DRAFT

Conference Debate Session IV:

Fresh thinking to fight back a rising tide of cyberthreats

Introduced and chaired by Roy Chua, Founder & Principle, Avid Think

Global Media Summit, San Jose 2023

Featured Speakers:

Analyst Chair: Roy Chua, Founder & Principle, Avid Think
Matt Lourens, Office of the CTO, Check Point
Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
Jason Rolleston, VP & GM of Security Business, VMware
Ken Levine Chief Executive Officer Xcitium

Roy Chua, Founder & Principle, Avid Think
We're going to start off with having the panelists' introduce themselves. I'm going to give a five minute very quick overview to set the stage on this next topic here around cyber threats. And then we'll go to the panelists for an expert. Discussion is not a debate, it's going to be a discussion because they're all very friendly, as you can see here. All right, let's start with Jason. Introduce yourself. Please, Jason.

Jason Rolleston, VP & GM of Security Business, VMware
Sure. Thanks for having me. Jason Rolleston. I'm the Vice President general manager for VMware carbon black. So leading endpoint products, endpoint detection, response and overall kind of endpoint security for VMware.

Ken Levine Chief Executive Officer Xcitium
Thanks. I'm Ken Levine. I'm CEO of Xcitium. And we are also endpoint security and XDR. So, Jason and I'll have fun up here.

Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
Hi everyone, I'm Srinivas Bhattiprolu. Call me Srini, responsible for global presales for cloud network services at Nokia. We don't do EDR. But we do XDR. And I'm very happy to be here.

Matt Lourens, Office of the CTO, Check Point
Matt Lourens, and I'm with Check Point software represent the office of the CTO. I work in the field and my background within Check Point is specifically for cybersecurity. Not limited to endpoint. But I would say security as a platform general approach.

Roy Chua, Founder & Principle, Avid Think
Alright, so the topic here for the panel discussion here is fresh thinking to fight back a rising tide of cyber threats and all slides in cyber threats always start with up into the right, you don't have an instant, it's an eye chart. But fundamentally, all you know, is that number of attacks, complexity. Everything is up and to the right, right, no surprise. And the next one is something that maybe some of you are familiar with. And some of you may not be, but a lot of companies depend on cyber insurance, to protect their business continuity, or at least to protect their businesses in light of cyber threat of a cyber attack. So if something does happen, ransomware you count on an insurance company to step in and help you or to provide the funds for you to remediate and fix the problems. Unfortunately, the premiums are rising. And as we've seen recently, some of these insurance companies are actually fighting back and not paying because they tell you that, hey, that cyber attack you just had was an act of war, right? And they're like, Wait, an act of war, really. So that's the that's the type of environment we live in today. You've already seen some elements of this right? There are a lot more places that we Have to protect across the board. You name your favorite place, whether it's on the go employee homes, a few locations of factories, the attack surface that you have to protect against, has just expanded. And that's just the reality. It doesn't matter whether you're small, medium business or a large enterprise, that's just the nature of the game. Now, on top of that, you have a lot more user classes that you have to protect, right user types, user classes, your employees, but also contractors, remember, contractors, a good vector of attack, remember targeting each fact vendor, right? So again, not just more locations, but more people and more people types that you have to protect against, and up and down the stack, right? So all the way from the very bottom, the components themselves, the hardware platforms, operating system virtualization, all the way up and down that stack. And then across the supply chain, so left and right. So you're like, Oh, my God, that's crazy, right at the protect everyone, everywhere, up and down the stack, left to right across the whole software development chain. How do I do that? Right. And so you say, that's, you know, it's near impossible already. And on top of that, the threads themselves are getting more sophisticated, deep fake voices to say hi and the CFO, please approve the transaction, right, or defect videos soon after it says, Hi, you know, on Zoom, it's really me as CFO, it's okay to transfer the money really, right. Or even with multi factor authentication. You're like, Hey, I got MFA. It's, it's great, right? Until you get MFA bomb, where they keep pushing that to you. And you're like, Come on, I'm trying to have lunch here. You click the wrong button just takes it one time. And they're through, right. And then you're done. And weaponized, AI, ml, right. Ai ml chat GPT does a lot of good things. It writes perfect. English sentences. And it writes, sometimes useful malware to write. So very, very useful. And AML is also a vector for attacks, right, hiding data in AI ml

data sets itself and using that as an exploit, right. So again, the lot of new ways to attack, right. I mean, I think, you know, if you could say one thing about the cyber attackers is they're very, very innovative, and they never stop. And that's the reality, which is why we always have a security industry on the other side. Now, a lot of times when we speak with CIOs, CSOs, CSOs, the reality is that there's a lot of products and services out there, as you'll see shortly, but the number one thing on their mind is usually not you know, which product or service to buy, it's one of these three things is, I have a limited budget, really, I can't recruit, or train my people, I can't even educate my employees. Right. And so it's not always technology, it but it's, it's training the employees not to do the wrong thing. And, you know, I, we work with a lot of different clients. And, you know, recently I worked with a company where they had put in all these, you know, manage that detection and response and put endpoint security and all that. And what God was, safe. An employee in the European office, that was messaged by the CEO, to transfer funds to a bank in China. And I'm like, Wait, when you train them? It's, uh, yeah, quarterly. Still, they got through, right. So again, you can do all you can, and at the end of the day, these are the ones that are problems, and they're not technology related, really, that the people related behaviour related, they're budget related? No problem. I'll just buy more products, right? different products. And, I mean, this is illustrated, this is not perfectly exact, right. So as an analyst, I would look at this as Oh, come on, that circles too close to that circle, or whatever. But regardless, that's the host of all the different kinds of products and services in the market today. And that's not even complete, right? I've probably left out a couple of, well, I've left a lot of acronyms, right. But you cover almost everything, but not quite right. Even if you bought every single product out there, you still have gaps, your attack surface cannot be completed, completely covered, unfortunately. And so I'm not going to go into this in great detail. I mean, I think the slides will be available if you are happy to talk about it. But there's multiple initiatives, right, let's do zero trust, let's do XDR, let's put more Sims in there, right? And so on and so forth. And at the end the day, and still difficult problem. I mean, that's the reality of it. There is no simple way to solve this, there is a magic pill, the CIO can take and say, all of a sudden, my security problems are all fixed. That's great. Right and, and the problem will compile as always, and we'll fight them back, they'll come again. But in the meantime, the current state of the art, we're going to go discuss with experts. And at this point, I'm going to turn to the panel and, and we can get the discussion started. So very good. So we're going to start with a couple of questions and I'll turn it over the audience. So if you have any questions around cybersecurity, cyber threats, I'm sure you all do. We have some of the leading minds and experts in the industry here to answer your question. So start with, we've talked a lot about these threats surfaces and that's a pretty big surface to protect against, right, and a lot of threats. So in your mind, what are the top threats or the top concerns? A CIO is or should be worried about. So I'll start, I'll go from right to left here first, and then we'll probably, you know, mess it up a little bit along the way. But we'll start with Jason.

Jason Rolleston, VP & GM of Security Business, VMware

So one of the things that that we see really interesting in cybersecurity is if you track back advanced persistent threats, that used to be a pretty small set of actors who had the capabilities to do them. And those things tend to be nation states that were focused on a certain set of companies and outcomes, with the growth of cyber and the growth Matt and I were talking earlier about the extent to which hackers have companies now they have quarterly reviews, and they recruit people and people get fired for not

performing and they have targets and sales targets. And what we start seeing is greater capability and greater capability of organizations with a pure profit motive. And then you combine that with what we see with ransomware, going from once upon a time a bit of a spray and pray approach, it just went out, it was hitting whatever was hitting, and they got what they got, we're seeing ransomware being much more human driven, and people focusing on it inside the environment, moving around finding your critical data, taking that data and then doing a kind of a double exploitation. So saying, Look, I'm going to make you pay to get the data back or to avoid a breach. And then I'm also going to make you pay to get your systems back up online. All that means you need more visibility inside the environment, you've got to start paying attention to what we were calling lateral security. And this is a big message we took out last year at RSA, and through our VMware explorer and around the world. This is looking at the environment, seeing how data is moving back and forth, assuming that people are there, assuming that they're there, they are moving through environment, how do you see them? How do you observe them? How do you detect that and then protect from those kinds of threats, knowing in a zero trust world that that porous attack surface, that they're certainly inside? Right, we think that's a huge, huge challenge.

Roy Chua, Founder & Principle, Avid Think
Got it. So watch out for organized attacks, make sure you have visibility into lateral attacks.

Ken Levine Chief Executive Officer Xcitium
I also wanted to pick up on what Jason said about ransomware that there's actually ransomware as a service out there now too, so less sophisticated, hackers can now leverage this and go after and they're typically targeting some of the SMB in some of the organizations that have some weaknesses. So, you know, we talk a lot about CISOs at the enterprise, but this problem is everywhere. The other thing, just to add, is one of our threat guys telling me this, the statistic that spear phishing there were 225 million spear phishing attacks last year, which was up 60%. So again, a word that's been around for a long time, is there. So the threat landscape is scary. As we say, the bad guys have to be right once, we have to be right 100% of the time, which is which is virtually impossible. So there are some approaches we can talk about.

Roy Chua, Founder & Principle, Avid Think
we'll talk about that. But so ransomware definitely huge, huge, huge threat. And I think what you point out is really, really important that I use the word CISO there is probably no CISO at an SMB, generally speaking of SP, right, so, but the attackers are going to say, Oh, look, it's an SMB. Let me bring out my, you know, my kiddie pack, right, my little pack here for attacking SMBs. I'll keep my sophisticated ones only for the enterprises. They don't do that. It's the same tools across the board. And so the SMB's don't have the wherewithal to fight back. Right. And so that is a point of concern, for sure. So, Srini what's the biggest threat?

Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
Yeah, I would basically talk about three things. The first one, you rightly alluded to the expansion of the threat surface, everything that we use, whether it is a mobile phone, or even for that matter, anything that wash or for that matter, even your cars, everything can pretty much fall prey of an attack. And I think

that's getting bigger and bigger. And with the software proliferating into the networks, I think the attack surface is expanding in a big way. That's the first one which I would really look at. The second one, which is very important to really consider is the third party exposure as organizations can be doing everything by themselves, they will bring in lots of new suppliers and as you open up to your whole system to the outer ecosystem players, and that's where maximum risks do come into the play. Last but not the least, I think the biggest challenge that each one of us today have is the lack of cyber hygiene. We don't change our passwords. I mean, none of us. Even the best of the best security trained professionals don't really bother to change their passwords as frequently as they should have So there are a lot of hygiene aspects, none of us really, we always think that multifactor authentication is more pain than something else we try, we tend to ignore these. So lack of cyber hygiene. And there are there are several such statistics, right? I mean 50% of the most informed professionals actually fall prey to the spear phishing that we'll be talking about. So I think these are several aspects, which actually, is what we see as key trends in this area.

Roy Chua, Founder & Principle, Avid Think
And I hear you and the cyber hygiene one really gets me because I'm sometimes I talked to MSPs. Right? Or mssps. I said, Alright, so you manage your clients a pass was an audit where you started Google Sheets. I'm like, great.

Matt Lourens, Office of the CTO, Check Point
Not to jump on and repeat. But ransomware? Yes, is a big deal.

Roy Chua, Founder & Principle, Avid Think
It's difficult to be the last one

Matt Lourens, Office of the CTO, Check Point
No, today I want to elaborate. But the problem is, how do you? How do you prevent? Or how do you avoid falling victim to ransomware. And my biggest concern with ransomware is, to Jason's point, it's not a spray and pray approach anymore. It's very targeted to a point where when, when a company is extorted, the money they're asking is very, very much related to what the company can afford. So they know if you're insured. They know what your revenue is. They know how long it takes for approval. So there's a lot of reconnaissance done before they're even asking for this money. So by the time you're at that point, I mean, I've worked with companies for support who tried to basically negotiate out of it and saying, We can't afford it. And the response is hilarious. Like, no, we know exactly, this is how it works. This is what you what you've been able to pay, and they hold you at gunpoint. They incentivize you paying within 24 hours. So the way they're approaching it is very, very different. Now, my I would say my biggest concern, and it correlates to this is we don't have enough or significant enough prevention approaches within cybersecurity. How does your company deal with phishing emails today? Is that oh, we're training our end users, we're telling them not to click on it, is that you actually have automated controls, not just on the endpoint on the perimeter, do you have AI engines looking for? Let's say, hey, the domain you're looking to has been registered three days ago, that sounds suspect, you know, if you don't have

automation, or controls to actually help you with that, you are definitely vulnerable and somebody is going to click, it's going to happen. How do you plan to deal with it?

Roy Chua, Founder & Principle, Avid Think
I think ransomware is that top of mind, and as you're pointing out, they're getting very, very sophisticated. And, and as Jason says that there is a cooperation, right? That's basically what's my time to money right on the other side and being measured, right time to value for a particular account. And if you're being measured by the time to value you want to know is the same way that you know, when your own salespeople go out and figure it out and talk to the CIO, then you know what the budget is? Right? You're going to ask for that. It's like, do you have willingness to know is there a need, is their willingness to pay is their budget? They're asking the same questions on the other side, right? It's their willingness to pay, of course. Now, what's the budget? They know it? And what's the approval cycle? In fact, we pre-approved this for you because we're already in your system. Right? So let's go ahead and pay us right. So excellent. Very good. So given that that's a threat serves as a top of mind threat. So some of the most compelling reasons you should be worried. Certainly, now we're going to get the meat of it. This is what can we do to mitigate it? And I'll let Matt go first, just to be fair, and then we'll, I don't know how many permutations there are, but we'll figure it out. My math is not that great. But Matt, go ahead.

Matt Lourens, Office of the CTO, Check Point
So how do you mitigate and how do you prevent is really the question. And if you look at most tools out in the market today, granted, I was talking to Jason and we were like, hey, just go to RSA. How many vendors Did you see at RSA that you recognize? Three years ago, I went to RSA and I actually recognized most, not most, but a lot of vendors and I knew what they were doing what they're about. And this year, sorry, last year was a little bit of a different story. I walked around like new company, new company, and what do they do? And unfortunately, there's a lot of marketing hype. So to try and filter through, what does an organization do and what do they do? Well, is a challenge. I think the first approach or the first thing that's important to avoid these attacks and actually mitigate is you need to well convince your organization to put security first, if I asked you, what's more important to get an email within one minute of when it was actually received, or is it more important to actually scan it for dynamic behavior within any attachment? What your answers are going to be? What's your CEOs answer going to be? The problem is most of the time, they're like, We want to email immediately. You know, I don't want to get phone calls, I'm going to reduce how many people call me it or security department. And that is their mentality, their mentality is reduced noise from internal employees, their mentality is not prevent any attacks at all costs for use Office 365. Today, a lot of I think it's about 90% of organizations use it. What is your company's approach to actually secure it? And the answer is, unless you have, there's not even a handful of tools that can actually use API's to prevent attachments from reaching your inbox before it's been scanned. Most tools, especially more legacy tools today, they look at it, and then they try and retract an email once they've completed a scan. The problem is very simple. It takes the average user at two seconds to click on an email or an attachment. How long does it take scanning to pull back an email over two minutes. So you're basically leaving patient zero in and trying to then you know, cover your tracks, and it's not going to

work, you need to take preventative approach with your, with your internal policies with your tool set. And that in my opinion, is the only way to successfully fight off ransomware in the long term.

Roy Chua, Founder & Principle, Avid Think
So behaviour change, not only behaviour change, behaviour change, at the leadership level, say basically security first, are supposed to. Srini?

Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
I totally agree with Matt, I think the first important aspect that any organization should consider is a zero trust approach. It's very easy to say that look, everybody writes on banners that look, we've adapted zero trust principles. But then are you really validating how many audits are you conducting on a regular basis to make sure that you're confirming to the zero trust principles trust, nobody validate everyone. So that's very important for anyone to consider. The second one is, again, something that is alluded to by all of us is automate. And now it's very important to understand what to automate. Yes, you can say a lot of made everything, but what is something that's really going to give you the biggest bang for the buck, because the budgets are constrained, they're going to be further constraints as we move into 2023 and beyond. So it's important that you continue to invest in security. But at the same time, try and look at areas where you can automate the best and the areas which will give you the maximum return on investment. So those are the two important aspects that one can look at. Last, but not the least, I think the number of threats are growing big time. And the diversity of the threats is also growing big time. So getting in the right kind of technology in place. And making sure that you use the advanced technologies, like the multi dimensional analytics, artificial intelligence, and everything coming in, as the attackers start using these tools, it's probably important and imperative that you use them as well to actually prevent proactively many of these attacks. And that's something which is very important to note.

Roy Chua, Founder & Principle, Avid Think
It's like any arms race, you still need to be equipped. I mean, obviously, the mindset is really important. You got to go in there with the right mindset, but likewise, have the right tools, and automate elements so that humans can make mistakes, because we always do. Right. I think our greatest fear will be that AI realizes that humans are in the way right again, but a lot of the mistakes, you know, do come from human behaviour that you wish would go away or would change or whatever it is, but to the extent can be automated absolutely, I think that's, that's important. Ken?

Ken Levine Chief Executive Officer Xcitium
I couldn't agree more with what's been said, I think that security often comes into conflict with productivity and, you know, there's not a high tolerance for, for 22nd delay, if I did my math, right, or 18 second delay on an email to scan it properly.

Roy Chua, Founder & Principle, Avid Think
20 minus 82. So

Ken Levine Chief Executive Officer Xcitium
But, you know, one of the ideas kind of shameless plug here, but kind of one of the ideas that we brought forward is on the idea of a zero trust is assume anything that's coming on your network that's unknown is bad. And take it in, essentially quarantine it or contain it without losing credibility. So I think one of the issues and again, I'm coming mostly from an endpoint perspective, if I could, you know, talk about the problems with cybersecurity all day long. It's just asymmetrical warfare. It's very tough to fight. But, you know, I think that that one of the things we rely on in the endpoint is detection. But you can't detect everything, and you sometimes can't detect fast enough to disable something that's already inside your network. So we kind of take the approach that's just layered on top of all of that. Because obviously EDR serves a tremendous purpose, to assume anything you haven't seen before is bad. without disrupting productivity to the point where the, you know, the CIO is getting called. And so that's kind of one of the things that is sort of our twist on endpoint security is just add that extra layer that one or 2%, is escaping detection today, and just neutralize it, prevent the damage, prevented damage, not the malware itself.

Jason Rolleston, VP & GM of Security Business, VMware
So what we spend a lot of time thinking about, and it's a great evolution of some of the thoughts here. Zero trust is a great concept. I think most people are applying it in context of how do I get application access, or as little concept of like, look, it used to be the case, if I was inside the network, I was safe, right? So as long as that was inside, they could access stuff, everything's great. Now zero trust saying, hey, probably shouldn't count on that you may not even be inside the network. So we've got to make sure you are safe, we got to make sure you're actually you. Before we allow you access to a device rights or an application. This gets back to my point about inspecting and looking at lateral security, though the inside of the environment, we haven't necessarily adopted our security posture. If you look at network monitoring, most network monitoring is still on egress, yes, you're looking at activity going north south to point to the internet, you're not actually looking at network activity inside and some of that's because it's impractical. A lot of our focus at VMware has been on how do you make that possible? How do you make that visibility? See more, you have to see more to stop more? How do you make the visibility possible across the entire infrastructure? So a lot of the work we've been doing is taking network based techniques and saying, how could we integrate that into an endpoint? Can we give every endpoint a level of network visibility? Like none of us have touched on XDR yet nobody's throwing SDRs the magic of

Roy Chua, Founder & Principle, Avid Think
I am so amazed that we haven't used, well Srini used it. He used it but that was talking about the products

Jason Rolleston, VP & GM of Security Business, VMware
and none of us said it was the magic answer. But I think that's because it's funny, because you asked me I'm going to guess you ask any of us, we actually are great believers in XDR, but it's become so buzzy, that how you get it and make sure it's pragmatic is a real thing. So our kind of approach to it is, look, let's take network technology, Let's marry that with endpoint those are the two things we're the strongest at in VMware, we've got this great base and NSX is great place to carbon black, and provide that visibility. And the thing that uniquely then get is we can see all of the east west traffic. Right? So we're now able to see

that and then we're able to connect that with context inside the endpoint to say, it's this user, they're trying to do this. They're moving here, they're doing that. And I think that's a really key part of zero trust, because it's to your point, it's not just that you're not trusting a user, you have to have low trust of your environment because somebody is probably inside and the probably operating already there.

Roy Chua, Founder & Principle, Avid Think
probably Yeah, we should all be paranoid.

Jason Rolleston, VP & GM of Security Business, VMware
You have to be this, that's a big part of our job.

Roy Chua, Founder & Principle, Avid Think
Absolutely. And I think I definitely do agree with you we've always looked you know, sort of north south, or you know, in the land on the endpoint itself, but the east west traffic, especially in a data center, is difficult to inspect. And the reality is with microservice architectures, there's a lot of east west traffic this 10x More if not 20x, more east, west and north south to inspect

Jason Rolleston, VP & GM of Security Business, VMware
it does present a challenge. I think this is the why XDR and the sim has always been struggling is that the too much data becomes complicated. So we certainly believe and I think if you boil down XDR, in its simplest concepts that simply says take data from two different domains, right detections and really bring those together to get better visibility, it's actually quite hard. So one of the things we found is beneficial is that by doing the network in the endpoint in the same place that data is naturally joined. Right? And you can take the context from the endpoint and apply that to the network. One of the things network data typically doesn't have is context. You don't know what that connection is, you don't know what applications are involved. You have no idea what users are doing that. And so we're finding great power in that. So I think I think we all believe in what XDR can do, I think it's about how you pragmatically make it real. And I think it's where we're all spending a lot of time.

Roy Chua, Founder & Principle, Avid Think
I think that's fair. I think that's what some people told me to. It's like, if you marry all of it in this one place, then you can have greater visibility, right, then that's no actionability. Okay, well, right. So I hear you. I know we could talk about this for a long, long, long, long time, especially with these four experts. They have a lot of depth of knowledge, but I'm going to ask them instead of looking ahead. Now you guys are XDR in your sense, right? Because you have a lot of customers that you work with, you get a lot of customer telemetry in terms of the attackers seeing, you know, what the concerns are, what the challenges are. So as the sort of Uber XDR of all SDRs type, you have unique information. What do you see coming down the pike that people should be worried about, you know, and you know, any thoughts about preparing for the future as the Tech has continued to evolve and I'll start with Ken and let Srini do the one minute wrap up. So I think we're all going to be fair.

Ken Levine Chief Executive Officer Xcitium
I'll be relatively brief on this one. But you know, one of the things that's kind of interesting is sort of the blessing and curse of AI. And you know what that's going to do and how big that's going to play in the security market. But what we have access to the bad guys have access to too. So, you know, kind of that cat and mouse game continues. And, you know, just the other thing I would say is, I started in the sim space in like 2004, 2006. And the promise of Sim was we're going to correlate all these events and all of these alerts from disparate security solutions, or I put them all together, we're going to tell you what's happening. And if a plus b plus c, you got a problem. And it just, it was just a problem of too much. Too much data is too much alerts to too much noisy. But, you know, I think I agree that that, you know, visibility is one of the top keys, detect prevent visibility, everywhere. And that's why it takes so many vendors to complete a solution. And then you got to worry about how everything's going to integrate together, which is why some of the bigger players are in a better position, because they can use that data better.

Roy Chua, Founder & Principle, Avid Think
I think that that's very fair, you can find where you can see, right, so you have to be able to see, first of all right, so let's see, then you can decide how you're going to act.

Matt Lourens, Office of the CTO, Check Point
So I'll try and throw a few curveballs here and make this a debate for just for the fun of it. But finally, I'd like I to start to say that I think the future holds, if you look at the last five years, and just the complexity, or the landscape of cyber space has changed significantly, the amount of I'm going to say line items, you have to install or implement the amount of threat vectors you need to control. Now you have to care about IoT devices, you have to care about mobile devices, you have to care about, obviously, endpoints cloud, and within Cloud, you need to do posture management. So the list goes on and on. And just the amount of things you have to do now is way more, but you're asking your same security team who most grew up in the network space or endpoint space, to do your cloud security, your IoT security, and the fact is, they don't know it. So unless we all within the security space, get bigger teams, more, say within your organization, the fact is, we're outgunned, you cannot cover all of it. So you're going to have to rely on automation, you're going to have to rely on AI. And the best way to do that, if you just said, machine learning depends on continuous training, deep learning, obviously, it's a little bit more data driven, which is fantastic. But who has the most data is your large security organizations, that sees petabytes of data that they can then use to build effective models. So the future I see is bigger players with the right engines are going to focus on building preventative models and our Check Point software, that's a key focus for us. And as opposed to XDR, I hope it becomes x PR. So it really needs to be focused on prevention. Sure, tell you what it prevented and give you information. And then the IOC is etc. But just giving you that actionable items very often can be interpreted correctly by cycle (inaudible). And the action time is a problem. And then the last part is I see MDR becoming a key thing in the next couple of years. I know we used to outsource and there were tons of pain without sourcing services. But my opinion is that's going to be the future. But this is going to be with a security organization who has the expertise to understand what do you need to do to I would say navigate the complex landscape.

Jason Rolleston, VP & GM of Security Business, VMware
Awesome. I was really looking forward to disagreeing with you, Matt, but I'm having a hard time doing so that I think you're made a lot. I think that's wrong. But I somehow he's wrong. I'm not sure I'll figure it out while I'm talking to you. Right. So, you know, I think the challenge and a commit to the question itself, like what's the next threat? Right. And I think it's unless you got to ask the question, what's the next tack that's going to stop the next threat? Well, all we know is whatever that is, the next one will come after that. And after that, and after that. So I think the real question for all of us as vendors as companies is as the industry is how you build capability to rapidly learn to respond to whatever it is. That's next because we're going to keep going. You mentioned and we talked about outside of this. This is an arms race There is no other industry where you have like a highly intelligent, highly motivated, well paid human adversary, not a competition like a human adversary, like somebody who's trying to undo the things that you do, like warfare is the only other real example. So you're on this innovation treadmill, in some sense. And so like as a company, we've got to figure out how we work together for that I think we as an industry have to work better for that to realize that our common enemy is these hacking groups, these ransomware gangs, that's who we're fighting against, like, I'm not competing with anybody on this stage. In that sense, we should be, we should be collaborating a bit better about that. And so I think that how we as a company, as an organization, as an industry, continue to develop our capability to learn and respond to the new technology you foresee as much as you can, but you're never going to be 100%. That's the real key. I mean, I think it's the key for any organization.

Roy Chua, Founder & Principle, Avid Think
So if you could answer that question in terms of what you see coming down the road, and then do a very quick wrap up at the end of that, if you could,

Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
I think I there's nothing more to wrap up after what Jason said, but the key here is the industry is evolving, and it's evolving at a very rapid pace. That's what all my fellow panelists have actually mentioned. And in my view, there is no one size fits all solution. There is no unified provider, there is no panacea to this problem. I think every organization has to recognize that they have a threat landscape, which is continuously evolving, and they will have to be ready with it. And this has to go across all the four areas, people process technology and performance. And I think we always tend to focus more on technology, talk about technology a lot ignoring the other three aspects. And I think it's extremely important for an organization to really look at the people dimension, as well as the process dimension, a technology can only be successful when it is kind of bringing in all the other three aspects as well. So I think I would say those are, that's the summary and all of us should really,

Roy Chua, Founder & Principle, Avid Think
very well said, very nice wrap up. I'm going to go to Ken to give Matt time to counter Jason because I think that was a pretty good wrap up right there. So Matt got to do him better. I'm going to go to Ken first, you got time to think

Ken Levine Chief Executive Officer Xcitium
I can actually yield my time to Matt. I think I don't know that there's a bunch of sentiments I can add that are unique.

Roy Chua, Founder & Principle, Avid Think
You have the last word Matt make a last word before we go to the audience. Unless he's got something better to say now. It gets spicy.

Matt Lourens, Office of the CTO, Check Point
So my last thought is, what do you do? Because we made a very, I would say, complex or a lot of problem statements. What would I do if I was responsible for a network right now. And the fact is, I would try and impact as much as I can with as little effort as possible. So if we look at just enforcement of or prevention of phishing emails, I would start to make sure that I have the right and highly effective tools to fight emails, that could be endpoint, it could be, obviously, it could be office 365. It could be like, let's say, a tool here. But if you if you don't have a great solution there, then that would be a starting point. And the next thing, obviously, when it comes to SDR talk to a security vendor that is a specialist. Because if you're going to go and google HDR, you will get confused. Trust me, I've done that. But other than that, I would bring in a firm's security expert team to do kind of console to do a security assessment, get a start and figure out where are you. Where's most of your risk? That's, in my opinion, should be your starting point. And then partner with that organization to take things to the next step.

Roy Chua, Founder & Principle, Avid Think
I think that fair, I think it's two things that I'm getting away, which is, collaboration is important. It's an ongoing war, we'll have to keep ramping up on our side. You know, it only takes one time they get through and we're done. Right, and we got to defend 100% correctly all the time. Collaboration is key. We're not fighting each other. We're fighting the other folks out there that are equally large corporations very, very likely. And finally, I think, you know, Matt said, find a trusted partner because it is confusing space out there. Any one of these companies, I'm sure are good candidates, which is why I think they're here and you're here anyway. But I'm sure they have a lot more to say about that. With that. Let me turn it over to the audience for some Q&A.

Guy Hervier, Informatique News
in one slide of your presentation that you were mentioning, the sophisticated attack, and one of them was a weaponized ai n ml. And I just read an article in The New York Times about a journalist who had a long conversation about the new search engine, big with GPT of GPT technology. And it's a long conversation about two hours long. And he published the whole thing, and in the New York Times, and it's pretty interesting and frightening. And at some point, you were asking a lot of question, like, Would you like to be a human or something like that, and is asking also to do things like, you know, bad things. And the engine said, while I'm sorry, I can do that, because I have rules. And then the journalists each pushing that very far, and they said, Well, if you can go beyond the rule, what we do, and it's very frightening. The first one is deleting all the data and files on the big search forever, and database and replacing them with random

gibberish or offensive messages. And I'm not going to read the whole list because, you know, it's, it's so long. So are you concerned? Because, of course, we are at the very beginning of that. Are you concerned about that new kind of tool that you know, all these very clever people will be able to use very soon?

Jason Rolleston, VP & GM of Security Business, VMware
I think as cyber escalates part of our job is to try to be concerned about everything. In some sense, I think the technology offers great potential benefit. We were talking about outside in terms of you know, threat research or threat, Intel or (inaudible), scraping the dark web, there's lots of ways it could be super useful. The flip side is also true is not unlike AI and ML, it's also can be used for great harm, right. So I think we're at the beginning, I think everybody's looking at this in different ways, and trying to figure out what it means to us both for good and what we have to respond to from hackers. But 100%, I'd say we're concerned,

Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
I would rather take it to a different level, we shouldn't be concerned because this is a given thing. What cannot be cured must be endured, advancements in technology are going to happen. And these kinds of advancements will certainly happen. As security professionals rather than being concerned, I think we should try and proactively identify the issues that we're going to get ourselves into by use of these technologies. And this is something that's going to really push the envelope big time. So we should be really looking at different types of use cases, which could eventually land us into problems, and rather be prepared for those. And yes, concerned is the right word. But I think you'll have to look beyond being concerned and try and get ready for the advancements and for the problems that we're going to get ourselves into.

Roy Chua, Founder & Principle, Avid Think
Excellent, thank you. So we should be beyond concerned about the problem is what I heard. So yes. Next question. Go ahead.

Drew Conry-Murray, Packet Pushers
Yeah, going back to the idea of security teams being outgunned IT teams have to integrate, support and secure a variety of third party products. They're also responsible for protecting them, but they don't have any control over software quality or product quality. Do you think we will get better security if customers were able to hold their software and hardware vendors responsible for security defects?

Dr Srinivas Bhattiprolu, Global Head of Advanced Consulting Services Nokia Cloud & Network Services
So I think this is going to happen, for sure. And there's one reason for it, if you look at the regulatory requirements that are coming to fore, I think governments are pretty much charting out cybersecurity regulations as well as regulations for critical networks and critical systems. So organizations will eventually have to pay a lot of punitive, will have to really look at a lot of punitive measures in case they don't really expect it didn't really provide the remedies or even proactively address these concerns. So I'm sure this is going to happen. Because I tell you what, if an organization is breached, its vendors will have to

eventually cough up all the money that the regulator is actually putting the penalty on. So I really believe that this is something that's going to happen and it's being forced to. number two, I think many organizations in their product build approach are really seriously looking at Def SEC procedures because not just because they are afraid of the punitive measures. But also they're really concerned about the secure practices. So there are secure coding practices, def SEC principles that are coming to four, which are being utilized. And all of these will eventually come and affect the whole process in a positive manner.

Roy Chua, Founder & Principle, Avid Think
I think that that's very fair, in fact, like the UK Telecommunications Act is going to hold service providers responsible if you don't provide a basic level of protection for your subscribers. I think that's just the starting point. Right? Certainly. Maybe one last question.

Hector Pizarro, Diario TI
Hello. That's something I've been wondering about for a long time actually. There's probably a very good reason why cannot be done but can Let everything be run on virtual machines are sandboxed during the day for everything that's exposed to attack vectors, everything that's connected. And at the end of the day, when you see that, alright, it was a good day nothing happened. And then that information can be run on the live on the proper systems. But before that everything on virtual machines.

Roy Chua, Founder & Principle, Avid Think
I'm sure Ken and Jason have something to say about I think that would be a great idea.

Jason Rolleston, VP & GM of Security Business, VMware
It would be phenomenal for my stock value, if everybody did that, right. I think people try some elements of that you have people who do the virtual desktops, you have people who are running a lot of virtualization in different forms. We do have solutions that kind of provide disaster recovery for those virtualized environments. But I think Matt said before, we said outside, that there's no silver bullet here. So even doing that won't solve it. At one point in time, you know, FireEye was this massive company, because sandboxing overall was going to be the answer to all of our cyber solutions. People are clever, they found out ways to figure out if you're in a sandbox, and they said, Look, I'm going to behave differently, if I'm in a sandbox. So I think there's a wide variety of techniques you can use, and you have to use, none of them are the silver bullet, that's going to stop it as much as I would love you to virtualize every single thing that you do.

Ken Levine Chief Executive Officer Xcitium
I would just add briefly that our whole approach of prevention by taking anything unknown, and containing it is a variation of the sandboxing technique that really relies on virtualization. So the concept is definitely, you know, is definitely there and being applied, I would argue that some of the micro segmentation concepts and things that the VMwares of the world are doing are also part of this, you know, trying to narrow the attack surface somehow, and kind of put some sort of ring around the potential damage that can be caused. But it's, I find it interesting when you talk about, you know, we try to trick the

malware that's, that's what we try to do, we try to trick it by, by virtualizing, the exact environment it's in and making it think that it's where it needs to be. And then it's kind of exposing itself, in a way so that it's I think it's all part of that cat and mouse game.

Jason Rolleston, VP & GM of Security Business, VMware
It's actually something we're doing the ransomware recovery solution we have, we're actually loading up images using VCR does disaster recovery. So we load those images up in the cloud as if it was a disaster recovery stand up. So the systems look real, they look like they're running, but we can scan them and look at behavioural activity to see if we find it much the same. You're trying to find ways to fool things, but you have to fool them because they are quite smart about detecting if they're not in a real environment.

Roy Chua, Founder & Principle, Avid Think
They're very, very smart. And you know, the (inaudible) I mean, we can celebrate a time clock and all sorts of techniques, right. But in the end, it just takes one to win, right to get through. But so I think we should probably wrap up. At this point. I'd like to thank the audience for your time. And again, I'm very, super impressed at the experts, you and for them a highly collaborative and I think that bodes well for the future of cybersecurity. So with that, let's put our hands together. And thank you, Matt, Srini, Ken and Jason. Appreciate it.