NETEVENTS

EMEA IT SPOTLIGHT

FINAL

Conference Debate Session III – Enterprise Security Considerations for the Cloud – Containers, Perimeters, and Access Controls

Chair: Rik Turner

Principal Analyst, Ovum

Panellists:

Jan Guldentops	Director, BA Test Labs
Aaron Turner	CEO & Co-Founder, Hotshot Technologies
Peter Galvin	Chief Strategy and Marketing Officer, nCipher Security
Philip Griffiths	Head of EMEA Partnerships, NetFoundry
Atchison Frazer	Worldwide Head of Marketing, Versa Networks

Rik Turner

Thank you, as you can see, they gave me a lovely long title for this session, so it's *Enterprise Security Considerations for the Cloud – Containers, Perimeters, and Access Controls*. So not a lot to cover really in the next half an hour or so.

I'm from Ovum which is a much smaller analyst house than some of the illustrious gentleman on the previous panel. We like to think we are small but beautifully formed. So here we go.

Right, my title again -here we go, I want you to divide that therefore into two sort of separate segments; one I'm going to talk a bit about cloud security, the next talk specifically about perimeters and access control. I'm not saying that they are not related

- they are - but they are slightly different issues which will then come together and converge later in the presentation because they do need to be talked about separately initially in my opinion.

So here we go; some cloud security. First of all, I'd just like to ask, a show of hands please, how many of you folks are familiar with the shared responsibility model for cloud security? Hands up, please? Anybody? Most of the only - the journalist community here. Do many of you folks know the shared security model?

I didn't see many hands going up amongst the journalists, so I'm going to take this thing off here, hang on. Oh, I like this, it's good isn't it.

Anyway, this is fundamentally important actually. If you guys leave here with nothing else from this particular presentation, do take this away in terms of this is something - I think it may have been AWS or Amazon as they're also known who came up with this initially.

Basically, what you've got here, quite simple as in the three different delivery mechanisms as it were all means of consuming cloud services, what is the responsibility for the customer and what is the responsibility for the cloud service provider? Straightforward that is; in other words, if you're in the IaaS, if you're in the infrastructure as a service, AWS or as you're - or whoever, they will take care of all the grey bits, but above that, it's down to you, sir. It's your responsibility. So, if you get it wrong, you are not going to get any money back from them if you are breached because you didn't secure those layers above you.

Similarly, if you are in platform as a service, you've got to take care of those top two layers. Below that, tough. Below that, fine. If anything goes wrong with any of the stuff, AWS will have to pay you some money back or whatever. But not up here, right?

Okay, so in other words, the shared security model which has been going around for a long, long time, but the shared security model is important for an enterprise that is moving into the cloud to understand what it needs to secure.

I would just add that the red but there, the red bits here are the bits that the security industry, in other words, the companies who only sell security and do not sell cloud or anything else, but just do security, that's where they make their money going forward in cloud. Make sense?

Of course, at the top, data is always going to be your responsibility. You better look after your own data. You'll find loads of versions of this if you do a Google images search, you'll find loads of different versions. I just put one more up actually because I like this one only because it also includes on-premise so you can see that that - in the old world of on-premise, you are responsible for all of that lot, the customer. Gradually, it decreases as you go across until we get to software as a service where effectively, it would appear that you have no responsibilities. Of course, you do because what this leaves out going back is the data at the top. They've left out data altogether.

But that is the shared security model; it is important to understand as journalists as well. It's important for you to understand this because it is essentially where the customer has to be thinking about his security issues. Now, yeah, I agree, all of that stuff about in previous conversations about least privilege and reducing it to the maximum and keep all of the security at the top level with the data and with the users, we can get onto that all in a minute. But essentially, that is how they have divided the world up and that is what you need to be thinking about as an enterprise if you haven't yet moved into the cloud. That's the kind of thing that they will be enforcing on you.

So, going further ahead, purely in the software as a service world, this was kind of the one that took off first. It was the easiest thing to adopt; I mean Salesforce's been a massive success for over a decade.

The issue with software as a service is that it was so easy to adopt, if you were an enterprise or if you were just an enterprise user, you could adopt software as a service really easily. So easily in fact, that your IT department didn't even need to know about it. If you chose to get into software as a service, take all kinds of different services and we've seen now, there are millions of services and I think someone was saying earlier on, you maybe choosing to use a software as a service offering as an individual user in your company that your IT department hasn't got a clue about. They don't know, which is where the whole notion of shadow IT initially came along.

To address that, and this is a Gartnerism (sic), we talk about CASB which is the Cloud Access Security Brokers. These were basically technology that would sit between the users down here on their managed or unmanaged devices and would basically be the brokers of that access to any of those multiple services up there. The CASB guys these days will have you believe that they also do infrastructure as a service; I have my doubts about that, but they certainly came along and it's certainly where they made all of their money in the CASB world doing securing the access to SaaS services.

That's by and large, that has happened. That's something for the last five years shall we say that that's been developing, but in my opinion anyway, that revolution is over. A lot of the CASB guys have been acquired by somebody else and are now disappeared into the belly of much larger security companies with big broad portfolios.

So CASB was the first security response as it were to cloud adoption.

When it gets into infrastructure and platform as a service, it's a bit more complicated. Going back to that security model, you've got more to worry about as the enterprise customer than if you are just taking software as a service. Of course, there is also the fact that there is the evolution of where cloud is going in the IaaS and PaaS world. It's moving from VMs - I mean again, we're talking about [cat containers] going microservices and serverless; I mean, I'm not going to get into all of that now, but suffice to say that they all have their own security issues around them. But in any case, it's not just a case of deploying as CASB that will enable you to secure your workloads or whatever in the cloud.

So, looking a little bit then at some of the technologies - and again, these are all Gartnerisms (sic), the acronyms here, the kind of things that people are talking about right now for the virtual machine paradigm of IaaS and PaaS, you'll see people talking about cloud work low protection platforms. Essentially, that seeing of my workload is under attack and then doing something about it, blocking it, remediating it, getting a whole new workload going, restarting it somewhere else. Then there is also these guys, these CSPM guys; Cloud Security Posture Management which is essentially a compliance function.

But it speaks to the fact that it's so easy right now to spin up another instance of something else either in the developer community or even in the actual production environment. Very easy to spin stuff up and all of a sudden, you've got another 50 VMs that you didn't know about within the security team or within a production environment.

Suddenly, it just becomes that much easier, so you've got to have some technology that runs around and says oh, we have got all these new VMs we didn't know we had, let's shut that one down, let's secure that, let's make it a little more compliant to the way our policies are.

I personally think that these two worlds will ultimately converge because CSPM is itself starting to move in the direction of actually doing the remediation rather than just alerting. So, I really do think that over time, those two will become one, I hope. It's one less acronym to worry about and it will just become cloud security.

It gets a little bit more difficult with containers, pardon the pun here, so proper containers, in as much as you are starting to see its smaller packages of code. There is the reigning theory anyway is that we are moving towards a DevSecOps world. In other words, you may have heard people talk about the shift left whereby effectively, it's the developers that become the people who are responsible for embedding the security, not a traditional developer concern, but we're starting to see that.

In essence, as we move from serverless, some things become more femoral which makes it much more difficult to secure them. In other words, they may only last - the life of a piece of code that's running in a serverless environment may be a matter of milliseconds. How do I secure it?

Perimeters and access control; the reason I want to make these separate is because this is the traditional world of virtual private networks which was great when everything was on-premise and all of your workers were in the office anyway and you could – you see also for remote access there. You might have a VPN that would be able to secure me working from home, but still using all the applications in the data centre. This is all very old-world stuff.

But now, you can see for yourselves. Not only are your applications moving into all kinds of other environments, but fundamentally, your users have gone everywhere. So, you've got the double whammy of the fact that people here, the remote users in - I don't know - a hotel room are accessing an application that happens to be sitting in the cloud that your IT department certainly doesn't know anything about, much less your security teams. So, I'm seeing a lot more complexity in terms of the actual access issue and the access control than there had been previously.

At that point, I'm going to throw it over to the panel. As you can see, we have four vendors on here, plus Jan at the end there. Jan, if anybody's been to a NetEvents before, you'll know that Jan is a very shy person and so you have to patient with him, but if you tease him a little bit, you may just get a few opinions out of him. But he’s quite timid.

But in any case, I’m going to with - let’s start from this end. Atch, will you start off explaining a little bit about Versa, what you’re up to and how - we’ll come back to addressing more the details of actual security in cloud and access control.

Atchison Frazer

Atchison Frazer; I look after marketing for Versa Networks. Versa is an innovator in the SD-WAN or WAN edge infrastructure space.

We are one of the few vendors who from the beginning actually built a full-blown next-gen firewall UTM and web security in the same platform as the SD-WAN functionality. The issue for our clients isn’t so much the on-premise traffic; all of the SD-WAN vendor’s typically will encrypt traffic that are handling on-premise at the highest standards.

We do a few other little tricks that we think are better; things like encryption key management is extremely important. But when the traffic leaves the on-premise node, goes out to the public Internet which never really was designed to provide the type of enterprise security that people really require, you lose visibility to a lot of the security concerns or posture as you mentioned.

You can’t distribute the policies unless you’re doing something like what we’re doing in the SD-WAN [unclear].

Philip Griffiths

Hi everyone, Philip Griffiths from NetFoundry. I head our EMEA partnerships. We are changing how the world connects their applications.

Looking at from some of the topics Rik was picking up, we make it possible, for example, someone who is a DevOps developer to create connectivity between their branches or their devices, their containers, their virtual machine environment, connecting anything anywhere, but using the public internet only.

But fundamentally, taking away the two problems of the public internet. That is making it incredibly secure and also performance and reliability that would normally you would see on a fibre network so that you can create this connectivity in minutes using APIs in a fully cloud-native approach.

Peter Galvin

Good morning everyone. My name is Peter Galvin. I run strategy for a company called nCipher and Cipher has a product that is a hardware security module that is focused on helping organisations protect business-critical applications and the information that they have.

What our customers are using our products for are the things like digital payments, doing lift and shift to the cloud, encrypting information and one of the key components of that is being able to protect the keys and so protecting the keys and hardware allows a very high level of assurance for those customers when they are running some of these business-critical apps.

Aaron Turner

Hi there, I'm Aaron Turner, founder of Hotshot. We are a security company that provides the best security to protect the least sophisticated customers from the most sophisticated attackers.

So, we take the power of very high entropy encryption, combine it with the location services that are available and essentially, help people shift to a true zero trust model for messaging, collaboration and identity. So, we are helping people do the hardest things in a simple way to protect digital identities and data.

Jan Guldentops

Somebody hacked - no, I'm Jan Guldentops. I have been playing around with security for 20 years, sometimes as a journalist, sometimes as a neutral consultant. What I would like to do today is take all these cool ideas, all the terminology and see what can be real and what are the problems with it.

Rik Turner

It's interesting that we have four vendors on this panel, none of whom really compete with one another. They each come at things in different ways. I would argue that the only one of the four companies that is a pure security company, in other words, the reason it exists is in order to secure stuff is actually is nCipher.

I personally think that Hotshot is really an application provider who happens to provide secure applications, but it is in the business of certainly selling applications with security wrapped into them.

I would say that I think of NetFoundry as an application networking company which can, if it needs to, sell alongside an SD-WAN, but it can also sell independently as an alternative to SD-WAN.

Of course, SD-WAN itself is a networking technology where what they do is, they wrap security into the SD-WAN offerings, if you like, in the same way as Hotshot are doing applications wrapped with security wrapped in. You could say that Versa are really wrapping security in from the outset into the SD-WAN offerings. So, it's a little bit of a different thing. But they've still got - each got their own takes on what are the great issues around cloud security and equally, around network access and access control.

I suppose I would like to start, Jan, what do you see today in terms of the people that you deal with, your customers and so on, what do you see is the greatest challenge right now for cloud security?

Jan Guldentops

Well, three points; first of all, my customers are using the cloud as an excuse. What they are doing is they can't get their security operations, their security up to speed, so we're going to outsource to the cloud and it's all secure and all the problems are gone. That's the first misconception I see all the time. We are going to the cloud just to be able to secure. That's one.

Second of all is, and I liked your comparison, I'm doing security for 20 years and we are still doing bolt-on security. We are not doing security by design. We still need add-on products to secure stuff. The second big problem that goes with cloud, right? It goes with everything.

The third problem is responsibility. No, I will rephrase it a bit more blunt. Chaos; that's the biggest problem we see with cloud implementations. It's all multi-cloud; most companies go multi-cloud or let's launch a [unclear] nimbus and they don't have a clue what the real inventories of their infrastructure is.

So that's the three points I would like to make. Do you agree, guys?

Peter Galvin

Well, I mean I think - I don't think the reason companies are moving to the cloud, at least in our view, is because of security. I mean I don't think that that's the driver, right?

Jan Guldentops

Not the only one, but yeah.

Peter Galvin

I mean most of the driver that we are seeing is that organisations don't want to spend any more money on data centres. They want to be able to move faster. IT organisations for many companies traditionally haven't moved very quickly. Why you see all this shadow IT activity happening is because even me as a marketer, it's much easier for me to go buy SaaS product than it is to have an IT organisation driving it.

I think the thing that gets missed and it's actually - even though that's a simplified model, is that organisations forget that they still have to protect their data, right? At the end of the day, no matter where you are on that cloud security environment, you have to protect your information, right?

Jan Guldentops

Even by law.

Peter Galvin

Even by law, yes.

Jan Guldentops

GDPR law says you stay responsible for your security operation and the security of your private data.

Peter Galvin

I agree and I think the other challenge is that they're used to the on-premise model and then they don't know how to - they are either lifting or shifting or they have got a bunch of people building native applications that they don't even know existed in these organisations, right?

Then at the end of the day, they come in, the security person will come in and say what is all this stuff that I have and how do I manage it and where is it?

Philip Griffiths

People are moving to the cloud and they have got these cloud-first strategies and everyone is trying to run as quickly as possible and the architecture is revolving over time. But they are inheriting the, let's call them legacy mistakes or some people call them best practice; what we now see as wrong used to be best practice where different parts of the organisation are doing different things.

So people might be moving to the cloud, but they are not talking to the security team and then all of a sudden, a company within that same country who may be a competitor or maybe a non-competitor, they get hacked and then all of a sudden, everyone is going oh wow, we really need a cloud security strategy. How are we going to do this?

Let's go out and buy a bunch of perimeter firewalls and see if that solves the problem, but we know that doesn't solve the problem. Really, we need to work from the ground up to create an approach which - and I think it goes to one of your things, Rik, of the cloud is not inherently secure. If you're going to go to the cloud and implement security, you need to work on that ground up approach.

A lot of people are, particularly in the CISO world, talking around the term zero trust. It's a very interesting term because it's been really hijacked by network and firewall providers [unclear] I'm zero trust. Fundamentally, you can't be zero trust if you trust the network or the perimeter. You have to abstract much higher than that, so in a cloud sense, we have to - I don't know if it's cipher HSMs, but if you go to Microsoft [unclear] or Azure you can create IaaS or PaaS run insecure enclaves. So, it's secure boot and execution, so you can make sure even if someone locally tampers with a data centre, they are not getting into your data or corrupting those applications.

At the same time, you need to build connectivity between those instances, those applications and people consuming them; whether it's server or client and abstract that from the underlying network so that you can make sure that secure. It's only when we do that real abstraction from the lower levels that we can start to talk around having what I would say is that minimum level of security for people's data and applications.

Rik Turner

Okay, thank you. Aaron?

Aaron Turner

I think the current situation we are in is that we've had a series of failures in IT where we have the self-deception that the firewall would work; sort of what Philip just said. We deceived ourselves to say there's a perimeter when there really wasn't a perimeter. Then because that failed, people through it in the garbage can and said well, let's go to the cloud because now we can maybe create a virtual perimeter and do that better. Then there's another failure.

The Verizon Data Breach Investigation Report came out yesterday and it showed that there was double the number of nation-state attackers against small businesses. So, how's the average small business going to defend themselves against a nation-state adversary? It's just not going to work.

So, what we see happening is essentially people throwing up their hands going, how can I as a small business defend myself against the most sophisticated attackers?

So, it's that series of failures and so I think what we do have to do in security is we've got to deliver a new solution that helps those least sophisticated people protect themselves from the most sophisticated adversaries. Until we bridge that gap, we will continue to see failures and people continue to try to climb those stacks and the structures as a service, platforms as a service, software as a service until they don't have anything left.

The owner of the business has essentially outsourced all of their technology to the point where they don't own anything because they failed over and over again. That's what we've got to innovate.

Peter Galvin

I think the worst part about what you just said is that if you look at a lot of the data about what people understand the threats, right, they understand there's threats to the information, but they keep using the same techniques that they've used in the past.

So is this kind of dichotomy that you are seeing within the security industry where security professionals is, they kind of know that there's other techniques that work and they should be using better authentication or they should be using better encryption and they should be using these tools, but they don't know how to view them or they are not educated enough where it seems like it's too difficult and so what do they do?

They just go and buy more firewalls and they go focus on that perimeter versus focusing on where are those breaches happening or protecting that information or building zero trust networks or really thinking about ways of doing better authentication and authenticating people before they can get to that information.

So, I think that's one of the biggest challenges.

Philip Griffiths

Yeah, I think that's really interesting where the education part is so important. I mean it's why we all have a job. When I'm speaking to a client and I was speaking to an organisation the other day and we were talking around their moving to the cloud. It was actually Azure for them and also some Oracle in Oracle data centres and we were talking through what we could do to provide them that secure connectivity into their environments where we take away the attack vectors of DDoS and man-in-the-middle and malicious internal and external workers from software-defined perimeters and zero trust.

One of their guys sitting in the room was then like way, does this mean then we don't need all those perimeter firewalls because we've effectively segregated every single component off so that it can't be accessed from the outside world and only people that should have access to it do have access to it?

We were obviously like well, I'm not going to tell you to go out and get rid of all your perimeter firewalls, but if you can start conceptualising what security looks like now that you've moved to the cloud and you don't have to just build one big perimeter, then it becomes a much more interesting way for organisations to progress and not just fall back on SaaS.

Aaron Turner

As long as they move forward with that full disclosure or full visibility, so for example, if we take a look at enterprise collaboration and email, right, Microsoft Exchange owned that market for so long, you look at how hard it was to keep an exchange server patched and to manage that. That's the reason why [unclear] exchange took off because enterprises were tired of dealing with the headache of managing exchange.

So, Microsoft goes in, takes over all the enterprise email and people go, well, I've solved my email integrity problem, but then they don't keep track of the global administrators for the Office 365 credentials and people are now hacking into the Office 365 cloud and taking over their email service in the cloud.

Jan Guldentops

Or basically phishing out 365 accounts where we have one of those guys doing that. The thing is, people like to buy their own illusions, their own magic bullet. Every X year, it's something new which is often not new technology and that's a bit - while it should be designed by - it should be by design. It should be security by design.

We're still not at that and we're doing it 25 years now?

Phillip Griffiths

Well, and this is the funny thing, looking at Office 365, if you speak to a Microsoft person nowadays, they say it's not the shared security model. They say get rid of all your security and just use Office 365 security because you don't want to have to go through a data centre or an extra hop somewhere where they are doing checks on that data. We've built all that into Office 365, so just trust us.

While I may not necessarily agree with that, that's what they've said in order to get the performance of accessing those applications. So that's why Microsoft are now working with vendors such as ourselves to have API integration so that we can break out someone out of the NetFoundry AppWAN and security approach so that they can just have that performance access.

Jan Guldentops

From hacker's perspective, if you are using Office 365 in the correct way as an enterprise, you are basically feeding your roles and your authentication into somebody else's cloud. It's a matter of time somebody is going to attack that real time.

Aaron Turner

Well, they already have. We've seen three or four used exploits against ADFS and Azure [unclear]. So basically, the bottom line is that for the standard enterprise, they should trust no one. Basically, try to build something where it is a true zero trust environment where you just trust yourself.

Jan Guldentops

And not even then.

Aaron Turner

And then, you can't even trust yourself, right?

[Over speaking]

Jan Guldentops

No, I approach it a little bit different. Trust is good, control is better, right?

Aaron Turner

Trust but verified.

Jan Guldentops

Yeah, you try to verify everything and that's what we are a bit missing. It's a bit religious; we need new gods. We trust - right?

Philip Griffiths

I don't like that term; I don't think it should be trust but verify. I think that's why I like the term zero trust because really, access should be based only on being able to show that you can be trusted.

So, for example, we work with a three-letter government agency where for their users to access applications on the cloud, they have to show five points of trust. They have to have a client on their laptop, they have to enter a password onto the laptop, they have to be wearing a watch with unspoofable hardware root of trust, they have to put their thumb on that watch to give biometric root of trust and that watch also measures their EKG, so it can't all be done under duress.

That is an almost unspoofable way of getting access to an application and the only way to access it which means you are - as part of the zero trust, you are making sure you're doing those verifications and checks along that process for that to happen.

Aaron Turner

But that is a way of - right, you are sort of verifying the trust?

Philip Griffiths

Yes.

Aaron Turner

You're just verifying the trust at the individual entity so that you know that whatever is doing that access is something you can trust, right? Because of that verification that you're doing.

Philip Griffiths

Sure, but the trust but verify is predicated on oh, you've got IP address or you're on my internal network so I'm going to trust you and I'll monitor your traffic. Instead of saying that, we should be saying, zero access, zero ability to have dataflow or visibility until you can show you have multiple points of trust.

Those points of trust depends upon the organisation's policy and how secure it needs to be.

Peter Galvin

And how paranoid you are?

Aaron Turner

Because you are trusting a thing or a device or a person, right and not where you are [unclear], right? Which is…

Philip Griffiths

Correct.

Aaron Turner

…where you want to be, right, because then you can also have policies associated with what the individual can access where they are based on what device they are using and what kind of access they can get to data and it provides a much higher level of protection.

Jan Guldentops

There is another important point, even that security, in my opinion, could be bypassed. So, everything can fail and everything will fail.

Philip Griffiths

Sure, networks are made for sharing information, so there is always going to be something.

Jan Guldentops

If the prize is big enough - I mean if the prize on the end of the hack is big enough, somebody will come up with something.

Philip Griffiths

Well, I think the key is just to make it harder than the next system. If you're harder and more expensive to hack, people find [another] system. So, it's just about having better shoes to run faster than the other people in the forest when the bear comes along.

Rik Turner

I'm just going to quickly dive in there just to say if there are any questions to this very talkative panel, feel free to…

Oh, there we are, look there's two. Hang on we have - and there's…

Audience Q&A

Steve Broadhead

Steve Broadhead, Broadband Testing. The point you're making Philip - and Jan will attempt to hack anything - but the fundamental problem there is IT is supposed to make life more simple and you're just painting this amazingly complex picture.

I'm just imagining my mother attempting to do what you've just described [laughs].

Philip Griffiths

Well, and this is where - yes, there is crazy level government things that can be implemented that take multiple points of trust, but at the other end of the scale, you can literally go on to our website, download a couple of endpoints, deploy into your cloud and in five minutes, you can create a network.

One of our customers connected seven AWS data centres in two hours the other day while doing another job which implements multiple layers of security by design so that you take away many of these threat vectors such as DDos, man-in-the-middle et cetera.

Now, obviously, you can make it more complex by integrating other things into it, but it's just a question of how much time you want to spend in that area and how much resources you can put into that policy so that the standard person can come along and do a very decent amount and if someone wants to take that further, they can.

I fundamentally, we believe that no one wants to buy - no one builds networks for networks sakes and no one buys security for security's sake. We do both of them because we need to connect applications and security is woeful by standard. The NetFoundry approach is to kind of solve both of those so that you can plug it into anything else as SDKs, APIs so that those things can have those problems and challenges solved out of the box.

Aaron Turner

One thing that we've tried to do at Hotshot as we try to make it so that a family or a small business can deploy nation-state level protections in 30 seconds or less.

So, we are trying to make it so that it's so easy to use and so intuitive that you get that prediction built in.

Steve Broadhead

Well, absolutely and that's what NetFoundry's doing, that's what Atchison's doing at Versa, right? What you're doing is fine; the problem is when it gets to the customer, they then basically often make a mockery of what you're trying to do by just adding lots of bells and whistles.

[Over speaking]

Like having a beautiful car that's designed perfectly for minimum wind resistance and people put a roof rack on it, right? It's the same concept, yeah?

Atchison Frazer

You're hitting on a really key point. Human error, let's not discount that as - yeah, you've got to - it's the automation imperative, right? I mean one of the great things about SD-WAN is you have one central control where it establishes all the policies across all of your edge nodes. You want to turn up a cloud, great, we're also the V-WAN and Azure, I'll give you the American vowel version of that.

There aren't enough CISSPs out there; Capital One has a thousand sites. They use digital labour delivered by Versa. It's all automated. We have the NSS labs, we're the only SD-WAN vendor that scored in the top vector of NSS labs rating.

So, at some point, you have to automate as many of these functions as you can, be able to reprogram as needed and set those policies and have complete visibility on-premise through the cloud and back.

Philip Griffiths

Yeah, I fully agree with that. Automation is the big key so that anyone can create it. In our world, a DevOps person, while they're using terraform to build their VPC or their infrastructure for code, they can also build the connectivity. You can do it as part of the CICD pipeline.

Where I think it becomes very interesting is because it's all software-defined because you're able to incorporate new capabilities. Instead of it actually being really complex for the customer, you can instead have really interesting conversations.

So we recently on-boarded the cloud-native bank who are working across the globe and I sat down with their CIO the other day and he started saying to me well, we want to move into the world of doing immutable transactions where we are using the blockchain and I think your technology would be useful.

I was like well, yeah. So if you're making these connections and we've got some [unclear] root of trust and we are taking the trust from the blockchain, we can create a transaction which from a legal perspective, you can say no one has spoofed it or done anything so that this electronic transaction with almost no humans involved in has legal bearing. That becomes very interesting for a financial institution where they can - you have those capabilities to do new innovative capabilities.

Atchison Frazer

But also, you can do simple things like your mum can do multiple factor - your mum can do multifactor authenticate, right?

Philip Griffiths

You mum could spin up a NetFoundry [unclear].

Rik Turner

There's one more question I want you to…

[Over speaking]

Jan Guldentops

It's genetic.

Atchison Frazer

We're going to demo that later.

Rik Turner

Okay, one more question over there, please for the gent with the…

Antony Savvas

Antony Savvas, IT Europa and Data Economy, among others. One big elephant in the room of course, which hasn't really been discussed that widely, I think generally, is the US Cloud Act.

We hear a lot about the potential of why are we being controlled by the Chinese Government like most Chinese companies in terms of having to hand over data on request, but how about the US Cloud Act?

I mean we might as well all give up because at the end of the day if a US agency wants your data in Europe controlled by an American company, it can have it. So, what are the security companies saying about this?

I've heard that companies should simply encrypt their data and control the encryption keys. So, if a US vendor has to comply with the US Cloud Act, all it can do is potentially hand over encrypted data, but what does the panel feel about this whole issue?

Peter Galvin

Well, I can speak to that because most of our customers are concerned about it and so one of the reasons that they are encrypting data and they are managing the keys themselves as to protect themselves from any subpoena activity. Because especially, not only the US government but other governments have the right to go ask for information and never even tell the person that data is being taken.

So, the only way you can really protect yourself from that is if you are encrypting the data, then it's maintaining ownership of the keys because they'll get encrypted data, but they won't be able to read it. So, they have to come back…

[Over speaking]

Aaron Turner

It's important that you own the algorithm, that you understand the algorithm you are using. As we work with customers on this topic, the first question we ask to the General Counsel is, which laws do you want to comply with?

Then you do the trickle-down because you can't comply with them all. You can't comply with US Cloud Act and GDPR in the Chinese data encryption law and UK encryption law. You can't and so you have to do the risk analysis to say, here's the trickle-down. I'm willing to run the risk of not complying with the Chinese encryption law. I'm willing to run the risk of not complying with UK and you have to go do that trickle-down.

Jan Guldentops

One of the big issues with encryption as there is one thing worse than not using encryption; using bad encryption.

[Over speaking]

No, I've seen that quite a lot and there's another problem with it is what's unbreakable encryption today will not be unbreakable in five years. In a cloud perspective, that's potentially the worst because your data still stays there potentially and can be decrypted within two, three, four years in an [economic world].

Peter Galvin

You can go to GitHub and you can see encrypted applications and then you can see the key is sitting right next to them when [get encrypted].

Jan Guldentops

That’s true, yeah. It’s key management too.

Peter Galvin

Right, so you have…

Aaron Turner

The best is when people use PGP and send you their private key.

Jan Guldentops

Yeah, people will stay stupid. I mean it’s the same thing with DevOps; am I the only guy who’s scared giving software engineers control over infrastructure? I mean I used to coin the phrase, it’s not DevOps, it’s DevFlops, but I mean it’s scary. It’s a brave new world and we’ll have to learn to live with it.

It’s a very round number.

Rik Turner

I think we’re reaching a natural end to this conversation. I think the people will remain stupid may be the lasting message there.

Aaron Turner

I don’t want that to be my quote.

Rik Turner

Thank you very much and thanks to the panel. Great discussion.

[end]