there are things that network security is the only thing – or there are things that network security has to do, like some cybersecurity functionality, like access control, and supporting, again, devices that can only be done from the network.

The challenge is how you do that. How do you follow the user when they're off the network? How do you follow the application when it's running in the public cloud? And more importantly, like Nikesh said, customers are asking us to consolidate more and more functionality that today they deploy in the network separately from the firewall into the single next-generation based platform that we have created. And to talk about that and the innovation around it, we'll go back to Lee.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

So, there's lots of innovation that's going on in next-gen firewall. There's two areas in particular that I want to talk through with all of you today that are of particular importance. The first is sort of piggybacking off what Nir was talking about, the importance of form factors. Okay? How do we take all the same capabilities and make sure that they can be deployed everywhere the in-line security is needed. And this is something we started driving several years ago when we expanded from hardware appliance form factors to software form factors with the VM-Series. Since that time, VM-Series has turned into the leading virtual next-gen firewall in the market. And then, from there, and more recently, we expanded into delivering these capabilities as a service with Prisma Access, which allows us to extend security out to mobile users, branch offices, retail environments, et cetera.

Now, what's particularly powerful about this in addition to being able to provide consistent security everywhere is the ability to have a single control plane to be able to manage this consistently as well. As Nikesh mentioned earlier, one of our very large customer acquisitions in the previous quarter was a customer who had been with us for a while with hardware in the data center. And in the quarter, they extended that using VM-Series and Prisma Access into a complete solution. And what was particularly exciting and relevant to them was the ability to get that consistent security, consistent control plane they can't get anywhere else.

Now, going hand in hand with this is the ability to use the firewall as a platform for delivering more and more capabilities. If you think about the enterprise security market, it is actually insane. The number of different security vendors that customers have to deal with is crazy. We have a running tally of the most number of security vendors that customers deal with when they come to our – [ph] or you continue to (00:30:35) hear about what we can do for them. I think the latest record is now up well above 200 different security vendors for a single customer they have to deal with and manage.

Now, we have been, from the very beginning, starting consolidate these through integrating best-in-class capabilities into our next-gen firewall. We did this with IPS. We did this with URL filtering. And we really substantially changed those markets. We took a bit of a hiatus, but we're back, with DNS Security launched earlier this year, our fifth subscription for the next-gen firewall. And we intend to extend this more rapidly going forward to be able to integrate what would otherwise be stand-alone capabilities and to be able to consolidate those into our firewall as a platform, importantly, to do that across all form factors as well.

Now, you saw the announcement earlier today, Zingbox for IoT security. I'll talk about that a little bit more detail in a second. But just to give you some flavor for the security services we're looking at, we're also actively working on and building SD-WAN as an example that we will be able to integrate across the different form factors in order to be able to, again, both simplify as well as provide better capabilities to our customers across their network environments.

Now, to talk about IoT, this is becoming very much a growing issue within the enterprise. As you can see from some of the things here. Even fish tanks can be used to break into enterprises and move laterally. Hackers are using IoT devices as both initial insertion points as well as the ability to move laterally across networks. Now, why is this? IoT devices have become very ubiquitous across the enterprise. By our estimation, what we've observed in both our own environment as well as others, for every employee, there is about three different IoT devices in the typical enterprise.

In many cases, IoT devices, they're unpatched. They're unmanaged. They're connected by definition. That's a security risk. I believe that every single 1 of our 65,000 customers [ph] hasn't (00:32:58) a growing IoT security need. And we will be unique in being able to deliver that as an integrated service to our next-gen firewall, obviating the need to deploy yet more hardware in order to get a very relevant and important new security service.

Without us, the options are looking at a handful of small vendors and trying to figure out which one to invest in and which one you're going to take the operational burden of trying to deploy it throughout your network. That is a very powerful approach that we are able to take by delivering this as a integrated service.

And so, with that combination of the evolving and expanding form factors, the ability to then deploy multiple and additional security services to those form factors, we see a great opportunity to address the network security TAM as well as an opportunity to replace what today is often outsourced manual labor with product in automation. You'll see that theme as we talk about the different areas, this ability to leverage automation to replace outsourced manual labor is one of the large opportunities we have in consolidating the products around us.

So, switching gears from enterprise to the cloud, okay? Now when we talk about cloud, we're going to talk about two distinct aspects of the cloud. The first, just about every enterprise is on some journey of moving some of their applications to the cloud, okay? Typically, as multi-cloud, they're often still keeping the data – part of the data center for some of the applications, so it's hybrid. That is one opportunity, very significant opportunity as you saw before. The second is to leverage the cloud to deliver security to the end users, whether they're mobile, branch office, et cetera.

So, let's start with securing the cloud. Now, a concept that all of you have seen probably a million times, but just an important concept is a shared responsibility model. Customers are responsible for the security of everything they deploy in the cloud. And as we've seen, many of these applications that they deploy are mission-critical, have incredibly sensitive data and they need the best security solution across multi-cloud and hybrid cloud.

Now, to put this in context, the world has moved beyond lift and shift to a large extent and will continue to move toward more cloud-native application architectures, which will require a cloud-first approach to security. You cannot simply take on-prem data center capabilities and simply move them. You have to take a new approach. What you're seeing here is a typical application that has multiple different components, which is very standard. Each of those components are often running in a different technology stack.

So, how do you secure an application like that, right? So, it requires a lot of the same security functions wherever the application is, but those security functions have to then be applied across all the different technology stacks. So, for example, you need to do vulnerability management, of course, and you need to apply that to VMs. The typical industry answer to this will be to say that's a product. The problem is you're going to get to that, every line representing a different product. Now, if you're an enterprise looking at that, that's a lot. We are at risk of repeating the sins of the past if we let that happen.

I firmly believe the Palo Alto Networks is the only company in a position and with a focus of preventing that from happening. With Prisma Cloud, our intention and what we are delivering to our customers is the most comprehensive cloud security platform that they can get. Taking these different capabilities, applying them across the different technology stacks, multi-cloud and even hybrid cloud, to help secure our customers' journey to the cloud.

And to be clear, there is a lot that is yet to be done. I anticipate that there are a number of cloud security technologies that haven't been invented yet that we will have to be thinking about. And we will continue to be very decisive and purposeful about building out this platform and continue to maintain its position as the most comprehensive solution.

Now, we talk about the other kind of cloud. And for that, Nir?

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Thank you, Lee. Maybe before that, I'm very excited about Prisma Cloud. When we started the company – and Lee has been with me since the beginning. When we started the company, we were going to build the next-generation firewall and we had a bunch of very large vendors that we had to go and displace, which we've done, right? We're today by far the largest network security vendor out there. It was a lot of work displacing them.

I think that with cloud, with public cloud security and with – generally, with cloud security, the market is open. There is the need. I don't see any other vendor in a position to do this. And I think that the numbers that you've seen and the numbers that you will see speak for themselves. Because to do this, you have to first have a firewall, because there is no way to secure the cloud without a firewall. You have to look at the things that only the firewall can look, and there are things that's running in the cloud that you need a firewall because you can't run endpoint security on them.

And then on top of that, you need all the different technologies that we've been building and acquiring and integrating over the last few years that I just don't see anyone out there that's even thinking about it, nevertheless, someone that has the different components that are required in order to go after the cloud security market. So, very excited about that, [ph] as pleased (00:39:03) as much as I was excited when we started Palo Alto Networks and went after the enterprise security market.

Now, once applications start moving to the cloud, which they are, enterprise network architectures and access architectures are changing. And the reason for that – oops, we're missing a slide here. Sorry. Okay. Yeah. So, the reason for that is that, traditionally, the way users have been accessing enterprise applications, which were running in enterprise data centers, was through remote access solutions like GlobalProtect, for example, and through MPLS – IP VPN, MPLS links. And those links were offering guaranteed bandwidth and guaranteed performance so they were great way to access enterprise applications.

Once applications start moving to the cloud, whether it's SaaS or public cloud, and once users are moving into smaller offices, into branch offices and, of course, become mobile, it doesn't make sense anymore to run all the traffic through the data center and then go out to the Internet. You want to have direct Internet access from wherever the user is, whether it's in a branch office or whether the user is mobile.

Of course, with the tradition of the cybersecurity industry, the way we're doing it or the way the industry is doing it is by offering more and more and more solution to try to do that, right? So, you have MPLS, and then you do site-to-site VPNs. And then, some traffic goes – SaaS traffic has to go to a CASB proxy, then we have a bunch of CASB companies. And of course, a favorite topic, the cloud-delivered security [ph] VI (00:40:43) proxy.

And maybe a side note here, and if I seem a little bit angry, then maybe because it is I am, because I feel like I'm playing a whack-a-mole game, because about 24 years ago, I had to kill the first generation of proxies with stateful inspection. If you remember, companies like Secure Computing, anyone here cover them? You're probably responsible for them having a higher market cap than Check Point at the time. Not sure where they are today, and companies like Raptor and others. And of course, proxies, always have the issues with proxies. They're slow. They break applications. They break networking. They break network optimization, network routing and so on. So, had to kill them the first time.

And then, 12 years ago in 2007, when we started selling our products here, we had to kill the next generation of proxies, the Blue Coats and the Websenses of the world, which again didn't make any sense. Proxies have never made sense. They're slow, high latency. They break applications. You can't run everything through them. They break networking and so on, which we have. We all know where Blue Coat is today, right, part of Broadcom, and I'm not sure where Websense is.

And now, it's déjà vu, right? Third time. Another mole is popping. We have to deliver security from the cloud. How we're going to do it? Guess what? We're going to do it with a proxy. Now, why would we do it with a proxy and not with network security? Because it's easy.

It's very difficult to become a network security company. It's very difficult to build something that can go into the infrastructure, whether it's physical or virtual, and provide the networking and the security, the [ph] packet (00:42:16) based security at the application level. So, vendors are taking the easy way out, right? Let's put a proxy, so we break application, so we break the network, who cares? Customers are going to pay for it anyways. And they're trying to use proxies to solve the issue.

So first, I think proxy is the wrong way to – and I don't think, I'm sure proxies are the wrong way. If I were here six months ago, I would say we're going to kill the proxy. After what you've seen and what I've seen the last two quarters, we have killed the proxy. But again – but I really think that it's not just the proxy. It's this mess that the industry is suggesting in order to fix the access challenges that are associated with the move to the cloud. And of course, there is a much better solution and that, by better solution, is what Prisma Access is about.

So, Prisma Access takes mobile users and it takes branch offices in a single cloud-delivered firewall, [ph] true (00:43:13) firewall-based – our firewall-based solution. It provides access to SaaS applications, with our CASB to public cloud applications to on-premise applications. And whatever comes next, this platform is going to do. And the reason this platform has been so successful in the last couple of quarters and is going to continue to be so successful is because when customers see this versus the mess that today is called access, again a mess driven by the cloud, the choice is very, very clear. This is the way to do it.

And if I look at our position in the market, there are not many firewall vendors out there. There are probably four firewall vendors that sell today. The other three vendors are busy trying to figure out why they can't sell hardware against our hardware. I just don't see anyone else today in a position to go and capture this huge access to the cloud market. I really like our position. I really like where we are today, and I certainly like where we're taking it in the future.

Sorry, I'll continue.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Video.

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

So now that we've covered...

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

Video. Did I cut you off?

[Video Presentation] (00:44:26-00:45:21)

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Can you imagine trying to access X-ray data through a proxy? They tried and they had to throw out a huge deployment of the proxy. So, going back to TAM, we think that cloud security in 2020 represents a very large

TAM, a very large opportunity. And like I said, I personally just don't see much competition over there and anyone that has the components to compete against us in cloud security. And then if you look at the automation that's needed in order to drive that security, automation that today is done by people, and we do that with software and analytics, the opportunity becomes even larger. Okay?

So now that we covered the first two pillars, let's move to secure the future. So, like Nikesh said, both enterprise security and cloud security are here to stay with us for a long time. And we have to do both and we have to be good at both, and we are going to be continuing doing both and be the market leaders in both.

At some point, these two converge into security operation system, because the security operation system needs to run both enterprise security and cloud security, and it all comes to one place. And there are big issues in the security operations today that just aren't – that basically make the security operations center not prepared for the future. And we've decided couple of years ago to go and fix that, to prepare the security operations center for the future.

So, let's first talk about what's not working in the security operations center. Most security operations centers are based around the technology called SIEM, S-I-E-M, security incident and event management. By the way, it has nothing to do with incident and event management, but whatever, we'll call them that. That basically collect as much log as they can from network devices and endpoints and applications and servers and wherever they can get logs from. And then, they have a bunch of static rules and/or manual labor looking at this data. And guess what they do? They generate alerts based on the data.

Now, of course, the data that's coming in already includes alerts, because if the firewall or the IPS or whatever found something bad or something bad was found in the public cloud and so on, on top of the alerts that the SIEM collects and displays to the user, the SIEM has rules, we call them correlation rules, that generate even more alerts. Some SIEM have some filtering mechanism to filter out alerts. Usually, they filter out alerts that's needed. Go and ask [ph] Target (00:47:48) why they had an alert that told them about the breach and only looked at it nine months later.

And then, all of that leads to reactive investigation. And what the industry is trying to do to fix that, because ask any customer, they'll tell you that the SIEM is broken. Right now, the solution to the SIEM is broken is we're going to switch to another broken SIEM with the hope that that other broken SIEM is going to be better, and it's not. And the more advanced companies in the industry have figured out that something has to be done. And what has to be done is you have to collect much more meaningful data from the network or from endpoints and so on, and provide much more meaningful processing using machines of that data, right?

So, the SIEM doesn't work. So, why don't we create a new industry called EDR? We're going to ask customers to put yet another agent on the endpoint. We're going to collect a lot of data from the endpoint. We're going to process the data with, whatever, machine learning, static rules. Maybe we'll put some people on it. We're going to find bad things, generate even more alerts because there aren't enough alerts already. And maybe sometimes, we're going to respond back to the endpoint.

Now, that's not enough. We have to do the same thing with the networks, so there's a whole industry called NTA, network traffic analysis, that's doing that on the network. Same thing, they collect deep data from the network using separate sensors into another data lake, process that with rules and whatever and machine learning and then maybe respond back. Usually, they generate just more alerts.

And the same thing happens for IoT, and the same thing happens for public cloud, and the same thing happens for SaaS. And I'm sure that with every new challenge, the industry is going to generate yet another vertical that's going to collect yet another separate set of data, and all of that because the SIEM doesn't do anything, okay?

We think that this doesn't make sense. Like specifically, EDR doesn't make sense. Like, why would you limit yourself to collecting data only from the endpoint, process data just from the endpoint and respond back, back to the endpoint? We think there has to be something much better than that, and that's what Cortex is about. Okay?

Now, maybe before that, this is a survey that Demisto, a company we acquired, did late last year before we acquired them. You heard it before. An average enterprise has to deal with 174,000 alerts per weeks. Usually, they have the capacity to handle maybe 12,000 and even that gives them a few seconds for each alert. It doesn't make sense. That leads to at least four days of investigating the alerts, so they figure out that they need to investigate, and some alerts, they just don't touch, are the real alerts that they need to handle. And we have to fix that, and that's what Cortex XDR is about.

And to do that, I'm going to have my products guy tell you how we're going to do that.

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

So when we think about securing the future, we're really talking about collecting good data, applying analytics against it, leveraging as much automation as we can because manual work can be error prone and obviously takes too much time, et cetera. But ultimately we're trying to get to a proactive outcome, trying to get away from the reactive, something bad has happened, let me figure out how bad it was and when it happened and things like; to proactive, how do we actually prevent the bad things from happening.

So, using that as a framework, it all starts with good data. There's a massive amount of money that is being spent on collecting logs and alerts, but not on collecting good data. You have to collect good data in order to drive good analytics, AI, machine learning, and things like that.

Now, to get the good data, we of course started with the best sources we know, our next-gen firewalls, Traps on the endpoint, started cloud services. We know because we can control those sources the kind of data, the rich, deep data that we can get in order to drive analytics. So, that is where we started. But now we are starting to extend that out to third-party sources as well.

The starting point for that will be other network security devices. We're going to start with Check Point and probably move on to Cisco and other things like that, because again, in the enterprise, there's still a bit of a mess of lots of different things. And so, while we try to move everyone to a better state, we can help by at least taking in that data, correlating, et cetera.

So, we are starting to now pull in third-party data to augment our data sources to be able to drive good analytics. So, what does good analytics look like? Well, good analytics, first and foremost, should be capable of detecting attacks that otherwise can't be detected. Cortex XDR does that for sure. In addition to that though, analytics is very powerful in being able to reduce the amount of noise and alerts that enterprises have to deal with. We have seen in certain environments up to 50x reduction of alerts by being able to just simply group them into incidents to be able to then investigate incidents as opposed to lots of alerts.

We've also then seen the ability to reduce the amount of time significantly in how long it takes to investigate an incident. By pre-stitching data together and showing the full view to the analysts, it is much, much more powerful and easy for them to go through the investigation, get to conclusion and ultimately provide automation.

Our aspiration here is to get orders of magnitude improvement even from this, which by the way to the SOC this is a massive improvement for they otherwise are. And we're going to keep focusing on driving these better outcomes.

Now, good data to good analytics, ultimately, to really good automation. Automation is where we can take a lot of the noise out of the system and really leave the SOC analysts with just what they need to be able to, to have to focus on. And again, you can see the level of alert reduction by simply automating the investigation response that humans don't have to do the work. Improving the meantime to respond; in some environments, well north of 90% improvement in how long it takes to respond to incidents. That is massive benefit to an enterprise, to the SOC.

And going forward, we have a view that we can even make this automation predictive in nature. But based on everything that we see across this growing ecosystem, we can build a network effect, as we have done in many other areas, so that we actually will be able to tell customers this is what you should do in order to achieve these outcomes. The cyber security industry needs to get more opinionated about how to achieve the right outcomes, as opposed to simply providing tools and their customers kind of do what they want with them. Automation is a key area for this.

Lastly, to bring this together, we are ultimately trying to get to a proactive response footprint where, again, instead of reactive, we're proactive. This is why Traps on the endpoint is so important to have Cortex functions. Not only does it provide really rich, deep data in order to drive analytics and other things like that, but it can actually prevent attacks from happening in the first place.

Every attack that is prevented upfront means fewer and fewer alerts that even have to be analyzed on the back-end. Additionally, this is the footprint that allows us to when we do finish – when the customer does finish the investigation, we can actually then automate the response back to an enforcement point to take action. So we prevent on the front-end, provide rich data, and then ultimately prevent on the back-end as well. And we can automate that entire sequence.

So, we bring this together, each one of these components is in itself best-in-class, but importantly, integrated together to form the foundation of a platform that can solve a lot of the challenges that Nir talked about that the SOC currently deals with and are growing. So, let's hear from one of our customers as they talk about their adoption of Cortex and what it meant to them.

[Video Presentation] (55:56-57:13)

Always cool when you can secure a state. And, of course, all this adds up to a large and growing TAM. The combination of endpoint protection, analytics, automation, and maybe most obvious in this case the ability to then reduce the manual outsourcing and pull that into product automation and analytics as well is a substantial opportunity we see as well.

And with that, I'd like to invite Nikesh back up and talk about execution. Nikesh?

Nikesh Arora

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

Well, thank you, Lee and Nir. So, as I mentioned, we spend a lot of time making sure we get our product strategy right, and Lee and Nir have highlighted where we plan to go. I hope you didn't miss the fact that Lee has committed publicly to deploying a lot of subscriptions in our firewalls and potentially deploying SD-WAN across every form factor. I'm just trying to make sure he hears me, safe to use, so that I can make sure I can hold him to it.

And we also talked about ingesting third-party data into Cortex, which is an extension of our version of our Application Framework from the past. But product is just part of our solution. Once you get product right, you've got to make sure you have the execution capability to put the product out in the market. And as I've analyzed enterprise companies, it's very interesting, there is very few, very large enterprise companies and many small enterprise companies. And it's interesting if you look at them, there is a distribution engine that needs to be created just commensurate with your core product capacity.

Companies get started. They get into a very good state with one set of products. And then either you have to keep innovating and adding more product to the portfolio of the salespeople, or you have to acquire product and be able to ingest it in a way that your salespeople are able to sell it. There's only one way to double revenue, either double the number of salespeople and make sure there's enough capacity in the market, or make sure you double the amount of product that a salesperson can sell and is able to sell to be able to do that.

Our intent is to do a little bit of both. And what I wanted to highlight is, in addition to product capability, we will also be working in our execution capability and making sure we have the go-to market. As Lee and Nir just highlighted, and I ended my last session with saying, we can address the $73 billion market. This is how that market breaks out. We think there's a $27 billion opportunity in network, approximately $8 billion in cloud, 13-odd billion dollars in SOC and endpoint protection, and about $25 billion in the automation, which needs to be deployed across all of those categories.

It's a slightly different view than you will see in the industry. Industry still believes there's going to be very large services market. We, on the contrary, believe that the services market is important for the architectural pieces to get cybersecurity right. But if you need a lot of people, to be able to manage security for large enterprises in the long-term, that is not going to give you the automation and the right outcomes, and it's going require way too much time while the adversaries are working on automating their ability to attack you and get to your precious data.

So, as you see, we have 65,000 customers and we have an amazing brand which people trust. Just to highlight, one of the first subscriptions we launched early this year, we've been able to deploy it to over 500 customers in a very short period of time. So, our sales teams know how the moment when you deploy a subscription they're able to add it to our firewall capability and get deployed in the market. Lee talked about our IoT capability. We want to make that available to every one of our enterprise firewall customers.

And one of you asked me, why wouldn't you go acquire a more complex IoT company, there are some larger companies in the IoT space that solve complex use cases. I understand why as a start-up you would go after a complex use case because that's probably where the large deals are. But the enterprise IoT is a need for every customer. Our sales people know how to sell it. We know how to attach this to our firewall. And our aspiration is that, for every subscription that we deploy, we should be able to get to thousands of customers, if not tens of thousands of customers, in a two- to three-year timeframe, which allows us to keep expanding both the TAM and our revenue in a leverageable way with our customer base.

And if you look at our current capabilities, we have 4,000 partners, we operate across 150 countries and we have over 3,000 people out in the field, which makes us the largest pure-play cybersecurity sales team out in the field. We want to turn that into a large distribution capability. We also believe that we have built the best execution team in cybersecurity. I know many of you wrote in your notes about the management turnover at Palo Alto Networks.

Palo Alto Networks have built a phenomenal company, which is firewall-centric and we have done some stuff in the cloud and some stuff in the SOC. It's very important as we go through this transition of building a multi-product, multi-platform cybersecurity business, that our management team represents our capabilities which are required to be able to sell multiple platforms in the market. And what we have done over time is we've made sure that we're managing the transition and upgrading our skill set for our team to make sure that we can actually go sell cloud, we can go sell automation, we can go sell AI, ML, we can go sell firewall.

I joined Google when there were 450 people in Google Europe. We took that team from 450 people to 5,000, and we quintupled revenue in five years when I was there. I left Google. Google is now on its fourth generation of management today and they far surpassed the quintupling of revenue from the early days. There were 100,000 employees.

So, as we go through evolution, you have to make sure you bring your management team [ph] to unlock them (1:02:53). And we're very comfortable that the transitions we're doing on the management front are a continuation of our desire to build the best execution. Rest assured, most of this management turnover you're seeing, they're all managed transitions, they're all towards the purpose of building this multi-capability cybersecurity sales team.

And you can see that we did our first $1 billion billings quarter in Q4 while we were going through these transitions, which tells you that it'd be a very strong field sales force, and they're all on board with our desire and ambition to build the best cybersecurity player in the world. The lag which Nir was experiencing. There we go.

In the last year, we've hired over 2,000 cybersecurity professionals. We have expanded our hiring [ph] remit (1:03:40). We now hire from 19 cloud and next-generation companies as opposed to purely enterprise hardware businesses, which had been a lot of our core sales team in the past. And we've built technology which allows us to cross-train our teams in cloud and in automation techniques. This allowed us to train 3,000 people in a week to be able to sell cloud.

Why this is interesting is – this is an important slide. This is what we anticipate in terms of how we are going to take this and build this into the larger enterprise security business. The way we do it is we ingest or innovate and build technology. We put them in speedboats. We have a speedboat for cloud. We have a speed for automation. We also start training our core sales team out of the field. And this gives you a sense of what proportion of our field sales force is able to sell our various products. So we've taken Prisma Access and 60% of our sales teams out in the field is now able to sell Prisma Access. This gives us huge amplification and leverage.

Prisma Cloud is closing in on 30%, 35% of our sales force. And by the end of the year, we will have integrated Twistlock and PureSec, allowing it to be part of the Prisma Cloud platform, which we will integrate seamlessly both from a contractual and from a usage perspective. So, every Prisma Cloud customer will auto-magically have container and serverless capability, and we believe that leverage is going to allow us to address 40% of our customer base.

Our plan is to get our speedboat teams to be able to sell to 90% of our entire – through 90% of our core sales force to our entire customer base, allowing us to leverage and the distribution we need to become the biggest player both in cloud as well as automation and SOC. No other player in our space has over 3,000 people in the field out there selling.

Not just that, we want to make sure we do this while we continue to delight our customers. So we have been able to maintain the leadership position and customer happiness and customer success out of the market. Not only that, we are not going to rest on our laurels. We have just announced to our field team, we're introducing an industry-first security incident assurance service, whereby if any of our customers unfortunately is in a breach situation or any customer in the industry, we're going to be there available until their breach is resolved, irrespective of what proportion of their products are Palo Alto products. So we continue to want to be at the forefront of customer success and customer happiness in our ability to execute.

So with that, I now – yes, there's been other conversation about the channel. I think there was one meeting we had with a channel advisory board, which I think every analyst has a feedback on. [indiscernible] (1:06:20) said that we've been tweaking our channel model just causing consternation. And this is just to give you comfort that 99% of our business still comes from the channel. And as you can see, in Q3 and Q4, because we revamped our channel programs to create more capability training and incentive for our channel, the channel-sourced business that we're doing has never been greater than we've had in the last two quarters at Palo Alto Network.

So, any noise around the fact that channel and us are not together in this journey to building the best cybersecurity business is just noise. We believe the true signal is shown in the results. They're actually allowing us to amplify our capability and they're really excited about our newer acquisitions and the direction that we're taking with the various platforms.

Okay. All right. This is our foreplay. Sorry, it's taken us so long to get here. But until we give you context, it's very hard for us to take you to what you're here for. So, with that, as you know, we've had a long history of success. We have increased market share in network security despite popular belief that we're not going to be able to grow our security business at twice the rate of industry.

The team and I spent a lot of time over the last three or four months looking at, do we need to go through a financial model transition at Palo Alto Networks. And I've read many of your notes about the two Ds, depression of cash flows, duration, what is Palo Alto going to do vis-à-vis ARR versus the term license, the perpetual license.

We tested the market. We talked to many of our customers. We talked to many of the companies going through a transition. And we're not going through any major financial transition, just FYI. Our customers like the way we sell our products to them. Our sales people understand how to sell products to themselves. We are going to be selling firewalls the way we've been selling them so far. We are not going to go to any term license model. We're going to stick with the perpetual license model. And some of our software form factors which sell and replace firewalls are going to be sold like firewalls are sold.

So, based on all of the analysis, whilst we will be building a huge capability to sell our next-generation security, we feel very comfortable that we will be able to maintain the 20% billings growth rate over the next three years as well as the 20% revenue growth rate over the next three years. I've had the privilege over the last three weeks of looking at every one of your models. I've read almost every one of your notes. And I can safely say that this 20% guidance is above the average of most of the models out there on the Street both on revenue and billings. But we stand behind the commitment and we believe we can grow our billings and revenue at roughly 20% growth rate going forward.

An important part I'd like to highlight, one of the shifts we're seeing, which I'm sure you guys pay attention to product revenues, as we call them, we are seeing a shift where we're replacing our competitors' firewall boxes with software form factors of Prisma Access. So, what we've done is we've taken our VMs, our Prisma Access sales, and our firewall sales and said, what would it look like if we considered them all as an upfront sale and how would our billings look like in the firewall category. So this is a combination of VMs, Prisma Access, and firewall.

We feel very comfortable that we will be able to grow the firewall as a category billings by 23% over the next three years, which we believe is still 2.5 times industry growth rate vis-à-vis how firewalls are sold and we think of our product. I will sure point you out to the fact that because we anticipate a large proportion of future firewall sales to be in the software form factor, there will be a revenue recognition mix shift which will come through, but we still believe the category will grow at 23% over the next three years.

Talking about the partnership, really excited about. We're really excited about our Next-Generation Security billings. We were able to achieve $452 million in billings in Prisma and Cortex in what we call Next-Generation Security. We're guiding to $800 million to $810 million of billings for FY 2020. And we believe we will get to $1.75 billion by FY 2022, resulting in revenue of approximately over $1 billion for Next-Generation Security revenue by FY 2022.

[ph] Just apart (1:11:00), it takes some spending to drive that fast revenue growth. So, FY 2019, we've been able to manage the acceleration of our Prisma and Cortex revenues by being able to reallocate from our core business. We believe that we need to invest between $100 million and $125 million next year to keep driving that revenue growth at the pace we are committing to. But we believe thereafter we will be able to keep getting operating margin leverage by 150 basis points in 2021 and 2022. And we believe the long-term operating margin for our business should be 25%.

I know you've been discussing cash flow a lot about us. We feel comfortable, despite these investments, despite the shift towards more services like software-based services and Prisma Access and VMs, as well as Cortex. We believe we will safely be able to generate $4 billion of free cash flow over the next three years, guiding to a long-term free cash flow margin of 30%.

So, before I talk about how we think about this, I thought it'd be important also to tell you how we intend to use the cash. What we've done on M&A, as you've seen, there was a fear when I came 12 months ago that this guy comes from Google is going to spend a lot of money and buy a lot of big stuff. Let me highlight the key tenets of my M&A philosophy.

First and foremost, I prefer avoiding overlapping products. Overlapping products are dangerous. We have products in most categories. I'm not interested in buying another endpoint company. I'm not interested in buying another firewall company because that requires to maintain two code bases, two sets of customers, and is no leverage for me. It's much more interesting for us to create innovation in the category and displace those competitors as opposed to acquire them and just create scale. We believe we have scale in most of our categories. Hence, we don't need to acquire customers in overlapping product category.

We prefer targeting blue oceans. We like areas where there's not enough people. We like areas where we can ingest technology and deploy it through our large distribution base, as opposed to go and participate in red oceans where there's a lot of blood and not enough profitability.

We seek technologies that will integrate across our platforms. If you look, we acquired RedLock. We're merging RedLock and Twistlock into a common platform. We acquired PureSec, which is serverless, which will be integrated as well. We're acquiring IoT, which will be integrated into our firewall capabilities. We acquired Demisto which is being integrated into Cortex.

So, we prefer acquiring technologies we believe fill an important gap and also provide leverage to our go-to-market engine, because if you acquire disparate products, then you have to go train your sales forces on different go-to-market capabilities and different USPs for our customers.

We prefer acquiring product excellence versus revenue. Because I have to pay a large multiple for revenue, I'd rather not. I'd rather acquire somebody who's built a great product and who has good early customers, exhibiting product market fit, every one of our companies that we've acquired, and I will talk about this slide in a second. And last but not the least, we focus on large TAMs. We're not interested in small TAMs unless they can be subscriptions, which can be added to our firewalls which allows us to consolidate the enterprise network.

So, with that strategy in mind, our approach in the first nine months, we force our teams to write integrated product plans. In fact, Zingbox and us have already started talking about what the product integration could look like, because our first and foremost intent is to make sure that integration is done ASAP. We see as soon as we acquire these good technology best-of-breed companies, we're able to improve their business plan by approximately 40%, which is what we've been able to do with Demisto, PureSec, Twistlock, RedLock and many of our acquisitions.

And we let their teams run their plays in the market, with go-to market support from our speedboats. Within months 9 and 24, we start introducing them through our speedboats to our core business, allowing us to get more leverage and more scale across the acquisitions. Then we target doubling their plans. Because of that, past 24 months, they become multiple accretive to us as a business. That's an M&A philosophy. That should give you a good sense of how we intend to use some of that cash flow. And as we and Nir have talked about, we are going to constantly make build versus buy decisions, so we can deliver best-of-breed to our customers. And if we believe that we're not going to get there fast enough, we'll make acquisitions, but the acquisition will be guided by the philosophy I just laid out in terms of smart product teams.

And what is delightful is, Nir and I was just sitting early and trying to count, of all the acquisitions, we have over 12 founders working in our company and our product organization from 12 months ago, and they're all committed to be here over the next two to three years as part of Palo Alto Networks. We make that a conditional acquisition, so they're supposed to stay there and we actually let them run their products. Because we believe the fact that they'll be able to go out against all odds, and build a great product, and build a great business. It is incumbent and imperative that we let them run that product for us at Palo Alto Networks, and we create the right circumstances, the right capabilities, for them to make that happen.

So, that's our plan in M&A. So I thought what I would do is, I would do what you guys would do, and see how do we compare against the industry. We believe we are already the largest cybersecurity company and we're growing faster than anybody else in our space. But this is only half interesting. I find this even more interesting. If you take Prisma and Cortex, which is our Next-Generation Security business, in the last 12 months, we grew our billings by 89%.

In the next 12 months, we're forecasting a 78% growth, which we believe makes us the largest next-generation security company compared to all the people out there who enjoy robust valuations and I will use the word robust. If you look at our forecast for FY 2022, we believe we'll be almost twice as big as any next-generation security company in our Prisma and Cortex category, whilst we're able to maintain our firewall business, generating huge amounts of cash flow.

So I like to call this the ServiceNow slide. I also reviewed many Analyst Day presentations and ServiceNow was kind enough to build the slide. And I understand this is where analysts geek out where this is something called the rule of 40%. You had your free cash flow margins and revenue growth and for some interesting reason over 40% is good and below 40% is bad.

Another problem is ServiceNow left us out of the slide. That's probably we're not – we're the old fuddy-duddy firewall company, we're not the next-generation security company. But we decided to make our own version of the slide, so at least we feel happy when we look at this. And we're delighted to see that we ranked second from the left based on our last 12-month performance. And we hope to stay far above that median of 38% over the next three years.

So, with that, this is what we expect from our company in FY 2022, we expect a 20% CAGR for total billings and total revenue over the next three years. We expect to get to $6 billion in total billings and $5 billion in total revenue by FY 2022. We expect that $1.75 billion of that total billings will come from our next-generation security services and approximately $1 billion of that will be revenue in FY 2022. We expect to get back to our current operating margins by FY 2022, the long-term target of 25%. And we expect to generate $4 billion of free cash flow by FY 2022. So, from here, a simple matter of execution.

With that, let me call my friend Kathy who can give you more specific guidance for FY 2020 and Q1.

Kathy Bonanno

Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

Okay. Thank you, Nikesh. All right. So, that's a lot. Talked a lot about fiscal 2022 and about what we see in the coming years. Let me just put a finer point on what we expect for fiscal 2020. So, am I moving these slides or somebody else? Okay.

Since it's a lot of data and information on the screen and these slides will be made available to you, I'm going to focus primarily on talking about the year-over-year growth rates. We will make these slides available to you following the call.

So, for fiscal Q1 FY 2020, we expect billings growth to be between 15% to 17% year-over-year. We expect revenue growth of 16% to 17% year-over-year. We expect non-GAAP EPS to be in the range of $1.02 to $1.04, which incorporates net expenses related to acquisitions, including the Zingbox proposed acquisition which we've just announced.

For the full year fiscal 2020, we expect billings to increase between 17% to 19% year-over-year and we expect revenue growth to be in the range of 19% to 20% year-over-year. As Nikesh mentioned, next-gen security billings growth is expected to be in the range of 77% to 79% year-over-year. We expect fiscal 2020 non-GAAP to be in the range of $5 to $5.10, which also includes net expenses related to our recent acquisitions. And finally, turning to free cash flow, we expect adjusted free cash flow margin of approximately 30% for fiscal 2020.

In this slide presentation, you'll also find some additional modeling points related to CapEx, estimates, share counts, tax rate, the impact of M&A on EPS. I'm not going to read them to you, but once again we'll make that available to you. So, finally, we've summarized our fiscal 2022 guidance for you as well on the screen. Nikesh already covered this, but hopefully the format for fiscal 2022 will be easy for you to digest.

And I don't think it's on the screen, so perhaps – yeah, perhaps I should move it since I'm holding the clicker in my hand. Sorry. So, while we are investing to capture significant market opportunity and we do see a gradual shift in durations, we expect it to be gradual associated with changing mix of our products towards more cloud and SaaS-delivered products.

As Nikesh mentioned, we're not anticipating a big bang event. And so, for the years beyond fiscal 2022, we're targeting our operating margins to be above 25% and free cash flow margins at least 30% or greater. So, that hopefully – we'll put some of your minds at ease. That concludes our prepared remarks and now we'll turn up the lights and be happy to address any of your questions.

Nikesh?

Nikesh Arora

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

Are you guys happy or – come on, give her a round of applause. Tough crowd.

Kathy Bonanno

Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

A

Okay. We have people running mics. So I see some questions.

David Niederman

Vice President, Investor Relations, Palo Alto Networks, Inc.

Please state your name and your firm before you state your question, please.

QUESTION AND ANSWER SECTION

Jonathan Ho
Analyst, William Blair & Co. LLC

Q

Thank you. This is Jonathan Ho from William Blair. One of the questions I have is regarding the next-generation growth. Can you unpack for us a little bit of the components that you see from that next-gen side and maybe how much that ties to the investments that you're making? Thanks.

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

A

Yeah. Look, we're not going to break down the individual components just yet. But in terms of the investment, as I mentioned, we've moved 1,000 people through acquisitions or through organic hiring. We've taken our Prisma and Cortex with next-generation security team to about 1,500 people out of 7,000 people, the highlights that we ended FY 2019 with.

We anticipate adding more people into those categories both for R&D and for sales. And we feel reasonably comfortable that our core team is robust in the size. So we'll be making small additions to our core team, but mostly we're focusing some of our newer hires into Prisma and Cortex. Some of that spending is also a full-year impact of what we already invested going into Q3 and Q4 of this year. So, some of it is a follow-on from Q3 and Q4 investment, which we will be able to manage with our budgets this year. But some of it is incremental hiring for Prisma and Cortex.

In terms of across the board, I can give you color that Prisma Cloud is doing phenomenally well for us. It's really – we need to be out there in front of our customers a lot more. There's over 20,000, 30,000 people selling public cloud between AWS, Azure, GCP, and Alibaba. There's probably a few hundred cloud security salespeople in the world. So, when we show up on customers and we show them a demo and saying, look, this is what you're not doing, they're like oh, shit, yeah, I got to go cover my security needs. And when I write applications, they're just not enough secure themselves. So we're seeing really good traction in Prisma Cloud. I think Nir made it abundantly clear how excited we are about Prisma Access and how proxy style securing cloud-native architectures is not a good idea. So, Prisma Access is a huge focus.

Demisto has done well. Post-acquisition it has followed the M&A slide I showed you in terms of expecting to double their business plan from where they are, so. And XDR for us has done really well because you got 250 customers in the first full quarter of operation, and we continue to see more and more with the addition of third-party data ingestion. And the way we think about ingestion, just to clarify, as Lee said, we just don't ingest data. We make sure our analytics engine can ingest that data and provide analytics and suppress bad alerts and give you a good signal and do data stitching. So, our ingestion philosophy is more a philosophy which works on building analytics around the data and then ingesting [indiscernible] (1:26:04).

So I think across the board, we anticipate robust growth. That's why we're comfortable guiding to an $800 million to $810 million number.

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

A

A lot of hands going up. Okay, [ph] Amber? (1:26:18)

Kenneth Talanian
Analyst, Evercore ISI

Q

Hi. Ken Talanian, Evercore ISI. When I look at that $6 billion billings number, how much of that is from your existing product set and what are your assumptions around kind of current acquisitions going into that and then maybe some of the future acquisition assumptions that build up to that?

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

A

Look, as Lee mentioned that we believe many of the cloud security products are not fully built in the market from a maturity perspective. If you look at serverless, serverless we think is 50% built. We bought PureSec, they have a product roadmap which is a robust product roadmap in front of them for six to nine months. So we believe there will be interesting cloud security based acquisitions we might have to do in the future which will fall in the M&A philosophy we highlighted.

So, some of those bolt-on technology which haven't been developed or anticipated and our desire to build a cloud platforms of the future, but there is no major plug in that number for us to go out and acquire revenue to reach that $6 billion number. We feel we should be able to get there with the majority of the products we have in place with small bolt-on acquisitions as we see the industry evolve, the product marketable.

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Q

Thank you. Shaul Eyal with Oppenheimer. Nikesh, you have put many concerns to rest over the course of the past hour. So...

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

A

Thank you.

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Q

...one question I had in mind is...

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

A

But you still have one, so go on. Everything before the but is to be ignored. Yeah.

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Q

As we think about your targets heading towards fiscal 2022 and above, have you taken into consideration any changes with respect to channel compensation, partners, anything with a go-to market? Or pretty much from our perspective we should be thinking about it mostly at a status quo going further?

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

A

There are no major assumptions in there in changing any channel behavior in the process. We are seeing more activity in the channel by telcos and by SIs like the Accentures and the Deloittes of the world or AT&Ts of the world or Telefónicas of the world. They're becoming more active in cybersecurity. If you look at most of the landscape, every telco, every consulting organization is building very large cybersecurity practices because they're trying to [indiscernible] (1:28:50) building cloud practices.

So, if you go, this is the biggest fastest-growing segment of the SI and SP space. So, yes we anticipate they will have a bigger role to play in how we are able to deploy some of our products in the future. But to us, that's just evolution of channel. If they end up doing more business, bringing us to customers, we'll be there with them just the way we are with the Optivs and WWTs of today.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Thanks. Saket Kalia from Barclays. Nikesh, you talked about no transition to a term license model, for example, for the firewall business, which was good to hear. But you also even suggested that maybe some cloud products could be priced similarly to the firewall. I think we mentioned that quickly. Could you just give some examples of that and when that could actually start to happen?

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

So, what I – well, sorry. Thank you, first of all, for asking the question. I want to make sure I clarify. Sometimes, our sales teams bundle our annual products into three-year deals and sell them like they would sell an upfront cash payment, which allows us to get the cash flow just the way we get the cash flow for our firewall products. And roughly three years is roughly the term for our hardware business in terms of contract durations.

So, that's what I'm saying that some of the cloud deals end up being three-year deals instead of annual deals, so we still get the benefit of the cash flow, so which is why Kathy alluded to the fact that we're not anticipating a lot of duration declines over the next three years. We believe – I haven't said this yet but I'm going to say it, we believe that the duration decline will be approximately 10% over the next three years. And hence, we believe we will be able to deliver the $4 billion of cash flow over the next three years.

Saket Kalia
Analyst, Barclays Capital, Inc.
Q

Thanks.

Imtiaz Koujalgi
Analyst, Guggenheim Securities LLC
Q

Hi. It's Taz Koujalgi from Guggenheim. Kathy, if I'm doing my math right, based on your billings guide for next year and your billings guide for the next generation of products, if I back that out, it looks like you're guiding to the core business growing at about 8% the firewall business, which is a big step down from the 24% product growth we had this year. Is that the right way to think about product growth next year in the high-20s?

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.
A

Yeah. I think it's a little bit higher than that, but, yes, that's close. The reason that we're looking at this firewall technology as a group is because we're very excited about what we're seeing from our customers in terms of demand for both Prisma Access and our VM series. And so, that security category, which Nikesh showed up on the slide earlier, we are expecting to continue to grow at very rapid rates.

Now, the mix may change a little bit in between there, but I think our forecast still holds regardless. And the firewall security itself, that inline security, that network security is still a very important component for all of our customers. But we're seeing great demand and great excitement about what Prisma Access can do by delivering that security in a cloud form factor, really security-as-a-service. And so we're very jazzed about our possibilities going forward in terms of being able to win deals that would have normally been one with firewalls, hardware with that particular product. And we think that we're the only competitor that can really offer these various form factors to our customers. And so we see a really terrific opportunity.

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

Just to elaborate on that for a second. You saw two examples, one Lee alluded to, a very large retailer and we had a video from another. In both cases, we were competing with firewall boxes. And we went in with Prisma Access with a differentiated strategy. These are very large deals. As I mentioned, one of them was over $10 million, the other one was close. But in both cases, we were able to displace the hardware form factor from competitors, because the competitors did not have a software form factor.

The good news is with the software form factor, deployment is a breeze. If you try and deploy a box in 2,000 locations in a retailer, it takes them a year-and-a-half or two years. With software, we can get there in three to five months. So, part of what we are trying to do is we're trying to actually force that shift towards the software form factor because, as Nir mentioned, we don't believe our competition has the capability to deliver this solution via a software form factor, which allows us both to be differentiated, reduce speed of deployment, allow it to run across 100 onboarding points for our customers. So, that's part of the assumption, which you rightfully captured. We're actually trying to engineer that bigger shift and trying to drive our business more towards the software form factor.

Imtiaz Koujalgi
Analyst, Guggenheim Securities LLC Q

Thanks. So, one more follow-up, Kathy. On the long-term target, comparing what you gave us last time in 2017, you had free cash flow margins long-term below operating margins. This time you reversed it. Your operating margins long-term are actually lower...

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc. A

Yeah.

Imtiaz Koujalgi
Analyst, Guggenheim Securities LLC Q

...than your free cash flow margin targets. What is driving that reversal? Is it just more recurring revenues?

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc. A

Yeah. Can I just clarify? When we are talking about long-term, and I'm glad you asked this so I can get it out there for everyone to hear, we're talking four to five years, right? And the previous guidance that we had given, our long-term was much, much further out when we're sort of growing at the rate of the market. It's the way we described it. And at that point in time, we assumed that we'd be on much greater cash taxpayer. And so, that was the reason for the lower free cash flow margins. But we're talking right now, long-term for us is about four to five years out. Okay? Thank you. And I said 4 to 5 years, not 45 years. I need to be very clear and enunciate...

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

45 would be great guidance. All right. Somebody has the mic. There's question on this side. David, behind you.

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.
A

And I saw a woman with her hand up, I want her to get a question. Fatima? Just don't ask us a hard one now. Just kidding.

Fatima Boolani
Analyst, UBS Securities LLC
Q

I'll go easy on you. Fatima Boolani from UBS. Just a quick point of clarification on the mix shift dynamics you're seeing in the core firewall business. Is that a displacement dynamic or are you seeing the mix shift within the refresh of your own installed base? I just wanted to clarify...

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

It's more of a displacement dynamic. I gave you one specific use case, but there are similar use cases in many places where whether it's a retailer, whether it's a multi-branch situation or multiple mobile user situation, we have customers with 100,000 employees or more who want to go to a Prisma Access type solution for the mobile users. So, it's mostly a displacement of competition dynamic than it is a refresh of our data center firewall business.

Fatima Boolani
Analyst, UBS Securities LLC
Q

Understood. So, my real question is...

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

Yes. I know I knew you were going. Don't worry.

Fatima Boolani
Analyst, UBS Securities LLC
Q

You talked about...

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

I spent three months poring over every one of these numbers with Kathy. So I know exactly where you're going. Please go.

Fatima Boolani
Analyst, UBS Securities LLC
Q

You talked a lot about automation in each one of the pillars of your corporate strategy.

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

Yeah.

Fatima Boolani
Analyst, UBS Securities LLC
Q

And so, as I think about your top 25 – or your 25th largest customer spending close to $40 million per annum with you, I mean, how should we think about that with the automation opportunity and the fact that you expect to double the size of your business in the next four to five years? I mean, what are some of the dynamics there, if your 25th largest customer is already spending $40 million with you?

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

So, let me use Cortex XDR as a use case, right? We have thousands of customers who deploy Traps. The version of Traps four months ago was not collecting data, sending it to central data lake, allowing us to do insights and analytics against it. We are able to go back to every one of those large customers and allow them to ingest data from there and upsell them Cortex XDR. So this is a use case for us where we take their firewalls, we take their endpoints and say, why don't you collect the data across the board. We'll analyze it to you, we'll reduce the signal-to-noise ratio and we'll couple Demisto with it and be able to give you automation going forward.

So, that's the use case, for example, where we can take our firewall customers, our endpoint customers, add automation to this. And that budget comes out of their SOC budgets because every one of our customers is building SOC. SOC is the fastest-growing category with about 20-plus-percent growth year-over-year, where people are deploying more people and more data ingestion and more data logging spend.

Fatima Boolani
Analyst, UBS Securities LLC
Q

And do you foresee that more coming out of the wallets of traditional managed security services providers you sort of offer these Tier 1 type capabilities? And where are those dollars coming from is essentially...

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

Those dollars are coming from both SOC dollars, if you will, if there is such a category, but they're also coming from efficiencies we're able to drive for those SOC owners. We're saying we can come in and instead of – we put up some interesting numbers up there, you put 8 times and 50 times in terms of alert reduction. Traditional approach to alert reduction is hire more SOC analysts. If you can walk in and say, I can reduce the number of alerts by 8 times and I can reduce the number of alerts by 50 times, that's a huge amount of savings, which is coming out of the SOC analysts that people to hire. And very few of our customers are able to scale up their SOC to hire 300 SOC analysts because it's kind of very interesting.

One thing I learned which I can talk about, very few customers delete policies. They're scared of deleting seven, eight of firewall policies because somebody wrote them with some wisdom in mind and the new guys says, holy shit, I'm not going to delete. And so, there's a poor SOC analyst trying to interpret, why is that an alert? And the problem is the alert keeps coming back because they have no ability to go out and remediate that and fix that policy.

So, part of what Demisto is doing is saying, okay, we understand you don't like these alerts. Let's automate this so you can start focusing on stuff that's important. That's how you end up with 174,000 alerts. And not that I'm a hacker or a bad guy, but if I understand how you prioritize the important alerts you should look at, I'll spend my time trying to figure out how to be under the radar.

So, part of our philosophy is we want to look at every alert out there and the only way you can get there is through automation, automation that works in the endpoint, automation that works in your firewall, automation that works in you SOC. So, that's why, if you noticed, every one of our products has a large automation TAM because we believe we're going to take away from those services and labor TAMs and put that into automation.

Fatima Boolani
Analyst, UBS Securities LLC
Q

Makes sense. Thank you so much.

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

[ph] Amber (1:39:10) in the back.

Sterling Auty
Analyst, JPMorgan Securities LLC
Q

Hi. Sterling Auty with JPMorgan. So, one question for Nikesh and Kathy. And if possible, can I throw a follow-up question to Nir if he still has his microphone?

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

Yes. Our entire management team is here, of course.

Sterling Auty
Analyst, JPMorgan Securities LLC
Q

All right. Fantastic. So, Nikesh and Kathy. Nikesh, you mentioned the 10% reduction in duration over the next three years. How much of that is actually going to be what you're managing that duration to versus what customers want? Because one of the positive feedback items that we received through the channel over the last quarter or so is, finally, Palo Alto being flexible on payment terms. And if, God forbid, we do roll into some tougher macroeconomic times, I could see more and more customers perhaps wanting to only pay a year at a time instead of three years upfront.

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

Kathy, you want to...

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.
A

Yeah. We are going to be very thoughtful about those trade-offs in terms of what sort of financial incentives do we have to provide in order to have our customers commit to us for a longer period of time. We talked about last –

that issue last quarter. And we talked about the fact that we were paying very close attention to the economics of deals like that where our customers really wanted to only pay us a year at a time.

And we're going to continue to do that. And if our customers demand more and more of that, obviously, we will adapt to what our customers are wanting. But we actually find that there are a lot of customers who are very comfortable with the way they pay us today, very comfortable with our billing practices to date. And so, we're not seeing this huge surge of demand. It tends to be occasional request that we handle on a one-off basis.

Potentially, it could become larger in the future, and of course, we'll adapt to that over time. But the big shift that we've been talking about – I'm sorry, Nikesh, is really driven more by the mix shift of the products and primarily the growth of Prisma Cloud, which we talked a little bit about last quarter having shorter contract durations [indiscernible] (01:41:13).

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

And Sterling, just to add to that. I've discovered the last 13 months, the industry has certain compensating mechanisms already in place where there are customers who want to pay on an annual basis in the industry, the channel wants to facilitate it [ph] to figure it out (01:41:26) with some sort of financing that show up at our doorstep with the entire contract duration's worth of cash flow.

So, it's been around for a very long time. And there are many enterprise companies which have financing arms and all different kind of tactics to enable that cash flow generation. So we haven't assumed any of that stuff. We believe that life will go on as normal. But I have the inevitable Nir here, [ph] maybe you want to ask a question. (01:41:48)

Sterling Auty
Analyst, JPMorgan Securities LLC
Q

Exactly. But one follow-up, Nir, when you were talking about proxies, you did Gen 1, kind of Gen 2, but when we're thinking about Prisma and the competition going forward, you didn't really kind of call out the name. So I want to be very specific in terms of understanding who you think...

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

You think we didn't call out the name.

Sterling Auty
Analyst, JPMorgan Securities LLC
Q

[ph] Nikesh, you touched upon. (01:42:09) So who do you think is going to be the core competition in terms of Prisma Access moving forward? I mean, we all think probably Zscaler is going to be part of it, but what about the Akamai's and the other companies that are in that space? And what do you think happens to kind of the traditional firewall vendors? Do they all get squeezed out or do they come up with offerings as well? Thanks.

Nir Zuk
Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.
A

Yeah. So I think the competition is Zscaler. However, I strongly believe that the right architecture and the right product at the end of the day win. And we've been through that movie multiple times, right? FireEye, for example, right? A long time ago, FireEye came out to the market and they had this idea of running sandboxes and signatures are dead and the entire world is going to shift to FireEye and some of you even bought that story, but it was the wrong technical solution.

First, sandbox is not going to replace everything. And second, from a technical perspective, if sandbox need to do prevention, no detection, it has to be in line and it has to be across the entire infrastructure, which means it needs to run off the firewall. And that's why they went their way, we went our way and we all know how it ended up for both of us.

So, I think that we're facing the same situation right now. There is the right technical way of doing something and the right way to deliver a product to the market, and there is the wrong way. And proxies have always been the wrong way and firewalls have always been the right way, being in the network, part of the network, being a packet-based device, participating in routing, participating in network optimization, and being able to support all applications, not just few applications, not breaking applications.

I don't know if you know it. Microsoft recommends that when you use Zscaler, you turn – you don't use Zscaler when you go to Office 365. Why? Because it breaks Office 365, because that's what proxies do and it's their own technical solution and I strongly believe that the right technical solution will win.

Now, if you look at what's involved in access, in the modern access into the cloud and back into the infrastructure – into the corporate infrastructure for mobile users and branch offices, you need to do a lot of different things. And our competition today, different competitors do different things. I don't see a single competitor that does both the application security part of it, the firewall side of it, the CASB side of it, the SD-WAN part of it, then back to corporate side of it. I just don't see anyone that has the complete portfolio to be able to do what we're talking about.

Yes, there are the firewall vendors. The firewall vendors, like I said, are still busy figuring out why they can't sell their hardware against ours, while we've been spending the last several years building our virtual firewall and building our cloud-delivered firewall to a point where I just – it's just – they're three to five years behind at least, plus the amount of time they are behind our hardware firewall, I just – I don't see competition from them.

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

Thank you, Nir.

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.
A

I'm going to recall...

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

What Nir means to say is, we respect our competition and we're glad that we're able to build amazingly large businesses and serve the customers' needs in cybersecurity. I think that's what he said.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

Matt Hedberg, RBC. It seems like every other question with investors is macro, you guys delivered strong results. Obviously, some very large deals this quarter and the guidance on a multi-year view is very strong. I guess, Nikesh, when you're out talking to executives, what is the pulse of buying behavior out there right now? And then I have a quick product question for Nir as well.

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

Yeah. What's interesting and maybe I'm going to ask our President, Amit Singh, who you have not seen in this context. He can talk more because he has been out there on the road grinding away. So you guys get to tell the good stories, while I get to go out there in the field and grind. So, let's have [ph] Amit come up and speak. (01:46:01)

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.
A

Oh boy.

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

[indiscernible] (01:46:05)

Amit Singh
President, Palo Alto Networks, Inc.
A

Hello, everyone. The climate for cybersecurity is quite strong, the acquisitions. It's driven by all the challenges you see in the papers and buying behavior is actually quite solid. The movement towards software and software-delivered is the real one. So – and we are actually very, very excited about the products that we have, both on the product side as well as the service delivery side of it, because these are cloud-delivered solutions, the background that I come from.

And interesting, when you look at any trend, whether it's how many software startups were funded, cybersecurity startups, all the way to the actual market spending, it's very, very solid. Your question was, I think, on the macro picture. We haven't seen any slowdown. We haven't seen slowdown. You saw some of the numbers we shared around pipeline, pipeline growth, partner generation pipeline. And clearly, our Q4 performance is a measure or a testament of being able to grow the core business while being also able to generate brand-new businesses and scale them.

Matthew Hedberg
Analyst, RBC Capital Markets LLC
Q

And then maybe just a quick product question. Nir, when you think about consolidating security spend, what's sort of your view on identity? Obviously, it's a hot category out there. What role does identity have in the Palo Alto platform?

Nir Zuk
Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.
A

Sure. So, first, most of our customers integrate our network security with identity because identity needs enforcement. And in most cases, the firewall is going to be the thing that performs the enforcement. Actually, the only case where it's not the firewall is when you access SaaS applications. In all other cases, it's the firewall that's enforcing the identity, sometimes the applications themselves as well. So that's the role of identity.

Now, if you look at the market today, I think most of the market is focused on what's called hygiene, meaning who can connect and who cannot connect to an application, which is interesting, but it's becoming commodity. I think the most – the more interesting part of identity is identity analytics. So being able to take identity events and figuring out attacks from the identity. So that's – I think that's one area that's not being addressed today by the market and is an opportunity. I think that's the other side of identity that is still yet to be decided by the market is how do you do machine-to-machine identity, especially in the cloud. And I think the jury's still out on that. And that's – that could be one day an interesting thing to look at.

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

A

Over that side.

Philip Winslow
Analyst, Wells Fargo Securities LLC

Q

Hi. Phil Winslow, Wells Fargo. I just want to focus in on the firewall platform billings slide and there you break out your firewall hardware versus Prisma and VM-Series. We've obviously talked a lot about Prisma Access here today, but wanted to focus in my question on the VM-Series. One of the questions I get a lot from investors is attach rate of VM-Series and attach rate of firewall in the public cloud environment. And so just kind of question to the whole team here is that, one, how are you thinking about contribution of VM-Series to the forward billings? But also, where are we in terms of increasing attach rates of VM-Series and call it, your hybrid cloud, multi-cloud security?

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

A

Quick clarifying question. What do you mean the attach of the VM-Series?

Philip Winslow
Analyst, Wells Fargo Securities LLC

Q

So instead of call it like the out of the box firewall that you get from a cloud vendor, Azure, AWS attaching actually your VM-Series through that workload in the cloud.

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

A

So we're very pleased with the VM-Series and how it's done. When it first came out, we were focused on the private cloud use case because at the time that was the – that was the first generation of cloud. And then it's evolved really well as more workloads are shifted into public cloud infrastructure. VM-Series today supports all of the major cloud vendors in U.S. Azure, GCP, Alibaba. It's evolved in a number of ways that are very specific to cloud in terms of how we integrate it with different orchestration platforms, how we do automation. We're the only security vendor, for example, especially supported with Terraform, which is one of the main sort of multi-cloud automation orchestration tools out there.

We are sellable to all different marketplaces. And we actually have a very nice business and growing business with VM-Series being consumed through the marketplaces. So, there is a lot of really good things that are happening there. I'd say the only sort of challenge that – may not the only challenge, but the big challenge relative your question is a lot of companies will first try to get by without real security. And the – through various mechanisms and often it's through unfortunate events where something bad happens to a company that triggers the people that actually really go back and pay attention.

But that's the only challenge is sort of getting people over the hump of trying the thing that they think might be good enough before they realize that what they really need is best-in-class security and understand that we can do the cloud integration aspects that they also need. Okay?

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

Okay. A question here.

Karl E. Keirstead
Analyst, Deutsche Bank Securities, Inc.
Q

Great. Karl Keirstead at Deutsche Bank. First of all, Nikesh, for a guy who a year ago said that you're no longer giving annual guidance, only next quarter, thank you for the reversal.

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

Appreciate it. All – adaptive, dynamic, earned.

Karl E. Keirstead
Analyst, Deutsche Bank Securities, Inc.
Q

Yes, yes. I wanted to, let's say, stress test your confidence in 20% billings and revenue growth over the next three years. And I guess I'm saying this in the context of you having just put up a quarter where you grew both metrics by 22%. So, you just put up 22% and you're saying you're going to grow 20% for the next three. At first blush, sounds a little bit optimistic, especially given that you're on stage as well talking about a hardware to software form factor shift, which if we look at firms like F5 and others that are going through this, it tends to be quite dilutive to your overall growth rate.

So, is it that that form factor shift you expect only to be quite gradual and you can kind of skate around it? Or is it that your emerging products are just growing so damn fast that despite that you can still get to 20%? Thank you.

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

First of all, thank you, Karl. If I'm allowed to clarify, I was not comfortable giving guidance when I walked in because I didn't understand the levers of the business, nor did I understand industry, nor did I understand the levers of the company. And I hate to stand up on stage and comment on behalf of 7,000 people without having some degree of confidence and comfort in our ability to deliver. So, I appreciate you guys enduring the last one year of our quarterly guidance. But I think, hopefully, we have given more guidance and put a large noose around our necks, now that we have to go out and deliver this stuff. So, thank you for reminding me of that.

In terms of our comfort level, I want to parse your question into two or three parts. One part is we are seeing unabated growth in cloud generally. And I alluded to the fact that there's not enough cloud security out there and there's not been enough people enumerating the need for cloud security. I will not take the name of the customer, but there has been a recent breach where it was a cloud breach. And I can tell you that got the phones ringing because people suddenly realized that you can have cloud breaches even though you're using a public cloud provider, security cannot be used as an open source set of tools. You actually you have to go find the security product to secure your cloud instances as you start putting more and more important crown jewel data out there. So, we believe that that's going to drive more of the VM use case. We believe that's going to drive more of the

Prisma Cloud use case. We're also seeing, as the question was asked and Amit answered, we're also seeing a lot of re-architecting going on as people go to their re-architecting of enterprise.

If you look at companies, right, there's no CIO out there who's not thinking about how do I go to the cloud. So, this is very important. So, if I'm going to the cloud, what do I do with my enterprise IT, what do I do with my security? How do I rethink it? And as they're rethinking it, they're rethinking their branches. You go to a retailer, retailer needs to put a lot of bandwidth into their branch. In the past, there was low bandwidth. You need to do your POS systems to work, that's all you needed. Today, they want the AR and VR in the store. They want to move customer data back and forth. Suddenly, they need security in the stores.

So we believe there is some degree of new use cases being created, which is driving some of the confidence we have in some of our newer services, and we believe our core business continues to be strong. The underlying core business and the customer base continues to be strong. We fully realize that we are going roughly from, let's say, $3.5 billion billing number to $6 billion number, which means we have to kind of double. And as I said, there's only one way to double, have more product or have twice as many salespeople and hope that there's twice as many customers out there that you can get.

So, we think the balance is right and we should be able to execute. We've done a lot of investing in FY 2019 in Q3 and Q4 and ramping up both our core capability as of some of our speedboat capability. Now we're stretching our teams to go out and deliver and we'll give it our best shot.

Pierre C. Ferragu
Global Team Head, New Street Research LLP (US)

Q

Pierre Ferragu, New Street. Nikesh, first of all, thank you very much for not changing your business model. Took me a very long time to figure it out and I spent most of my time...

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

A

[ph] Taken me 12 months (01:56:08) to figure it out. We had to go figure out what the other guys [indiscernible] (01:56:11)

Pierre C. Ferragu
Global Team Head, New Street Research LLP (US)

Q

Exactly, [indiscernible] (01:56:13) done so far, that's great. And it gives me the opportunity to ask more of a product question to Nir. And so, you explained very well how you plan to completely crush all proxy-based competitors. And I was wondering – and you defended very well all the – all what you have already in your development in the next-generation firewall and all what you've done from there. But I was wondering how you transfer that benefit to technologies you're acquiring. So, for instance, if we look at the components of Prisma Cloud, when they came in first day, what did you do? How did you integrate their technologies with your existing technology? How did they benefit from that? And then your clients using it, how does it benefit from having a Palo Alto Network firewall and having Prisma Cloud in the same environment?

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

A

[ph] Go head, Nir. (01:57:06)

Lee Klarich

Chief Product Officer, Palo Alto Networks, Inc.

A

Yes. Thank you for the question. So, Nikesh mentioned a couple of the principles that we now apply more vigorously in terms of the incoming companies, level of responsibility we give them, the expectations we put on the founding teams of these companies to continue to execute as well as to build an integration plan. And it's interesting enough, you asked about Prisma Cloud, that was formed out of the basis of two acquisitions, Evident.io and RedLock. The integration of those two together took us about four months. Four months to integrate two products into a single platform. It now forms the foundation where we'll be able to then further integrate Twistlock and PureSec into that platform as we continue to extend it out.

Again, pulling the leadership teams of the companies into this together in order to make sure and then building an execution plan, it includes the integration that we all agree on very quickly after the acquisitions happen. And we're very much in the midst right now of executing on that with an expectation that by the end of this calendar year, those will now be new modules in the Prisma Cloud platform.

So a lot of this is around giving the right people the right responsibility, the right accountability and then executing. And we're showing that we can do this with very good success. On the customer side then, what they're seeing is very easy adoption of additional cloud security capabilities showing up in the same platform that they're already used to, they simply get to consume and deploy against their cloud workloads, which is a very powerful go to market and adoption aspect that the products are enabling. Yeah.

Nir Zuk

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

A

Yeah. Another example will be XDR. So we bought an EDR company, we bought an NTA company, right, Secdo and LightCyber, and integrated both together. Nobody believed we can do that. Nobody believed we can take network data, take endpoint data, combine them together and generate meaningful analytics based on that. And we're the first one to do it. And like I said, EDR, NTA, at their – on their own, don't make sense, and now we're going to integrate – we plan to integrate more and more things into it.

Now, the other type of integration that we have, which I think we partly asked about is when we buy someone like Zingbox or we develop something like DNS Security, it becomes a service that is attached to our firewall. And all the customer has to do to use it is to flip a switch. You flip a switch and you use the service. And you test it for a week, a month, whatever. You like it, you buy. If you don't like it, you don't buy it. And most customers that turn it on, they see things that they just can't not – not buy the product.

And the interesting thing is that those services apply to all form factors. So if you have a physical firewall, you do that. If you bought Prisma Access, you turn it on, you do that. If you went with a competitor, with a proxy competitor, and you want to do IoT security in the branch, which you do, like you need to secure printers and you probably have IP phones and video cameras and other things connected to the network in the branch, what do you do? You have to go to an IoT security company. You have to buy their products. You have to deploy it in the branch and you have to do deploy it in 2,000 branches, if you have 2,000 real points and somehow operationalize it.

With Palo Alto Networks, if you're a Prisma Access customer already, you turn on the switch, immediately it applies to all your branches. You like it, you buy it. You don't like it, you don't buy it. It's that simple, okay?

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

Another question, right next to the gentleman.

Keith Bachman
Analyst, BMO Capital Markets (United States)
Q

Hi. It's Keith Bachman from Bank of Montreal. Nikesh and Kathy, for you. Is M&A inclusive or exclusive of what you just put up on the board? And what I mean by that is, as we think about the revenue outlook and billing outlook, I assume that the context of that is mostly smaller deals, probably don't move the M&A, but I just wanted to see if you could clarify.

And it relates to you as well, Kathy, on the margins. This year, you're suggesting that margins go lower, but thereafter, they'll move higher. And so, is that, again, M&A neutral? So if you do some deals, you might ask for forgiveness for the margin growth that you're suggesting in the outer years if, in fact, you do pursue M&A, even some smaller deals that might pressure those margins. So, inclusive or exclusive is the shorter question of M&A.

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

So to give you a framework, it's exclusive of any large M&A, which has a significant revenue acquisition component. So, if you go buy a company for $100 million of revenue, that's not part of our plan. As I said to the gentleman earlier, there's no plug in these numbers that we're going to be acquiring $200 million, $300 million of revenue growing at 50%, right. That's not a bad stuff.

We're not looking for M&A as a strategy. We're looking at platform as a strategy. Now, in the platform context, if you think about are we better off going back? And for example, we built Cortex XDR from the acquisitions. We put it a – we've got the teams to integrate. We didn't sell it for six months. We got them to integrate and sold it after they put it together. Twistlock, RedLock, PureSec, we integrated and then we're deploying across our platform.

So, if you find there's a product need and the product market fit that needs to be integrated [ph] on a strong (02:02:29) platform, that stuff will have to be acquired. And we'll keep you posted as we acquire them, what the impacts of those are financially. We've not built in any expectations saying we're going to be doing $500 million of acquisitions every year. It's going to have certain EPS impact. We're going to take that and bake it into these numbers. These are raw numbers, organic. Kathy has told you, FY 2020 has a $45 million...

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.
A

M&A.

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

...M&A. [ph] $43 million (02:02:52) for this year. After one year, we roll that into our organic numbers. So, FY 2021, 2022, there is no – there'll be – unless we do something every now and then, there's – those are clean – those become organic numbers.

Keith Bachman
Analyst, BMO Capital Markets (United States)
Q

Okay.

Nikesh Arora A

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

One thing, I think there was a clarification question, which I want to announce publicly. Somebody asked a question about the duration of 10%, is that every year or across three years? The answer is, it's over three years, not every year.

Trying to keep my friends out of jail. I heard that broadband is poor in jail. So – and still on MPLS.

Michael Turits Q

Analyst, Raymond James & Associates, Inc.

Sounds like a good idea. My wife has just finished watching the Orange Is the New Black last night, so I don't want you there.

Nikesh Arora A

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

Okay.

Michael Turits Q

Analyst, Raymond James & Associates, Inc.

Michael Turits from Raymond James. Question on – for Nir, Lee, you guys talked about SD-WAN and SD-WAN is big and a big part of what Fortinet has been talking about for some time. So, I'm trying to think about, first of all, how do you become an SD-WAN player? What are you going to do with it? Is it similar, I think, to what Fortinet's doing and saying, hey, we can do this too with functioning SD-WAN or we're going to use it to help improve GlobalProtect cloud service's networking component because that's also a big place that Zscaler wins is by doing networking that they say salespeople money.

Nir Zuk A

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Yeah, doing networking with the proxy, that's interesting, but...

Nikesh Arora A

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

He doesn't need any more encouragement.

Michael Turits Q

Analyst, Raymond James & Associates, Inc.

I just want to get [indiscernible] (02:04:25) perform for a while.

Nir Zuk A

Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

Yeah. So, SD-WAN. SD-WAN, so maybe 30 seconds on what SD-WAN is. So, just so we're on the same page, as applications move to the cloud and it stops making sense to the MPLS, you want to – you start using regular Internet connections, right, DSL, cable modems, whatever, D3s, E3s, whatever you can get. The challenge with that is that they don't provide you the same reliability and performance guarantees that MPLS does.

So, all of a sudden, you start relying on applications in the cloud like Office 365 and G Suite and Salesforce.com or your own application support in public cloud, but you cannot get the same guarantees. So, SD-WAN is about taking multiple Internet connections like a DSL from one provider and a cable modem from another to DSL or a DSL in LTE or 5G, so on and so on, and somehow doing some kind of networking tweaks on them such that with the two or more links, you can get the same reliability and the same guarantees more or less that you get from MPLS, of course, at a much lower cost, much higher bandwidth, which is what those applications in the cloud need.

Now, there are multiple ways of doing that. You can do it in the branch itself, meaning you can take the firewall that sits in the branch and you can add SD-WAN to that firewall and do that – those networking tweaks to make those multiple Internet connections appear much more reliable. And we're doing that, meaning we are building that and that's going to become a subscription on top of the firewall, that's like Lee said, where if you deploy our firewalls in the branch, we do that. And in that respect, it's somewhat similar to what other SD-WAN vendors are doing, of course, with the differentiation being much better security, but we always win on security.

The other option to do it, and which we do today as well with SD-WAN partners and we'll continue to do, is to use SD-WAN to bring the traffic to Prisma Access. Prisma Access, which is a bunch of firewalls deployed in the cloud, need the traffic together. Now, you can do it with traditional [ph] IP6 (02:06:31) tunnels or something like that, a much more efficient way to do it is with SD-WAN. So, you program your SD-WAN, your software-defined WAN, to bring the traffic to Prisma Access and then you do all the security work in Prisma Access. The advantage of that is that you don't have to deploy a new security box in the branch every few years because technology goes stale and you need to upgrade, which is kind of like painting the Golden Gate Bridge, right? You start, you deploy 2,000 branches. By the time you finish the 2,000th one, you have to start from the beginning. With Prima Access, you don't have to do it. And that's where the real differentiation is.

So, doing SD-WAN in the cloud rather than doing SD-WAN in the branch and using SD-WAN just to bring the traffic to the cloud is the right way to do SD-WAN, but for that, you need to have something like Prisma Access. And you need to have a networking Prisma Access, not something that breaks the TCP connections and restarts them, which is not networking based. It's called a proxy.

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

QED. Yes.

Michael Turits
Analyst, Raymond James & Associates, Inc.
Q

Do you need to acquire SD-WAN?

Nir Zuk
Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.
A

Do we need to acquire? No. Like Lee said, we're building SD-WAN.

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

Okay.

Erik Suppiger
Analyst, JMP Securities LLC

Q

Erik Suppiger, JMP. Couple of questions, one on the free cash flow margins. Is the primary cause for the decline this year duration or what should we think of as the primary hit on the margin front?

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

A

Yeah.

Erik Suppiger
Analyst, JMP Securities LLC

Q

[ph] And then I have (02:07:59) a second question after that.

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

A

Yeah. The primary reason for the decline is the same primary reason you see for operating margin decline. And that's the investments that we're making not only organically to drive the new areas of our business, but also the M&A investments that we've made.

Erik Suppiger
Analyst, JMP Securities LLC

Q

Okay. And then...

Kathy Bonanno
Chief Financial Officer & Executive Vice President, Palo Alto Networks, Inc.

A

Which is why we expect it to turn around. Yeah.

Erik Suppiger
Analyst, JMP Securities LLC

Q

Okay. Then, for Nir or Lee, XDR, is that product production-ready? How much of that – how can we gauge the success of XDR from here because we've had traps out there for a while? Is this something that's going to be a viable competitor to CrowdStrike at this point or how should we be thinking about that? And how much of that is getting sold outside of your installed base?

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

A

So, as we mentioned earlier, we're actually very happy with how XDR is done. Now, it's early. We announced it about and released about four and a half, five months ago. You saw the results for the first full quarter, the number of customers we added. So, very excited about the initial market reception, customer reception to XDR. And the messages that we talked about here are things we're hearing from our customers, very powerful, the ability to integrate the – and stitch the endpoint data with the network data, no one else can do that, no one else can give them that end-to-end visibility, reducing the number of alerts, reducing the amount of time it takes them to actually investigate incidents. So, all the things we said here are – they're here because that's what we're hearing from our customers that have adopted XDR. Okay.

And the interesting aspect of this is that is enabling us to really sort of change the conversation with our customers to one that is a very strategic conversation about the shift toward not just endpoint protection, but the shift toward analytics and ultimately toward automation and [ph] time that it (02:10:06) with Demisto. Okay?

Nir Zuk
Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

A

Yeah. So, going back to the proxy...

Erik Suppiger
Analyst, JMP Securities LLC

Q

And about proxy.

Nir Zuk
Founder, Chief Technology Officer & Director, Palo Alto Networks, Inc.

A

Now that's almost similar. No, this is another case where I think that the right technical solution will win. EDR doesn't make any sense. It really doesn't make any technical sense to limit yourself to collecting data just from endpoints, limiting yourself to processing data just from endpoints and then responding back to the endpoints where we all know that attacks happen across the entire infrastructure. They can start in the SaaS application and then take over in the endpoint and then propagate through the network and end up in the public cloud where your data is.

The right technical way of doing it is to collect data from multiple parts of the infrastructure into one place, use your analytics or your people or whatever it is to go through the entire data, find the attacks base and information in the entire data. And when you find an attack, it doesn't matter where the signal came from. You want to respond back to the entire infrastructure, which is kind of where Demisto comes in, responding back to the entire infrastructure. And I just don't see the competition doing that. I don't see the competition doing more than just basic endpoint, data collection and response.

So, assuming we get the right marketing and the right sales and marketing around it, go-to-market, and there are some missing product features, I think that next time we'll be able to talk much more about where we are versus the competition in there.

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

A

If I may elaborate on that from a market activity perspective and given that we've only had four and a half months worth of great experience with the product in the market against the competitor you mentioned. Remember 12 months ago, we didn't have a dedicated sales force that could compete in terms of a point-by-point basis against some of these competitors because we had a core sales team, which was not as fully adaptive selling this product.

Now that we have speedboat teams out there, I think it's fair to say we saw CrowdStrike in – between 25 and 30 deals, which were in our installed base because that's where we went after first. And I think the numbers we were able to beat them in 75% of the deals we saw them in our installed base. Again, it's one data point, but we're slowly getting our act together and getting better at this stuff. But six months ago, we didn't have a product. Traps would not compete against EDR because Traps to endpoint protection did not do XDR. We launched XDR, we've made Traps free. We have thousands of customers using Traps. Our first target is to go to the customers who already have Traps, [ph] where we have data, (02:12:59) they only have a firewalls. Who better than them to make sure that they can buy XDR, and we're delighted that 75% of them CrowdStrike [indiscernible] (02:13:08) more deals that we do because they have a larger sales force, but we're delighted that we were able to beat them in [ph] 25% and 75% (02:13:14) of those deal.

Shaul Eyal
Analyst, Oppenheimer & Co., Inc.

Q

Thank you. Shaul from Oppenheimer again. Maybe question for Amit or Kathy. European performance, whereas it has been quite stable over the course of the past probably two years now. I think this quarter and last quarter not as strong as we have seen before. So, is it a macro issue, maybe a UK-specific issue, maybe tying it to a former macro-related question that was asked?

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

A

It's just a great opportunity. Really, it really is Europe, strong adopter of – cybersecurity is actually on the headline. And that is national legislation in countries to go fix it. And we're just investing in the team, giving them resources. We love the leadership team there. So, it's actually a growth opportunity for us to do – continue to do well and actually do better in EMEA.

All right. We've got one in the front, then two in the back, on the right.

Andrew James Nowinski
Analyst, Piper Jaffray & Co.

Q

Thanks. Andy Nowinski with Piper Jaffray. So, just had a question with regard to Prisma Access. At the Gartner Security Conference a few months ago, Zscaler was on stage at the keynote and they had a few customers on stage as well that said they tried your GlobalProtect Cloud Service, which you're now calling Prisma Access, and didn't get the performance that they were looking for. It wasn't scalable. I guess can you just talk about how you've changed or fixed the performance in the architecture?

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

A

We – the company was not an existing customer. And they had actually selected said competitor, but we had an opportunity to get in one last chance. And they told us the same thing. And we said can you share with us the test that you're doing. And it was provided by the competitor and it was a flawed test. We were able to show them how it was a flawed test. And after they redid the test to no longer be a flawed test, Prisma Access performed wonderfully. So – and that was before the most recent update to Prisma Access where we now have over 100 onboarding locations around the world. So we are very pleased with the performance of – performance capabilities of Prisma Access as a globally deployed cloud solution.

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

A

And as the video you saw, which talks about 1 million employees and hundreds of hospitals, they ran a full POC against the same competitors, so hopefully...

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

A

Which is already deployed.

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

Sorry, which is already deployed, yes. All right. Questions on the back. And we're coming to the end of our Q&A session, but we'll take a few more questions. Some there. And then let's go to Brad first. I don't want to end with Brad.

Brad Zelnick
Analyst, Credit Suisse Securities (USA) LLC Q

Thank you very much, Nikesh. I really appreciate it.

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

I want to go out happy, okay?

Brad Zelnick
Analyst, Credit Suisse Securities (USA) LLC Q

This is a fantastic presentation today. My question is actually really simple.

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

Yes.

Brad Zelnick
Analyst, Credit Suisse Securities (USA) LLC Q

Three months ago, if we listened to your remarks in your earnings call, you talked about a transition.

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

Yeah.

Brad Zelnick
Analyst, Credit Suisse Securities (USA) LLC Q

There's not much of a transition.

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

Yes.

Brad Zelnick
Analyst, Credit Suisse Securities (USA) LLC Q

Why?

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

Good question. I'm glad you asked it. Four, five months ago, we were going full speed ahead analyzing every which way we can make this transition to a fully ratable model. And when we sat down and looked at it from an accounting perspective, a legal perspective, a go-to market perspective, we would have to impact the channel, our salespeople, we all stepped back and said, okay, why are we doing this? Our customers are buying billions of dollars of products from us. They have a motion. Our sales people know how to quote it, how to sell it. And we sat there and said, we're doing it because the industry likes ARR models and software models. I personally like money upfront. Cash flow is a good thing. And then you go out and hunt, use some this year, the rest you put it in [ph] cold store (02:17:42) and use it in year two, in year three. [ph] Why do you (02:17:45) have to go hunt every year if I'm going to go to analyze model. So we just felt that we were trying to unnaturally change the company's business model and transition to a place, which is more akin to a pure software SaaS ARR-based model.

And we are just kind of a hybrid business. We have the firewall business very strong, building the next-generation security business, which we believe is going to be very strong, and some of the characteristics of this we really like. We like the upfront cash, we like the cash flow that this brings us, we like the fact that it gives you long term deferred revenue, which allows you to be amortized. So we decided that we're better off going this way. So this is why we're here.

And then, we were comfortable that we've analyzed everything – every Sunday. This Analyst Day has been in the making for six months, right. We've been trying to look at what we want to come and tell you, what's important, what's not important. As I said, I probably will never read as many research notes that I've read in the last six months from all of you guys. Apologies to you, but I have a day job, but I did read most of them and I did read what you guys are concerned about and I understand why you like those models. But we got to run the company the way we want to run the company and the way the customers want us to deliver the product. So that's why.

Srini Nandury
Analyst, Summit Redstone Partners LLC
Q

Srini Nandury, Summit Insights Group. Nikesh, recently, VMware acquired Carbon Black.

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

Who?

Srini Nandury
Analyst, Summit Redstone Partners LLC
Q

VMware.

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

Can I ask you which company? Sorry, I missed the question.

Srini Nandury
Analyst, Summit Redstone Partners LLC
Q

VMware...

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

Yeah. I know VMware very well.

Srini Nandury
Analyst, Summit Redstone Partners LLC
Q

...acquired Carbon Black.

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

Carbon Black, yes.

Srini Nandury
Analyst, Summit Redstone Partners LLC
Q

Okay. So the question is this. We're trying to make sense of how the landscape is going to be evolving. It looks like VMware is going to be acquiring more companies in the space. And what does this mean for the whole security landscape going forward?

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

I can't comment on VMware's strategy. There are a lot of people who believe security is important, right, and they're all stepping up their acquisitions in security. And I think that's probably accurate. You will see a lot more acquisition in this space because I don't think 2,500 vendors are going to survive. And one of the questions early gentlemen asked was buying behavior. I firmly believe in the next five years, you will see more consolidated single vendor buys than you will see multi-vendor buys. Maybe over 800 EBCs at Palo Alto Networks where customers show up. And I haven't seen a customer who's actually espoused his desire that he or she wants multiple vendors to be able to secure their environment. They're looking for a solution which integrates across multiple solutions.

So, if any company out there, whether it's VMware, whether it's Microsoft, whether it's Broadcom can actually take products and integrate them, I think they're going to win. So the question is not acquiring. We can all acquire companies. Acquisition is the easiest part. The question is can you actually integrate them? Do you actually get leverage from integrating them into your platform? Acquiring a customer, putting them in an ELA and making them free or being part of your lodge, what did I hear that, platform level. So there's a new term you will hear soon in the security and [indiscernible] (02:20:37) ELAs to PLAs because people have disparate products, security and consulting and chips, and you can put them all into a PLA now. It doesn't that have to be an ELA anymore because it's more than an E to P. But those are interesting thoughts. I think the true need of the customer is an integrated platform. So if people can deliver an integrated platform, more power to them. Yes, as Nir just articulated, you need firewalls and endpoint [ph] to be able (02:21:04) to work together to be able to do next-generation security. Similarly, you need containers, serverless public cloud workloads to do it together.

And I will tell you [ph] an unrelated (02:21:16) anecdote, and I apologize if it doesn't apply. When I worked at Google, one of the businesses we started to go after was display advertising, [ph] nothing to do with (02:21:27) security. And Google had no horse in the race. They didn't want to display property. Microsoft had one. Yahoo had one. And they're both very good at selling their own display properties, but they were not good at cross-market selling because typically they defaulted to their own product. And my concern is when you're struggling at cloud native players like AWS or Azure or GCP or VMware with their own set of hybrid solutions, you default to better integrations and better alignment with your core product and you don't do as good a job of across industry security solution, across industry product.

So, our hope is we'll be the platform of choice across multiple platforms as opposed to platform that integrate security and try and bundle it when you buy their platform. So if I don't want to deploy VMware, would I be deploying Carbon Black today? I would have or may have. Tomorrow, I suspect the integration [ph] is speaking going to be (02:22:17) stronger. Now, I'm not sure which strategy gets you more revenue, maybe gets you more revenue given their scale, but I think the long-term outcome is that you want a multi-platform solution, which is somewhat platform-agnostic, so it can actually make it work better for you across multiple cloud platforms.

All right. Last one or two questions. And well, I want to make sure you guys don't leave here with questions unanswered. Go ahead. Upfront. I'm sure I'll read about it tomorrow or the next week. So why didn't I ask the question, guys.

Q

Excellent. Thank you guys for having this presentation, and really compelling product vision. And it's great to see a value proposition that's not just – like, you got to be secure because we're going to scare the crap out of you, but also we're going to provide value ...

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

A

We do that out in the field not here.

Q

... but we're going to provide value by making it easier, more effective to do the securities. So there's a dual value proposition that customers must see. I wanted to drill down into sort of the firewall market overall. Nir presented a really good sort of rationale of why firewalling isn't going to go away. We're still going to be doing firewalling, but it seems like where we're going to be doing that firewalling is going to change. So, I guess the question I had is, should we expect kind of the traditional firewalling done from an appliance at the edge of the network? Is that part of the market going to be stable, increasing, declining in the midst of a broader kind of firewalling capability that still grows?

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

A

So, I'll give you some data point and then I'll have our product leadership answer that. I went back, and as part of preparing for the Analyst Day, I looked at enterprise IT spend over the last seven years, right, because it's typically the end of life for most IT infrastructure, between 7 to 10, depending on what it is and where you buy it. There's approximately $1 trillion, $1.2 trillion a year that's been spent on enterprise IT. The reason I go track that is because I think security is 3% to 8% of that number, but in financial services, the government, it goes to 8% because they're very security conscious, others go to 3%.

So, if you think about it, there is approximately $12 trillion to $15 trillion of plant out there in enterprises, which is IT infrastructure plant. I just put a slide up there, which is a Gartner slide or Goldman Sachs slide, [ph] I kind of know are those (02:24:44) Goldman Sachs, maybe it's from this morning, which talks about the cloud disruption opportunity of $1 trillion in 2023, right. So, either you're telling me that we're going to stop spending in enterprise IT and the entire IT market is going to go down and all we're going do is spending in the cloud. Or are you telling me, people are still going to spend $1 trillion to it, growing at 3%, and a lot of that is still going to go to enterprise IT? So, I suspect this transition is going to take longer than we think that people are still going to be spending in enterprise IT.

Now, [ph] on to (02:25:13) the margin, it may be smaller number because people are shifting to cloud. And what it's doing is two things. One, it's making people re-evaluate, as I'm going to make that shift to the cloud, what do I want to buy that allows me that transition? And that's why one of the large retailers we talked about, they're going to the cloud. They don't want to just buy hardware firewalls, they want to make sure they can get VM. So, the cloud instances, they can get a cloud-delivered architecture for Prisma Access.

So the question is we expect this transition to happen in the next five to seven years, a lot of it. Do we have products that satisfy the three use cases: the datacenter use case, the transition use case to the cloud and then the new architecture towards the cloud? So, we think that's why the product strategy is aligned towards this transition. We think that shift is going to happen. It'll happen on a customer-specific basis depending on how ready they are. It'll happen on an industry basis. So, those are some of the moving parts, but we think firewalling is around for a while for the people who are still investing in datacenters. But I'll let my product colleagues elaborate on the...

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

A

Sure. So from a product perspective, the firewalls get deployed in lots of different places. They get deployed in the datacenter, they get deployed at headquarter, gateways, regional sites, branch offices [indiscernible] (02:26:23). And the – some of those use cases are more attractive to shift the form factor. So, for example, applications moving to public cloud. The form factor choice would be software for lots of different technical reasons that are mostly sort of straightforward to understand why you want to do that. For example, you can't shift the hardware device to Amazon and ask them to deploy it into your AWS account. You have to use software form factors.

As we talked about for branch offices, retail, mobile users, there is a shift that we are driving with Prisma Access that we believe is a very good shift both in terms of the customer outcome as well as what they need and want to be able to accomplish. But there is still – as Nikesh was saying, this investment in the enterprise infrastructure over the last seven-plus years, there will continue to be a lot of investment and that infrastructure has to be protected, so particularly in the larger central sites, regional sites. And the world will be hybrid for a long time, meaning datacenters, there will still be a lot of hardware that will need to be deployed against that. And one thing we didn't talk about today, but it's very important. This is – in a lot of those places that I just mentioned, the performance of hardware starts to become really important, right? If you think about a large headquarters with 10 gig connectivity growing, you want to do internal segmentation or to segment IoT devices and things like that, which that might be 100 gig, some of the larger datacenters, hardware still has a very important role to play in a lot of those core use cases.

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

All right. I think with that, we'll call an end to the Q&A session. I want to say thank you to my management team here who's been part of the journey in getting us here so far. I also want to use the opportunity to shout out to our 7,000 employees around the world who work hard to deliver results that we have to deliver, and hopefully will keep working hard for the next three years to achieve that targets and beyond, to achieve the targets we've outlined.

With that it's my pleasure to invite you downstairs for some cocktails and some demos in case you want to geek out on some of the products.

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.