NETEVENTS GLOBAL IT SUMMIT

SAN JOSE, USA

OCTOBER 3 & 4, 2019

DRAFT

Conference Debate Session VI - Rapidly Evolving Trends in Cloud Networking Security and Cloud-Native Security

Introduced & Chaired by Scott Raynovich, Principal Analyst, Futuriom

Panellists:

Kevin Deierling	Senior VP of Marketing, Mellanox Technologies
MK Palmore	Field CSO, Paloalto Networks
Kelly Ahuja	President & Chief Executive Officer, Versa Networks

Scott Raynovich, Principal Analyst, Futuriom

Happy Friday. It's Friday. I think we forgot about that talking about everybody stealing our passwords, I forgot it was Friday. So, guess what we're going to talk more about security. So, the topic of this panel is Rapidly Evolving Trends in Networking Security and Cloud-Native Security. I have absorbed all of the security discussions so maybe I'll try to take it in other directions so that we don't repeat ourselves too much. That never happens in the technology industry, right?

Panel Speaker – Male

Never.

Scott Raynovich, Principal Analyst, Futuriom

So, I'm just going to give a quick overview of some stuff I look at. For you guys who don't know me, I'm Scott Raynovich and I've followed this industry for about, I'm afraid to say, almost three decades now. Futuriom is an independent research firm and we focus really on cloud infrastructure, networking and security, as it applies to those things, and really focus on gathering end user data. I spend probably half my time talking to end users and doing surveys; survey every other month to find out what their challenges are and what they're looking for.

Of course, you know, we're all hearing about cloud and networking and security. What are the issues here? Well, the biggest issue is the cloud, as we heard on other panels, has changed everything right? It's changed traffic patterns, behaviours, network architectures. All the traffic is, or most of the traffic, is going to the cloud now. It used to be in a self-contained world of a corporate WAN or a LAN and now everybody's hitting things in the cloud. This is creating more bandwidth demand overall, of course. It also requires a more flexible architecture. You can't just install a firewall and have that be your security. You have to have security apps distributed throughout wherever your users are going.

There's another challenge which is appliance sprawl. You used to have one gateway or switcher router and now you have hundreds of different kinds of devices with different characteristics and different protocols, that's a challenge. It's going up the stack into the software layer. We have orchestration tools and visibility tools and so these are kind of all the things that the network and IT managers are struggling with. Just kind of a multipronged challenge and if you look at the way networks work now, it used to be very simple. You had a corporate office and a datacentre and branches, and you would connect them all and lock them all down but now people are going all over the place. Right? They're going to hit cloud services from their home, they're going back through datacentres to go to the cloud service, they're connecting to cloud gateways.

So, the way we connect and what we're connecting to has become more complex. We talked about MPLS versus internet or using a private MPLS network or using a business quality internet or using home broadband, so all these are considerations into how we secure the network, right? So, I was looking at some interesting architectural diagrams which brings us to the next challenge, this is a NIST view of cloud architecture. The question is where do you put security, right? There's so many of these different technology layers and architectures. Well the answer is you have to put it everywhere. You have to look at the security at every layer of the network, every layer of the cloud.

Brings us to the next problem is this is a highly reduced slide, okay, this slide could really be 100x as big, but this is just a few of the technology tools that CISOs have to look at when they look at all those layers in the NIST diagram. You know, you're talking about your end-points, are you talking about the container security inside the datacentre, are you talking about the firewall at the edge, are you talking about - there's literally hundreds of tools that these CISOs have to look at and evaluate to attack the specific problems. So, I know you guys love to sell technology but, you know, you look at the end user perspective, it's literally overwhelming.

They're looking at their screens, they have dozens of tools, thousands of alerts are popping up, their heads are exploding. The main problem with security is not that we don't have these tools to stop it, it's the human management of dealing with them and this is the trend. The trend is it's a management issue, it's not a technology issue. If you look at all the major breaches, whether it's Target or Chase or the IRS or Equifax, it almost always leads back to a human error. Either there were things that were flagged that weren't paid attention to or there were decisions made not to invest to patch web servers and so it's really an organisational issue as much as a technology issue.

Heard a lot about SD-WAN so I'm going to just go over this real quick because that was all about SD-WAN but basically the way I view SD-WAN and why it's helping security is it kind of makes encryption and VPN and secure networks default rather than having to set them up separately. It automates them. When we survey our audience almost every single survey I have done this year, I would say security pops up as the number one thing, whatever you're talking about; some cloud infrastructure, cloud networking. We did this SD-WAN survey. We asked 136 service providers in enterprise what's driving their SD-WAN implementation and better security came out on top. I mean, that's not to say all the other benefits of SD-WAN that you've heard about aren't important.

Let's get our panel to talk about these issues, because there's so many of them that are challenging the customers. So, Kevin Deierling, VP of Marketing with Mellanox, I'm going to introduce you really quickly and then have you talk a little bit more about what you're working on. MK Palmore Field Chief Security Officer will Paloalto, Kelly you've met several times already, the CEO of Versa. So, I'll start with Kevin and you can talk about your role right now, what you're focused on, everybody real quickly. Kevin.

Kevin Deierling, Senior VP of Marketing, Mellanox Technologies

Yeah, so I'm Senior VP of Marketing at Mellanox Technologies. We're a high-speed networking company. We do NICs, which is SmartNICs, and everything I've been hearing today, you know, it's interesting. You know, talking about security and it's always secure the network because the attacks are coming from outside but more and more in the cloud model they're coming from inside because the cloud model invites third parties that are potentially untrusted right into the middle of your datacentre. So, that old security model of perimeter protection is not adequate. It's important, but it's not adequate and so we're really about addressing those limitations.

Scott Raynovich, Principal Analyst, Futuriom

Excellent. MK.

MK Palmore, Field CSO, Palo Alto Networks

So, good morning everyone. MK Palmore at Palo Alto Networks. I appreciate the invite from NetEvents and being able to participate in this event. It's been, I think, two years since the last time I was able to attend. In my current capacity, again I'm a Field CSO with Palo Alto Networks. I just joined Palo Alto Networks this year after finishing up a 22-year career with the FBI and so the conversation that you were having earlier on about threats and adversarial approaches to environments certainly was something that I could wade in on.

In my current role at Palo Alto Networks part of what I do is get out and evangelise quite a bit on the subject of the changing nature of security. At Palo Alto Networks we're concentrating on (1) securing what we consider to be the old school approach through the presence of our next-gen firewall, but we also have a decided eye towards a future as it relates to cloud security and certainly issues around SOAR products and automation. So, what we see is the high complexity in the changing nature of cyber security and at Paloalto Networks we're moving towards making sure that we have a product line that answers the mail on those issues. So, looking forward to the discussion on cloud.

Kelly Ahuja, CEO, Versa Networks

Good morning. You already know who I am. In terms of slides, I think Scott you need to update your prior slides. Versa wasn't on that security bucket that you had on the vendors.

Scott Raynovich, Principal Analyst, Futuriom

Oh, sorry.

Kelly Ahuja, CEO, Versa Networks

I think given some of the work that the NSS Labs has done recently, you need to make sure that we're also in that. So, we think that security is something, now I can talk about that compared to the last panel, which is security is something that is fundamental to any network and you cannot separate network and security apart any longer. This is not just true in the wide area network and SD-WAN clearly isn't happening without security. Security is a big concern for whether it's enterprises or providers, even inside the network, because the old model of how you do VLANs and zone-based firewalls is just not scaling. It's operationally - because if that was the second part of your question Scott, was really about management and that's becoming very complex.

So, whether it's in the datacentre creating segments to be able to isolate applications because they can be come threat vectors, or in an enterprise or a branch where printers can become threat vectors, you've got to protect all of that even inside the enterprise, not just outside the enterprise. So, security is going to be indeed pervasive across every environment and the edge as we knew it, the network perimeter as we knew it, was really about the external edge but in the future, it's going to be about internal perimeters and everything is going to have to get protected in every possible way.

Scott Raynovich, Principal Analyst, Futuriom

Excellent. That kind of brings up to my next point is we were talking earlier about encryption and I know Kevin will have a lot to say about this because Mellanox has done a lot of work here. But networks traditionally have been a barrier sometimes to security because of the overhead of encryption and you would like to encrypt everything but sometimes it incurs a performance [hit]. So, tell us - let's talk about the trends towards encrypting data and networks and whether networks can keep up with the security demand.

Kevin Deierling, Senior VP of Marketing, Mellanox Technologies

Yeah, so I'll jump in. You know we just introduced a new network adaptor product that performs encryption at 200 gigabits per second line rate. So, we do this for point to point encryption with Ipsec, we do it for TLS, so that's sort of the transport layer, and we encrypt data at rest on the hard drives. So, the point here is this is going to become ubiquitous technologies. Today, normally, you'll have an encrypted secure tunnel from the client, what we call North/South traffic from the client, into the datacentre and the cloud. But once it's in the cloud, then people are assuming that's a trusted model and inside it's not encrypted.

It's just no longer true. You're bringing bad guys right into the middle of the cloud, you're charging them to put their workloads into your cloud and you have no control over what those workloads are. So, we're seeing two of our major customers now adopt encryption inside of their no-longer trusted - we heard the zero trust model - we're seeing two major cloud and [word of] household name companies that unfortunately I can't name, are customers that are going to deploy security inside of their datacentre and everting will be secured. So that even if the network is compromised internally, the data will all be encrypted.

Scott Raynovich, Principal Analyst, Futuriom

Excellent. Thanks. I have a question. On the first panel we heard that we should all use a VPN. How many people use a VPN on a daily basis? How many people like log in from internet wi-fi in the hotel here and do not use a VPN? See yeah, so I have been trained, after hearing a hundred of these panels, to use a VPN, I use it all the time now. But as we can see, it was almost like half the people are being exposed to this dirty wi-fi right now. So, it's clear that still encryption and VPNs are not default. So, MK, tell us Palo Alto's view on what you guys encrypt, how much will we encrypt years from now? Does everything have to be massively encrypted?

MK Palmore, Field CSO, Palo Alto Networks

Yeah, so I mean we're touching on lots of subjects. I would say that now in terms of a best practice, encryption certainly has risen to the level of being a considerable best practice in terms of data at rest and also data in transit. So, I think we will continue to see high levels of the use of encryption, largely because we have to understand from the approach of the adversary that any opportunity that the adversary has to access data, means that it's an opportunity for them to infiltrate and then subsequently monetize the access to that data. So, this idea around encryption, again, I would put in a bucket with the cyber security fundamentals, meaning let's get to closing down every avenue of approach that we can in terms of preventing the adversary's opportunity to monetize both access to information and the information itself.

Scott Raynovich, Principal Analyst, Futuriom

Great, thanks. Kelly, you got something to add?

Kelly Ahuja, CEO, Versa Networks

Yeah, so clearly encryption is going to happen, and we give the ability to everyone to be able to do it where they want it and when they want it. So, for example, if I'm using, in the wide area network, an MPLS service, well do I need to use encryption on top of that? Maybe I do, maybe I don't but that's an option that should be a settable thing for the end administrator to be able to figure that out. Our job isn't to determine where encryption has got to be used. Our job is to be able to provide ability to encrypt wherever a customer needs it. Now clearly when you're in a datacentre at a 200-gig interface, you do need hardware assist and if there is hardware assist available, every system should use that to do it because that's going to give you the best performance.

But, in smaller systems, you know even for white box designs that have hardware assist, because some chip that Intel's provided does something or the other, you've got to be able to use it and you've got to be able to use it efficiently because it's going to improve performance. But that said, encryption is something that's coming everywhere. In fact, if you look at Wi-Fi 6, there is also a WPA3 standard that's coming out which has WPA3/OWE and that OWE stands for Optional Wireless Encryption, where they are actually going to be using encryption even in the wi-fi domain to be able to provide that connectivity.

So, encryption is going to happen. I think it's going to happen everywhere.

Panel Speaker – Male

Yeah. Can I just jump in and respectfully disagree that hardware assist is sufficient? So, hardware assist is some of these extensions they have in the Intel CPU that actually can do the decryption in software and it accelerates that. However, if you look at all the other things that we've heard talked about today with overlay networks and virtual machines, and hypervisors that switch between the virtual machines, all of that is actually being done in network hardware today and the network adaptors steering the traffic to the correct virtual machines, terminating TCP/IP and accelerating that with checksum offloads et cetera.

If you use software to decrypt the packet all of those things break. All of the hardware accelerators that companies like ourselves have put into the network interface cards over the last 20 years, all break because when you have an encrypted connection, all of the information we need to look at overlays and TCP/IP headers and checksums, all of it becomes encrypted because there's a giant IPsec tunnel. We don't see any of it. All of our accelerations break. So, I don't actually think that hardware acceleration in the CPU, and Kelly didn't say that, that he was specifically talking about that, but I actually think it needs to be inline in the network adaptor.

Panel Speaker – Male

We can agree to disagree but…

[Laughter]

Panel Speaker – Male

That's why it's a debate.

Scott Raynovich, Principal Analyst, Futuriom

Excellent. Yeah, let's cause some more tension. There's not enough tension. We have a, traditionally known as a firewall vendor. I don't know if you guys still call yourselves that. Then you have an SD-WAN vendor but the SD-WAN vendors, to me, are sounding more like firewall vendors these days. You know talking about their security stacks and their next generation firewalls, passing these great NSS tests that we heard about. Then the firewall vendors are it seems like now I get a couple of press releases a day with a firewall vendor with SD-WAN in the headline. So, why don't you guys just team up and all merge and just be one. Isn't it the same thing now?

[Laughter]

Panel Speaker – Male

We're doing a little bit of that. You may or may not know as an audience, Paloalto Networks has gone through the process of acquiring several sort of best of breed entities over the past 18 months or so in an effort to align with what is our vision of what the future looks like and it does involve a little bit of consolidation in terms of what the industry looks like. You know, we've aligned, and we still put resources behind the idea behind the next-gen firewall. We think firewalls will remain present both in physical and virtual form in environments. Our added caveat to that is that we think firewalls should deliver a number of services to our customers. In other words, you should be able to turn on and off services with the presence of the firewall.

We also are doubling down on the concept that most enterprises are in some way, shape or form in the process of a cloud journey. We understand that most enterprises understand the efficiencies that they can leverage from the cloud and are moving to use it and so in our acquisitional phases we've acquired companies that provide security around access to your digital information, and the cloud, regardless of where you happen to be on the planet. You know, the third phase of that we like to think of as sort of the cyber security of the future which we believe involves a tremendous amount of automation because most enterprises certainly cannot scale from a workforce standpoint to what's needed in the cyber security industry and so we feel that automation is going to play a large role in that.

We are, in addition to automation, kind of doubling down on this issue about the cyber threat intelligence. This idea that no one entity sees the entirety of the threat landscape but if you use a patchwork approach and sort of cobble together visions of the landscape, you can extract data and information that enables you to provide security services to your customer base from a wide variety of sources.

Scott Raynovich, Principal Analyst, Futuriom

So, what about you Kelly? Do you need the Palo Alto guys around or are you just going to…

Kelly Ahuja, CEO, Versa Networks

[Laughter] Well you know…

Scott Raynovich, Principal Analyst, Futuriom

…do it all yourself?

Kelly Ahuja, CEO, Versa Networks

When a market is hot, Scott, everybody tries to go after it, and you know try to attach their stuff into that market. Everyone of the incumbents, including others that have been on stage during the last couple of days, have tried to do that. But candidly, this is a new space which requires new ground up innovation when it comes to SD-WAN and candidly our approach has been not to really drive a certain specific direction for the customer but give a customer an option. We're an open platform. We have many customers that use us right beside Pal Aalto. We actually can sit beside a physical Palo Alto or we can take a virtual Palo Alto VNF and put that onto our software and service chain that together.

We can do that with Fortinet, we can do that with Riverbed, Silverpeak, Cisco, you name it. WAN optimisation companies, security companies, it doesn't matter. The key thing though is you have to solve the customer's problem and most of the customers have an existing environment where you have to fit in and be able to allow them to have a smooth migration. Whether they move to a cloud or stay on-prem, it's really going to be their call and every customer is going to be different. You're not going to have one recipe that applies for everyone and you've got to give them the flexibility to do it. You've got to have the versatility and that's where the name Versa comes from, to be able to allow them to do that.

Audience Q&A

Scott Raynovich, Principal Analyst, Futuriom

Wow, excellent. Very nice. Well I think I'm being asked to push forward into questions here, so if you guys are ready let's take some questions. Anybody got a question? Yes, sir.

Anthony Caruana, CSO Magazine

Anthony Caruana from Australia. I'm kind of a little bit interested in the encryption sort of comments you all made. Isn't encryption just table stakes now? Isn't it just what we expect because we saw lots of data over the last few days pointing to some fairly significant data breaches? Lots of data has been stolen and in almost all those cases, there's some encryption in these peoples' systems. Don't the bad guys just walk around - because eventually the data's got to be unencrypted at some point to be useful. So, you know, I accept that we need encryption, but people try to make it sound like it's the answer but it's just like one small hurdle really for a determined bad guy.

Scott Raynovich, Principal Analyst, Futuriom

You mention I guess this TLS thing. You were saying, Kevin, earlier this morning when we were talking that these webscale vendors don't actually encrypt some of the server to server traffic. So, that's a vulnerability, correct?

Kevin Deierling, Senior VP of Marketing, Mellanox Technologies

Yeah, so I think one of the things - security is typically still on the edge. As much as people talk about encryption, and I'm using encryption here, security is much broader I agree, but today most of the data within the datacentre is in clear text and so if you can deliver encryption and decryption at line rate with zero penalties in terms of performance and penalties in the sense of the CPU, the most expensive part of your datacentre infrastructure is the CPU and the memory subsystem in your servers and, of course, the storage itself, the flash. Those are the expensive things. If you can encrypt everything that's moving and everything that's at rest constantly, eventually you're going to have clear text to the application and now you just need to make sure that those applications are constrained. That the service provider policy and the security policies are in place and they cannot be compromised.

That's where the SmartNIC comes into play that actually puts a computer in front of the computer to actually ensure that - we'd love to have all of these guys' security policies running on SmartNICs so that they didn't even have to run on x86. Compromise the x86, who cares? There's a separate security domain that's protecting by putting a computer in front of the computer with the SmartNIC. So, that's the vision we see. We think that's where the market is going. Some of the big hyperscale guys are already there.

MK Palmore, Field CSO, Palo Alto Networks

Let me add a different twist to this. You mentioned sort of in the preface of your question, you talked about how encryption - I think I'm assuming you're saying it can't be the complete answer, and I would absolutely agree with you. If you look at adversarial approaches, if you look at successful breaches, nearly 100 per cent of them have some component of a violation of just plain cyber security fundamentals. Many people ask, okay, what are those fundamentals? You pick out an easy example. One that I like to utilise quite a bit, the CIS 20 critical security controls. If you go through the post-mortem of nearly every breach, certainly the high-profile ones that have happened over the past few years, the infiltration method, the point of access, the threat vector utilised by the adversary, is always about the fundamentals.

So, for as long as security in network defenders, as long as we have an absence of the fundamentals, as long as we leave sort of the easy low hanging fruit available to adversaries, they will continue to pound on this. These folks are experts at return on investment. They're going to take the easiest path available to them to gain access to networks. So, yes, we can have lots of conversations about things like encryption, but encryption quite frankly is a subset of some of the basic things that we need to be doing in order to secure environments.

Panel Speaker - Male

I completely agree with MK. Encryption, while it is a technique, it is not the full answer. You need many different things. Certainly, encryption at the datacentre is a good thing. No one is going to argue that. But if you take a look at an enterprise that's got printers and devices that are connected, it may not be possible for them to use encryption in those devises because they've been around for a while. So, you have to have multiple different types of solutions to be able to address that.

Secondly, a lot of threats come not just from somebody being linked - [-listened] into the network, but your user identity. So, identity brokers and somebody taking that on is also a concern. So, when it comes to security, it's a multifaceted, multi-layered, multi-segmented approach that you have to take.

Scott Raynovich, Principal Analyst, Futuriom

Excellent. Great. Well we're running out of time folks but thanks a lot. Let's thank our panellists and move onto the coffee break.