NETEVENTS
2015 CLOUD INNOVATION SUMMIT

DRAFT

Debate V:
Breaking Bad - New Developments in Cloud Security

Chaired by: Rob Ayoub

Research Director, NSS Labs

Panellists:	
Grady Summers	Senior Vice President, Cloud Analytics, FireEye
Iben Rodriguez	Principal Architect, Cloud & Virtualisation, Spirent
Mike Curtis	Vice President, Marketing, Wedge Networks
Ryan Potter	Senior Director, Cloud Strategy & Alliances, Fortinet

Good morning everyone and we're going to continue this security theme that the previous speaker started. And what a great presentation. I've got to tell you, I think, as we were unfortunately chatting in the back of the room, we don't entirely agree about some of the triviality of what we discussed. There's just a lot of factors and I think that's one of the things we're going to really hit on in this panel is there is some phenomenal technologies, some phenomenal approaches to security today but the actual implementations in addressing and tackling the training and certification problem is really a significant challenge for the industry.

So we all know the concerns when we talk about moving to the cloud, moving to managed services. Things like concerns about losing the data, what do we about forensics, who actually owns the breach. Nobody wants to own that part. Everyone wants the data, everyone wants the applications in their cloud, but nobody wants to own it when something goes wrong.

A huge challenge also is that security players think like this that in fact the industry still has a challenge with being very box-centric. Everyone wants to hold their firewall. They want to point at the rack thing, they want to know where it is. Hey that's my firewall, I can see those connections. As we move to a virtualised world, as we move things into private clouds and public clouds, that's a much harder challenge because then where's the firewall. Well, I don't even know. I've [spread out]10,000

of them, how do I manage that now that I can't even -- I can't see it, I can't put my hands on it.

So even though we like this box-centric approach, what's the world moving to? We've seen it this whole conference. Virtual appliances, Guido talked about the whole entire virtual infrastructure layer. Things like mobile endpoint security, how do we secure mobile phones. You know we're really good, we were really good as an industry, relatively speaking I guess, about securing our desktop. At least we knew what to do. We knew what needed to be on there. What do we do in a mobile phone world?

And what about application specific security services? [inaudible] really talked about the future being things like NFV, containers, but what's the practicality for a world of professionals that still want to hold on to their firewall?

And these are the kind of things that we're going to talk about today with this great panel is how do we get there from here. How do we get to -- cloud security is such a nebulous term, no pun intended. How do we get to securing our data, our applications and our virtual machines as we move them off premise into somebody else's datacentre. What about what happened with Snowden? What have been the impacts of that internationally for US-based companies. Those concerns are not going away.

Got a great panel here today and I'm going to let the folks on the panel introduce themselves quickly and then we'll dive right into it. I want to keep it pretty interactive today, so obviously we'd love to take some questions from the audience. But we can certainly talk for a long time. We found that out this morning. Grady, do you want to start?

Grady Summers

Hi, I'm Grady Summers. I'm a Senior VP for Cloud Analytics at FireEye. So FireEye of course is a pure play security company that's got a lot of different security products. My particular business line is a cloud-based product that takes in data from whether it's enterprise, cloud based or virtual environments and provides monitoring and protection and instant response capabilities. So we're in a unique position of being a very big consumer of cloud services, we run on Amazon, but also very big resellers and ISV who builds a product that does run in the cloud, so you get to see both sides of this argument.

Iben Rodriguez

Hi everybody. I'm Iben Rodriguez from Spirent. Spirent is a test and measurement company and I'm new there. I'm helping Spirent work with their customers who are interested in leveraging cloud and virtualisation technology. We see a lot of activity there and so far it's been a lot of fun. Working with a lot of customers, very active migrations from local legacy box technology with firewalls and load balancers to using those services in either a private cloud in their own datacentres or hosted in the public cloud, like an Amazon or a Google or Azure.

Mike Curtis

Hi everyone, I'm Mike Curtis from Wedge Networks and I guess I'm the bright eyed and bushy tailed start-up of the group. We're very much optimistic that the disruption afforded by cloud certainly and also on the networking side, NFV and SDN gives us a tremendous opportunity to rethink security. I think Rob's correct and I think even though that's true, you're still as you got layered security over the last 40 years in the enterprise world, we're going to see that layered security obviously still exists as we look at this sort of transformation in IT.

So at Wedge, we've talked about securing the cloud itself certainly. We actually focus a little bit more on the networking side, I guess you could say, the cloud networking side around NFV, highly scalable high performance security applications running as network virtual functions. So from a go-to-market perspective we focus on really everybody with very large datacentres. That can be carriers, but as well as very large enterprise.

Ryan Potter

Morning everybody, Ryan Potter, with Fortinet. I'm primarily responsible for our hyperscale and the cloud business. Not surprisingly, that means that I spend most of my time with Amazon Web Services and Microsoft Azure. Coming from a very traditional security background, with a lot of established physical product deployments and [inaudible] quite a few challenges both in terms of customer perception and market perception in terms of these migrations.

Rob Ayoub

You know even from my own perspective, NSS Labs has a deep history in security product testing and the idea of cloud, how do we test things in the cloud is a huge challenge even for us. I want to get to the testing part in a little bit, but to start off I really -- that diagram I showed, the traditional network rack. We can argue the world is moving towards cloud, but security players in particular are very tied to their firewalls. When we talk to customers, that's a big struggle.

From your perspective, when you're working with your customers and obviously, you have a broad range of some very large installed base, versus Mike, sort of new and then Iben, I'm sure folks coming to you asking these questions about testing, how are you seeing your customers actually work to adapt? Do they work to change it or are they fighting it? Or they want virtual versions of what they have in place already?

Ryan Potter

Coming from the perspective of millions of physical devices installed and hundreds of thousands of enterprise customers and carrier and service providers, there is an early, initial, we'll just copy what I have today, get it working, get that toe in the water, figure it out. It's really part of the initial assessment of what's going to work economically, what's going to work from a technological perspective and what can I manage on a day to day, what can I live with.

And trying to predict that has been, I think it's a mixed bag. You've seen some folks who are very successful, some folks who have gambled and it's paid off and others that have [inaudible] and reassessed it three or four times.

I have some unique challenges in that I have a very broad set of customers, with an extremely broad set of expectations. So at the most simple, there are a few factors that we probably go into from a regulatory and compliance perspective, just as things that you'd go to jail for, or if you look at some of the breaches in the last 18 months, you've seen many C-levels lose their jobs based on breach.

Grady Summers

That's interesting, but I want to interject here. You talked about compliance and there is a need for these security devices in your organisation to be compliant. But the example that we're talking about here, twice now this morning, the person who lost their job because of the breach, they were compliant actually. So let's not get confused about the difference of compliance versus security. So it's important to have security in addition to being compliant. So you want to use the right tool for the job, I think is the main point here.

Iben Rodrigues

One of the things that was said earlier is that the network is all about software, it's a software business and I agree that's the direction we're moving. But we all use computers today. Look at on the desk here, nobody is just using a software, you have hardware in front of you in the computers in the networks and firewalls and everything. Even your technology running on Amazon is on hardware somewhere. So the hardware is not going away. People still need to buy hardware and it still needs to be secured. So I agree we're moving in that direction and I wonder how that's changing the way we think about it.

Rob Ayoub

Absolutely. And Mike probably, it's more a question for you and Grady also. Mike in particular, you are completely [inaudible]. So when you get customers coming to you that either have existing deployments or are working to move things, you're sort of seen as the [fresh] approach.

Mike Curtis

I might have to plead the Fifth on this one somewhat in that if we've done our job qualifying the opportunity, we want to try to get in, in the stream of folks who are looking at advanced projects around NFV that are already exploring the next chapter of how they're going to do things. So actually these gentlemen have much broader experience in terms of how do folks address managing your enterprise environment now in the cloud and your cloud applications, cloud environments. So how do you not do things twice, both operationally and from the whole client's perspective, Grady can probably speak about that.

Grady Summers

[inaudible] your question about folks who love to have their rack of hardware. As ISVs, we're selling, we have customers who are really split into two camps. Some are saying, I'd really like to [inaudible] in the cloud, can you just run that for me on [inaudible] using [technology deal]. But we're seeing an emerging group which is very exciting, maybe 10% to 20% of the prospects we talk to who say, hey, I want it cloud-based security solution here, I'm done with racking and stacking appliances and training up administrators and getting paged in the middle of the night [inaudible].

Rob Ayoub

That's what I'm saying, they're not done. They can't be done. You don't just walk away from your datacentres or do you?

Grady Summers

If you look at companies like General Electric, I spent 13 years at GE. Dozens and dozens of datacentres, about to migrate their datacentres globally. And they've stated, they've gone on the record saying they want to reduce 90% of their data footprint in the next three years.

Mike Curtis

So it's a three year plan. So well that's what I'm talking about. So you have an investment in capital equipment and your business processes and your IT processes aren't going to -- three years is pretty aggressive. Maybe if General Electric can pull it off to transition to 100% cloud from maybe 90% local on-prem today, that's very aggressive. So I think we should start thinking about it and that's what we're hearing about today. But let's not forget that there is a legacy of investment of IT professionals, training. Is General Electric going to have training for those -- all their IT staff?

Grady Summers

[They certainly will]. But I think one point that you make that I'll pick up on is it's easy. I would argue for customers who say hey, I'm done with the rack, I just want to be done with that and move to a service [inaudible]. They can make that kind of discrete decision within their business. As an industry the need doesn't go away. [There are going to be] people who wake up in the middle of the night to worry about the old machines. So that retraining issue is very real.

Rob Ayoub

Transition. Going back to the legacy question now and I think this is a really critical point, there's also legacy perceptions in the industry as well. So the point was brought up yesterday that are cloud services inherently more secure just because of the nature of the beast that they have the people, the talent. How many security engineers does Amazon or Google or CenturyLink or ATT Verizon have versus your own organisation and yet there's still this again administrators want to hold on to their

security, even the organisational politics of forcing folks [inaudible] can't put it out there. How do you all see that playing out today? How do your customers deal with that concern?

Grady Summers

We face that a lot because as customers are considering moving security services to the cloud, they always raise that question. And I just point out that pound for pound, server for server, there's so much more scrutiny from the cloud providers on security. I remember spending a three day session at one of these cloud providers going deep on their security. A team of 300 people dedicated to securing the environment. We asked a question about log retention, how long do you retain logs and they looked at us and said what do you mean. How long do you keep logs for the environment before you roll them? We don't ever roll them, we keep them forever.

So I think that kind of blows the minds of a lot of enterprises who have a security team of five or six people. They don't realise just the benefit that accrues to them from a security perspective by moving to a provider.

Iben Rodriguez

It depends on the maturity of the organisation as well. A lot of banks who have been around for a long time, won't keep them forever. I think it's seven years in the US that you need to keep your records for depending on your compliance issues. And that's a good point. Is it just about trying to be compliant or are you trying to be secure? So each business is going to have to answer that question and address it individually based on the policies that they have, the people that they have working there, the future growth, are they a growing business or are they a stable business.

There's all sorts of factors to consider and some businesses actually are fine to delegate the building of their applications, like we mentioned the exchange server. If you used an exchange five years ago and your mail server is running out of disc space and getting slower, are you going to move your exchange servers to Amazon or some cloud partner. No, you're going to go to Office 365 or Google Apps or something.

So it's a matter of doing what's right for your business. If you're a telecom industry or a carrier or you're building a datacentre and you're providing services for other customers, those are the kind of consumers that we deal with today. It's not end users but actually the service providers and the people that are building datacentres. And they have to test what they're building before they move it out. So that's a much different type of business than a bank or a mom and pop or a Target.

Rob Ayoub

Ryan and Mike, well, let's go downstream and both of you, Ryan in particular, very channel driven a lot of non-traditional, large part of your business actually relies on the VAR or [first] support. So how does this idea of 300, 500 dedicated security engineers translate downstream?

Ryan Potter

Even more than the [VAR], maybe providing that additional physical infrastructure and then maybe the installation of it. The business is extremely dependent on managed security service providers and those run the full gamut from the largest telecommunications companies that are providing a leased line circuit to -- you still probably have an office somewhere. You have a datacentre somewhere. You may have a public or private or most likely hybrid cloud environment that you're dealing with.

The managed security service providers are really capitalizing on it better than anyone I think right now because they have the experience of managing and security equipment that is not theirs, not even physically accessible to them and previously unknown to them too.

Rob Ayoub

Mike, from your perspective on the MSS side, is that different for you all than say this traditional [ISP]?

Mike Curtis

I think that's all [good] perspective. I think just to maybe add one high level point on it, just to reframe for folks, one thing that unique about the security space that does not exist anywhere else is we've got the threat that is always a moving target. That's the one that is unique to our space. So what that translates to is complexity. The complexity never really will go away.

Yes, we've had some massive disruptive innovations around computer architecture. But I think architecture will make security -- I wouldn't use the word easier, but there are some new architectural constructs that do things differently. But I think the theme is the complexity will always be there just because of the nature of the moving target.

Iben Rodriguez

That's an interesting point. If we acknowledge that you have a legacy datacentre to support and it's going to take a few years, three years, to migrate all to the cloud, what are you going to do for those next three years. Your existing staff is going to be overworked learning new technology. And there are a number of new attack vectors as you change from any old technology to any new technology. Even if you were to keep things local and go from one vendor to another vendor for the same type of function, you're going to increase your attack surface and the skillset of your employees can determine your probability of attack.

We were just reviewing the Verizon Data Breach. Have any of you guys heard of that? It comes out every year and they go over all of the attacks and compromises that have been made over the year before and they rate them. And one of the main things was mis-configuration and training of your employees, people making mistakes, human error. So it's important to consider outsourcing that security operation, maybe bringing in some extra help.

Grady Summers

You actually make an interesting point. I think one side effect of the fact that you're going from a traditional datacentre into the cloud and you can't concurrently train a person to do both overnight means that a lot of companies they are starting to get into the cloud are treating it just as it's another hosting provider because you're moving a physical server in your datacentre into a virtual server at Amazon or Azure, [inaudible] tapping inside the [inaudible] services.

Iben Rodriguez

They want to do things the same way as they used to do.

Grady Summers

Exactly.

Mike Curtis

That's actually a great point and it brings up another question. Why now do you see and I think I know the answer. Are the customers basically just -- I know what I've got, so I'm going to move that to the cloud and really the follow on, how long is it going to take before we really do think about re-architecting things to take advantage of the cloud and not just pretend it's the cloud, but I'm comfortable with my existing deployment so I'm just going to [inaudible] into the cloud and just run it the same way.

Grady Summers

I think that happens as soon as you start getting those monthly bills from Amazon.

Iben Rodriguez

That's a good point. We were talking earlier people start using a public cloud provider and they pay every month and maybe if they do do it the traditional way and they have four servers in my datacentre and they're getting old so I need four servers in the cloud, that's one way to do it. But that could be actually very expensive because four servers over a few years, will end up being a lot more expensive. It's better to think about your application that you're moving maybe it's a web server or a financial system, a database of some sort and how can you move that to the cloud more intelligently.

And Guido was talking about this earlier, I like the timeline. He showed the history of [inaudible] virtualisation or software defined networking from 2009 till now. It is ready for mainstream, but NSX is still not something publicly available that you can download from the Internet and use. There's a lot of universities and what not that are still working on developing the research. It's going to take five years or more. I'm glad to hear about GE's project, but I'm interested to learn more on that.

Ryan Potter

I think in terms of new development something that I feel maybe going unaddressed more often than not or is it not being thought about is and this is maybe some [inaudible], but the idea of instant response in the cloud, anyone remembers Code Spaces. I know a lot of people, [inaudible] providers would like to forget that. I encourage you to look it up. You have a company that disappeared entirely into a breach. And this is something that has the potential to affect a lot more companies, a lot more services that people depend on.

Grady Summers

That's an excellent example, Code Spaces. Please look that up and do some research on that. Moving to the cloud can be done right and have big benefits, but it can also be done wrong. They were a company that was around for a few years using the cloud and because of some human error and mis-configurations, it wasn't just a breach, that company closed down.

Mike Curtis

We get that question a lot about instant response in the cloud. It all comes down to visibility. I think you mentioned this in your introduction about forensics in the cloud and [inaudible]. And this is where again I get excited about what the cloud can offer a company that's migrating because we work with clients who are trying, they're struggling to instrument their endpoints, how can I get more good data off of my endpoints. Meanwhile you migrate over the cloud, I use Amazon as another example. You've [inaudible] CloudTrail which is their [logging] service an you get I think 43 different subservices from authentication to key management, performance monitoring, all split out automatically. So where you're struggling to do that on-prem, you flip a switch and you get that service [inaudible].

Rob Ayoub

Not to belabour the point, but we keep mentioning Amazon. We had this conversation earlier. Amazon we feel like is setting the bar pretty high. For the other and there's a lot of service providers, telcos as part of this audience, from your perspective and obviously different products and we understand that -- I understand certainly that they're different and they certainly have their place. But what do the current service provider telcos need to borrow or really think about as they make it like the Amazons and Azures?

Ryan Potter

A lot of it comes down to business agility. I don't like the term but the born in the cloud companies that are -- you started from a [inaudible] perspective and that's another sort of security rabbit hole that we could go down. Oftentimes the innovation curve is amazing, but it's when they start to actually try it for real and they move something that is either regulated or personal identifiable data into that new

environment and then are coming back to check the security boxes after the fact, there's a very dangerous window of exposure there.

The other aspects that kind of build on that, from a scale and automation perspective, scaling security is a different mindset. There' a lot of basics that you can accomplish there in terms of the compute and basic network segmentation. But when you start looking at scaling analytics, not only is the volume challenging, forget basic network access logs, but look at application level control of previously unknown applications, that are home grown in the cloud, there's a vast array of things that people aren't considering.

And there's amazing opportunity too. You're going to have some, I won't say boring but very measured sort of examples as large enterprise customers that have long history and vast Microsoft deployments go into Azure, you'll see that it's going to be very predictable. But you also see very exciting things happening like three weeks ago at the San Francisco AWS Summit they made the machine learning APIs available to everyone. That speaks of huge opportunities for customers to innovate entirely new security models.

Mike Curtis

I might add, you're talking about carriers and service providers and this is more on the networking side of things. But theoretically no one is better positioned to understand identity from a networking ingress/egress traffic standpoint [inaudible]. So if it's predicated on this perimeterless world, this is an opportunity for the service provider if they do things right with these enabling technologies, NFV and SDN and the cloud is in there as well, they're positioned to execute security policy and do things at a higher level potentially.

Iben Rodriguez

So more dynamic security policies.

Mike Curtis

Security for network servers.

Iben Rodriguez

Yes, there's things like dynamic security policies that would allow you to have more access based on your location. Is that what you're talking about? If you're in the corporate office with some additional security controls, you have more easier access to your data with less security controls than if you were travelling remotely in a foreign country, you might get some additional.

Mike Curtis

And Rob I think you asked what can other providers when they look at Amazon. I think if I am competing against Amazon, [inaudible] by half a dozen different

providers as an alternate platforms and no one can compete on functionality. What they can compete on is the fact that some of them are not American companies. There are sovereignty concerns and even with our platform we can run it completely in Germany but it's still a US company running it. And as much as it pains me to say it, there are many companies, many customers out there who simply don't trust it for that reason.

Iben Rodriguez

Again it comes back to knowing your business and if you're a global business and you have offices worldwide, you want to use the right tool for the job. So it doesn't make sense like GE to move all your things to one service provider and get out of your local datacentres. You're going to need to keep some local presence and probably you want to avoid the vendor lock in so why not as Guido was showing earlier use the best of breed products depending on your application and the location of your business.

Rob Ayoub

Are there any audience questions. We can sit up here and we've got plenty of topics to cover. If there are some questions, we'd love to take them in the next ten questions or else we'll go down a few rabbit holes around [inaudible] testing. Any questions?

Hans Steeman, Telecommagazine

Hans Steeman from the Netherlands. To what extent is hardware from Chinese vendors being protected by these kind of solutions? I know that you guys, the Tier 1 providers are not allowed to use Chinese systems because of backdoors. How can you fix it with a software approach.

Iben Rodrigquez

Using the software to determine where your data is located and who can access it and such?

Hans Steeman, Telecommagazine

The risk at least to my understanding why Chinese hardware is not allowed here in the Tier 1 providers are the backdoors that are expected to be there, same as the US based equipment.

Iben Rodriguez

Back to the questions about the chips and your supply chain.

From the floor

Yes.

Iben Rodriguez

Actually that's an interesting topic. There's a big movement if you follow the Open Compute project. One of the things they're doing is open sourcing those firmwares that go on the chips of the motherboard so the BIOS and these types of firmwares are historically made by the vendor and you have to pay a small fee. For example, Intel used to charge to use the [PXE boot network] and there was a license fee for that or royalty. So there's a big movement away from that kind of closed type of service to open source. But even open source can have backdoors in it. That was the ShellShock and some other attacks recently that have been around years and even though it was open source no one found it. There's no perfect answer.

Ryan Potter

At Fortinet we rely very heavily on the rest of the industry third parties to provide independent tests and analysis and that ranges from UL safety certificates all the way up to application layer testing. We also do some things relative to the scale of the service provider hardware that we deliver. We do the vast majority of our assembly as well as our firmware load in the US now. So there are things that vendors are doing to address those on all levels.

Iben Rodriguez

It's kind of like what you see in the food industry or some of the other industries of knowing the supply chain. There are some different restaurants that go all the way to the farmer and they know where their food is being grown and they follow the food all the way, be it coffee or what have you. And you have to do that for your computers if you care about this. The computer is the same thing, follow the supply chain. Go back to where your devices are being manufactured and visit the factory and make sure that you know how it's getting to your customer.

Mike Curtis

I think there's also goes back to what we were talking about some of the opening up of information. So much of the advantage of the cloud has been that you just run it, you just throw it up there. And especially in security there is a need for at least a window or at least some sort of data sharing information, information sharing to allow that comfort level to happen. So not really necessarily on the physical side, but it does that end to end problem where is my data going, how do I know that it's not going outside the [inaudible].

Sean Hackett - 451 Research

You kind of stole my thunder a little bit there. So Sean Hackett from 451 Research. First is a comment. I think there was a lot of good discussion here about legacy sort of infrastructure in datacentres. 80% of the data footprint today globally is still owned by enterprises. So that's shutting down a datacentre and putting it out in the cloud is a big endeavour.

Second is and you just hit on it. I think it's overblown with the fact that a lot of enterprises -- the fact that service providers have a lot of capital to invest in security people. I think enterprises know that, but what they're afraid of is the risk that they're assuming. So why do I rob banks? Because they have all the money. So I'm a real target if I'm a service provider. And if I'm a mid-sized enterprise, I can hide myself a little bit.

And I think another thing that they're really afraid of is the black box. What am I not seeing? And there's a service chain. So when they talk about security, they rarely talk about the toolsets that are required, but they want to know more about the process and transparency into the process and that's something that service providers aren't doing today. So I think you folks can help with that.

Rob Ayoub

Grady, you're on the analytics side. I'd love to hear your perspective on that, that sort of issue, thinking about forensics and because you're collecting that data.

Grady Summers

We are. You're absolutely right on the black box. That's been a traditional concern. As I mentioned in a lot of ways now we're starting to get much better forensic data from the cloud than we did. We monitor both environments in the cloud and the enterprise and the data richness we get from the cloud environment is much better.

Deployment and assumption of risk is really interesting. I'm starting to see though a change there. Customers are starting to wake up to the reality that the risk they assume by running applications in their own datacentre with their own limited security staff is in itself a huge risk. So it's getting to the point where it's [inaudible] the status quo was really good and I assumed risk if I shift it, to realising the status quo is broken and all my peers are getting hacked, I'm not sure I want to continue to assume this risk, maybe there's someone who can help me offload some of that risk.

Who's making that decision? It's the CIO or the CISO. And they are transferring risk at some point. Somebody told them that our servers are secure. Whether it's in your datacentre or in Amazon or whatever it is, somebody is trusting someone else. So it's that attestation of [risk]. Do you trust your people, are you willing to risk your job?

Mike Curtis

And after your people have told you for years that you're insecure and you keep getting hacked.

Sean Hackett

Those are really good. So is Amazon assuming the risk. Probably not, right. If you look at the way they write their SLAs, probably not. They're trying to drive developers to drive more resiliency into their software so they don't have to assume the risk. [inaudible] service providers of the risk is --

Rob Ayoub

Amazon does assume risk on for the IaaS side, all the compliance. They do say and they're very clear it's shared responsibility. And it is a little tricky and we haven't seen it proven yet. And --

Grady Summers

It is an interesting point. If a breach does occur on Amazon at the infrastructure level, the [PRI] we haven't seen the test case yet. So that is a really great point.

Ryan Potter

In theory that shared security model you draw the stack and it comes up to a very high point where this little bit at the top is the end customer's responsibility. What are you touching that application, what are you developing and how are you protecting that then it becomes a bit of a pyramid there.

To the point you were making, and secondly, I think one of the things I worry the most about, not the CISO or the CIO being -- their ability to trust their staff and the employees, but the legislated and often regulatory budgetary mandated migrations. These are happening actually most predominantly in civilian federal and some of your larger organisations. You must have this into AWS cloud or you must have into this platform by this date and those are quite interesting because the natural reaction is to match requirements. So it's copy

Grady Summers

Let's be clear here though. You're talking about a different type of cloud. It's a community cloud that is focused on a specific industry like the US government or --

Ryan Potter

Sure except the civilian federal government, those are going into public AWS regions. And when you're trying to copy something like in AWS and many IaaS providers there's no Layer 2. Traditional networking architectures do not operate the same way and so when you start using that as the basis for your security model, you're already going down the wrong path.

Grady Summers

Just to be clear I understand what you're talking about, you're talking about like VLANs and segmentation right.

Ryan Potter

No [VRP], no broadcast exactly. Your [inaudible] model changes just in terms of those networks are [inaudible] for availability. But it's basic fundamentals that the people have to come at from a different perspective.

Also we'd be remiss not to mention Google as a -- we've been very focused on IaaS [inaudible] offering, exactly as well as the SaaS vendors. Enterprise SaaS security in the cloud is a whole another topic.

Rob Ayoub

So we're not going to solve it today and I think we've [inaudible].

Grady Summers

I just want to respond to the [inaudible] comment. We were at RSA this week and there was a lot of talk about docker and container and Kubernetes and we even heard Guido talk about containers this morning.

We've talked amongst ourselves and there's -- none of our customers that are really security conscious and regulatory compliance concerns are using their container technology yet. But that's definitely something we're tracking and trying to see at what point it's going to become more interesting to us. But we're not sure where that stands right now.

Rob Ayoub

So lots of great challenges ahead, not going away today. But all of us will be around later today if you want to try and track us down later. But we can talk for hours on end, so we will. Thank you very much.

[End]