THOMSON REUTERS STREETEVENTS

EDITED TRANSCRIPT

CYBR - Cyberark Software Ltd Investor Day

EVENT DATE/TIME: MARCH 06, 2018 / 1:30PM GMT

CORPORATE PARTICIPANTS

Adam Bosnian *CyberArk Software Ltd. - EVP of Global Business Development*

Ehud Mokady *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Erica Smith

Joshua Siegel *CyberArk Software Ltd. - CFO*

Marianne Budnik *CyberArk Software Ltd. - CMO*

Ronen Zoran *CyberArk Software Ltd. - Chief Revenue Officer*

Roy Adar *CyberArk Software Ltd. - SVP of Product Management*

Shay Nahari

CONFERENCE CALL PARTICIPANTS

Erik Loren Suppiger *JMP Securities LLC, Research Division - MD & Senior Research Analyst*

Fatima Aslam Boolani *UBS Investment Bank, Research Division - Associate Director and Equity Research Associate Technology-Software*

Gray Wilson Powell *Deutsche Bank AG, Research Division - Research Analyst*

Howard Shepard Smith *First Analysis Securities Corporation, Research Division - MD*

James Edward Fish *Piper Jaffray Companies, Research Division - Research Analyst*

Kenneth Richard Talanian *Evercore ISI, Research Division - Analyst*

Sterling Auty *JP Morgan Chase & Co, Research Division - Senior Analyst*

Dipak Rath

Donald Welch

Everardo Trujillo

John R. Rogers *American Financial Group, Inc. - Chief Information Security Officer & Divisional VP*

PRESENTATION

Erica Smith

So good morning, everyone. I want to thank those of you who joined us this morning here in New York as well as those of you who are on the webcast. My name is Erica Smith, and I'm the Vice President of Investor Relations here at CyberArk.

We have a busy agenda for you this morning. We did have product demonstrations that were out in the foyer this morning. The CyberArk experts will be here at the break and again at lunch. So if you didn't have an opportunity to have a product demonstration, please take advantage of that opportunity to learn more about our solutions.

Udi Mokady, our Chairman, Founder and CEO, is going to kick off the day with a keynote. We are then going to move into our product differentiation. Roy Adar, our Senior Vice President of Product Management is going to deliver that message. And then we're going to give you a unique approach, where Shay Nahari from our Red Team Services is going to talk about the attacker view. Last but not least, before the break, we're going to have our customers come up and give a presentation, a panel discussion with Marianne Budnik, who will be moderating, and to talk about how privilege fits into their security strategies.

When we come back, Marianne Budnik, our CMO again, and Ron Zoran, our Chief Revenue Officer, will come up, and they will discuss our go-to-market strategy and the market opportunity and how we're going to go about taking advantage of that market opportunity. And then from there -- sorry, Adam Bosnian is going to actually review our partnerships. He will kick off right after the break, and he is our Executive Vice President of Business Development. And then we'll go into Marianne and Ron. And then Josh Siegel, our CFO, will go through our financial model as well as our balance routine of revenue, growth and profitability.

Before we begin, we want to remind you that we will have forward-looking statements here today. Those forward-looking statements come with risks and uncertainties, and we're going to direct your attention to our 20-F, which is filed with the Securities and Exchange Commission. We also are going to talk about GAAP and non-GAAP financials. There is a reconciliation which'll be posted to the website.

With that, I am going to turn over the day to Udi Mokady, our Chairman, Founder and CEO. Udi?

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Thanks, Erica. Good morning, everybody. Excited to be here, our first Investor Day since going public in September of '14. And as Erica mentioned, we're really -- it's an opportunity for us to give you a deeper dive into the CyberArk business, the business opportunity and also a chance to hear from a broader set of our team. And for me, the most exciting element is we also have some of our select customers here, as Erica mentioned, for you, so really a broad deep dive into CyberArk.

We'll follow these pillars as we go out throughout the day, privileged security as a critical layer, our innovation as the key to our continued leadership, the large market opportunity that we're looking at, our strong land-and-expand model and how we partner with our customers, our channel partners and our tech partners and our powerful business model, delivering growth with profitability.

As we -- I mentioned the IPO 2014 when we went out. This is kind of the snapshot of key metrics. And we've delivered strong business momentum on all of these fronts. Customer count, we had 1,800 customers. We more than doubled to 3,700 global customers. From a revenue presentation, from $103 million, we more than doubled to $262 million of revenue in 2017, operating income from $22 million to $52 million, significant growth in 2017 and record cash flow of $81 million in the year 2017 compared to $23 million in 2014.

From the customer growth, it wasn't just the numbers, but also the increased quality of our customer base. This is a snapshot of 2014. We had about 35% of the Fortune 100 and about 15% of the Global 2000. This is the picture at the end of 2017. About 50% of Fortune 100 companies selected CyberArk. And we more than doubled, so about 30% of the Global 2000 enterprises have selected CyberArk.

And what we're seeing is continued diversity. And Josh will present it in his slides and how we continually diversify the verticals that we play in, but in each key vertical, we get selected by the market leaders in those verticals. And it's very important for us for all reasons, but it's also strategic. Those are top influencers in those verticals, and we work hard to make them successful and thus expand in the verticals.

So we can see manufacturing 20 of the top 25, telco 18 of the top 25, IT services and software companies 22 of the top 25, insurance 20 of the top 25, in the banks 21 of the top 25 banks. Some of them are sitting here today on the analyst side, and you know who you are. On the energy 17 of the top 25, just to give a bit of a snapshot.

We stay true to our mission of providing a critical layer of privileged security to secure enterprises and governments against advanced attacks. And we stay true to that mission, but that mission has expanded. The attack surface has expanded, and the sophistication of the attackers. The opportunity has expanded, and so has our mission to go after it and secure our customers.

If we look at kind of the scope of privileged security in 2014, when we first started, and we'll dissect this by 3 vectors, the privileged actor, so who needs administrative access to the keys to the kingdom, the infrastructure that we are securing and the applications that we are enabling and securing.

So in 2014, primarily -- if we scoped out our customers, primarily, we looked at on-premise environments. And so the mostly human actors, mostly administrators were using our technology. The infrastructure that we were protecting, primarily on-premise infrastructure, operating systems, databases, network infrastructure, etc. And the applications were primarily static on-premise applications, some homegrown applications.

The world has changed, and we strategically embraced that change and grew with it. The new norm as we see it today is very much most of our customers and prospects going to a hybrid business model, of course, adopting SaaS for some of what used to be their legacy applications. And one of the biggest evolutions, revolutions is the adoption of DevOps, the ability to release code at speed and leveraging native cloud architectures, like containers and microservices, to do that.

This is not a phenomenon that's going to go away. This norm actually enables an organization, enables their digital transformation. So what we're seeing is that this has become a competitive differentiation to enterprises to adopt DevOps. There is a correlation between the speed of code release and top line growth and the ability to beat competitors. And we see it from our customers. The DevOps evolution and revolution is taking off, and they're adopting modern architecture to be able to release code faster than the competitors and embrace digital transformation. And we align with that early and are running with it.

So if we look at the picture of what applications look like today, you have the full breadth. On the left, kind of the legacy monolith applications that I mentioned in 2014 snapshots, primarily dealing with human users and agent based and all the way through virtualized and containerized to microservices-based applications, where machine and code replace some of the human functions, and services are run up and down swiftly.

And so with that, the privileged actors have changed. It's expanded beyond just the human identities that need to be secure. More and more code and automation is driving code to provide functions that are human like, and we call them machine identities. So the privileged actors have expanded from not just human identities to also machine identities.

As we look at a snapshot of today's privileged security scope along those 3 dimensions, you can see that the scope advanced dramatically and with it our market opportunity. So if we -- back to the humans, the privileged actors have expanded. So beyond admins, we deal with privileged business users, with SaaS admins, with DevOps teams and developers and with machine identities, code behaving like a human, automation processes that need to be managed and authenticated and given secret -- they all need credentials to make their connections and their communications that they are doing.

On the infrastructure side, the letters in black definitely remain. All of our customers have infrastructure to secure on premise, but we've expanded what you see on the green here through our endpoint privileged management. We expanded to endpoint, containers, infrastructure as a service, orchestration tools, platform as a service and variety of DevOp tools. And on the applications, we've expanded from the on-premise, homegrown applications to also helping secure and enable SaaS applications and cloud native applications.

And Roy after me will elaborate on all of these fronts, but this is how we're looking at the expanding privileged security opportunity from a scope perspective and securing the keys to the kingdom, expanding it from the on premise to the DevOps and cloud kingdom.

And with it, the attack surface is exploding. While all of this is growing, more and more connectivity, our customers are seeing more and more elements of their network get virtualized and the need to protect so many assets and expanding -- that are expanding rapidly. There's more things to attack. There are more places where an attacker can land, which makes our mission even clearer and more impactful to our customers.

In a recent survey, Forrester put out that, in 80% of major attacks, the attack was trying or the attacker was trying to go after privileged accounts as the lever to move up the stack and get to the information they wanted to steal or the destruction they wanted to create or that includes the ransomware and other attacks.

And it doesn't matter anymore if it's an attacker operating from the inside or an outsider that made it on the inside. Attackers need privilege. Attackers need to get a foothold and expand and move laterally, whether it's on premise or in cloud infrastructure, to get and expand their attack. And CyberArk is positioned in this place where we can break the attack chain and do it across all these dimensions, on premise, hybrid and cloud environment.

And as we look at our play with regards to the other investments that our customers made, it was always very important for us, and you'll hear it from Adam that security is a team sport. And it was always important for us to be additive to the investments that our customers made.

And what we're hearing back is actually that privileged security is a foundational layer that complements the other investments they are making, whether it's in cloud security, their SOC through SAM tools, their network security, endpoint security. You can't have control over the IT kingdom without privileged security, and CyberArk is that core central layer that is protecting the sensitive infrastructure, the assets and the data of our customers, integrating and complementing and securing their other IT elements and information security layers.

Through continued innovation, we've created the most leadership and the most differentiated technology offering, from our core privileged account security, vaulting and aggressively rotating credentials so they're not known to a human and they're not static. Threat analytics is combined with that through our extension to the endpoint and capturing and protecting the attacks on privilege already at the endpoint to DevOps and applications, as I mentioned earlier, so the most robust and wide privileged account security platform. And delivering it through the journey that our customers are taking on premise, hybrid and cloud is central to our strategy.

And we augmented and are augmenting our R&D efforts with strategic M&A. And today, we're really proud to summarize that we've been very successful with the M&As that we've done today. We're standing here with very good experience of integrating them, keeping key talent and quickly introducing those acquisitions to market. We've taken a very strategic approach to enhance our offering to go -- we've done build-versus-buy analysis in order to see, how do we get faster to market to deliver value to our customers?

From a financial perspective, we see a couple of things. First of all, these acquisitions, if we take Viewfinity and Cybertinel, these acquisitions together form our endpoint privilege manager. They deliver more than 10% of our business. That solution is 10% of our business within 2 years after acquisition.

If we look at Conjur, which combined into our AIM solution and was acquired last year, AIM and Conjur in 2017 was 10% -- the combined was 10% of our business. And that combination was in 5 of our top 10 deals in 2017. And another financial element here is that we did this all through funding it through our own cash flow, all of these acquisitions funded through internally through our own cash flow.

As we look, we pioneered this space. And we're proud to stand here to be the pioneer and the market leader of privileged security. And we worked hard to get here, and we work hard all the time to open up big gaps and run fast. And so when we look at market leadership, we look at three aspects, leading from a market perspective, from a technology perspective and customer satisfaction.

So of course, on the market side, we've delivered a 5-year CAGR of 41%, delivered this significant growth, and we've done it globally. You'll hear from Ron later on. We go after this opportunity, and we go after it in a global fashion. We are the pioneer of the space, and our DNA is all about innovation. All through the years, we've innovated ahead of our competitors. We've coined every term in this space. We've coined every new element in the privileged security space, was coined by CyberArk.

And we did this in line. Well, you see the purple here. The attackers have been innovating and accelerating their attacks. And this is a visualization of some of the biggest data breaches out there. First of all, and I know some of the analysts are closing tracking here, we definitely see the big breaches and the scope continuing to scale. CyberArk has been innovating in line with that and putting a lot of efforts to be ahead of the attackers to secure our customers.

Some of the examples here. As golden ticket attacks came out, CyberArk came out with a solution to detect and prevent Kerberos-based attacks. We were the first to market with threat analytics to be able to analyze and find anomalies and to detect the attackers. Early on, we were the first to vault credentials and do it first for humans and then expanded to applications. And I'll leave some more here for Roy. But expect us to always be the ones investing in innovation and being the market leaders ahead of the curve.

Another very important element to me and to the CyberArk team is to deliver best-in-class customer satisfaction. As we scale, as we grow, as we work with customers in over 70 countries, we're seeing more than 90% renewal rates. More than a third of our customers come back to buy more from us each year. And we now have the most experienced professional services and customer support team on the planet in privileged security.

We have a dedicated customer success team -- you'll hear more about it from Ron -- that works to make sure that our customers are successful. We want them secure. We view this as a long-term partnership with our customers and invest a lot in it.

And we've also adopted a think-like-an-attacker mindset. And we trickle it through our team. We trickle it through our partners, where everything we do has to be definitely helping our customers comply with the various audit regulations but, first and foremost, helping them address the advanced attacks that are out there. And so how do we help them start and manage their privileged security programs in a way that best secures them and their company?

And as we look ahead, and Marianne will double click on this later on today, we're looking at a massive total available market opportunity for CyberArk for $44 billion. We've dissected this, looking at the greenfield new logo opportunities out there across verticals and across geographies and also the opportunity within our loyal and expanding customer base. And we're going after it with the CyberArk team, but also with more than 350 active channel partners that we have out there and also in partnership with 70 tech vendors that Adam will speak about later today.

So this is the exciting opportunity we're looking at. And the team will shed some more light on how we're doing it. So to move on to the next pillar of innovation and how we march ahead with continuing innovation, I'm excited to introduce our Senior Vice President of Product Management Roy Adar. Roy?

Roy Adar - *CyberArk Software Ltd. - SVP of Product Management*

Good morning, everyone. Pleasure being here. My name is Roy Adar. I'm Senior Vice President of Product Management for CyberArk. I've had the pleasure of joining CyberArk about 12 years ago and seeing the first set of customers adopting privileged account security for a long period of time. So I'll be happy to share some of that today.

So the 2 aspect, the 2 pillars that we will cover in this session, first, is to review why privileged account security continues to be a critical security layer and how that layer is evolving with modern architecture and modern enterprise. And also, we'll discuss our efforts and our activities and continual innovation on the product side.

So just quick overview of our products and technology. Basically, our solution is made of 3 parts, 3 components. The first one is the core privileged account security, which is I'll use the term the basics that many of our customers start with. In addition, there is the DevOps and application identity. And the third is the management of privilege on the endpoint.

Now our platform that runs this is designed to support all the infrastructure, all types of infrastructures that our customers are running, being on premise, cloud or hybrid. This is the more common recent infrastructure in most customers.

And when we designed the platform and built it, we designed it to meet scale, to be flexible to allow our customers to scale and grow with the solution. It was very important for us to also build the platform in a way that supports standards for integration. We believe very strongly in the team effort of securing customers. And therefore, we invest a lot in integrating with other security vendors and other security technologies.

It's also, of course, very important for us to invest in the security of the solution. These are the keys to the kingdom. This is something which is very important to secure in very effective ways. So this starts with the core digital vault patented technology, but the focus on securing the platform is something that goes through everything that we do.

Now finally, what we've been investing a lot recently is both in simplifying our solutions to allow customers to deploy faster and get the security benefits quicker, but also do that at lower cost of management and lower cost of ownership. And this is something we'll talk about.

So as Udi mentioned, innovation is really an important part of everything that we do. We invest a lot in bringing solutions to our customers in a proactive way, ahead of -- trying to stay ahead of the attackers and ahead of attacker trends. As Udi mentioned, several of the recent attack trends are things that we address, being the analytics and golden ticket detection.

But it's also more than that. It's also innovation that we invest in to allow our customers to innovate themselves. So when our customers want to adopt new and modern technologies, we want to be there with them to help them secure their environment as they adopt modern technologies.

So for example, when customers started adopting public cloud, we introduced solution to secure the cloud console and cloud access keys to again allow customers to adopt that with more controls and confidence.

One of the concerns that many of our customers raise before adopting new types of technologies is the concern around maintaining security and controls over the new assets and the new technologies. And therefore, it has been important for us to make sure we're there with our customers whenever new technologies are being adopted. So the public cloud and cloud consoles are one example.

The other one is the privileged account security for DevOps. Again, when customers are adopting DevOps and methodologies, we want to be there to help them secure their assets as they roll out the DevOps pipeline.

So innovation for us is really something that's coming from 2 main sources. The first one is a cybersecurity research team that continuously tracks trends in how attackers operate and continuously figures out how to provide security solutions for these attacks. But also, we are very close and keep very close with our customers and customer deployments to hear as early as possible, what are their needs, what are their planning, where are they going, what are they considering and how can we stay there and be the trusted partner for them to secure their adoption of new technologies?

Now overall, when we look at where we're investing our development and product resources, it's around 3 main categories. The first one is simplicity. Simplicity is really about allowing customers to adopt and deploy privileged account security in a faster way, more automated way, more cost-effective way, be able to secure more of the environment faster, again at better cost of ownership.

It's about being ready to secure them in their cloud and DevOps and SaaS effort, being able to provide the security controls to allow them to adopt these technologies and modern technologies going forward in a secured and controlled way.

And finally, it is very important to us and has always been very important for us to help organizations defend against sophisticated attackers. So if I look back 12 years ago when we started, many of the drivers for what was then the enterprise password vault was compliance, was operational efficiency. If you recall at the time, organizations had physical envelopes with passwords in them. And there was value in automating that process. So that's where demand started 12 years ago.

But in CyberArk, we always looked at this as really the security problem, as a vulnerability that it can be very easily exploited by malicious insiders or external attackers. So we always looked at this space as a critical security layer that organizations really should protect and secure. And that's been something we have been evangelizing over the years.

I think today it's much clearer. And we'll also hear from Shay Nahari in a few minutes from the attacker's point of view of why it's important. But to us, this has always been the key factor. And going forward, we'll continue investing in keeping up with attackers out there and helping organizations stay a step ahead of the attacker.

Now not too long ago, our customer environment looked mainly like this, on-premises infrastructure. The privileged actors were mainly the IT teams, IT admins or (inaudible), and applications that were developed by the organization.

But today, the new norm is a little different. As customers are adopting cloud technologies, the infrastructure is now no longer on premise. It's also in other places in the cloud. The way that applications are being developed today is also as if customers are adopting platform as a service technologies to build applications and DevOps methodologies to automate IT operations. And even when possible, customers prefer to consume applications as a service, so SaaS applications rather than developing their own, again having a little less control over the code and the application in securing of those assets.

Now the result of that is that the list of privileged actors grows. So it's not -- it's people first. So there are more people who are privileged actors in the modern enterprise. So it's not just the IT admins now. It's the DevOps teams. It's the developers. It's the SaaS admins, additional people. But also, it's additional applications and additional pieces of code that, due to the automation of IT operation and due to DevOps methodologies, now there's much more code application out there that is privileged and need to be secured and protected with privileged security controls.

So the reality for organization is that the modern enterprises have more privilege vulnerabilities or more vectors for attackers to come in and abuse their privilege, so more things that need to be protected by privileged security.

So our mission and our goal here is to make sure that we help our customers maintain control of privileged security in the environment, both in their current needs, but on an ongoing basis. As they continue to adopt modern technologies and modern methodologies, we want to help our customers secure that environment for privileges.

So how do we do that? What are we working on in order to achieve that? So as I mentioned before, 3 parts to the portfolio, and we'll cover that. There is the core privileged account security, the DevOps and application identity and privileged on the endpoint. So we'll touch each of those topics and see what we're doing and how we're helping our customers.

So for core privileged account security, one of the first and main efforts, and you've seen that in our end of Q4 release of Version 10, is a focus on simplifying the solutions, simplifying the platforms, allowing our customers to adopt privileged account security at scale in a more simple way, more automation, more simplified administration and so forth. We also simplified and streamlined the licensing model of the solution. And now organizations can get the core privileged account security products really using one line item.

Something we strongly believe in and have believed for a couple of years is that analytics and leveraging analytics technology is very effective and very important capability for privileged account security. Leveraging threat analytics allow organizations to get earlier visibility at attempts either by malicious insider or external attackers to go after and abuse privileged accounts. So we believe threat analytics is really a basic part of a privileged account security solution. And therefore, we are now including the privileged threat analytics as part of our core privileged account security solution.

And finally, the securing and support for cloud assets and cloud methodologies is something that we invested a lot in, in our core solution. We announced end of 2017 a new integration, lambda-based integration with AWS that allows organizations to automatically secure access keys to newly introduced assets running on AWS. And in general, the objective to automate the process of onboarding and securing privileged assets in the cloud is something that is very important to us in the core privileged account security.

Now as we mentioned before, it's not just people. It's also applications. So our DevOps and application secret management allows us to help secure the growing numbers of code and applications that is privileged and need to be secured.

So as a result of trends of adopting more automation and more IT operation automations and more DevOps technologies, there are many more things that used to be manual and today are automated and scripted. And those operations, those activities can be highly privileged and need to be secured in a different way. So we are investing a lot in both securing the automation of those solutions, but also allowing integration with the DevOps tools. And Adam will mention more later.

So for example, when we look at platform as a service and DevOps solutions, we invest in integrating and allowing customers to secure code together with adopting Jenkins, Dockers or Red Hat solutions and many others.

Now it's also very important -- when working with DevOps and the developer community, it's also very important to allow them to get started faster. So one of our decisions last year was to make the Conjur product available also in a community edition, so an open source edition. This allows development teams to adopt privileged security for their DevOps assets in a much quicker streamlined way with much more control of how they want to deploy and how they want to implement the solution in their environment, so really allowing them to get started faster and roll out a DevOps pipeline in a more secure way.

So finally, the third piece, managing privilege on the endpoint, this is a solution that is very important especially at the early stage of attacks. Many attacks start at the endpoint. I think it would be fair to say that most enterprises assume that endpoints will get compromised. There's a lot of investment, there's a lot of attempts to prevent that or to limit that ability of attackers to compromise an endpoint and get the foothold in the organization. But I think the working assumptions of most professionals we speak with is that the endpoints will get compromised. But in our view, it's really what happens next that is where there can be a lot of security impact.

So one of the main things we focus on in that area is to help organizations block an attacker's ability to do lateral movement once they compromise an endpoint. And the real -- and the key for that is really to limit or block access to the credentials that can be found and exploited on the endpoint, which actually enable attackers to move laterally across the organization. So blocking lateral movement on the endpoint is something which is a very effective way to help contain attackers who compromise the endpoint.

But it's more than that. So it's not just blocking the lateral movement. There are also things that are known best practices in the industry that, with the endpoint privilege manager, we help our customers automate. So for example, having list privilege management, an application controller or whitelisting are really known security best practices that are proven to be very effective at making it much harder for attackers to compromise the endpoint.

So although these best practices are known for a long time, list privilege and application control or whitelisting, although they're recommended as security best practice by many security analysts for years, the challenge has always been that it's just hard to deploy. It's hard to deploy at scale in organizations just because of the need for automation and flexibility when wanting to successfully deploy those technologies.

So with endpoint privilege manager and based on the Viewfinity acquisition, we're allowing customers to adopt those best practices, the list privilege and application control, in a much more streamlined and effective way. So they're getting better proactive controls. And in addition, we introduced the ability to help prevent credential abuse once an endpoint is compromised.

And finally, one of the benefits of this solution is that we provide an integrated view as part of the privileged account security solution that allows organizations to have controls on privilege access from the endpoint and all the way to all their datacenter assets in our solution.

Okay. So to wrap up this section, we covered the following. We talked about the importance of privileged account security as a critical security layer that continues evolving and growing with more privileged actors and more infrastructure that need to be secure, application credentials that need to be secure and modern technologies that our customers are adopting, where we help them secure and protect privilege across their environment.

Our objective in investing in innovation is really to help customers stay ahead of attackers and allow them both to protect against the latest threats on privileged security, but also to adopt modern technologies with more confidence, knowing that there are security controls that are available for them as they adopt the modern technology.

So with that, I want to thank you and invite Shay Nahari, Head of Red Team Services, to share more from the attacker's point of view.

Shay Nahari

Good morning, everyone. My name is Shay Nahari. I'm the Head of Red Team Services CyberArk. In this talk, I'm going to demonstrate why privileged security is a critical layer in every organization.

If you asked 10 people, what is Red Team, you're probably going to get 10 different answers. So I'm going to tell you how we at CyberArk see Red Team and how we practice both internally and externally with our customers.

We see Red Team as an adversary simulation which allows organizations to detect and respond to targeted attacks, all the way from detecting the breach, stopping the breach, investigating the breach and preventing future breaches. We look at both the people and the technology controls in organization.

The second goal is to allow organizations to tailor their solutions to attacks they would likely see in the real world. For prospects, it means help them identify their crown jewels, but more importantly the path attackers will take to those crown jewels. For existing customers, we help them better utilize CyberArk solutions they already have to real attacks.

Now I want to walk you through a real Red Team engagement we had with one of our customers, a big technology company at the time. To protect the innocent, let's call them Acme. Acme is a mature organization which invest multimillion dollars a year in various security products, all the way from perimeter defense to endpoint protection systems.

And Acme just migrated most of their crown jewels to their public cloud. They moved to DevOps methodology, starting pushing code directly to production. They already had their customer information in the cloud due to their SaaS business model. And they also had their financial and HR records stored on the cloud.

Acme approached us and wanted us to do a Red Team engagement, simulating an adversary trying to breach their cloud information or cloud infrastructure and gaining access to those crown jewels.

Now most of our engagements start as an assumed breach. As Roy said, you should assume something is already compromised and take it from there. However, Acme insisted on us starting from the outside. So like most attacks, we decided to go with phishing. We cloned their email portal and got a few of their employees to put their credentials into that phishing site. We then used those stolen credentials to get code execution on their machines through their Outlook profile. Once we gained access to Acme's network, the first thing we did was collect information from within the network, collect information like privileged accounts and who has what type of level within the organization.

Now I want to demonstrate the attack from that point on. On that endpoint that we compromised, the first thing we did was to dump the local credentials stored on that machine. That credential was shared with other machines in the network. That allowed us to move laterally to make that first jump to that second machine.

We compromised the secondary machine, an IT workstation, and repeated the process, dumping the credentials again. We then found a domain privileged account on this machine. Now in other on-premise organizations, that might be a game over because, at this point, we had the ability to compromise any other machine in the network and gain access to any crown jewels on premise. However, as we said, Acme just migrated most of their crown jewels to the cloud. So we needed to change the approach. We needed to find a way to pivot on that on-premise access that we already had to that cloud infrastructure.

So using our newly acquired domain privilege, we decided to go off of developers. We ran after a DevOps engineer and got our code execution on his box and gained control over the machine. Once we had access to his box, we found a remote connection tool used to connect a remote server. We also found a privileged account in a way of SSH key stored locally on the machine. We proceeded to take that SSH key and use it to connect to a single machine in that public cloud.

Quick recap, we now from our attacker machine connected through that command control server, through that compromised developer workstation to a single machine in the cloud. Now although we still did not have the crown jewels we were after, we've just successfully proven we can migrate, we can pivot on the on premise to the cloud infrastructure.

Now let's stop for a second and talk about cloud. There is a quote from Chris Hoff, which I think is currently the SVP of Cybersecurity Defense at Bank of America Merrill Lynch. And it says: If your security sucks now, you will be pleasantly surprised by the lack of change when you move to the cloud.

Let me tell you why. Cloud providers allow you to assign identity to machine. Those machines have privilege associated with them. So for example, if you would like to allow one of your servers to communicate with, let's say, a storage device, the way you go about doing that is you expand the right level of privilege to that machine, and it will be able to communicate with that storage device. Those privileges are stored as API keys, which is accessible and can be retrieved by any user with any sort of level of access to that machine.

It is your responsibility to make sure that you assign the right level of privileges to the identity of the server. Now with that piece of information, let's go back to our story. The next thing we did was to create a brand new account under the same cloud provider as Acme. We then used our access to that single machine to retrieve those APIs I was just telling you about. Unfortunately for Acme, those API keys had full control over the environment.

We proceed to take those API keys and make backups of every single server Acme owns, 175 servers to be exact. And we took those copies and attached them to our account. We now had access to every piece of information stored on that server, intellectual properties, customer data, financial records.

The worst part was that Acme didn't even know their entire cloud infrastructure got stolen because we didn't access all of those servers. We accessed a single server, retrieved that API and used that API to make a copy of their environment.

Looking back at what Roy showed us, look at any infrastructure and see all the places that we the attackers used privilege to compromise the organization. The first, we compromised a workstation. We used privilege to credentials that we'd gotten through phishing. Once we gained that initial access, we dumped credentials on machine. We used local account to make that initial lateral movement, repeated the process until we found a domain-wide privileged account. We used that privileged account to make the jump to that public cloud and used the cloud proprietary API to copy the environment.

Looking at the same design, let's look at what the defender could have done in order to mitigate the attack. So first on the endpoint, even assuming attacker will get some sort of code execution on the machine, defender needs to ensure that, 1, the user or attacker in that point doesn't have local admin privilege on that machine, the list privilege approach that Roy talked about, and 2, that the attacker is not able to steal credentials already on the box, ensuring properly managing credentials even at the endpoint level.

Next, ensure that organizations don't use shared privileged accounts within the infrastructure, preventing that first lateral movement that attackers make. And that very sensitive information, very sensitive privileged account, especially one used to access cloud infrastructure, whether it's directly to servers, to management portal or even pushing code to production, those API keys are not stored locally on the user machine.

So some of the trends we see in 2018 and beyond. The first one is the threat landscape, the rise of cryptominers. Cryptominers will likely replace ransomware as the main attack stream for attackers. It simply gives them more bang for their buck. More infections immediately means more monetary gain for the attackers. Different payloads, same path and execution method, privilege will continue to be used to distribute those payloads.

The second one is hybrid model. This is not new. We've been seeing organizations doing that in the last couple of years. Organizations will continue to do that through 2018 and beyond, expanding to cloud while maintaining presence on the on premise.

For some of the talks we had with both prospects and customers, we see a lot of organizations treat their cloud infrastructure as a separate entity, as something that the vendor needs to take care. Organizations need to start looking at those infrastructure as an extension of their own on premise and apply the same methodologies and tools to secure those resources as they use for their own on-premise infrastructure.

And that matches what cloud providers have been saying for years, right, that shared responsibility model, where it is the cloud infrastructure vendor responsibility to give you that infrastructure and tools to manage that infrastructure. However, it is your responsibility to secure the data that you put on it. That's your data. You need to secure it.

The third one is privilege. Privilege will continue to play a role, a critical role in nearly every attack scenario out there. Whether it's distribution of malicious payload or bots like cryptominers or ransomware, stealing proprietary information from customers or exfiltrating sensitive information, like PCI or PHI data, or plain old money grab, transferring money out of company accounts, attackers will always look for privilege to execute those attacks.

Thank you. Now I'd like to welcome up Marianne Budnik, our Chief Marketing Officer, which will discuss privileged security with 4 of our customers.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Thank you very much. Okay. Come up and join me? Are we on? Okay. While the panel's getting seated, first of all, thank you, all, for joining us this morning. We really appreciate the time that each of you are investing to get to know this market of privileged security better, to understand how this market is expanding as the threat landscape is expanding. And I think we've really put together an agenda today that lets you hear from the CyberArk experts, but equally important to hear from our customers.

So each quarter when we talk, we get questions from you on a variety of topics. One of the questions that we get frequently is, how is CyberArk doing across different industries, right? Is privileged security really a critical layer of technology for all industries? So again, we're pleased today to have customer representatives from 4 different industries here with us today.

We also get questions about, what is the journey like for an organization, right? Where do they start? How do their environments grow and expand over time as their organization grows and expands? And so we've got customers with us that also are going to talk about where they're at and hopefully give you better insight into what the journey is like, where people get started, how they grow and expand over time and give you insight into how that maps to the expanding CyberArk portfolio. Okay?

So with that, what I'd like to start by doing is giving each of our panelists an opportunity to first introduce yourselves, tell us a little bit about your history, where you start with CyberArk, just a brief introduction. That would be great.

Everardo Trujillo

Can you guys hear me fine?

Marianne Budnik - *CyberArk Software Ltd. - CMO*

We can. And I think, Eve, we're going to have you and Dipak switch seats so that everyone in the audience can see.

Dipak Rath

We don't look like each other.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Got it? Okay. Dipak's up first.

Dipak Rath

Hey, guys. Good morning. My name is Dipak Rath. I'm responsible for Security Operations at Home Depot, been with Home Depot for good bit of 3.5, 4 years. My security career started 15 years ago in the retail industry as well. Currently, I'm responsible for security operations, which absolutely encompasses privileged access management -- can you hear me? All right -- encompasses CyberArk, particularly the journey with CyberArk, which I'm going to dive a little bit into, started 4 years ago. And we are at a very mature state of CyberArk. I'm happy to be here. Thank you.

Everardo Trujillo

Hi, everyone. I'm Eve Trujillo. Eve's short for Everardo. A lot of people cannot pronounce my name. I'm currently Cybersecurity Operations Manager for Sempra Energy Utilities. We have -- so includes our corporate office, Sempra Energy Corporate. We're a shared service, or my team is. Also, we have San Diego Gas Electric in San Diego and SoCalGas, which is up in LA.

I've been with the company 15 years on and off. I say that because I left twice and came back. My career started in cybersecurity officially in want to say 2003. Unofficially, I was doing a bunch of hacking with the white hat side of it since I can remember in college, have held down many positions through the years and part of in the cybersecurity pen testing, architecture, et cetera, so in a nutshell.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Don?

Donald Welch

Hi. I'm Don Welch. I'm the CISO at Penn State University. I think the interesting thing to keep in mind about universities is that we have almost every kind of compliance requirement that any company has. We have an airport. We have a nuclear reactor. We have retail operations. We have health system, etc. So that keeps me fairly busy.

I started getting into cybersecurity when I was still in the Army and a professor at West Point. And over beer, of course, friends and I determined that West Point really started -- need to teach cybersecurity. And so we got the program going. I've spent some time in retail. I ran an IT and network services company and have been a CISO twice, once at the University of Michigan, where we first expanded our implementation of CyberArk, and then most recently with Penn State, where I have brought CyberArk to Penn State University.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Thank you.

John R. Rogers - *American Financial Group, Inc. - Chief Information Security Officer & Divisional VP*

And I'm JD Rogers. I'm the CISO of American Financial Group. So our company is a financial and insurance, specialty insurance company. So as we were talking about the university has a lot of diversity, we also have a very decentralized organization. So we're made up of about 36 different business units that all run kind of like their own company. So I have to deal with 15 IT organizations and 8 CIOs within my company.

And I started there about 10 years ago, was brought in to build security program for the annuity financial side of the business, built that up. CyberArk was actually one of the first tools that I brought in with that venture. And in late 2013, early 2014, we created an enterprise security group that I was asked to lead for the whole company. It's really the first of its kind for our company. We don't do centralized hardly anything. So I was brought to standardize security across the entire enterprise. And again, CyberArk was a key tool to achieve our mission across the company.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Right, well, thank you, again, for being here. Dipak, let's start with you. So 2014 really was a year that I think broadly in the retail industry saw concerns around security at point of sale and others. And in that environment, you joined the Home Depot in 2014. And I think you've talked about a few things. You've talked about how you're able to very quickly make significant gains in your security posture between 2014 and 2015 and how, since then, you've gone on to really expand the security footprint of the organization, etc. So it'll be great if you could take us sort of through that journey.

Dipak Rath

Sure. And it's a journey which will continue, right? There's no finish line to this journey. But as you rightfully said, 2014 is went we truly started a privileged access management program in earnest along with others. I don't think I need this other mic. All right.

When we embarked on this journey for privileged access management, it was very clear to us that we had to do something about the credentials and especially the privileged credentials and have a complete management and control of those.

We were very clear on what we wanted to achieve. We were clear on that there is no single technical control which can solve all the problems for us. And how do we integrate CyberArk and the different controls it provides, the rich control it provides with controls coming from our network, our firewalls or our directory services?

For us, the key requirements were, one, is to have network isolation. That is to not allow, even if there is a compromise in privileged account, to not allow the lateral movement, and funneling all our privileged sessions, which had various IT admins gaining to datacenters and so on, so forth, funneling it through more control and a centralized access management control such as CyberArk. That was our first requirement.

The second requirement was to be able to have stronger authentication at the very frontend of access, right, so having 2-factor authentication integration with whatever tool that we picked at that time was key to what our requirement was.

The third was to be able to walled privilege accounts and rotate those credentials as soon after use so that you have a randomized set of credentials across your IT landscape, makes it much, much harder for the bad guys to -- even if they compromise one system or an endpoint, to be able to move laterally in the datacenter.

The fourth one was -- for us, was to make sure that we have very enhanced monitoring and session recording capability. This would come hand in hand in forensic investigations, so on, so forth.

And last but not the least is to be able to dynamically retrieve credentials as applications need them and not to have the need for our partners, our customers, that's what we call in the retail space, to have hardcoded credentials in scripts and so on, so forth.

When we look out in the market and we evaluated CyberArk, we essentially were very impressed with the rich portfolio of capabilities CyberArk provided. There are 4 things that we looked at, product capability. Second is the ease of deployment and integration. The third is the service and the support quality. And the last but not the least is flexibility in contract and pricing negotiations. And we were pretty clear that it's going to be CyberArk for us.

We've come a long way. It's a journey, an endless journey sometimes. It feels that way. But starting off with early wins and starting off with, first and foremost, understanding what's the current state of your threat landscape in terms of privileged credentials, building up on that and just taking control of the most important highly privileged accounts, in the Windows world, it would be the administrative account, or in the Linux world, it'd be the root account, taking charge of those and having a good control because 9 out of 10 times, the bad guys, the threat actors or the adversaries are going -- they're looking for those kind of accounts.

And then building up on that and having more session management, jump access, providing the isolation from your sort of lesser trusted environment, the campuses or the offices and so on, so forth, to the more trusted environment, your datacenter, and then building up on having better and better integration with the rest of the security tools.

So you don't want to have a tool that you bring in and you just slap it in and without having proper integration from a lifecycle management, better integration with [SIM] tools, better integration with identity and access management tools. And the journey continues for us into the cloud. The march to the cloud for Home Depot has started. And we want to take these technical controls to the cloud. So that was kind of from the beginning to where we are today.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. So what Dipak talks about, Ron is going to speak later this morning about our go-to-market model, and Josh is going to talk a little bit about cohort analysis. But one of the things we're most proud of is the initial program that we launched with prospects, which we refer to as our 30-day sprint.

And I think many of you have seen the publications we have on the 30-day sprint and how CSOs leverage a quick engagement with CyberArk to identify, right, those highest value assets, the crown jewels, right, where they exist throughout the organization, how we work with organizations to rapidly enhance the security posture and to really get the most value most quickly and then from that deploy a series of expansion portfolio over time, but excellent.

And I think, as we talk about it, Roy just spoke a little bit about, right, the cloud and DevOps and the future. And I think we've talked about 2018 being the year of Home Depot moving to the cloud, right, so looking at different aspects of the portfolio. And what do you have in the cloud right now? You're moving -- you've got certain applications that are in the cloud. And I think this year that's sort of the next phase of the journey within Home Depot.

Dipak Rath

That's correct. And I think the march to the cloud has begun. We've identified what are the critical applications we want to bring to the Cloud as well. We always look at hybrid models from an operational resiliency perspective. And I'm thrilled to learn more and more on the roadmap of CyberArk in terms of native capabilities. And that would be very interesting to explore and perhaps implement.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. All right. Well, thank you for being with us. Eve, Sempra Energy, could you talk a little bit about that for us?

Everardo Trujillo

So the journey, like you saw before, the attackers are looking for those, the root access, right, or the privileged access. In the hacker community, back in my users when I was started -- got root was one of the things, right?

So for us or for a cybersecurity, information security professional, in a utility, which I don't know if you guys are familiar, but things tend to move slower in huge companies. We have our operational technology, which is our SCADA, which controls actual things in the field, right? So we have breakers and all those sorts of controlled network.

So for us, when we were looking at privileged access management, we also did an RFP. So we did a bakeoff, and as well, we were very impressed with what CyberArk had to offer. And this was back in 2013.

So it's a journey that has no end. I agree with you. And it's been very interesting because our whole goal is to make sure that those accounts are managed. When I say those accounts, I mean the privileged accounts, right? So being in a utility, you have to go in phases because many people, many sys admins have been there for years, sometimes decades, and they're not very accustomed to change.

So we started with small wins. We were looking at privileged accounts for service accounts, so machine to machine. We have requirements within our environment to rotate those passwords, and the complexity of the passwords are pretty big. And we rotate those passwords annually. So we focus, for example, on the databases, applications, connect to databases sometimes. Developers hard code those into their code and things like that. So we've leveraged CyberArk to get away from that.

It was a huge win for IT folks and for us because now you have CyberArk -- we started with the vault -- taking care of those passwords for them and instead of investing -- I don't know -- 80 man hours to change all their passwords on an annual basis. Now they don't have to worry about that. So that was a great win. And we slowly have moved into other phases. And so we started expanding shared accounts within our IT environment. And it's been a process that has improved our efficiency overall operationally.

And then moving forward, we're looking at local admin passwords on our endpoints. That's one of the things, one of the requirements from our IT support is, when they're offline and/or they have to log on remotely, they need a local password, local admin password. And that's where we've been leveraging CyberArk to also manage those for us instead of having our support team get sometimes their trusted partner have that password. Now we have it in CyberArk, but no one knows the password but CyberArk. So that's been a few wins for us. But we still have a lot to do. CyberArk has been actually one -- a tool that we've been using that has been -- given us a lot of success.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Excellent. And again, when we talk about use cases, I think the role of third-party vendors is one, again, from a threat landscape perspective and the exposure raised by third parties given access to the network and access to operate, I think that's an area we've discussed. You've had particularly leveraged CyberArk.

Everardo Trujillo

Yes, so utilities, right, we have a large footprint. We have many systems. We have many trusted vendors. So Siemens is one. We have SCL. They're all industrial control systems. And they're the experts on their systems. At times, we don't have operators that have the skillset.

So what'll end up happening is we have trusted partners come in and manage those systems for us with privileged access, right? So obviously, there's a lot of -- in my mind as a paranoid security guy, the threat is, if they're compromised, now they have a direct connection into us. We've seen that before. And it's just one of those things where it just makes sense to have them use a tool like this to manage those credentials.

Again, it's an uphill battle, but having the top down executive support, we have our CISO, our new CISO just joined I think 6 months ago. And he has been an advocate for this. He knows what the threat is. And everyone on our team, leveraging our top executive support, we've been slowly moving towards that. At least every single new vendor that we're bringing on, we're making them -- we're not making them. We're having them come through CyberArk. And we're just looking at the rest of them and making sure that they're doing that as well.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Perfect. Thank you. Don, so you have a long, very successful career in cybersecurity. But you've been at Penn State now for just over a year. So I'd love to -- you've worked with CyberArk before. But I think if you could help share a little bit about coming new into a very complex, diverse organization and just talking a little bit about to start, right, how you assess the opportunity and how you assess the needs of the organization and where you got started, would be great.

Donald Welch

Sure. Yes, so universities, to be great, the faculty needs to have a lot of autonomy to be able to innovate, to be able to push the bounds of research and be able to come up with better ways to teach students to serve the community.

All those kinds of things are the things that make me pull my hair out, right, because I want control. I want uniformity. I want a standard that makes security easy. So understanding how to adequately protect the university while not hindering the mission was critical.

So we identified those systems that I think are high risk to the institution where, if there is a compromise, there's serious fines, there's damage to community members, there's reputational damage, there's the potential loss of research funding, all those kinds of things that would really have a large negative impact on the university.

As I came in, Penn State had had a pretty public damaging breach. A couple of years before, they'd had trouble hiring a CISO. But because they'd had this large breach, and I know they put a lot of money into it, I was expecting a much easier transition. What I found is, without some strategic thinking about spend on security products, that we had spent a lot of money, but really still had a lot more risk than the university could tolerate and a lot more that I was surprised on.

So after a fairly quick assessment, I had 4 initiatives that needed to be funded and put into place right away. And one of them was privileged access management. So I would dispute some of the data that was put up here earlier saying 80% of attacks involve privilege management. I would say, of those attacks that are really going to cause strategic damage to an institution, I would say almost 100% requires some amount of access to privileged accounts. At least in my experience, every one that I have seen have used privileged accounts.

So getting privileged access management was absolutely vital. We started that almost right away. We being a public university, we went through the RFP process. Even though I was very happy with CyberArk, I let the team make the choice. And they came up with CyberArk as the best solution.

I think critical is obviously protecting those privileged amounts -- excuse me, accounts. But at Penn State University, we deal with about 14 million events per day. So the key is to bring all those into some type of a tool where they can be analyzed and we can prioritize where we spend our time investigating so that we can find these attacks before real damage is done.

So the analytics part and the monitoring the behavior of our system administrators on top of the privileged access management was really critical to our strategy to be able to bring this information in, correlate it with other indicators of compromise and hopefully protect the institution.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Thank you very much for that. All right. And then, JD, I think you win the award for I think longest customer on the panel. So American Financial Group started working with CyberArk I think in 2009. And so we're going to have you take us through that journey.

But what I really think is exciting about American Financial Group is, like most organizations out there, you're going through this digital transformation right now, right? And I think you're all aware we acquired Conjur the midpoint of 2017 really to help organizations who are on that journey for digital transformation to work with their developers and to help enable top line revenue growth. And it really is sort of the next frontier where we're moving. So love to have you take us through your journey and talk about that aspect in particular.

John R. Rogers - *American Financial Group, Inc. - Chief Information Security Officer & Divisional VP*

Sure. Yes, before I get to Conjur and that, I'll kind of start in the beginning because it lays the foundation of trust in the tool and the technology. So yes, I came into American Financial Group in 2008. So one of the first things I did was bring CyberArk in for our financial division.

Again, privileged access management is a key. I agree. I think 100% of the true compromises deal with privileged account takeover. So it was really kind of a no-brainer, get this foundation in. And so we brought it in, in 2009, very successful implementation within the financial division of my company. And CyberArk was a -- has been a great partner the whole time.

One of the things that made us really successful is the partnership of coming in and help us solving problems, not wanting to I'll call it nickel and dime us every time we had a question. You really just partnered with us to help us achieve our goals and put the solution out there.

So that worked great. When our -- my group was formed, at the enterprise level, like I mentioned before, we have 15 IT organizations that are used to doing everything independently. So all of a sudden, this big monster came in from the top that was going to -- they were all afraid -- tell us what to do and take over everything. And so my directive was to standardize security, but do it in a -- they coined the term collaborative execution. So I had to get everybody's buy-in but still execute on the things that needed to be done.

So one of the things right out of the gate that I knew would be an easy win and a value add for everyone was to implement CyberArk across the entire organization. I knew they had problems. A lot of the IT groups were failing regulatory compliance things. A lot of the pen tests that we were doing they were failing because of privilege -- lack of privilege management.

So it was a simple win that I could come in and say: Here's a tool. We'll implement it. Look how easy it is. And it worked great. So it built a foundation of trust as we rolled this out across the enterprise to take over those administrative, those root accounts that have been talked about. People were actually excited about it. So we could offer this solution for them.

There's always a little bit of IT -- whenever you have to change their processes, there's a little pushback on, what's this going to do to me? But as we identified kind of what I'll call evangelists in each area to educate them and send them back into their groups, and it worked out really well. So we built a lot of trust. We got a lot of credit from them. They started passing compliance checks. They started passing penetration tests better. So we really got the buy-in that was great.

And so it is a journey. I mean, there's always more and more things. Some of the groups are further along than others. But as they got their hands on the tool, we even did a little bit of a I'll call it a dog and pony. We had -- again, CyberArk partnered with us, came in, did a demo to our IT groups of here's everything the tool can do. This is what we've rolled out so far. But this is everything it can do. They actually got really excited about it and started coming to us saying: Hey, I want to use this feature. Can I do this for my application development? I want to take advantage of some of these things. So it pushed our roadmap faster than we expected, but it was all good.

And then most recently, to your point on Conjur and the digital transformation, Dev stuff is changing with our organization. It's changing, faster speed. Some of the stats that were thrown up there, everyone wants to go faster with their DevOps, and we're no different. And so there was a large initiative to experiment with true DevOps containerization, development, the whole 9, extreme paired programming, all these new things and changes.

So there was a project that was slated to take I think it was 18 to 19 months. According to the DevOps methodology, they could do it in 4 months. So when you start talking that type of savings and cost, the business listens, and they want it.

And so the timing was perfect with CyberArk's acquisition of Conjur because I knew -- from what I'd seen, this was going to be successful, and I knew it would take off like wildfire. So I wanted to get in early to build security into this new thing that was growing within our organization before it took a side step, and then I had to come in later and pull it all back and try to secure it.

So the timing was perfect. We partnered with them and right out of the gate to see how we could implement this in. And what was nice is that it's the same problem. Just because everything's changing, the technology's changing doesn't mean -- it's still the same problem. You have credentials. The way everything work is you've got to log into something. And someone needs to manage those credentials. So just because there's new cool talk terms like containerization and microservices, it's all the same thing. It's just a little bit different.

So they had the problem of, what do I do with these credentials? How do I spin up all these containers very fast? And obviously, given to their own devices, they'll just -- well, let's just use the same password on all of them and spin it all up really fast, and which is great for them. It's horrible for us from a security standpoint.

So we were able to come in with Conjur and some of the AIM technology and really partner with them and solve it in a way that, again, helped them see the value. I always want to come in and not be the security hammer telling them: I'm going to slow your life down, and I'm going to make this -- I want to come in and add value and say: I want to make your life easier and more secure. And we were able to do that with Conjur and AIM. And so it alleviated a problem that they were trying to solve on their own.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent.

John R. Rogers - *American Financial Group, Inc. - Chief Information Security Officer & Divisional VP*

And we were very early in that process, but it is proving itself out.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Thanks for sharing that with us. I think common theme that's come through here is operational efficiencies, right? So in addition to CyberArk obviously takes very much a security first focused approach. But think one of the things that came through I think independently from each of you was this focus not just on having a security-first approach to secure the enterprise, secure the organization, but the operational efficiency that you've been able to drive through your teams.

Excellent. One other thing that comes to mind, we've touched a little bit on this, or each of you did, but when we talk about drivers for this initiative, we talked about security first. We also talk about compliance. So it would be really interesting for me to hear. Maybe each of you can talk a little bit about that dynamic within your organizations, right?

How much is your focus on privileged security driven by compliance versus how much is your focus on privileged security really driven by the security needs of the organization and what that dynamic -- you're each in different industries. You each face different regulatory requirements. Maybe we could kind of go down the line and have each of you spend a couple of minutes talking about that compliance versus security aspect.

Dipak Rath

Starting with me?

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Starting with you.

Dipak Rath

Yes, so drivers for us clearly, we looked at compliance and being compliant with the different external/internal regulations that we're subjected to is essentially a byproduct of doing the right thing. And that's one of the core values of Home Depot as well, doing the right thing.

We looked at it from the -- so let me start with the benefits we've gotten out of the program. And those have absolutely aligned with what we had intended as drivers from the get go of the program. First and foremost, our resilience to be able to prevent or protect ourselves from pretty typical post-exploit activities, such as credential tests or privilege escalation or lateral movement. And so these are the basic parts of advanced security attack anatomy.

We have seen that that has positioned ourselves, improved our responsiveness to incidents along those lines. I know some of the metrics that we measure on our -- we really looked at the incidents that we encounter or anomalies that we detect in our systems and see how the controls that we put in place using this tool have prevented from full-blown incidents and so on, so forth.

The second one you alluded to is operational efficiency. The fact that we have a single sort of funnel into our more highly valued assets in the datacenter, we have a better way of monitoring and controlling that access point, not from the point of security, but also from the point of operations.

So if we have any incidents where we have experienced some outages, not necessarily in CyberArk's system, but anything which is behind CyberArk, we have a better way of doing root cause analysis, better way of identifying what may have caused the issue and consequently restoring services without a major impact to the business. So that's the operational resilience part of it, worked out really well for us. Traditionally, we looked at MTD or RTO, SLAs. And we've tracked very well and improved with -- as a result of implementing this solution.

Thirdly, we have the video recordings. We record pretty much all the video we can, particularly on the Windows side of the house. On the Linux side of the house, we have keystroke loggers and so on, so forth. And they come out to be very handy in terms of completing a forensic investigation. So that has worked out very well for us.

Last but not the least is cost reduction. We used to spend ungodly hours in terms of managing and rotating the passwords as per compliance subject to the PCI in our space. But having a tool like this has significantly reduced the laborious, labor-intensive effort or process and has pretty much automated all of it. And as a result, we are able to produce the compliance report in a much faster way.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Great. And you talked -- I think you just touched on SLA. So you talked about levels of SLA. I think we were talking earlier. You were talking about where CyberArk fits in that sort of hierarchy of things that relates to SLAs.

Dipak Rath

Certainly. Various organizations have a different way of sort of associating the criticality of the services they provide. In our space, we start with the platinum-grade SLA, which is having the least amount of downtime that the company can endure or tolerate.

CyberArk in our organization is at the platinum-level SLA. We have used quite a bit of architectural and full-tolerant and load balancing capability of the tool. And we've taken it to the Nth level. All our access to our datacenter is all funneled through the tool, the infrastructure. We are a brick-and-mortar store. Our company, we've got 2,200 stores across North America. Each one of our store is sort of a mini-datacenter. So any compute which takes place in -- whether it's in a store or a datacenter comes through the infrastructure today.

Heavily used PSM and PSMP. Those are the privileged session manager and privileged session manager proxy by CyberArk. One of the things I'll point out, the PSM, as we embarked on this journey 2 years ago, it was in a very nascent stage of its evolution, PSMP that is. And CyberArk has partnered very well, all the way to the leadership level, to help us achieve that goal of bringing scale. And at the early stages, there was some concern about scale and so on, so forth. But the team has worked very closely with us, the R&D team and the professional services team, to help us get it to the stage where we can say proudly that it is a platinum-level SLA service that we provide in the organization.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

That's great. I think, certainly, being able to deliver platinum-level SLA at extraordinary scale is one of the things that we think of as a strong differentiator for CyberArk. Great. Thank you.

Dipak Rath

Thank you.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Eve, energy, utilities, highly regulated environment.

Everardo Trujillo

Yes, very highly regulated.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

How does that fit with your security-first approach?

Everardo Trujillo

Well, so if you don't know -- in case you don't know, NERC CIP regulations, they're very heavily regulated, right? One of the key drivers is obviously -- that regulation, we also have SOX compliance to deal with. But for NERC CIP, if there's any violations, it can be up to $1 million per incident per day. So if you have five minutes in one day, that could be up to $5 million. And recently, one of the utilities was fined. And it was a $2.7 million fine. So obviously, that's one of the things that we're focused on.

In my personal opinion, being compliant does not make you secure. It's having best security practices that actually makes you compliant. With that mindset, within our company, we established a cybersecurity framework, NIST 800-53, which if you guys don't know what that is, it's actually standards which dictate how to do cybersecurity.

So thinking about, for example, first, I'll go into a SOX use case. So we have third-party vendors coming in giving support to our SAP systems. There's potential there for violation. So obviously, when we look at our NIST 800-53, there are families of controls. One of the controls is access control. So there's a bunch of things that you need to do to comply with that, right?

So for us, having CyberArk, just kind of we're done with that. It takes care of your password strength, your access controls, your privileged access. It gives you forensics. It gives you logging, the recording session. It has been well done for us. It's -- when you go back, if there's any incidents, you can do your forensics.

Then you have the NERC CIP side of the house. And same thing, it's -- I have a little bit of issues with the NERC CIP compliance and the regulations because, for example, some of the wording in there is: You need to put these controls in where technically feasible. What does that mean? That's kind of like a loophole for me. So if you have an audit and say: Well, it wasn't technically feasible for us to do this, and you can probably provide background for that. But for us, it's not an option.

And same thing for our transmission and our distribution systems within Sempra. Obviously, our utilities, we're talking about public safety here. Obviously, there's the financial penalty, but there's also public safety, right, if you don't have electricity, your hospitals, military bases, schools and whatnot.

So and just last week, we deployed a separate instance of CyberArk into our NERC CIP environment. So that's our transmission, which obviously is a great tool because it provides evidence for us to be compliant. So it's a great tool for us as in we do have an audit coming up in September. And that's where you can get penalized if you don't have certain things. And I can just say, for access controls, we're good because we do have CyberArk in place, which also provides the proper evidence to our auditors to ensure that we're doing the access control part of it.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Great. So check all the compliance boxes, but at the end of the day, it's about the bigger things, public safety, security, etc., that really drives your mission.

Everardo Trujillo

Correct.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Absolutely. Excellent. Don.

Donald Welch

Yes, so security and compliance sometimes overlap, which can be helpful. Compliance is a real risk for the institution. And things like personal health information, the compliance failure can result in a serious fine or potentially worse, but I don't think it would be just for an exposure without an actual loss of information.

But especially for us, we've got so many compliance requirements to deal with that, if we're secure and don't have a breach, then it's less likely anyone's going to dig into our compliance. And like Everardo had said, the -- I lost my point, sorry, that you were going to say there.

But the idea is, with the -- if you can secure and understand when an attack is happening before damage is done, then you are much less likely to get in trouble with compliance and much less likely that someone is going to investigate. And if you've made the kind of mitigation decision that he was talking about earlier in terms of interpreting the compliance, if you don't have a successful attack, it's much more likely that you'll be able to defend that.

If there is a successful breach, then a lot of people will question your mitigation decisions. So that balance between security and compliance is important. You have to meet those compliance requirements. But ultimately, it's the security. And as I said, I think privileged access management is foundational. If you're not doing it and you're not monitoring and you don't understand the behavior of those accounts, then I think you've got a big hole in your strategy.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Thanks. Thank you, Don. JD?

John R. Rogers - *American Financial Group, Inc. - Chief Information Security Officer & Divisional VP*

Yes, I agree. It is nice. I think of security and compliance kind of like a Venn diagram, and there's some overlap. But definitely, if you're compliant, you're not secure. And sadly, in some cases, if you're secure, you're not necessarily compliant.

But I try to drive my security much like these guys. Our program is I want to build -- we have a risk appetite for our company. And I want to make sure we meet that risk appetite. So we deploy tools and technologies and processes that, first and foremost, secure our environment. And then along the way, so far, we've been able to meet compliance. And CyberArk is one of those tools.

And we do have a lot of different compliance. We have SEC regs, all the insurance regs from different states. The New York DFS just came out. We have -- we're global. So we have GDPR. And we're in Singapore. So we have Singapore MAS and all this other stuff. And so CyberArk does play a key role to check off just a lot of that foundational compliance boxes for us. And our internal audit group loves it because it gives them all the information they need in a nice format for them to validate and check off. So it actually saves them time. They loved it when we standardized the tool across the whole enterprise globally. It saved them a lot of time in their compliance work.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Great. Thank you.

Everardo Trujillo

Can I make one more comment?

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Absolutely.

Everardo Trujillo

One of the other drivers for us, I don't know if you guys were familiar with -- in 2015, December 2015, there was an incident in Ukraine, where there was an outage of 250,000 customers without electricity or gas in the middle of the winter. I think it was only -- but it was the very first incident where it was a cyberattack.

So a year after that, NERC -- we're regulated under NERC -- had all the utilities in the US do a tabletop exercise to mimic what happened after the forensics had happened. And we sat down with our stakeholders, our -- everyone in our response team to go through that exercise. And if you remember, the gentleman that was doing the lateral moves, the privileged account, so obviously, that went -- it took it to the cloud. In this instance, that lateral move in those privileged account took them to the SCADA network, to the control network.

And at that point, the operators that were controlling the actual industrial control systems, they were locked out. They were actually literally watching their screen turn off systems, and those systems were -- and long story short, when we did do that exercise, we're like: Okay. Obviously, we know that they harvested credentials. It came out of memory.

For us, our assumption is that the attacker is already inside. You have to operate that way and that they already have those credentials harvested. So how do you stop them? And one of the things that came to mind is multifactor authentication. And obviously, CyberArk provided that for us. And that's why we're -- that driver to implement CyberArk in our transmission system. That was just one of the other drivers I wanted to mention.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. Thank you for mentioning that. I want to also -- JD, you mentioned GDPR. So we get questions frequently about how GDPR is factoring into our business. And frequently, we get asked that question in the context of EMEA, where certainly it's a European regulation, and certainly, it focuses the EMEA geography, but equally so in the Americas and other geographies, right? So think it's interesting to note GDPR and the influence that GDPR is having on organizations based in the US as well.

Okay. All right. Last question, I think final comments from folks. And I think, Eve, this keys off the point that you just made, which is you have a broad security portfolio. Everyone in this room is thinking about, how does privilege fit into the broad landscape of security and the investments broadly that you're making in securing your organization? And so given the landscape of the tools at your disposal, just sort of in closing, I'd love it if each of you could comment on the role that privilege plays and how privilege fits into and CyberArk fits into your security portfolio.

Dipak Rath

Defense in depth, it's a well-known principle, security principle. Many organizations already appreciate what that stands for and have implemented in earnest. And so we have in our organization defense in depth. The adversaries are going for something of value in our particular case. Various industries would have a different motivation from what their adversaries -- in our particular case, they're going for something of value which would fetch them some money in the black market.

So data is the key. That's the soft belly of the beast. And so you sort of start from the data protection side of the house, ensuring your data is encrypted in rest. In transit, you have some activating monitoring going on in terms of DLP, data loss prevention, things of that nature.

Overlaying on that is you have your privilege access, privilege access management. How are they getting to the data, right? So having investments done in CyberArk and having that as, if you will, concentric circles, just outside the data protection is the privilege access management. So we've made investment in that space as well.

And we have very well integrated between those 2 sort of technical controls. And if you go further out in the defense in depth, you're looking at endpoint security. And Roy mentioned about the tool that they have in endpoint security. So that's where -- basically where it all starts, zombie setup workstations as servers, privilege escalation, and they're getting into the data.

So proper investment in that space as well and having proper integration of intelligence between what's going on, on the endpoint with what's going on with the privilege access and then ultimately what's going on in data exfiltration from a DLP perspective.

And then you go further out, and you have your perimeter and your network security. So tying it to your firewall and tying it altogether, it's not easy. It's absolutely not easy. There are so many different technologies. And oftentimes, they play together well. Sometimes, they don't. But having integrated sort of defense in depth kind of view in terms of what the motivation is of the adversaries and how you're able to improve your event detection and anomaly detection, that's the key. So it's just -- again, just slapping the tool and expecting that you have a secure environment is pretty naive.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Thanks. Eve, you started by saying you assume they're in. You assume the attackers are in. What role does privilege play?

Everardo Trujillo

I wish I'd gone first because I'm kind of going to relay what you just said. Defense in depth is absolutely something that we look at. But yes, so we have the sort of tools that's not just one of -- CyberArk is one of. We do network anomaly detection at our substations that ties into user behavior.

But so going back to the example of that tabletop exercise with NERC CIP, one of the things that, during that exercise, is we're assuming they're in, right? And someone -- and during that table exercise, he was an operator that said: Then why even implement this thing if you think they're already in, right? And I said: That's a great question.

And so the threat actors -- going back to the Ukraine incident, the attackers were in their system for about almost 10 months learning, and they're very patient. So our threat is nation-states, right, so foreign governments, Chinese, Russian, you name it. We're under attack.

So they're very patient. And they've already -- let's just assume that they already have connections here and there. And they're trusted. They harvest the credentials. We're thinking that they are administrators or are administrators doing the work. You put another layer in there, and now you're -- okay. What just happened? We don't have access anymore? What just happened -- to the attacker, right?

So it makes it harder for an attacker, easier for an authorized user. And one of the things that came out of that meeting was we need to put something like this -- and obviously, we look at it from a secure requirement control. CyberArk is a tool that, like I said, checks off access controls for us, NIST 800-53, access control families. This is it. So yes, this is how we're dealing with that.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Great. Thank you, Eve. Don.

Donald Welch

Thanks. We can assume that bad guys will get in. They have a lot of resources. They have a lot of talent, especially when we're talking about national intelligence agencies, but even the level of cybercriminal gangs is really reaching that level. But all of them are willing to devote so many resources to getting what you have. And if you can raise the cost for them to go and get what they want from you or cause the damage that they want, chances are they're going to go somewhere else. So the old joke you don't have to outrun the bear; you just have to outrun the people you're with.

So privilege access management will raise the cost. Yes, my guess is the Russians could go and do what they want without ever getting privileged access, but that is going to be really hard to do and so raising that cost without correspondingly raising the cost to your institution. So Yes, there's a financial cost, but there's also a political cost, a business overhead cost and so forth.

And when you add all that up about how much you're going to raise the cost for the bad guys and raise your own cost, the value of privilege access management is huge. And I think it's probably better than any other tool. You can't just deploy privilege access management and call your network secure, but in terms of a single investment, I think it's the best investment out there.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

All right. JD?

John R. Rogers - *American Financial Group, Inc. - Chief Information Security Officer & Divisional VP*

Yes, I would completely agree with what these guys said. It definitely is defense in depth and layer of securities. And I always -- as I'm trying to relay this to executives and things, I have a picture of a house or a castle, if you will. It would be pointless to go spend massive amounts of money to put the latest, greatest lock on your front door if you have a completely shaky foundation, right, and so because the whole house is going to fall over.

And where I see privilege management in that is the foundation. So in my story I already told you that, it was the first thing I implemented in the financial division. It was the first thing that we rolled out across the whole enterprise. And it's because I truly believe it is one of the foundational tools that you have to have in place.

I agree that you -- they're going to come in. They're going to try to get privileged accounts to get the big compromise, the big data breach. And so you just need to have it in place. It's not the only thing, but you need to have it in place. And it just -- it doesn't make sense to spend a lot of money because, even in the demo that you gave of the phishing, if you -- there's a lot of MIME boxes full of all the security vendors that could spend billions of dollars on technology.

And some of them are really cool. But at the end of the day, if I implement that and don't have privilege management, all it takes is a person clicking a phishing link and giving away their credentials, and it's game over. And that couple million dollar investment went out the window. So it really is a foundation to build on top of all the other security things to make sure that they work well.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Excellent. All right. Well, thank you, all, so much for the time today. We really appreciate it and appreciate the partnership. Thank you, all, very much.

Adam Bosnian - *CyberArk Software Ltd. - EVP of Global Business Development*

Great. Thank you. Great panel this morning and great morning session, and really glad to be kicking off the second half of the day. My name is Adam Bosnian, and I run the global business development for CyberArk Software. And I'm here today to talk about how partnerships extend reach and extend CyberArk's reach within the organization and really extend the privileged security reach within an organization.

We're really

(technical difficulty)

in perspective as something that is really supporting the continual innovation and the leadership expansion of CyberArk out there, because the way that we're partnering, what we're partnering, and some of the categories we're partnering are areas that have not been focused on in the industry very often, and yet they've become very impactful for our customers. And we'll touch on that as I go through the presentation.

Security is a team game is a comment that we first started talking about, about 3 or 4 years ago. And at the time, I wasn't really hearing it back from the industry that much. And yet I go to a lot of different events and go to a lot of different conversations and you're hearing it back, that security is now being understood as a team game, because the fundamental reality is that there is no one solution, no one approach, no one vendor that's going to solve all of today's security challenges for an organization, never mind all the security challenges that companies are going to be facing tomorrow as they become even more advanced, as they are today.

So we really need to find a way for the security industry to work together, to work with the partners and the advisory folks that are out there and, most importantly, work in conjunction with the customer, because together as a team we compete much better against our common enemy, which is the attacker out there.

So security is a team game is a major premise of everything we're doing from our partnering and our business development. And the way that ends up getting illustrated is in our C3 Alliance. Now, the C3 Alliance is really all about that call to action to the vendor community saying we need to do things better together. Our customers are expecting us to have things working together out of the box on day one, not expecting to have to pay to get things working together for some custom implementation at day 200.

We want you guys to work together, number one, because we have valuable information, valuable data that may enrich those other solutions. They have valuable data that enriches what we're doing across the board, where we really have now 1 plus 1 equaling 11 rather than having individual products within an environment, yet not a security fabric created within that environment. So that was really one of the core principles of the C3 Alliance and continues to be.

And number two, it was really a call to action around privileged accounts as well, highlighting to vendors the importance of privileged accounts within their own solutions, the importance of privileged accounts when their solutions are doing work with that environment, and the importance of securing what we're delivering to the customer and how we start to leverage additional value through these types of integrations and these partnerships.

And the result is today that we're able to talk about having over 70 different partners within the program, over 100 different integrations and across a range of different categories from DevOps and discovery to authentication and analytics to identity and access management, and even something called robotic process automation that a year ago we were just starting to hear about and yet today is having impact within our customers and within the privileged security implementations that our customers are doing. And we'll chat on that in a second.

Now when we look at the impact that the C3 Alliance program has, it's really about having the benefits of the vendors working together, both technically and in the field, marketing and sales wise, to accrue those benefits to the customer, help them do better today and help them build a foundation so they can start to pivot and take action against new threats without having to always go out and buy yet another widget, yet another solution out there, bringing those solutions together.

So the first benefit that the customer has really communicated back to us that they see from the program is that the program exists, the CyberArk has made a conscious decision to invest in the C3 Alliance, because this is something that they want. They want their vendors talking together. They want their vendors working together. They want their vendor products to work together already without having to pay for it. So the fact that CyberArk has made the decision to go invest in it and made it happen is something that already is viewed as a differentiator by them.

Now, number two benefit is very often specific integrations allow us to really increase the impact within an organization where we are really ahead of the game in terms of the types of integrations and partners and vendors that we work with. And when they look at other solutions, they don't see -- never mind the program, they don't see these types of integrations, and robotic process automation being one of them that has become important in this past year. And it's something that we really led the arena in and it's something that's exciting to us. And I use it just because it's a new category that we haven't talked about, but it's very interesting.

The benefits also accrue to us and to our partners as well. So when we're in and working with a prospect or even an existing customer, the more people that are talking about privileged security and the more people that are talking about the benefits that accrue when we bring these solutions together, the better off that that customer or that prospect is hearing.

And so having the partner involved in the selling process, involved in the validation, yes, we are best of breed in what we do and we know CyberArk is best of breed in what they do. And that's why we've worked together with them to do XYZ. So having the team working together really brings a lot of impact in that field, not only good security posture and improved security hygiene within that environment, but also helps increase our win rates out there, right, because we're really showing that the top tier partners are working well together.

And then the second one -- no, excuse me, the last one I think is one that really is something that can be exciting as we move forward is having the partners start to bring us into opportunities and having us start to bring partners into opportunities where we may not always have the -- we may not have all the ears in all the places, and yet as someone talks about privilege and that opportunity pops up, and they say, hey, have you talked to CyberArk, we'd like to bring in our key partner, CyberArk, it really can make a difference in building that pipeline and helping to go and drive the revenue side of the equation as well.

So C3 Alliance has a range of benefits from the customer all the way through to CyberArk and obviously to our partners as well, and that's why we're really excited about it.

So I'm going to use a couple of examples, a couple of case studies that illustrate those types of things, and we're going to talk about ForeScout, Okta, and Red Hat. And we'll start with Okta. And Okta is a great company, does great work around the multi fact authentication and single sign-on, and out there talking about helping organizations either move a little bit more into modern identity management or change over what they already have.

And they were talking with a prospect out on the West Coast, a large energy organization, talking about an identity transformation project. They wanted to move off some legacy solutions. And during the conversation, the topic of privilege came up. And CyberArk's name was introduced by the Okta folks in saying, hey, are you familiar with CyberArk? Have you worked with CyberArk? Would you be interested in with CyberArk with us because we have a really good partnership with them?

And what was nice about that is not only did the sales teams ultimately end up working very, very well together in that scenario, but more importantly I think the sales technical teams worked really, really well together in that opportunity because they brought the SE side on Okta and the SE side from CyberArk, worked together to show the out of the box integration of how Okta can be used to authenticate into CyberArk for that privileged user and how that SSO functionality can flow through to that privileged user.

And they showed that in the demonstrations and evaluations where the customer, the prospect, saw two leading companies joined up at the hip, both sales and technical wise, seeing functionality that he wanted on day one, that it was there on day one, and that both organizations were going to support it moving forward, because that's ultimately what the customer wants. I want better security. I want these things to work together, but I want to know that you guys are going to support it today and into the future. And when you guys are partnered up, we know that you're going to do that.

The end result of that opportunity is Okta was chosen from the SSO side. CyberArk was chosen from the privilege side. And both products are being implemented or rolled out as we speak; really great example where Okta heard privilege, brought CyberArk in and helped impact the pipeline.

ForeScout, very interesting company, recently when public. They're about device discovery, seeing what devices are coming onto the network, what are leaving the network, and how to control and make sure that those devices are doing the right things within the environment. And what's interesting about this is that our customers and our prospects, having heard the application security challenge, the importance of not only managing the power access of heartbeat users, of human users, but those machine identities that Udi mentioned earlier this morning is also critical. You need to manage that privilege of both types of users.

And here you have an application like ForeScout that wants to identify what devices are coming on and off the network. And one of the ways they do that is they need to log into the switches and the routers within that environment to gather the information that they can therefore go ahead and analyze and provide here's what's new, here's what's moving around. If you don't secure that access to those switches and routers, you've now created yet another security problem within your environment while you're trying to fix security by having better awareness of what devices are coming on and off.

So our customers have heard that and they're taking action, and so now we hear them asking the question. Hey, when we're using ForeScout, can we use CyberArk to be able to solve that application security problem that exists within applications like ForeScout? Absolutely. And we've heard several -- and we've had several different examples here, customers, prospects and actually customers, joint customers of both CyberArk and ForeScout, that have raised that and that both we and ForeScout have raised.

And now we're finding that we're able to secure what ForeScout is doing as they do a great job. And we have other interactions and integrations with them that we'll speak about, but really a neat vignette or series of vignettes around application security and how, in this case, 1 plus 1 equals much better security and equals 11 for those customers.

And the third one we'll talk about is Red Hat. And you heard me talk about the application security machine identity challenge. In this case, it's that same problem but writ large in the DevOps space. We were working with one of our customers in the Far East, a large airline. We were working in that security side of the house, talking our privileged and how do we bring privileged security within that environment. At the same time, there was a DevOps project being kicked off and being initiated, something that was separate from IT security.

And the IT security folks that we were dealing with were aware that there was a DevOps project that was going to kick off, but didn't really have the visibility. They were focused on what they needed to do. But because we had heard that and we have a great relationship with Red Hat, both with their OpenShift container platform as well as their Ansible automation offering, both of which were being looked at by the customer, we joined up with the Red Hat folks just to stay in contact.

And the staying in contact was really important because, once things started to move forward DevOps side, we were -- the Red Hat team was able to let us know that things were progressing on that side. We were able to bring that information and share that with the security side, bringing those two teams together.

And it was the timing that made the critical part here, because having that joined up conversation happen when security says, hey, DevOps, I know you're going to do XYZ and we could help make sure that it's secure and not slow you down, because we're already working with the vendor and the vendor you selected are already integrated, great message to that customer, great impact for the customer from a security perspective, and obviously for Red Hat and for CyberArk in that equation as well. So a really great example, again, around that machine identity side and the important of it writ large in the DevOps world in OpenShift and with Ansible.

So you've heard me talk a lot about where CyberArk has very often focused. And that's what's exactly in the middle of this screen, is that we usually focus our efforts on the IT security side of the house. That's where privilege lives and that's where privilege is usually brought in and then brought out to all the other areas.

But we're starting to talk to a lot more of the constituencies within the organization and not only raising the importance of privilege to those constituencies, but our partners are able to raise the importance of privilege in those constituencies, which are maybe their core areas of focus and where they sell into. And those conversations end up feeding their back into security, and ends up having not only better security for that organization but very often larger opportunities for CyberArk and for privilege within that environment.

So let's take a couple of examples. So we talked about IT operations. It's all about keeping the trains running on time, keeping the systems up and running, knowing what's within your environment. And we talk about securing the application access. Well, BMC and ServiceNow are two companies that do discovery of assets, discovery and orchestration and automation within the environment.

And that discovery requires a credential to go do the discovery within that environment. And if you don't secure that, you may have an awareness of all the assets that are in your environment, but you're creating a security challenge. And we're seeing that as a driver when we talk to IT operations saying, hey, we're using these tools. Can you help secure them?

Or very often we have this IT operations team reaching out to the security team and saying, hey, we hear that you guys have an integration with ServiceNow that can secure what they're doing. Can you tell me about it? And now there's an inner dialogue going between the organizations at the customer, and now the partners are able to support that around the edges.

So we BMC and ServiceNow both on the securing of those solutions but also on solving -- excuse me, on supporting the workflow and the efficiency work that these guys do with their ticketing systems, and having -- and being part of that ticketing flow as well.

I'm going to bring up ForeScout again because ForeScout, not only do they understand what devices are coming on and off the network, but as an IT operations team wants to know what's coming on and off the network and the security team wants to know that those things are secured from moment one, CyberArk and ForeScout have an integration that allows CyberArk to consume information from ForeScout so when a new device comes on the network, if we're unaware of it, ForeScout makes us aware of it.

And now that device is now secured with privileged access from day one rather than some post fact scenario out there, so helping IT operations become more secure and pointing the privileged security challenge back to the IT security team to create a larger implementation.

This is operations. A different game, right? They're all about doing things cheaper, faster, better with it's the ERP system, the HR system, and in this case I'm going to use that robotic process automation scenario because it's a big conversation out there. Software robotic process automation is about automating the manual handwork that many employees do, freeing them to go focus on more of the headwork, the thinking part, but for the company savings lots of money because those software robots can run 24/7. They can run across geographies, different time zones, a lot of cost savings.

So the business operations folks get infatuated with the cost savings they're doing to have. But guess what? All those software robots need to have the same kind of access to the systems and the data and the devices that are out there like the normal people that were doing the work out there. And the way they do that is through a privileged account. And so if you don't secure that robotic process automation platform, you end up having a much larger attack surface than you had when you just had people doing their work.

And what we've seen are deals and rollouts of RPAs being slowed down or halted because the security question comes up. And the business operations team don't have an answer of how to secure it, but they have a financial imperative to try to move forward. And out of the box integrations with partners like Automation Anywhere, Blue Prism, UiPath help that pain go away.

We show it on day one. We're able to get it up and running in a matter of hours. And they're off and running and their project is not slowed down. It's actually enhanced because now the security team is onboard and able to move forward.

Identity is critical, right? Three, 4, 5 years ago identity and security were very much separate paths within organizations. And the belief and our belief very strongly is if you don't have identity in the security equation you don't have a very strong security posture. You need to know who is doing what, when, where and how on the systems. You need to have that knowledge within the environment.

So identity and security really are closely knit together. And that's why we have very strong partnerships in the identity space, certainly on the access management side as we talked earlier about Okta, and with Duo as well, so being able to support knowing who wants to access system X as admin, the authentication side into CyberArk, both multifactor authentication and the single sign-on; very good partnerships with the access management side, as well as on the governance side so the organization is now aware of all accounts, all users, all accessees when they're looking across their organization.

Without the information that CyberArk has about who is accessing things as an admin or, maybe more importantly, what applications are accessing targets as power users, that governance view that SailPoint delivers is not providing the full view. It's only providing what the end users are doing, and yet the governance mandate is you need to be able to look across the whole organization.

So we have a great relationship with SailPoint and other governance players. We support -- we've announced an integration with SailPoint that I think is doing extremely well, and we look forward to doing more things moving forward in that arena as well.

You've heard cloud throughout all of the conversations today, and cloud is a major area for privilege. As companies are going through their digital transformation, they now need to consider the new environment that they need to secure. They need to secure the access to that environment, as you saw in Shay's presentation. They also need to secure all the things that are created within that cloud environment.

And so we've worked with all the major players, AWS, Microsoft, and Google, to do those types of integrations so that we now secure the access to that cloud environment. And again, not just the heartbeat access to that environment but also the API, that programmatic access to the environment that often is not very well secured and is liable for attackers to go after.

So we have those integrations in place. We're able to secure all the things that are created within those environments. But we've also worked with all three of these players to make sure that our product can also be deployed and run within their environment. Most of our customers are going through the transformation where they're leveraging CyberArk on-prem and extending it into the cloud.

But for certain all-in customers or certain all-in applications, they want to CyberArk solution to be running in the cloud for the cloud, and we've been able to prove out that our solution is able to do that, be deployed and work well within that environment in all three of the environments that we have on the screen.

And then when we have those cloud environments, obviously we want to start to do a lot more automation and orchestration. The whole idea behind DevOps is get the people out of the deployment and monitoring and development side of the conversation and let the machines do their work. Well, there's a lot more machines that need to do that work out there, and yet they all have that same security challenge of how do I trust each other, right? So how do we make sure that when Chef needs to go and talk to another solution that that other solution can trust Chef?

And then as they create things, there are going to need to be secrets, credentials that are therefore provisioned out there. How do we get them out there? And that's where the power of what we're doing with Conjur really comes in strong in terms of our integrations with companies like Puppet and CloudBees and Red Hat and a range of the DevOps tools.

What's neat about what's going on in the DevOps world is we sometimes talk about DevOps solely in the cloud environment, but you also see DevOps being used internally in organizations as well. And so really, the beauty of our AIM solution, our Application Identity Management solution, and Conjur and the integrations that we have for both of those products with the DevOps tools, it is able to serve both sides of that house regardless of where the privilege challenge might be through DevOps, on-prem or in the cloud.

So C3 Alliance is really all about security is a team game, bringing organizations, bringing partner together to deliver out of the box integrations that deliver more security for the customer, more value to the customer, and helps them create a security fabric within their environment rather than dots of individual products within the environment.

We've been doing this for a couple of years now. We have, like I said, about -- excuse me, over 70 partners, over 100 different integrations out there and a range of different categories that are delivering impact to our prospects and helping us move deals forward, delivering impact to our partners as they start to see more value being brought into the environment through leveraging privileged security from CyberArk and the privileged information, and certainly more impact at the customer level, because now they have these products working together and they can start to not only get benefit A and benefit B, but as I bring these things together I have more visibility, more awareness, more ability to respond, more ability to protect my organization without always having to do things post fact and spending more money.

So that's C3 Alliance. That's the story, and how partnerships are expanding the impact of CyberArk and privilege within our customers. Thank you.

I'm pleased to introduce Marianne Budnik, our CMO, to talk about the market, and hand over the floor.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Thank you very much, Adam. All right, am I on? Okay, here we go.

So privileged security is a large, high growth market. Hopefully our discussions this morning are enabling you to have perspective on that market from a variety of different dimensions. But where I'm going to go is I'm going to talk a bit about this $44 billion opportunity that Udi talked about earlier. And with that, help you understand how we've broken down that opportunity, how we talk about market segmentation, etc.

So $44 billion global opportunity, and it starts by understanding that privileged security really is a critical layer in the environment. We're breaking down this opportunity quite simplistically for you along the dimensions of revenue bands.

So we look at the market as organizations that have more than $1 billion in revenue and organizations that have less than $1 billion in revenue. But it's important to understand that CyberArk, as the leader in this market with nearly 4,000 customers, has an enormous amount of data that we analyze and assess to understand, at this stage, profiles of the most successful implementations, profiles of maturity of markets. That really gives us the insight to understand who within those market segments we believe are adopting the technology, adopting privileged security, at what rate and pace as we build out our assumptions around the TAM that we serve.

So first and foremost, above $1 billion we serve all organizations. We view that right now as approximately 16,000 targets that we're addressing in this market. When we look at organizations below $1 billion, we look at a pretty robust model that includes factors other than revenue band. It includes numbers of users. It includes vertical industry that people participate in. So there are a number of factors when we start to look at the midmarket and the midmarket opportunity. And from within that at this point, we really are looking at 28,000 organizations that today, with today's portfolio of products and today's go-to-market model, we are actively addressing, so 44,000 organizations globally as part of our TAM.

With that, again, CyberArk is the leader in the market with footprint already today in 17% of those organizations at above $1 billion. And so we see that as a strategic benefit that the organization has. This means that 17% of organizations with revenues today of greater than $1 billion have had a first purchase with CyberArk and they're in those early stages of adoption, the early stages of the journey that you heard several of our customers talk about this morning.

For organizations with, again, simplistically below $1 billion and the dimensions of target markets I talked about previously, we have a 5% footprint so, similarly, enormous opportunity within those organizations; $44 billion overall.

The second dimension that comes into play when we think about TAM is not just how many organizations we're working in today, but when we look at the profile of those organizations. Again, Josh is going to do some cohort analysis. We have enormous amount of data at our disposal that allows us to model out, from initial time of engagement with CyberArk, the typical path that an organization of a certain profile follows with us.

And so, when we think about the addressable opportunity, for organizations over $1 billion you can see that we have just about a 3% TAM penetration, so enormous upside within the existing installed base in addition to the large greenfield opportunity that we talk about regularly. For organizations below $1 billion, we look at having about a 2% TAM capture today; again, enormous room for growth within the existing base in addition to greenfield.

All right, what are the drivers? We talk about risk. We talk about CyberArk taking a security first approach. We believe that by enabling organizations to take a security first approach, compliance and audit are satisfied though they do help along the way. Every industry has its series of regulations. More and more we see those regulations very explicitly referencing privilege as something that needs to be satisfied, but that alone does not satisfy the opportunity. So we see the aspects of security and compliance, risk and compliance coming together and, again, contributing to the overall opportunity.

With that, I am going to introduce Ron. So Ron Zoran we have the pleasure of introducing as our head of global sales organization. Globalizing our sales organization was a very important initiative for us in 2017; excited to have him come up here and talk about how we are going to go to market and we address this $44 billion opportunity. Thank you.

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

Thank you. Thank you, Marianne. Hi, everyone. I'm Ron Zoran, CyberArk's CRO. I've been with the company since day one, so just shy of 19 years; started in the R&D organization developing code, moved to professional services, then channels, then sales. It's a privilege and such a pleasure to meet you guys at last face to face, so I just want to thank you personally for making the effort and joining us here.

And today I'm excited to share more data about our sales execution. So as you know, we globalized the sales organization early Q3 of last year. We aligned all theaters under one umbrella with the goal of better capturing the vast market opportunity. We strive to do a few things; first to, I would say, streamline processes and also, very importantly, to take some best practices and just share it across geographies, elements such as deal closing discipline, such as focus on demand generation, global account management, productive channel, obsession with customer success, and more.

One change we introduced globally which we shared with you in the past is our risk-based approach. I would like to spend just a few quick cycles, shed some light on that, because this is fundamental in many things that we are doing in the field.

So we are learning how attackers operate from breach remediation activities we are personally involved in, how attackers move around during incidents and also how they constantly tweak their go-to-targets and their initiatives. Of the organization that were involved in the largest most recent breaches, over 40% turned to us, which presents a great opportunity for us because we can get very close to the action and learn firsthand how attackers operate.

This experience, combined with obviously the knowledge from our Cyber Labs as well as our Red Team, this experience is driving a lot of our product development activities as well as rollout methodologies. This knowledge of how attackers operate and how to best CyberArk a network in order to stop them is unique because it's based on contemporary reality. It's based on real incidents and personal experience versus hypothetical theories.

Sharing this knowledge adds value to any security team around the globe. It changes the discussion from compliance to audit. It elevates the importance, the urgency, and the priority of the CyberArk program. And it results in a win-win for our customers as well as to our business.

So as we expand our sales team, we also share with them the latest and greatest from recent incidents. This expansion of manpower as well as knowledge results in a few things. First of all, we definitely have better geographical coverage, but also it helps us to become trusted advisors, touch many more local security communities, and grow much further and much deeper within our existing customer base.

What you see here represented in gray in this bar chart represent the size of the entire global sales team. That includes outside sales, inside sales, channel managers, sales engineers, and customer success. The leadership base of our global sales organization is solid with almost no turnover. For example, the average tenure of our sales directors globally is 5.8 years.

So this is our sales engine. Our outside reps are collaborating with advisory firms and with our VARs to serve the $1 billion plus market. Our inside sales organization is partnering with our VARs to serve everyone else. As you can see, our partner ecosystem is instrumental in everything we do. On the VAR side, we focus on quality versus quantity, and we work very closely with our selected partners.

Since IPO, the growth of our indirect business outpaced the overall growth of the company and the direct/indirect business mix shifted from 50/50 to 61% indirect business last year. We also increase the amount of our trained channel engineers 43% annually.

In addition to that, we work very closely with the major advisory firms. They help us in a couple of ways. First, they help us to complement and enhance professional services. Currently there are over 300 advisory firm engineers trained and focused on CyberArk. It's up from basically none at the time of IPO. In addition to that, they also help us with C level access and influence. Last year we experienced 32% growth in influence deals.

One more element and a very important facet in our execution is our land and expand mechanism. Expansion can be either up-sells to enlarge initial scope; cross-sells to defend more categories such as critical assets, data center entities, endpoints, applications; and last but not least, expansion to defend DevOps in the cloud.

For example, this is a healthcare company. Their original driver back in 2012 was audit. A couple of years ago it shifted to risk as their CISO mandated risk-based rollout as a top priority. The initial scope was merely PV, PSM, and OPM. It continued with an up-sell of more users, followed by a cross-sell to defend applications with AIM, and then last year a couple of additional up-sells for more user, AIM for mainframe, with future plans to defend their DevOps, so we will secure this customer all the way from mainframe to the cloud.

Another example, this one is an energy company. Original drivers back in the day with risk, SCADA security, and NERC audit. The original scope was merely PV, PSM; continued with an add-on of both products to defend their SCADA environment, then followed by a cross-sell to defend their endpoints with EPM, followed by a couple of additional cross-sells to OPM their Unix as well as to manage SSH keys.

Josh will present a couple of slides of the financial outcomes of this land and expand execution. And speaking of Josh, that's our next presenter, so please? Thank you guys.

Joshua Siegel - *CyberArk Software Ltd. - CFO*

Great. Thank you, and it's great to be here, exciting to be here four years after our IPO to hold CyberArk's first investor/analyst day. And so thank you again for coming.

I'm going to spend about the next 20 minutes talking about our powerful business model that reflects all the things that you heard about this morning historically, and a little bit also, of course, going -- looking forward into the future a bit.

And the business model really begins at first, and you heard it several time today, landing the new customers and then nurturing those customers, expanding those customers over time, but doing it across all the theaters that Ronen just talked about, doing it across all verticals, and doing it across using all of our product base. And at the end of the day, we're getting a financial model which is giving you sustainable multiyear growth, high growth, with profitability and cash flow.

So we looked at revenue growth, 41% five year CAGR hitting $262 million, 56% of that revenue coming from products, 36% of that revenue coming from our recurring maintenance stream from our over 90% maintenance renewal contracts, and 8% coming from professional services, consistent with many years going backwards. Of course, all of this is across our multiple geographies.

So we're landing new customers, and we're doubling since 2014 the 1,800 customers that we had to nearly 3,700 customers at the end of 2017. And we saw each of the geographies, each of the 3 theaters, contributing to that growth of the new customers.

We also enjoy a healthy mix, 40% of our revenue being generated from those new customers and 60% of the revenue being generated from existing customers. Now if you recall, I think over 20% of our customers, of our new customers, are buying three or more products. So we do expect that going forward we'll still see more than 50% of our revenues each year coming from our existing customers.

Also increasing is the footprint of where our customers land in CyberArk or their add-on purchase. Last year we had a record number of $100,000 plus deals, 659, a 26% increase year-on-year of over $100,000 deals. If we parcel that out and go only to the above $500,000 deals, we hit 92, also a record number of transactions, a 73% growth year-on-year between 2017 and 2016. And again, if you look at the chart, you'll see that every single theater around the world is contributing to the growth of that large -- of those large footprint deals.

Geographically we're consistently generating revenues across all 3 theaters, 62% each of the last 2 years from Americas, 31% to 32% from EMEA, and the balance coming from Asia-Pacific/Japan.

And regardless of the geography, we're selling across many, many verticals. Banking continues to be our leading vertical with 29% last year. It's our largest installed base. It's generating, obviously, the most maintenance renewals. It's also generating services. It's also having more and more of them coming back for adding on new licenses to the products they have or crossing over to new products.

But in addition to the banking vertical, we see 10 other verticals producing 4% or more of the bookings pie last year. After banking, we have manufacturing, government, insurance, healthcare, and energy all producing 7% or more of the bookings last year.

And we're particularly excited when we look at certain verticals that we made particular investments. If we want to take the U.S. federal, for example, we invested significantly in the last several years not only in getting the right certifications necessary to sell into the U.S. government, but also building out a strong go-to-market team several years earlier to that and keep building that even to the present day. And that's really helped us get the global government vertical to 10% of total sales last year.

And if we think about what Marianne talked about and what we heard about this morning, it's really every enterprise with a meaningful IT infrastructure really needs to secure their privileged accounts. And we're even seeing verticals that are much less regulated, maybe transportation, or not regulated at all like IT services or retail and wholesale, also contributing at least 4% of our sales, representing really the true opportunity that's in that large market that Marianne just went through.

Across all those verticals we're really selling our entire product base. Ronen talked about our core privileged account security, which includes our Enterprise Password Vault, our Privileged Threat Analytics, and Privileged Session Manager. And that's clearly been our large -- that's clearly more than the majority of our sales, but when we look at last year we see new product sets around our Application Identity Manager, Conjur, sales and our Endpoint Privilege Manager now contributing, each of them, 10% of our product sales. And so we're really starting to see more diversification across our entire product set.

And I've heard a few times today that people were setting me up to talk about our cohort analysis. And I think it's really important, because when we talk about landing new customers, it's important to us because these customers are continually coming back year after year to do more business with CyberArk.

Obviously they want to continue their support contracts. I mentioned already over 90% renewal rate with our support contracts, but also they're coming back for more services. But we also see 1/3 of our customers each year coming back and buying more licenses for product they already have or crossing over and buying into new products that CyberArk has been innovating and been bringing to the street.

And if you want to kind of look under the hood and more quantitatively at these cohorts, and we took the cohort of 2009, for example, which has now been out there for 8 years, and we look at what that cohort did between 2016 and 2017. It actually increased another 1.4x its initial first year purchase back in 2009. So over that 8-year period between 2009 and 2017, it actually multiplied 6.7x its original first year purchase.

And if you kind of go deeper into the cohorts and you look at the cohorts that have been around for 7 years ending at 2016 and 2017, we saw 5.5 times its initial year purchase. And if we want to look at cohorts that were 6 years old that ended in 2016 and 2017, we saw 4.2 times its initial year purchase. And what they're re-buying, 2/3s of it we estimate to be more product and more licenses, and the remaining 1/3 being the recurring revenue stream coming from support and services.

So what you see on this slide is basically kind of a sketch of our 25 largest lifetime value customers. And what you have here is, in the dark blue you see the first time that those top 25 customers purchased with CyberArk. Coincidentally, the top half of that in the dark blue are all those that purchased prior to 2012. We just grouped them together. And the bottom half are those -- most of them have purchased since 2012 and still fall into our top 25 lifetime value customer.

What the light blue or the gray indicate is every single add-on purchase by quarter that they did with CyberArk since their first year purchase. And what I think this tell you is, and I think Ronen mentioned it just earlier before, is that CyberArk has -- really focuses on becoming a trusted partner over time, over many years with its customers. And these top 25 customers now, from over the lifetime, have acquired 7 times their initial first year purchase, which on average was about $1.2 million.

This revenue growth and the business model and our strategy has also been able to contribute to us being able to general significant profitability for more than the last 4 years. Last year we generated $52 million of non-GAAP operating profit with a 20% operating margin. We've also consistently generated cash flow from our financial model with generating over $200 million in cash flow from operations over the last 4 years and hitting $81 million in cash flow from operations last year or a 31% cash flow margin.

And that cash flow together with our growth in the business has allowed us to build a very strong balance sheet over time. It starts with $330 million in cash and no debt. This type of strong balance sheet over time has allowed us to continue to make ongoing investments in the business; given the massive market opportunity that we're talking about, allows us to also invest in landing new customers, expanding those new customers in an organic fashion.

And then also inorganically, it has allowed us to use cash flow from operations to fund very strategic acquisitions that we've done, the four acquisitions that we've done over the last several years. We've talked about Cybertinel and Viewfinity, and more recently the acquisition that we did this year with Conjur.

The second piece of our balance sheet is around deferred revenue growth. For those of you who have been tracking us since the IPO, you'll be happy to see that our deferred revenue continues to grow aggressively year in and year out, reaching $105 million at the end of 2017, 43% year-on-year growth.

And the other thing that you'll be glad to see and we're happy to see is that that deferred revenue really reflects bona fide recurring revenue stream. For those, again, who have been with us for several years, even the deferred perpetual licenses that you saw in 2014 and 2015 in those gray pieces of the chart, those have now been refreshed into true SaaS -- into our true introduction of SaaS products and some initial term-based licensing that we've done.

So I'd like to now also talk a little bit about how we view balancing growth and profitability. Take a look at it -- we'll take a look at it briefly historically and then take it as we see going forward. So historically CyberArk has always built the company, has always guided for at least 20% growth because of the opportunity that it had in front of us.

And as you see, back in 2015 and 2016 where we massively overachieved on those growth targets, we also were able to fully really lever our model and massively overachieve as well on our operating margin, hitting 27% operating margin in those first two years after the IPO in 2015 and 2016.

When we think about the next few years, the medium term, we still believe, and you heard it this morning about the market opportunity from our existing customer base and from the greenfield opportunity, that we can absolutely continue to grow and are setting targets to build the company to grow around 20% growth year in and year out, and be able to do that consistently, responsibly, and return 17% to 21% operating margins. Our 2018 guidance fits within that medium-term strategy that we broadcasted just a couple weeks ago, with 19% to 21% growth on the top line and 18% operating margin on the bottom line.

Now when we think about going out further beyond the medium term, when we think about when CyberArk matures, when the market opportunity matures and we will eventually see perhaps growth rates that drop below 20%, that drop below 15%, at that point we will be looking to really return bigger operating margins. And we're confident that we'll be able to see a long-term target at the right opportunity for leveraging to 27% to 31% non-GAAP operating income margins.

Now if you look at our R&D and our G&A today, they're really already at the right levels, really working efficiently but still producing the type of innovation and scaling the infrastructure as necessary.

We might see a few points of decrease on the gross margin, and that will really depend on how much our SaaS products contribute to the top line. As we all know, SaaS could have some impact, some negative impact, on the actual gross margin. But really, it's going to be a focus. When we believe and when we choose that it's right, that the growth opportunity has matured and is not a high growth or a 20% or north growth opportunity, that we'll be able to get further efficiency out of our sales organization, out of our channel reach, and really bring sales and marketing to 33% and 37% levels of revenue.

Now we've been near those levels already at much smaller scale. So from our perspective, we're confident that at the time that we want to do it down the road, we'll be really in a strong position to be able to hit those new targets of 27% to 31%.

And with that, I'd like to turn it back over to Udi to summarize, and then we'll jump into QA.

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Thank you, everybody. So before we jump into QA, just a quick summary of what you saw here. What we wanted to illustrate for you today is our excitement about the opportunity that we're -- the team excitement about the opportunity that we're looking at. We pioneered and are leading this market, and continue to innovate and lead as we go. We see further acceleration and expansion with our customers continued adoption of modern technology and DevOps, and you heard some of this today.

We've globalized our sales force. They're energized going after this opportunity, armed with 350 active channel partners and those technology alliances that Adam talked about as part of our C3 that are helping us better and deeper integrate with the security strategies of our customers.

We really have the opportunity to continue to lead the space and provide an impactful critical layer of security as you've heard today. That's the number one thing for us. We're really making a true impact on our customers and are thinking along with them in this partnering.

I really want to thank the customers that were with us today and absolutely our 3,700 customers that teamed up with us over the years, and our 1,000 plus CyberArk team that is really fulfilling its mission every day.

So thank you everybody, and we'll move to QA. We'll get the executive team up here and kick it off. Just to save time I'll take the first one. Tom?

QUESTIONS AND ANSWERS

Unidentified Participant

We heard about your opportunities and how you address them. Can you speak about your challenges? And how do you look at challenges on a few levels, competition, go-to-market, implementation also challenges?

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Sure. So I'll kick it off and the team will lean in. I think as a market creator, as a pioneer and the one that scaled the organization, we have the opportunity but also the responsibility to achieve that scale and capture the market while keeping our customers happy, and you saw a select group here. We give it a lot of attention as to go after the greenfield but continuously deliver, roadmap, and help existing customers.

Both and very much aligned with that, one of the things that, as were already mentioned, is as this layer becomes more widely adopted and as it becomes a critical no-brainer, a foundational layer that every company needs, we have to deliver it in a simpler fashion. Version 10 that we talked about was the beginning of that, but it's a big initiative for us, to continuously invest in simplicity. It helps our existing customers and it helps new customers, helps our channel partners to help us with the scale.

Another element, again, with the growing importance, there's been a shortage -- to talk about challenges, with the growing importance of this layer, there's been a shortage of the skill set. And we've heard it back from our customers. We have had customers have to hire from each other. And so I would say it was a bigger challenge 18, 24 months ago, and we've invested in it. Shahar, who is with us also today, runs our Global Security Services. They also have global training, invested in wide trainings across the globe to enable more of our customers to carry the weight. But that's going to be an ongoing effort.

So I touched some of the, I would say, growth pains which we are fortunate to have as the market leader in the space. But if anybody wants to add here, you can jump in.

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

Yes, just on the implementation and competition, just to answer your question, Tom, first of all on the implementation, definitely I want to echo what Udi said with regards to skill set. And we identified that a few quarters ago, and we are focusing on enabling and training. And we have new programs that we actually are introducing this year.

We've very excited with version 10 that was introduced end of last year because it allows us to implement faster and secure our customer faster. As you saw, it's part of everything that we do. So it was important to us to just do that faster.

There is a trend in the market within our customer base to try and do -- whatever organizations that are being breached are doing in the first few days post breach they are trying to do before. And it's a quick sprint and it's helping if -- version 10 helps to expedite that, sorry. So that's on the implementation.

Competition-wise, this market was always very competitive. I've been here for almost 19 years. It was always competitive. I don't see a material change. It is a very hot market, so by definition not just customers and prospects are flocking to it but also investment, also obviously other vendors. But in our world, that's nothing different. It was always competitive and it's still competitive. So it's good to be a market leader and continue to compete and win. Definitely competition is out there.

Unidentified Participant

I just wanted to start out with some of your comments around the TAM analysis. You pointed to about a 3% dollar penetration within the $1 billion and up camp as well as about 17% of customers. What has to happen for that penetration level to rise? And what can you do to maybe accelerate that cadence over time?

Marianne Budnik - *CyberArk Software Ltd. - CMO*

So I think that's part of how we capture the market. We talked about the journey that people embark on with us, and I think the points that we've made around training and education, right? So we have a strong call for more education from within our customer base.

Shahar and his team have made significant advances in terms of developing online training and education. We're running global training events globally. But again, an educated customer is able to consume and adopt the technology and grow their deployment with us more quickly. And so the big focus on training and education will obviously help us to capture that.

And then there's the absorption time I think in terms of, as people are looking broadly at their landscape, the organizations consume. I think we have a high level of confidence, given the analysis we're able to do, of the existing customer base, of the journey that people are going to take over time. And we have some organizations that started with us early that really are at the forefront. And then we have other organizations, and you hear about the new logos we add every quarter, people who are earlier on that journey, but we're confident in the journey that we expect them to take given all of our internal analysis.

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

I would say that in some segments of the opportunity, there's an opportunity for the customers to not go back and fix the privileged security issues like on their on-premise environment, but actually get it right as they migrate to the cloud. So we can see where, if we get it right, like what JD described as they're going after DevOps and cloud, you can put the systems in place and do it right from the get-go. So that will be a different flavor of adoption in the new environments.

Adam Bosnian - *CyberArk Software Ltd. - EVP of Global Business Development*

And just to add on to it from my own little parochial view in the C3 Alliance side of it, the conversation that we're having with a wider part of that organization, right, talking about privileged security with the IT security area, there's going to be a natural evolution of how security and privileged security generates from there.

But as you talk to all the other organizations that are around there, now understanding they also have the challenge and pointing that back into the IT security organization, I think that can help us really start to address the larger opportunity of privileged security in that organization by talking to the many rather than just the core.

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

And just one more thing just to expand on what Marianne said about patterns, so it's much easier for us nowadays to recognize certain patterns based on industry. And we can be very, very accurate with that. For example, let's take airlines.

If Airline 1 is spending X with us, Airline 2 is spending 10X with us, and Airline 3 is still not a customer, then two things are apparent, right? One is there is no reason why Airline 3 will not -- shouldn't be a customer. And second, we need to understand the journey that Airline 1 took and kind of mimic that with Airline 2. It's just going to be -- rise all boats here. So it's much easier for us nowadays to do this analysis and be very accurate and expect certain things from our field execution based on that.

Fatima Aslam Boolani - *UBS Investment Bank, Research Division - Associate Director and Equity Research Associate Technology-Software*

Fatima Boolani from UBS. I have one for Josh and one for Ron. Josh, for you, as I look at the medium term model, you're obviously being a lot more assertive around the investment profile in the next couple of years. I want to understand why that wouldn't help accelerate revenue growth from current levels, especially in the context of what Marianne talked about regarding the TAM. And then a follow up for Ron, if I may.

Joshua Siegel - *CyberArk Software Ltd. - CFO*

Yes, I think when we look at the investment for growth, it's also to invest for the current year but also to ensure that, when we get to the end of the year, we'll be able to look out at another growth year horizon in multiple years. So a lot of the times when we are starting to invest this year, for example, it's things that will really take into -- will really have an impact only towards the end of the year and have an impact on 2019.

So the real return is not just about thinking about what's happening on this year. But it will put essentially some of a drag on this year's operating margin because of a multiple year growth trajectory that we want to create.

Fatima Aslam Boolani - *UBS Investment Bank, Research Division - Associate Director and Equity Research Associate Technology-Software*

Fair enough; a question for Ron. As the portfolio has expanded and your sales motions have been changing and you're attempting to sell more into the installed base and, again to Marianne's point, your penetration within the installed base is still pretty low, how do you think about reducing the friction for both new and existing customers to keep expanding? And then your thoughts around offering modules or packages or sort of ELA type agreements to get customers to really go standardized on CyberArk and the entire portfolio?

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

Yes. So first, with regards to kind of the, I would say -- I'll just call the balance between land and expand, so as Marianne said, the opportunity is extensive and we would like to continue landing. There is no expansion without landing first, right? So we understand that. We are excited about that. We don't necessarily guide for that, but we have all reasons to believe that we'll continue to acquire new customers at a healthy rate as we are right now.

What excites us is that on the efficiency side it takes more effort to land a customer and then less to put them on a journey, right, on what we call the CyberArk program, the hygiene program, even less to do cross-sell and even less to do an up-sell. So for us, it's exciting opportunity to have so many sitting in so many doors that will allow us to expand over time. It's just a matter of focusing the guys doing the right things with our precious time to get the best return on our time investment.

So we need to strike this balance. We've been doing it so far. We believe now that under a global organization we can learn from one another and fine-tune the machine much better.

Howard Shepard Smith - *First Analysis Securities Corporation, Research Division - MD*

Howard Smith from First Analysis. I want to follow up on a theme of a couple questions here, reconciling the growth trajectory with the TAM. So a $44 million TAM, $300 million company growing at 20%, market leader. Is this just a multi-decade TAM to be penetrated? Or help me kind of reconcile those number as you're thinking about them.

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

It is -- when you use TAM, it's not obviously an annual TAM. It's a lifetime value TAM when we look at these accounts. And as Marianne explained, we analyze based on our experience this type of company, how have they grown with us; the smaller types of companies, how have they grown with us. So we're looking at a huge opportunity, but it is a lifetime. It's an opportunity that CyberArk is going to go after in the next and future years.

We are the market leader, and we have to strike this balance. It's still a market where there is education in selling. It's still a market where different geographies are not as educated on privileged security as a critical area. It's becoming much better, and we're seeing more geographies step into the game. But there is work to educate and sell as we go after this opportunity.

And obviously, the way we guide is responsibly based on what we're seeing and how we manage our pipeline, and balancing short-term opportunity with long-term opportunity.

Howard Shepard Smith - *First Analysis Securities Corporation, Research Division - MD*

And just a question in terms of geographic mix as we look out longer term. Do you expect -- it's been a little steady. APJ is going up a little bit. But as we look out longer term, do you look at this market opportunity, the $44 billion, as 1/3, 1/3, 1/3, 70% or 60% U.S., 30% EMEA? Just broad number of how maybe you think about the geographic penetration of that $44 billion.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Yes, I'll give a rough number. I think when we looked at the breakdown of the numbers by geography, we were looking at -- it was a little less than 1/2 was Americas and a little bit more than 1/2 was outside the Americas. So EMEA is a very strong market for us. We feel good about the opportunity there. And again, if we look at the TAM that we presented was today's TAM based upon the number of accounts specifically that we have identified and the parameters we've identified them on, we feel good about that number.

Unidentified Participant

Thanks. I just wanted to follow up with Ron on the globalization of the sales force that you described. So you've been onboard for the past few quarters. I'm just wondering if those initiatives are largely complete. And if so, or even if they're in process, can you maybe talk about what you're seeing in terms of sales productivity?

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

Yes, sure. So first, we are very -- I would even use the word proud of the EMEA team, how they came together after the organizational changes during the summertime of last year and delivered a record quarter in Q4. It was a very good sign, very good momentum.

But we just hired Rich, and he's experiencing many different ways...

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

The VP of EMEA.

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

Yes, exactly, the head of our EMEA organization, experienced in security sales, very experienced in channels being the head of global channels at RSA, very successful, experienced leader in EMEA.

So our focus in 2018 is to create consistency. As I see, most of the changes are effective and behind us. But our focus is on consistency, and it's still the beginning there.

Erik Loren Suppiger - *JMP Securities LLC, Research Division - MD & Senior Research Analyst*

This is Erik from JMP. First off, on the 20% growth for the medium term, is that something that we can think of organically? Would acquisitions be over and above that and should we be adjusting? How should we think of the most recent acquisitions?

Joshua Siegel - *CyberArk Software Ltd. - CFO*

Yes, I think when we look forward and based on the opportunity that we see, on an organic basis certainly we see 20% as a target, as the target to grow. But that doesn't mean that, as we kind of look forward and look at potential M&A and strategic M&A opportunities, that that may not contribute. In some cases, it may be filling in gaps in technology or adding more future sets to our existing products.

So we constantly, as this market is changing -- and you heard this morning a lot about how the IT infrastructure environment is changing all the time and even changing where we need to kind of predict where it's going. So I think it's not fair to say that all M&A will absolutely be incremental. Some of the M&A is thinking about how do we best use our capital on the balance sheet versus expending it on R&D.

So in some cases we may choose to do acquisitions instead of building in-house, in which case it's just part of our organic, so to speak, growth. But I think -- and the types of acquisitions we've done historically have really been very much in tune to where we see the company and the market growing organically, even though there might have been an acquisition. And I think going forward we'll see some acquisitions that contribute to our organic growth. And there could also be acquisitions that will be incremental, expanding our market size that we talked about this morning or already including significant revenue that we don't -- from the first day.

Erik Loren Suppiger - *JMP Securities LLC, Research Division - MD & Senior Research Analyst*

And then Marianne, the lower portion of your pyramid, you said 28,000 companies that are less than $1 billion in revenue. The 28,000 is a small segment of that account, that volume of businesses. What parameters did you use to come up with 28,000?

Marianne Budnik - *CyberArk Software Ltd. - CMO*

So the 28,000 we look at as the subset of the big market that we're actively serving with our products and go-to-market model today. So we looked at a variety of factors, again based upon our ability to analyze transaction data over time, targeted this segment. So we looked at revenue of the organization. We looked at industry the organization participates in. We looked at number of employees, a variety of factors.

And again, that's a model that we feel very confident about, again, given the variety of factors. And our focus at this stage really is on how do we apply our resources towards the most productive targets at this time, and look forward to -- again, I'll emphasize that those are today numbers.

Kenneth Richard Talanian - *Evercore ISI, Research Division - Analyst*

Ken Talanian at Evercore ISI. Josh, I guess this one's for you. When we think about your medium-term targets and long term targets, what consideration did you give to new verse existing customers within those targets? And then to the extent that you're successful in cross-selling and up-selling, could we actually see upside to profitability as a result of that?

Joshua Siegel - *CyberArk Software Ltd. - CFO*

Yes. So I think -- and also what I talked about in the last two years, we've seen 60% of our revenues coming from existing customers. And we anticipate that certainly doing more than 50% going forward from existing customers is going to be the trend. It could even go up a little bit from -- it could even go up from the 60% because we're landing with a wider platform.

Over the last couple years, we've really increased how many of our new customers are already taking a bite out of multiple products. And I think Ronen mentioned before it's even easier, a shorter sales cycle, to sell more seats of the same product compared to necessarily crossing over to new products.

So I think that we'll see that still the majority, or more than 50% and probably 60% plus, of our business coming from existing customers. I think that, to your answer, to the extent that we're still able to grow the pie at the right growth, overall growth that we want to grow it, and more of it is coming from existing customers, I think in the short run that won't necessarily bring super efficiency.

But certainly over the long term it will bring efficiency, because in the short term we have to still build out our customer success infrastructure. And again, we have 3,600 customers, 3,700 customers almost, to take care of. And so that requires that infrastructure to sell to them.

Kenneth Richard Talanian - *Evercore ISI, Research Division - Analyst*

Okay. And I guess as a follow-up, you've seen a tremendous increase in the number of channel partners you've had originating deals. How has that lowered your cost of acquisition over time? And what kind of leverage could you get there if that inflects in terms of growth?

Joshua Siegel - *CyberArk Software Ltd. - CFO*

Well, I think where we got sales leverage is particularly -- and I can go back. I believe it was in the 2016 year where we really outpaced our target plan for revenue that year. And we saw really a big operating margin increase, well beyond our guidance, and we achieved 27% operating margin. I attribute that to the fact that we -- a lot of that overachievement came from the channels.

So in one respect we had the channels giving you that extra revenue. In another respect, it is while there might be a bit of a higher discount, but we don't need to have as many account executives on the ground in order to bring that business.

Gray Wilson Powell - *Deutsche Bank AG, Research Division - Research Analyst*

Gray Powell from Deutsche Bank. So I actually wanted to follow up on the last one. You guys have roughly 30% penetration of the Global 2000. It's a pretty impressive statistic. I'm guessing that most of the companies in that category already have a privileged account solution in place, so I'm curious. Do you see room for that 30% penetration level to move higher over time, or is your growth in the large enterprise portion of the market, is that really being driven more by customers expanding their footprint with you and taking in more products?

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

I guess, Ron, I think it'd be interesting to highlight how we've seen even globals that had something come back, yes.

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

Yes. So with regards to what we're doing in the, let's say, high-end of our high-end, all right, in the Global 2000, we still see over 80% of our kind of new business engagements are still greenfield regardless of where it is. So still not a rip and replace kind of play, although we do see some rip and replace but really at the edges. So we still expect to acquire more footprint in this category.

In addition to that, you're absolutely right. The upside is immense in those 30% that already own us. The fact that we have a foot in the door, based on our statistics, is just on average 20% of what we should be able to do based on today, without adding new products, without any more time and more expansion.

So you're absolutely right. We go both directions, but we still expect and see greenfield within the Global 2000. And I think we have a few anecdotes that we even mentioned, right?

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Yes. We have examples that, even if they had something, it's not a classic rip and replace where that solution was strategically placed but more something that was bought over time for compliance reasons. And when they looked at it from a risk-based perspective and the journey to the cloud, they -- it was almost like a new deal and an opportunity for CyberArk.

So we consistently go after the high-end, again, looking at most of it as greenfield. But the rip and replace opportunity is out there as well.

Sterling Auty - *JP Morgan Chase & Co, Research Division - Senior Analyst*

Sterling Auty from JPMorgan, so a question for either Ron or Udi. So I want to try to understand. Ron, you made the comment earlier, allocating your precious resources and then the comment that 80% of what you're seeing is still greenfield. I want to understand what is the biggest constraint to the growth. Is it finding deals or having deals out there or having enough feet on the street to make sure that you're in the deals, versus maybe there's still just a big -- even though you've been at this for a long time, is there still just a big market education hurdle to get over to show the benefit of what the solutions do for the customer?

Ronen Zoran - *CyberArk Software Ltd. - Chief Revenue Officer*

So yes, you're right. In a way, there are many lucrative ways that we can apply our resources to get more of the opportunity. But I will answer your question with one word of caution about we absolutely need to balance this. As the information security leader, we need to balance everything that we do every time we hit the accelerator with just the sheer fact that we need customers to be deployed correctly, to be deployed securely, and it's very dangerous to go too fast without making sure that our customers are successful.

So we're just trying to balance this because we see -- to Erik's point, we see a very long-term horizon. So we want to just do it right so we'll be able to capture it for the long term.

Unidentified Participant

If I just ask a follow up on what Sterling asked, Udi, if I look at the challenges differently and I tell you that I double your budget tomorrow, double the budget for the next few years, how do you spend this extra money? You have to spend the money. How do you spend it? What problems do you focus on?

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

So of course, there are some things that are, I would say, on our competitive advantage elements that I'll keep here. But it's exactly striking that balance. I think we continuously invest in feet on the street for capturing the greenfield and the opportunity, but balance it with sustaining the R&D and the innovation and the security services part of our organization and customer success.

So I think we got to this point by partnering with the customers early. They told us, hey, this is mission critical, are you -- when we were a small company. Hey, this is mission critical. Are you going to be there for the long run for us? Are you investing in the scale that we have? And some of the examples you saw here are of top global organizations. And we always were striking that balance and able to scale with them, provide high availability in our solutions. And so we would invest in both, both capturing the opportunity and in making sure the customers are successful.

The other lever, which I think is a lever that I always grade ourselves that we could do much better, is the channel lever. And you see it in Josh's long-term model. It's one of the areas for us to achieve scale and also improve the bottom line. Some of that extra budget you gave me I would also put towards really making our channels more and more self-sufficient, doing it across -- and doing it across the globe.

But again, we think we're very unique in the way we have been balancing growth and profitability. As we work on budgets, as we look at our annual plans, there's no let's leave money on the table. There's let's execute with long term in mind.

Unidentified Participant

And is the fact that you are a niche player focusing on one area only of security, is it a constraint? And I'm asking it because when you talk to Cisco or any of the firewall companies today, they speak about platform and they speak about the need to consolidate platforms and give a single point of management. So how do you balance the fact that you are very concentrated but you sell to customers who want to have a more consolidated view?

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Oh, absolutely. I love that question. I think you saw four customers up here today not wanting to have this be a feature of something else where you lose focus and not make it critical.

We call it the Privileged Account Security platform. We've taken an approach where privilege is foundational to any other IT initiative that our customers will have, and even to their security initiatives. You won't have a secure firewall if the administrator can come in and change the rules and open it up. You won't have a secure database security product if the administrator can change the rules there.

So we are foundational to all of our customers' initiatives, but we take a platform approach to say we'll take it all the way across their entire environments. We'll take it all the way from their human side into the application and code. We've seen in the past companies that -- or larger companies like CA enter the space and try to get the benefit of the scale and platform. And we really successfully win against them because our customers have security at heart and not just single source.

I think we fast forward the information security industry. Definitely there will be -- there won't be so many startups out there and there won't be that many variety of vendors. It's very hard for customers to work that way, but there're also not going to be single players. The attackers are innovating. They're innovating as we speak. We investigate this all the time. And therefore, in foundational security technologies, it requires the focus that we have.

It doesn't mean we won't expand. But whenever we -- whatever we will expand to, we'll make sure that we're not neglecting this foundational layer and that we're making -- we're always looking for the things that really make an impact to our customers.

Augmenting that is what Adam works on, and his team, on the C3 Alliance. This approach of a team sport, our customers really appreciate. And so yes, they have Cisco and they have Splunk and they have Palo Alto and they have Check Point. And they appreciate the fact that we give them out of the box integrations and, to quote him, create a 1 plus 1 equal 11 on the value and not try to create another feature to alleviate something else there, but actually give them more value.

Adam Bosnian - *CyberArk Software Ltd. - EVP of Global Business Development*

And just to add on to that, Udi, I think it's really -- security is not a good enough scenario, right? It's a best of breed. So while the vendors may want to suggest that platform is the way to go, we're seeing the customers really focusing on privilege as important and wanting to bring the best functionality and vendor out there regardless of where that privilege may be happening, sometimes even within the platform players where there's a privilege challenge in that. Some of the things that we're securing within the organizations for privileged access are privileged access for some of those platform players as well.

So I think it's really the combination that makes the stronger security fabric than any one vendor out there does. And we're finding that resonance as we talk more and more and expand the C3 Alliance from the customers, from the advisory folks, but maybe most interestingly from the other IT and security vendors coming to us and saying we want to do more of this, not less of this.

James Edward Fish - *Piper Jaffray Companies, Research Division - Research Analyst*

Jim Fish, Piper Jaffray. I guess the first question is around the $44 billion. We've gotten a bunch of questions here already on the TAM. The IDCs of the world say about $2.3 billion, and understanding that's actual spend versus greenfield. And yet, Ron, I think you even said like 80% is still coming from existing but -- or from greenfield. Can you help us bridge the gap there? Because even if you take that kind of $2.2 billion and the 80% and all that, you get multiples less than the $44 billion.

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Yes, just Ron -- I just want to accept a few corrections. Ron was referring to that in new business deals we've found that 8 out of 10 are still greenfield. Josh referred to the amount of revenue we get out of the existing customer base. And the $44 million, as I mentioned, is not an annual TAM, right? It's a lifetime TAM.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

Sure, absolutely. I'm happy to talk a little bit more about that. So there are two sources that we compiled the TAM from. One is we look at external data, Data.com data, in terms of how many organizations of what size, vertical, etc., profile exist out there in different segments. We also have our own internal data in terms of who is spending with patterns over time.

You heard from different panelists today. JD talked about the fact that they started with us in 2009 and are continuing to expand their environment today, as you look at the early days of laying the foundation and expansion through to now looking at DevOps and cloud and sort of the next frontier, if you will.

So we look carefully at our own existing footprint today. We look at the journey that we expect each of those customers to take. We have our go-to-market resources dedicated to working with those customers to make them successful along every leg of that journey. And we have increased confidence every time we're engaging with them in terms of the journey they're taking and where they're ultimately going to go.

Again, as the market leader, we feel like we have deep insight into behavior and, similarly, from the Red Team perspective and what's happening in the threat landscape. We showed some images today of the expansion of threats, and we're investing from an R&D perspective to ensure that we're staying at the forefront of what's happening.

And so those factors together, when we look at the number of organizations that exist, the footprint that we have and the profile of activity over time with those organizations, what we see happening in the market from a technology perspective and our investments, we feel like those come together to give us a high level of confidence in the market we're serving today with the products we have and the go-to-market we have that that's the opportunity we're going to capture.

James Edward Fish - *Piper Jaffray Companies, Research Division - Research Analyst*

Got it, and then just one follow up. You guys are talking a little bit more about getting down into the midmarket where traditionally, kind of going off the last couple questions, you've seen more of that platform approach or even a SaaS approach just because midmarket doesn't have as many security ops. Could we see one day CyberArk shifting a product more geared towards the midmarket that it is more subscription-based, or how are you going to address sort of the competitors there like Centrify that are already offering subscriptions geared for the mid-market? Thank you.

Marianne Budnik - *CyberArk Software Ltd. - CMO*

So I think it's a two-part answer. I'll take the first part and then I can hand it to Roy. So again, we look -- I think Eric made the point. When we look at midmarket today and we look at applying our resources, for us it's a question of focus right now. There are 28,000 organizations that we feel CyberArk is absolutely the best solution for and we've actively targeting that subset of the midmarket today.

In terms of the future, I'll let Roy talk a little bit about products. But we're talking about today's TAM, today's customers that we're addressing, and 28,000 is the number that we feel very confident that we have the best solution via technology combined with go-to-market to serve.

Roy Adar - *CyberArk Software Ltd. - SVP of Product Management*

So from a product point of view, a lot of the work that we've done with version 10 focusing on simplification, automating the deployment, simplifying the deployment, of course helps our large enterprise customers, of course, but also serves many benefits also for the mid-market customers and mid-market organizations.

A couple of years ago already we certified our products to be installable and supporting running on the public cloud environment. So midsize organizations can install and deploy our solutions fully in the cloud, saving resources and making the deployment simpler and faster.

We also work with a service provider organization, many service providers who help their customers not just in installing the solution, which is really day one or week one of the program, but also giving them best practices and helping them manage the policies correctly, helping them decide on the controls that would be most effective for them in a more consultative approach. So that range is something that helps us meet the needs of midmarket organizations without requiring those organizations to invest too much in having their own homegrown resources.

On the subscription comment, just to follow up to your questions, we have been offering the product also on a subscription basis. And that's been something we have available for a couple of years.

Erica Smith

Okay. With that, we are out of time, but we'd like to invite you all in to have lunch and some follow-up product demonstrations. And thank you very much for your time.

Ehud Mokady - *CyberArk Software Ltd. - Founder, Chairman, CEO & President*

Thank you.

DISCLAIMER

Thomson Reuters reserves the right to make changes to documents, content, or other information on this web site without obligation to notify any person of such changes.

In the conference calls upon which Event Transcripts are based, companies may make projections or other forward-looking statements regarding a variety of items. Such forward-looking statements are based upon current expectations and involve risks and uncertainties. Actual results may differ materially from those stated in any forward-looking statement based on a number of important factors and risks, which are more specifically identified in the companies' most recent SEC filings. Although the companies may indicate and believe that the assumptions underlying the forward-looking statements are reasonable, any of the assumptions could prove inaccurate or incorrect and, therefore, there can be no assurance that the results contemplated in the forward-looking statements will be realized.

THE INFORMATION CONTAINED IN EVENT TRANSCRIPTS IS A TEXTUAL REPRESENTATION OF THE APPLICABLE COMPANY'S CONFERENCE CALL AND WHILE EFFORTS ARE MADE TO PROVIDE AN ACCURATE TRANSCRIPTION, THERE MAY BE MATERIAL ERRORS, OMISSIONS, OR INACCURACIES IN THE REPORTING OF THE SUBSTANCE OF THE CONFERENCE CALLS. IN NO WAY DOES THOMSON REUTERS OR THE APPLICABLE COMPANY ASSUME ANY RESPONSIBILITY FOR ANY INVESTMENT OR OTHER DECISIONS MADE BASED UPON THE INFORMATION PROVIDED ON THIS WEB SITE OR IN ANY EVENT TRANSCRIPT. USERS ARE ADVISED TO REVIEW THE APPLICABLE COMPANY'S CONFERENCE CALL ITSELF AND THE APPLICABLE COMPANY'S SEC FILINGS BEFORE MAKING ANY INVESTMENT OR OTHER DECISIONS.