Network & Data Center Security

October 7, 2021

Draft Transcript

Featured Speakers:

Analyst Chair: Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware

Mark Fox, CEO, NetEvents
Hi everyone, I'm Mark Fox CEO of NetEvents, delighted to welcome you to this session on network and data center security partner for this event today is the Dell'Oro Group, and we have the head of their cybersecurity research, Mauricio Sanchez, who will be chairing today's session, and introducing the panel. So Mauricio over to you.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks a lot, Mark. Good morning, good afternoon, good evening as the case may be, again, Mauricio Sanchez from Dell'Oro Group, really glad to be here with a distinguished set of panelists, including Jordan LaRose from F-Secure, Gail Coury from F5, Dr. Ronald Layton from Sallie Mae, and Vivek Bhandari from VMware. So we're here to discuss the network and data center security in the age of COVID. Before we get into our discussion. I'm going to spend the next several minutes discussing some of our research because we're a quantitative market research firm, wanted to bring a little bit of the perspectives as to what we're seeing, specific to the network security landscape. To all of us the pandemic has been very trying over the last 18 months and through enterprise it's been no different. What we've seen is an acceleration of three tectonic IT shifts that were already there but really

accelerated, somewhat like an earthquake which has shaken to the foundation of every enterprise throughout the globe. For us was the shift towards the cloud in the enterprise digitalization so the massive movements of workloads, as people disperse. As this became distributed, we saw a huge influx of workloads and as that takes place there's a lot of things that could go wrong. We'll talk about those during our conversation today. We've seen a massive shift in that move to some form book cloud based architecture on the workplace front. I think we're all still poster children of this of having to work from home and little did we think that 18 months later, any of us would still be working from our home office. This feels like it's going to be the new normal as we look towards the future, some form of hybrid work with part of the week from home, part of the week in the office. All of this is then raised, the importance of that online business experience so enterprises that weren't necessarily digital or having a strong face to the on the internet and to their clients and to their workers now find themselves really having to dial that in. The conversation we hear is really increased around what is a business's online digital experience, from a security perspective? Security has become even more daunting for many of the security practitioners out there, probably feels a little bit like an army of one like this fellow here and in the dark room, whether it be again the misconfigurations that lead to data leakage into bad things because as Wall Street called out a human error is often the culprit of cloud data center breaches. This last year in particular, and then summer timeframe, was extremely trying as the ransomware hit the front page news with folks like Colonial Pipeline, getting hit really hard and causing a massive outage of their facilities, and most recently there has been another example of how, in Russia Yandex had to propel, one of the largest DDoS attacks in history. And so during this pandemic, the security hacker community the cyber threats, haven't really slowed down. In fact, they probably have accelerated in many respects. So, as we look in this landscape, we start thinking, okay, so where were enterprises today? What is one of the facets of their journey? We're going to discuss a number of facets, that's where the panels come into play and so for a lot of enterprises when we think about networking, a lot of enterprises are still on what we call a legacy network architecture. That classic hub and spoke that has worked for many decades, It was a tried and true model with the inside of the corporate network trusted, and that everything backhaul to that central data center, before we got sent out to the internet and the internet at large was the space that was untrusted and so there was a huge moat, so this was a model that worked well, but given the tectonic shifts that I outlined in terms of the enterprise digitalization the workforce reinvention, as well as the need to have a strong online business presence. I think over the course of this pandemic, a lot of enterprises have started to, to understand that this architecture no longer fits what's needed. There's any number of issues here beyond the security landscape that are researches, as found to be the case of this classic network architecture model, ranging from Port app experience to again any of the security threats that I outlined, let alone the complexity and rigidity and the high network costs associated with this all leading to hair on fire of the IT staff. Just the enormous amount of pressure the IT operations face to keep up this old way of doing things in a world that no longer really fits this this model of operation. So, in our research we've been starting to look at how leading organizations are looking to address this specific challenge. What we've seen is the rethinking of when network connectivity and security. This drive to combine the networking and security in a much more coupled fashion than that in a tight fashion with the aim to provide the agility to that allows the reconfiguration of networks, and in a real time fashion, being able to have dynamic scalability that if there's additional network and security processing required that can be

done, no differently than app developers have been accustomed to spinning up New Virtual Machine new containers. Being able from a networking perspective to say, okay, I need more bandwidth, more capacity at this particular point in networking for these particular applications and users. And then lastly, raise the bar on the security front, being able to ensure that from where we're coming with a most centralized perimeter security, we move into a world where security is distributed and available to where the action is happening. So this led to a new class of architecture solutions with some enabling technologies. So what we've been seeing over the course of those last 18 months, and this journey, perhaps started a little before that with some early innovators in the vendor community. They rethought the legacy network, and taking enabling technologies from the networking world that came into view over the course of the last several years. For example on the networking side SD LAN on the security side, some form of a cloud secure web gateway with advanced functionality. What we've seen is a marriage of these two technologies into a new type of topology and network architecture. That it's fundamentally premise on the cloud native instantiation of services network services and security services in the cloud that the enterprise can latch on to. And all assets that need to communicate with one another can be able to leverage this network in the cloud. To be able to provide that connectivity, and this is what the industry getting into the academic side has been calling SASE, or secure access service edge. So we see this as the next wave in networking. To be able to get to service those pain points that I outlined that have arisen in the legacy architecture, and service of enterprises that are moving towards greater amounts of digitalization contending with a remote workforce, a distributed workforce, and highlighting the need for better online business presence. The vendor community has responded in kind, what we do is track technology markets down to vendor level on a quarterly basis. What we've seen is that this intersection of networking and security has brought those players in, or in security, out of the woodwork to participate in this new market, providing a converged networking security solution. So many brands that we recognize from the networking world as well as some that are up and comers are coming from adjacencies that we probably at first hand wouldn't necessarily contemplate as being network or security vendors, They're all coming into this frame of being able to want to participate in this solution journey. And why is this the case? So, the reason the conversation is so exciting for the vendor community is because of the appetite that we foresee that will take place from the enterprise side. These markets are converging into this new class of products and new style of architecture. We see this as a significant opportunity for the vendors participating and we quantify this from the perspective that last year this was a sub 1 billion dollar market. But over the course of the next several years we see a doubling of this market and putting it on the pace of surpassing and entering double digit billion. So this is a massive need that the vendor community has jumped into. Here at Dell'Oro we're very keen on seeing how this market evolves, and then ultimately how this is going to be embraced by enterprises.

So with that, hopefully it presented a slice of facet of a challenge, and the particular set of solution dynamics that we see happening. I'd like to introduce my distinguished panel, we're going to be discussing similar topics, what do they see as challenges, what do they see as the technology solutions? And then we're gonna dive into the last piece, which I call the vegetables on my dinner plate, the operations. Because all too often we forget and sell short the fact that operations is part of the

equation to a successful security journey. So with that, let's start off with the introductions here and Jordan please, the floor is yours, give us a little bit about what you do at F Secure.

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Thanks Mauricio. Hey everybody, I'm Jordan LaRose I'm the Director of Consulting and Incident Response for F-Secure North America. Basically, my role is focused with me and my team doing boots on the ground incident response operations. penetration testing, design reviews, risk assessments. All of the things that feed into a successful security program. So I've got a lot of frontline experience dealing with things of that nature.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks for that, on to you Gail.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, thank you. Hello everyone. As Mauricio said my name is Gail Coury. I'm the Senior Vice President and Chief Information Security Officer for F5, and so on the frontlines every day with security and the challenges that we continue to face as technology changes and shifts rapidly. We have to keep the old stuff going on, we have to keep the news, we have to get involved and make sure we have security addressed in the new newer technologies as well so every day's a new day.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks Gail, on to you Ron.

Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
Good morning or good afternoon or good evening everybody. I'm Ron Layton, I'm the Vice President of Converged Security Operations at Sallie Mae. I've been in the private market for about three years, I have previous experience with the US Secret Service, a number of technological assignments involving both technology and cybersecurity. I think the two are related but different. I was a deputy director in the National Cybersecurity Division. When I had that job that was a bit of a convergence job where immediately after 911 I had law enforcers and intelligence professionals who worked for me and with me, and that was a bit of an unusual new experience because prior to that, those two silos, could not talk to one another. I was a deputy CIO for the Secret Service, as well as the first appointed Presidential Liaison to the White House. At Sallie Mae one of the things that I do is I've got one foot in physical asset protection but I also have another foot in cyber. And so the idea is to take two distinct silos of information, both physical assets and both physical and cyber and merge those together in what we call converged security operations, so thank you for having me today.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks Ron, and last but not least, Vivek on to you.

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
Yes, thank you. Hello everyone. I'm Vivek Bhandari, the Senior Director of Product Marketing within our Networking and Security Business Group at VMware. I go to market for our network security solutions, and also the zero trust positioning for all the different capabilities we offer to our customers. I've been in security for a really long time, so even prior to VMware I've been in different sort of roles, product management, product marketing roles at small and large companies. Google, Cisco, startups, VeriSign, and it's just been a fascinating journey, I mean for all of us here, just looking at how the security landscape, both from a threat perspective as well as a solution perspective has been evolving over the last couple of decades. We are really at this critical point where we really have to challenge ourselves, both as technology providers and from a solution implementation perspective, from a customer perspective in how are we approaching this problem? And really start looking at it in a very different way with a very fresh perspective and approach, and hopefully we'll get through some of those conversations here, so looking forward to it.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Fantastic. So clearly we've got quite a distinguished panel today with a lot of institutional knowledge. So with that, let's jump into our conversation, a three-parter discussion, discussing challenges and discussing technology innovations and solutions. And then lastly, talking about the operations in the enterprise teams who need to deploy and consume this technology. So our first discussion is around the threats, the challenges, the landscape. The question to the panelists today is, what are the top security threats enterprises are facing today? I'd love to hear it from the perspective of what you guys are seeing day to day. Gail, I'd love for you to kick off with a perspective of what you see for your firm.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, thank you very much. I think the challenge we have today is multi-faceted. The technology changed, literally overnight when COVID hit, and we immediately moved workforce home. There's this concept that was very clearly articulated with Mauricio's traditional architecture diagram where you had a perimeter on your network. Your employees were on your corporate land when they were in the office, if they happen to be remote they would VPN, but you still have this concept as I've seen, and many enterprises I'm sure are much like F5. We have moved so many of our applications out of our data centers today. One of the top goals I think that we have within our technology services organization is to be eventually completely out of that business. I think about how our workers do their work today remotely from their home offices. They very rarely are getting on VPN so when you think about that, where are they going for their application services, their business needs, to be able to do their day to day job? So, it's a very much an expanded attack surface, right? I still have stuff in my data center, not quite moved yet. I have stuff in applications that we're using SASE for. We're in multiple clouds across the world to be able to not only manage our employees, but to support our customers, so that attack surfaces quite large and you think about the applications. These are the threats to the applications, the threats to the end user, threats to your devices your users are connecting from. This brings us back to really having to get into a place of zero trust because we don't know. You have to

validate all of the things about the user, even with multi factor authentication you think about that. I have an individual who is trying to connect, let's say from halfway around the world, but their multifactor, their phone is sitting somewhere local, and wherever you are, you think about that. This is not a real individual user who's trying to connect. Do you think about, oh is the application the right application? Are you validated, your device is there, a way for you to say, I know who this user is, I know the device they're coming from, and that device is healthy. So you think about that and then you touched a little bit on ransomware, I think as a CSO, and I know many of my counterparts, this is one of the areas that keeps us up at night, because of all of this expanded tax attack surface I just talked about. Then you have phishing coming in and sometimes the human factors that you raised earlier, who's going to click on what and what is that machine connected to and how is malware going to spread across your network? We've seen this happen over and over. I think attackers have decided this is a very lucrative business for them. It's pretty easy for them to get on the system and to be able to launch their malware to encrypt a lot of data and hold companies hostage. So, you think about all the protections you have to put there, and then it's still all the other things that you still have a network left, I still have to protect that network, I have all these users, remote again, that expanded attack surface. It's a lot. And so nothing goes away, you just get more and more and more added to your plate to think about where you could have a successful attack and you only have to be wrong in one place, right. So, that's a challenge of defense.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Wow. It was so many areas that I heard you touch on. But very much what we hear from the enterprises that we interacted with over the last 18 months, the challenges that COVID presented, and just how it turned the entire enterprise sideways to practically double, if not triple the amount of work that was cut out for the SEC ops, not just a sec ops. I should be honest, all IT teams did heroic efforts to patch together to respond. So, not sure how you get your sleep, how much sleep you get in a given night, given the all the long list of things, but I'd like to hear from the other panelists in terms of what are the things come to mind in terms of the security land, challenge landscape. Anything else comes to mind from the other panelists?

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
So, as somebody that's on the front lines of incident response I definitely see a lot of these same issues that Gail has mentioned. But some of the trends that I've been seeing I think have been really really interesting and represent attackers adapting to the new defensive measures that we're putting in place, the new technologies that we have, to stop more classical attacks like ransomware. And it's funny, I'm saying ransomware is classical right, it's really only been around for a couple of years but that's how quickly the industry is moving nowadays. So one of the trends that I've seen recently that I think represents a huge threat to the industry and is something we're gonna have to adapt to quite quickly, is ransomware attackers are not just targeting computers anymore, they'll go in, they'll attempt to do the classic Kill Chain, expand their access across the network, deploy the ransomware. But what they'll also do is target key servers, key users on the network, exfiltrate intellectual property, could be blackmail information could be anything they see as valuable or something that they can take and then do I

guess you would say a more true to life, ransom. Where they'll take that information and they'll hold it hostage and say if you don't pay us this money we're going to leak this information to the public Internet. I've seen them in many cases put their money where their mouth is if they're not paid off. So, this is really a big challenge for the industry because with classical ransomware in order for it to be effective, it needs to target the entire network. It needs to affect the backups and really stop everything in its tracks. But for this more targeted type of attack, they only need to compromise that one critical server, or they only need to compromise that one key user account before they're able to ransom and threaten the business in this way. So, I think what this really points to is a need for the industry to increase security even more, which is already a challenge, right, but now we have to think about, okay, our crown jewels, we're trying to protect them already. But now, how do we make sure that nothing goes in or out? This isn't just your key database, but this is your CFOs laptop that he's got sitting on his desk at home in Florida. It's a really complex problem and I think one that every company needs to target differently, but it's certainly something to think about and I'd be really interested to hear what the other panelists have been seeing as well and if that's something they've experienced too.

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
I can jump in here just to add to that perspective. So at the start Mauricio nailed it right, like we all know this massive digitization, we were already all on a journey of digitization for years coming. The pandemic certainly just accelerated that, it went from zero to 60 in 2.7 seconds or whatever, this latest start from Tesla in their cars. So we really accelerated this and it's become a field day for the attacker. It's really amazing when I engage with folks like customers, Gail and Ron, who are actually out there with the charter of protecting their organizations. That's a huge, huge responsibility and it's gotten much more complex with all this distributed organization that we have today now. Where apps are everywhere, users everywhere, we have all kinds of devices. The apps architectures are fundamentally changing with containerized applications and the modern app phenomena where we have these apps sitting across with so many more components and across multiple clouds. It's really created a field day for the attackers because now, the attack surface has exponentially grown, it's just become so much easier now for the attackers to find their way. As Jordan had put it, it's all about finding that just that one initial compromise point and then making your way into the network to the sensitive assets and either exfiltrating IP or locking it up with ransomware and it's challenging. Some of the things that we are seeing in addition to just what was already mentioned, for example we're seeing the use of legitimate ports like RDP. So RDP tends to be a very commonly used port by attacks to move laterally within the network once they make their way through the initial gate. We are beginning to see phishing, and email remains one of the top vectors from an end user perspective to be able to do that initial delivery of malicious code. Obviously we have talked about ransomware and that is top of mind for everyone, we've seen this huge surge in ransomware again but what's also growing and worrisome is the use of zero day exploits. Compared to the last two years in 2021 alone we have seen more than two times the use of zero day exploits in the wild. And, zero day exploits, something for which a lot of the traditional security defenses that rely on signatures or known behavior, can't really react. This is somebody with a mask on masquerading as something else and just moving freely, and that's worrisome as well. So that's just some of the additional things we have seen, the use of legitimate boards being used internally to move laterally within the networks and zero day exploits.

Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
Just a couple of brief comments to backup what everyone else has said, one of the things that I actually don't see that I would like to and I think everyone will share in my enthusiasm towards this, I would like to see budgets for security expand as much as a tech services has. So that would be a wonderful thing to see. The other thing that is not talked about a whole lot but we are certainly seeing across the enterprise is ransomware as a service. This speaks to the level of collaboration of threat actors that oftentimes law enforcers should adopt a more collaborative approach, just like we do in the private market where we'll pick the phone up and call a buddy who's the CISO and say hey what are you seeing? We are all better when we collaborate, and the threat actors have picked this up rapidly, and they've always been better collaborators on the offensive side rather than on the defensive side which is where we play.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, I would agree with that. Just a couple of things. Before I took the role of CISO at F5, which I did in the last seven months or so. I ran a business. As a general manager for one of our online security services business or cloud based businesses where we were protecting you know hundreds and hundreds of customer's environments and exactly as Ron said DDoS attacks. DDoS as a service is something that the hackers have gone into, the enterprise market. You look at what they post about their service offering and their high customer quality, what they deliver and so on and so forth. Their customer service is actually people in somebody's basement, but actually today its big business. So you can do all that. We've seen the DDoS attacks grow to the next point on having zero day vulnerabilities. The other piece I wanted to mention that we haven't talked about is a lot of bot traffic and credential stuffing traffic that is really focused on applications. We've seen all of that right, and I saw many different organizations summon highly targeted organizations, Some very sophisticated attacks that are going on against these particular assets that these organizations have, so again, it's a lot to cover as an organization, as a CSO, and you're absolutely right Ron. We would like to see the increase in the budget to help us address some of these challenges.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Well that definitely sounds like a call to action and I want to go back to the operations but before we do that I'd like to shift the conversation because we could spend all day discussing the (inaudible) nature because that's really what stepping out to me, that's just how enterprises feel. This is a daunting, and I think from what you guys had been touching on, I'm sure our audience feels the same way now that, oh my gosh worst work. Can we start given that the tech services expanded, things are in flux, new threats continue to come, the tech community is becoming more savvy, more service oriented to a degree that's even better than the defensive side as Ron pointed out. So let's move to discussing a little bit more of the solution side. I think we started a little bit in our first conversation but I'd like to push it and zero crystallize our discussion around first the technology aspect, right. So what are the solutions out there that enterprise should be thinking about? Also, what are technologies that may be the point today that you think that enterprises should stop using?. So we'll start with you, Vivek, on this question.

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
Yeah, sure. I mean this would be a really fun one for us to chat through. Again we talked about the threat landscape and we all talk about with these new evolutions of architectures like SASE for example which is really aimed at protecting the end user traffic. No matter where they're walking from, and no matter what applications they're accessing, and yet delivering that high performance, the most optimal end user performance. When that is super important things like identity and we do all of that stuff for example at VMware I think one of the things, and Gail touched on the zero trust as a paradigm is being really important. What we're beginning to see is a lot of the organization start thinking of, I need to secure my end user traffic and use solutions like SASE and Z DNA concepts to secure. While that is super important in that approach to zero trust, what's equally important is the fact that all these workloads, and we talked about it right, like all these lateral movements Jordan talked about how things actually get into the network and all that stuff that's happening within the cloud and across these clouds, because as we know, almost every organization is now shifted to a multi cloud strategy where the applications are hosted. We have to secure the workload access as well, it's not only about the user access because yeah sure if the vaches device or credential gets compromised, that's a problem. But if a critical database, or an application within the cloud gets compromised. That's where the damage happens, and so securing the workloads within and across the clouds and all the traffic from the workload out to all the traffic that's happening is equally important, so we really have to start thinking of concepts like zero trust spanning from users and devices accessing the front door of these applications with all the access policy applied, but then taking that inside and across the clouds to make sure all the traffic that's going on because keep in mind, majority of the network traffic today is that east west traffic. And that's why we have a real have to call this, the battle today has shifted from not the north south right, which was the traditional perimeter which has largely obliterated. But, east, west, is the new battleground. Right, and we really have to start thinking about solutions that can work at scale for this growing internal traffic, east west traffic across all our applications. I know we'll talk more about this but having the ability to have these solutions span out these workloads work at Cloud Scale, be distributed because that's how our applications and components are, and also automated because I know Ron and Gail, you guys, there's never enough budget from a security perspective to secure everything but what if our security solutions and architectures could go along with our application architectures, and they were largely automated where security just goes with it and you don't need all these ticketing systems for people to configure the policies, or hundreds of security operations personas. They're combing through all these events so I think that's where it starts getting interesting where you can get scale, with a lot of these fundamentally different approaches, But yes, I think I would start by saying, we all thinking of immediately securing users, especially in this pandemic time, what we need to secure the user access. Secure the workload access as was super important because that's where all the damage really happens.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks for that Vivek, definitely hearing you say that the focus point should be on the workload side and from the other panelists, you guys agree or is there another piece of technology landscape that you think enterprises should be focusing on?

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
I agree with Vivek. We had a five spin on many of our years. It's a security now application layer, where the application lives, right, and I think that is super important, but I think all of the components there. When you think about zero trust, and as I look at it and I know if you talk to different security people you probably get a different definition from each one, But, I am not only securing the application, whether it's a traditional application or an agile application and modern application. We need to think about how do we integrate security? Vivek is actually very spot on there, API security, how these micro services connect to each other. Those are very, very important. How do you secure the data? That's a piece that we haven't talked about because the data itself should be independently protected, how do you secure the user, how do you have, positive strong identity, absolutely needed in today's day and age, and then how do you make sure you authenticate the device? Again, you know that device is healthy before you allow that connection to occur. And this is all because we don't have that perimeter anymore. And this is why we have to change the way we think about security.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks for that. Jordan, comment?

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Yeah, sorry I was going to say that. I totally agree with what Gail is saying. There's so many aspects to defense and so many potential technologies to consider when you're thinking about how do I secure this network, how do I secure all these individual aspects to it? You hear the term defense in depth thrown around a lot in the industry, it's for good reason. It's a really important part of the strategy and the thing I always say to clients who are either in the middle of or maybe recovering from a cyber-attack is there is no silver bullet to security. There's no one piece of software that's going to solve all of your problems. I wish there was, it would make my job a lot easier. But, unfortunately, it's all about understanding all of the different levels of technology, all the different levels of risks that you have, and identifying the right solution for each one of those individual pieces. So, when we talk about what technologies you can use, it's really difficult to single in on a single one. However, what I will say is, if there was one piece of sector technology that I had to recommend for security for a wide scale kind of zero to 100, as far as your security strategy goes if you're not already using one, EDR is super super important. Right, it's that visibility it's basically your eyes when you're looking at your network right. There's so many potential dark corners, can be in user space, could be in data centers, could be server side where attackers can be hiding, where they can get in, Vivek was talking about zero days, these can pop up anywhere. They can be on any system. We haven't even touched on supply chain security but that increases the risk tenfold. How do you possibly combat all of these different angles? Step one is

always going to be that visibility piece, and I don't think there's a better way to do that than with EDR. You know you can identify those behaviors in users that are maybe unusual, you can look for things like GoIP differences and logins to try to figure out if your users are coming in from places they shouldn't be, There's a laundry list of things that EDR will do for you, but like I said, it's only one piece of the puzzle. In my mind it's the first step you should be taking, and really trying to implement an effective enterprise wide security.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
For those that don't know what EDR stands for Jordan EDR is?

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Endpoint Detection and Response, sorry I should have clarified that.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
No worries. So I guess, digging into that because what I'm hearing is Vivek and Gail focused on the workload side, and you brought us close to the other side, Jordan, to the endpoint. Because at least classical EDR, if I can use that term has been more focused on the end user devices, but is there a linkage here of EDR percolating into the workload. Do you see that happening, hence bringing the perspective of Vivek and Gail, that we have to focus on the workloads together with the visibility telemetry that classical EDR solutions provide. Do you see a role going into the data center sign on workloads space for EDR type technologies?

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Go ahead, Jordan.

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Sorry, I don't want to steal the floor but I would just say when it comes to workloads, ultimately even in a distributed cloud type environment, everything is a collection of endpoints. Even if it's a Kubernetes cluster, you have individual pods that are all individually functioning endpoints. So you can deploy EDR to all of these things. Should you deploy EDR to all those things is another question you have to think about and answer for yourself. But the beauty of EDR is, you can also use it as kind of a perimeter solution if maybe there's a portion of the network that needs high availability, you're not sure if you want to throw something in there that's going to impact performance, you just deploy EDR around that perimeter, and at least you have visibility to see if anything is going in or out of that segment of the network, especially if it's a critical one. I don't know if that was where you were gonna go with it, Gail, but I'm interested to hear your thoughts as well.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, interestingly, we both believe there's real risk here and an acquisition we closed just this week with a company called Threat Stack is really focused on being able to manage those endpoints and exactly

as you said it could be a Kubernetes cluster, it could be a number of components that make up your cloud environments, and getting visibility when you're in a multi cloud environment. I'm excited about being able to use this technology, but when you're in a multi cloud environment and you have lots of lots of instances and components that make up those instances that you have, you do want a single pane of glass. I think every cloud provider probably has some offering independently, but then you're looking at multiple places and you can't correlate them across your environment, and include the other events that you're collecting off your endpoints, etc. I do agree that is critically important for security organizations, SOX to have visibility to so that you're getting as full a picture so that you can react as quickly as possible,

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
Just to add to that. I 100% agree right. Jordan started talking about the importance of EDR, and I think Mauricio you said it right, EDR, and Gail said it as well. EDR does extend that out so it's not just use a device but that's where a lot of that started, but that endpoint detection and response does absolutely apply to our workloads, whether they are virtualized physical or containerized workloads sitting across the multi cloud environment. But here's another thing, this is a term which might again be new for some of our listeners. Enterprise, endpoint detection and response is evolving. But now what we're beginning to hear of this new architecture called extended detection and response. So what's extended detection and response in the simplest terms? Extended detection and response is when you can take your endpoint detection response and your network detection and response. Keep in mind, network detection and response is also technology that's looking at traffic using both signature and behavior based techniques right then applying all the ML and everything. But that's network detection and response, and that's taking independent policy actions and analyzing but now if you could bring these both together, where each can benefit from the context of the other. So for example an endpoint detection and response technology detects a new process spawn up on an Apache server that it has never seen before, but by inherently that doesn't mean it's bad. It gives it a low score, and now it sees that it's making a connection out to the database server, requesting a couple of million credit card numbers. Wait a second, that's definitely not a good thing. The network gets the score from the endpoint detection engine and can take a policy action in real time to stop that transaction from happening. Very simple example but that's the power of what extended detection response can do where you can bring today's endpoint detection and the network detection and response together. And I think that's going to be super cool as the industry evolves with maturing that solution over the coming quarters and years. And that's gonna really help us combat some of these threats.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
I agree, and the more we can use AI or machine learning to be able to make that response automatic, the better we're going to get at defense right. That's where we need to be, because guess what, that's where the hacker community already is. Oh, they use a lot of automation, and we need to step up our game there.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
And that's a perfect segue to the last topic here for the last couple minutes about operations. So, Ron. I'd like to hear from you to kick off our last topic here but not only is it set up for success I guess going back to our first question and the way you mentioned, if your boss is hearing our podcast or our webcast today, you're asking for more budget. So that almost sounds like that's an implicit statement that enterprise IP teams are not set up for success today because you're not being funded for the expanded threat surface. Is that where your head is or somewhere else?

Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
No, my head is there. So these problems are interdependent and multifactorial, so I wanted to jump in on just the last comments with EDR. First of all from a strategic and tactical perspective, number one, you can't respond to it if you don't see it. So, visibility is key. And we are all over, in my business, all over edge devices, and I got to tell you, in practice when you really start to do this, you get alarmed to death because you got to wrap those policies around these devices. And what happens is you get a bunch of alarms, and you've got to really drill down into the alarms that require human attention and human attention is really precious in the work environment, because of the sheer volume of instances, and the sheer volume of alarms that you get. Which ones weren't my attention, and which ones should I not pay attention to, that's a completely different subject, but it's something that I am sure that we all see now to get to the operation side of this, and success, I want to say this right off the bet. You got to go out, the first thing that you need to do, you think it goes without saying, but it's true and something that needs to be said, You need to go out the first thing you need to do is hire good people with the appropriate skill set, so I would say this. Good people can't overcome bad strategy and good people can't overcome bad leadership. So you need to get the right players in place to do the best that you say, define success. And obviously, success is one of those things where you're looking at buying down or decreasing risk. Everybody agrees with that, but everybody is going to have a different definition of what success actually is in operations. And so for me I think success is preventing bad things from happening quite simply, you're providing a value based on what did not happen. So there's a psychological tendency to undervalue the things that did not occur. So think about running into the boss's office, the big boss, the CEO, every day and say, hey, I prevented 5000 attacks last week. And you're going to see how that, how you're greeted well okay well run along kind of a thing. The point is that when you work in the space of prevention, it's very hard for others to wrap their head around what you do and you're an IT operations, you are a cost center, you are not a driver of revenue. So you have to contend with all of those things that are that are in the business. Also if you're a cybersecurity professional success means that you got to vet those products to make sure that they don't represent additional risk to the business, But you know what that takes time. So, that time is actually counterproductive to other areas of the business, because the business just wants to go out and jump on board with these new solutions in these new products, You're probably going to be seen as an inhibitor to speed, and those kinds of things are just things that you're going to have to deal with. So I think maybe the first thing after you come up with a good definition is come up with what your priorities are. much harder than you think because there's so many independencies interdependencies of one particular thing one tool to another. There's an old saying if everything is important, nothing is important.

So just to sit down and say well what are my five priorities is very difficult. I would say that one of the things that you need to do is nail down the fundamentals. Identity access management is a really really big deal, but it's probably a good idea to date myself at this point. When in 2004 I was a deputy director of the National Cybersecurity Division, a pretty big deal to be honest, you know what the most popular password was? Password 1234. If you do a Google search today, the most popular password is password 123456. So the point is when we see the amalgam of techniques and tactics used by the threat organizations, they don't always have to use their fastball. Yes they are highly advanced, but they can still use these low and slow techniques that still work, why would I show you my complex stuff, when the old stuff still works fine. But the reason that it works fine, is because sometimes we've not done what we need to do to, to close the front and the back door. Really fundamental cyber hygiene is still not being performed at a level that we would like to see, and I know, the second part of this question is a question of evolution. How should your operations center evolve? Well the truth is you need a good strategy, but what happens to organizations, all the time, is you got a great strategy but poor tactics. So things like zero trust zero trust is an approach, but everybody does it the same way. So at the end of the day there should be a sign hung up on all the organizations that say this, you need to be tactically focused but strategically aligned. So all of the tool sets, they all build up to that strategy that you say that you're doing. Another way of saying this is that as the threat evolves, you need to build in the ability to be nimble, and the ability to respond as the threat landscape changes with the fast balls, but also with the low and slow stuff.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Go ahead.

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
I was gonna say I love it, I mean that was just super awesome to hear Ron, right. I mean just to add coming back to that operations, they give some tactical or very specific examples and I might take a little contrarian view here, you know, to some of the stuff that we're discussing. We'll probably tied to some of the things Mauricio asked, like what stuff we should stop using as well, right. I don't think the answer is we need to throw more security tools necessarily, like most organizations are already allowed grappling with so many different tools, so many different console's that frankly we have created more complexity with more and more tools getting out at which is effectively an enemy of security. It doesn't work that way. And as we talked about all the trends that how it has changed everything I think frankly, it is madness for us to continue to use yesterday's architectures, point black box solutions and appliance based architectures to really enforce security. Now, that has to be turned on its head. We really have to start looking at this from an operational scale, and better security perspective. Things that can be distributed cloud scale maybe even delivered in software and more flexible rather than just being appliance centric, and all of a sudden we realize maybe those budget needs may come down, maybe the need for more people to continue to arm those security operations center will come down because now we're using more effective modern tools that are more automated and can give us better coverage so let me pause them. See if others have to add anything,

Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
So I also want to tack onto your comments. I would say this, you very rarely hear this, I'm passionate about this, so threatened vulnerability are a very unusual symbiosis. And so, the threat itself is starting to look like the level of complexity, contributes to the threat, when you look at various operating systems that we all use people don't realize these are 40 and 50 million lines of code, with an 8% or 9% error rate. So as you begin to compile these things and aggregate these things, the level of complexity contributes to a significantly higher threat landscape. And so that which we believe is done for good is starting to have a deleterious effect on all of us. Totally.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Very, very sage words of wisdom. So with that, we need to wrap this up. Thank you, I think what I heard is bringing it back to basics right, don't get stuck in a shiny chrome, bring it back to basics, it's good people. That's good strategy, it's prioritizing and making sure that you're focused on where the threats are, which, again, if everything is as a first priority then nothing is really the most important. And this last couple of minutes I'd like to give you guys each an opportunity to provide some closing remarks, starting with you, Jordan, what closing remarks and other final comments do you have for our audience.

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Yeah, so I'm tempted to dive into so many of the topics but instead I think one continuous thread that we've had through all of this is security is really about visibility and understanding. And, today's day and age, seeing your network, seeing your exposures, seeing everything that's out there and happening is critical and understanding what it is that you're looking at is just as important, and that's really where things like having good people, having effective but single points of technology like EDR, all of those things can come together and give you that visibility and understanding that you can use to then dive into specific processes and places and things like that. So it's a super complex problem but if I had to boil it down, that's probably how I would do it.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks, Jordan. Onto you Gail.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, we've had such a good dialogue this morning and I think security today is continuing to be so challenging. As security professionals we have to adapt to the new technologies, we have to adapt to the way modern applications are being built, we have to fit in seamlessly in to those processes to make sure that we are delivering the best quality applications for our business users and we have to cover all aspects of the technology stack. We have to look from network to operating system, to middleware components, to database, to application, to endpoints, to identity to all the ways that we connect those applications together, API security have talked about all of that. It is a big footprint that we have to cover. And, yeah, that's why I'm in the business. It's a bit of a challenge every day but it's also a time

to be able to learn and grow as a professional as well. So thank you very much for listening to me today.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thank you Gail, on to you Ron.

Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
Very briefly, I would tell everyone thank you for listening today. I will also tell you this quite succinctly, the silver bullet store is closed. There are no silver bullets out there, and it's not necessarily the strong perimeters that will survive the strong securing of applications or workloads, it's not that it's the adaptation. That's what we need, we need more folks who think that you need to be nimble, you need to be adaptive, and you don't want to be in the space where you're always responding to the threat that was six months ago. The adaptation needs to be at speed, and as long as you're thinking and you have people who have that mindset, you're in a much better condition, thank you again.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks Ron on to you Vivek to close out.

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
Yes, this was a super engaging and fun conversation, thank you all for listening. I think again as we start looking forward, my guidance would be let's start looking at these security architectures and solutions fundamentally, differently, right. Let's not be constrained with the architectures and solutions of the past, we got to think of things that can be really cloud scale distributed, things that are built into the infrastructure, and give us that automation and operational scale, and then we can collectively combat this growing security challenge much better.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks for that. I'd like to thank my panelists, I do expect that our audience is taken away a lot of food for thought. And with that, I hand it back.

George Rickman, NetEvents
Hi, George here from NetEvents, I just wanted to remind the press we're now going into the media Q&A. So you can raise your hand virtually and I can unmute you, so you can ask your question to our panelists. We also have a Q&A feature so if you would prefer to type your question, then we can answer it that way. So without further ado, I'm going to move into the queue Q&A now, and I believe we actually have a question already from Hector Pizarro, from DiarioTI.

Hector Pizarro, Diario TI
Thank you very much to our panelists for an excellent, excellent event. You see, the recent wave of ransomware attacks proves that organizations are not properly protecting their assets and processes, exposed to the outside world. So I read somewhere, I think it was last year, that Gartner says that through 2025 99% of cloud security failures will be the consumers fault. I think it's so bad. Do you agree on that?

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Who from the panel would like to take it, Jordan? Gail?

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
I'm happy to jump in on this one. So, Yeah, I think that statistic is really interesting honestly because when you think about cloud it's an environment of inherited risk, right. As soon as you purchase any kind of cloud technology, could be an EC two instance in AWS, it could be volume, whatever it is, Amazon is essentially giving you all of these technologies, all of these things but most of the risk and most of what is put into those technologies is under your control. So, when they say 99% of the default is going to be on the consumer, it's because you're in control over what you put into the cloud. So, when you're designing your infrastructure and everything you really do need to consider that almost all of the risk is on you. The only thing that say Amazon is going to be liable for is, I don't know if somebody breaks into their data center plugs in a USB drive and hacks into your system that way, which hopefully is very unlikely I suppose you either thinks it's a 1%, so yeah I think that's really what's key to understanding that statistic is that inherited risk concept.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, I would agree with Jordan, and I'll tell you, prior to my time out of F5. I was at Oracle for a number of years and my last position there was a CSO for Oracle Cloud, which meant I oversaw infrastructure as a service, platform as a service and software as a service that we were delivering for customers. There is, in my experience there, in seeing how customers utilized those different layers. They don't realize how much responsibility they have. We would detect environments that were compromised, we would isolate them and contact the customer. The customer would say, Oh, I thought that was your responsibility, take care of that or security or whatever. It isn't right, as you move from infrastructure, which were Jordans crack, that the end customer has more responsibility for security, I mean basically they're given a hardware platform to be able to spin stuff up but everything they put there, they have to secure, they have to monitor, they have to keep current, and then if you go to platform. Some of that is done by the provider, and you have to be very clear about what the provider does and what they don't do, and when you go to SASE obviously, there is more responsibility that the provider takes on. So I think there is a lack of understanding for the average cloud user, and so that's why I think this is going to happen and I will also say we've talked a little bit about people, process and technology, I was having a conversation with a fellow CISO, I won't say who they were, where they're from, but they had a ransomware attack that occurred in their environment, and they boiled it down to, there was an individual administrator who decided multi factor authentication to get onto their systems was too

much, too arduous to do, so they decided to turn it off. And so when they turned it off, there was their entry point into the environment so again you can have lots of good technologies in place but remember that the people, process and technology and the people are so important.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
And its good leadership. Good. George, any other questions?

George Rickman, NetEvents
Great, thank you. So I have another question here from David Carr who writes for SC Magazine, a security publication, this is actually specifically for Ron. Can you tell us how you're approaching the SASE concepts for moving security to the edge? How far would you say your organization is on that journey?

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
As one of the players in the market on the SASE front I can certainly provide some perspective. We have a major event going on this week. VMware recently announced with our SASE platform, the ability to have edge computing, and its security built in and available as part of that service. So absolutely this is a huge area of innovation from the era where we are beginning to see this demand pick up on the need for edge computing. Whether it is to deliver the right optimal end user experience for certain applications, you really need to have the compute, the analytics, everything as close to the end user as possible and that's why the edge computing is important but then security has to go hand in hand with it. And so as part of our 150+ SASE distributed pops that we have globally. We are making (inaudible) security so your standard, security stack that would apply in addition to that, security capabilities that will come in bundled with the edge computing platform, right. So let me stop there and see if others want to add anything else to it.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Ron?

Dr. Ronald Layton, Vice President, Converged Security Operations, Sallie Mae Bank
Yeah, I mean the only thing that I would add is that, you know, as a business, at Sallie Mae we were the first financial institution to be 100% in the cloud, we're in multiple clouds, but we recognize the need to be able to compute on the edge. Matter of fact, a lot of the edge security oriented visibility fits squarely within my bailiwick. So, I, along with others, have gone out to secure appropriate tools to make sure that I've got visibility on the health status of what each one of those edge devices are doing and I mean everything from the operating system to the MAC address to who that device is talking to, to be able to ensure that that we're as secure as we need to be.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks for that. Any other comments from the panel, regarding this question? If not, George, do we have any questions?

George Rickman, NetEvents
Yes, I have two more questions. So this question is from Steve Broadhead who writes for Computer Weekly, it's a bit of a long one. And he says, workers in the future will be split between conventional workplaces and remote locations, renewed focus on digital transformation and demands a new generation of software appliance to protect data and networks, and the adoption of multi cloud models to be sustained, and the need for high network capacity and low network latency. So how can SEC ops and NETOPS using the traditional multivendor DIY bolt on approach to security, possibly move to manage this incredibly complex model is the only solution therefore to fully outsource networking and security as a single hybrid service, and is an if so, what happens to the legacy infrastructure and product, investment? So that's to anyone.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Who'd like to tackle that one?

Jordan LaRose, Director of Consulting and Incident Response, F-Secure
Yeah, I'm happy to take a stab. Honestly, if I were to make a prediction, I think, and now is really a model for the future, I think we're always going to be living in sort of a hybrid environment. At least across the industry. So, if you look at traditional on prem solutions, let's say like Active Directory, for example, it's the bastion of Windows Network Computing now, as offering a way to import either part or wholly import your active directory into the cloud, right. There still may be on prem, devices there might be some servers that belong to the company, but then maybe the domain controller or something is in the cloud. That's just one example of where you can have your cake and eat it too when it comes to networking right. What we have now is options. I think that's something we've all been talking about for a while now, and it's really up to each individual business to consider where they want to stand. For some a fully outsourced cloud based model is what makes sense, for others you're going to want that on prem level of protection for all of your maybe sensitive data, your databases, etc. So, I guess, I don't think we'll be at a loss for options, I think it'll only expand as time goes on, even though I think we've all sort of been lamenting the amount of options and sort of amount of things you need to consider when you're thinking about these things. But overall there are ways to even hybridize user working environments if everybody's remote. There's still options like virtual desktops that you can give to people, Vivek, I'm sure you're familiar with the virtualization that you can use through things like VMware, the list goes on and on. But essentially, I think my prediction, at least, is there's always going to be a wealth of options and it's only going to increase over time and give us more granularity over what solutions that we do implement.

Gail Coury, Senior Vice President and Chief Information Security Officer, F5 Networks
Yeah, to add to that, I've long been a proponent of reducing the number of, we talked about this a little earlier, tools and vendors that you have in your supply chain right and so you're looking at identifying those critical partners you can align with, that you have confidence with, that have integrated solutions because guess what, I don't want to integrate them. It's too challenging, but being able to have visibility, not using point solutions, but selecting those couple of key vendors that can provide you the visibility at those different layers that you can bring together and have a full single pane of glass. So I think that's where we're going. I do think that using managed services and outsourcing some of your security for those organizations that don't have the ability to staff 24 x 7 x 365 or to be able to get the expertise that is a very viable option.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Thanks for those perspective. Okay, moving on to the last question, George?

George Rickman, NetEvents
Yes, I have one final question, they say zero trust is a term that has seen a lot of vendor marketing abuse. How is VMware zero trust, not just another abuse? I guess that's for you Vivek?

Vivek Bhandari, Sr. Director of Product Marketing, Networking and Security Business Unit, VMware
I guess yes, absolutely spot on. Right, I've heard the word ZT bossing 100%, like that is absolutely what is happening, Everybody seems to be just jumping on to the zero trust bandwagon and it's unfortunate because just wearing the customer hat it just is so confusing. If every security vendor out there, screams, yet our zero trust before and after the solution name it's just so confusing. And so yes, I 100% agree and empathize with the question there. At VMware, we have positioned our solutions first of all, and I think Gail had said this, it's not a product, it's an approach, it's a philosophy, it's a journey for the customer. VMware actually has a broad set of security solutions, and quite a few of those do not fit in in the zero trust architecture and we have deliberately kept it super simple for from an end customer perspective Hey, it is basically two broad areas, secure your user access to the applications and secure your workload access, right. Those are the two pillars, and then you certainly need certain modern sock tooling and capabilities. We have talked about visibility. Jordan talked about the importance of that, those become important. So, the way we talk about zero trust at VMware really, it's securing your user access using solutions like ZT and SASE. Secure your workload access with the right EDR for the workload and all the network segmentation and inbound inspection of traffic techniques and that largely starts getting you there in terms of an approach. Obviously when you look at SASE, things like device security Identity and Access Policy to application becomes important. On the workload side, like I said segmentation and inbound inspection of all that east west traffic is important and there are a number of different tools, we certainly offer a bunch of solutions that help customers on their journey. Our solutions are more taking an approach of software delivered built into the infrastructure to make it really simple and operationally scalable, but there's a number of tools out there, and that's really how I approach it is, it is true, there's a lot of ZD washing. Our positioning has been, keep it simple. We have a number of solutions that can help you on a journey, no one single solution or platform will ever do the

trick. Right, so being fully aware of that and making sure you can Interplay well with the ecosystem is equally important. So let me stop there.

George Rickman, NetEvents
Thank you Vivek. We have a few more questions from the media audience but unfortunately we were out of time so we will send those questions over to our panelists so that they can answer them offline. That's the end of the Q&A so I'll hand back over to Mauricio.

Mauricio Sanchez, Research Director, Network Security & Data Center Appliance, SASE Market Research, Dell'Oro Group
Again, thank you for everyone who attended. I'm sure everyone got a couple of nuggets, and is walking away with some fabulous food for thought. I appreciate our panelists time and look forward to continuing the conversation offline. So with that back to you Mark.

Mark Fox, CEO, NetEvents
Thank you Mauricio, Great job sharing that session and to say thanks to the panel. Media would have found that really interesting, and there is some additional information for the media. So as for transcripts of this session if you didn't record it using otter AI. Helen will be sending through the full transcript of this session, obviously in the hidden area on the website that you have the link to. There are speaker bios, photos, media kits, etc. as well as Mauricio's presentation. So you can download that and we will be producing a webcast and a podcast of the event, we will be editing this over the next few days, and you're obviously very welcome to link any of your stories to the podcast, to the webcasts that we produce. So thanks again everyone for attending. Really appreciate it. I'll see we've got media from North America, Europe, and also, Eastern Europe as well so Vladimir, I see that you're on. Stefan, as well. So, thanks for the media around the world, and, and we look forward to welcoming you to the next event. Thanks very much.