NETEVENTS

CLOUD INNOVATION SUMMIT

FINAL

Debate Session VI – Driving true innovation with Cloud and Mobility: IoT, Big Data, Analytics, Security and more

Chair: Casey L. Quillin

Director, Data Centre Appliance and Storage Area Network Market Research, Dell'Oro Group

Panellists:

Eric Hutchinson	CEO, Spirent
Hari Makkala	CIO, Delta Dental
Paul McNamara	VP Strategy for Cloud, Ericsson
Bob Metcalfe	Professor of Innovation and Murchison Fellow of Free Enterprise, The University of Texas at Austin Cockrell School of Engineering

Casey Quillin

Okay. So my name's Casey Quillin. I'm an analyst at Dell'Oro Group. I cover the datacentre. And so I'm going to introduce an amazing panel. We're going to have a discussion, hopefully a debate eventually. But I'm also going to talk briefly, and I'm under no illusions about who you're here to listen to, but I am going to touch on a couple of points about the market so we get an idea of how these things affect real products.

I again come at it from the datacentre and how the cloud affects the datacentre, so the couple of slides are more or less the cloud and its impact. But I'll let you take a look at things.

First, the panel. Eric, who is CEO over at Spirent. He has held a number of positions with the company, a wealth of information on the things we're going to be talking about. And Hari is going to be our resident use-case guy from Delta Dental, who's

going to help us understand how we use these things in the real world. I'll let you read over the bios. We're going to beat up on Paul because he wasn't able to make the breakfast and so he doesn't know what the questions are and so things are going to be a little tougher for him. But he's also going to tell us how this actually gets scaled and delivered. And then lastly Bob, who, as you know, invented Ethernet. And he's also a professor at the University of Texas. And so we will get to the panel momentarily.

So why does the cloud matter in terms of the market? There's a couple of things. The change in who purchases equipment is very important. In the past we've had a number of discrete enterprises, who purchase equipment based on things like who their sales rep were, whether they had a good rapport, or maybe more importantly best of breed. But as that changes to cloud purchasing, the priority now becomes price. And that is because the cloud folks are only going to purchase what they really need in terms of functions and features. And they're going to make sure that it fits what they need, and what they need is inexpensive equipment, whether that means vendors who strip down functionality for them or they build their own. Not all can build their own, but some obviously can, as we've seen from Facebook and Google.

So the cloud as a customer, again, is a very different animal than the enterprise. Content providers, like Google, have done their own, like I mentioned Whitebox. So if we look at Whitebox switching for example, it is greater than 10% of the market in Ethernet switching, which is a very big market.

The other piece is the outsourced cloud, and again, that's where this buying preference comes in. But as companies, and we believe they will, as enterprises continue to move to the cloud and ultimately put most of their infrastructure or applications in the cloud or have services delivered to them from the cloud, that's going to drastically change the amount of equipment we have on premise. So that's the other trend. So we take a look at what this means.

So in terms of servers, we've moved from about 30% of server adoption coming from the cloud in 2014 and expect that to be more than 50% in 2018. If we look at it from an Ethernet switch perspective, it’s not far behind. So these are real numbers and this is a real impact. And now somehow I'm going to try to tie all this together.

So my contention or contention at Dell'Oro Group has always been that if we look at trends like SDN, cloud, mobility, Internet of all Things, some more prolific than others and some further along in terms of their adoption than others. But the end result is there's been too much focus on who gets hurt. Who loses? Because the reality is that as long as vendors can adapt and are able to change, given what's happening around them, it's not a matter of who gets hurt or who goes out of business. I think what we should be focusing on is who wins. And who wins is the end user, both enterprise customers and the end users who actually use the devices.

So with that, we will open it up to the panel. I'm going to start off – I think I'll start off with Hari. As a user from Delta Dental, maybe you can tell us a little bit about how the cloud and mobility is actually a benefit to your organisation, and maybe a specific use that you've been able to do with it.

Hari Makkala

Sure. From a cloud perspective, we're – again, I'm going to give a perspective as an enterprise and also working in a healthcare sector. So there's a lot of ambiguity and in terms of where we can use cloud. So we're definitely looking to use for developing and testing. But from a mobility perspective, we're very excited. The opportunities are limitless as you look at Internet of Things. We recently launched a product. Delta Dental has a second brand called Dentegra. And as part of the Dentegra Smile Club, we launched a connect a toothbrush. So kids can actually use the toothbrush using the gaming. They can brush and we actually help them brush. They gain rewards by brushing the right way and for two minutes a couple of times a day. So it's kind of exciting.

But also there are benefits. There's no correlation between improving healthcare and brushing benefits. But who knows? Dental hygiene could be an opportunity. But again, from a healthcare perspective, trying to launch those type of use cases, on the medical side we're seeing a lot of use cases, like you may have heard, like blood pressure cuffs or insulin pumps. Real use cases for in consumer. So there are a lot of innovation. Very exciting times. But also, at the same time, a lot of concern and challenge around how do you balance on security.

I know the earlier panel discussed about whether do we go on to be in compliance or should it be driven by security? I can tell you from a healthcare perspective, the compliance requirements are being the major driver for securing sensitive data. And it's a big problem. In terms of in 2015, they say that healthcare industry will be plagued by data breaches. And one data point that I picked up from experience was that they expect healthcare industries to expend $5.6b just to address data breaches. So there's a lot at stake from a privacy and security perspective. At the same time, there is limitless opportunities ahead of us.

Casey Quillin

Thank you. And then to Bob, as someone who understands networks and also as a professor at a major university, how do you see or what do you see as the benefits of these things and maybe some of the challenges?

Bob Metcalfe

Well security is the big one. People are reluctant to take sensitive data and move it out of their premises into the cloud. So we're going to have to solve that problem. By the way, one way of solving it, I've thought, is to not put the data in the cloud. So my medical health records, I'll just keep those. That way you won't have to protect them.

By the way, HIPAA, you have to deal with HIPAA.

Hari Makkala

Absolutely.

Bob Metcalfe

I think in our conversation earlier, you made two great points about HIPAA, which I'd love for you to repeat. One has to do with how hard it is to comply and the other one is what that doesn't mean.

Hari Makkala

Yes. See, HIPAA is for covered entities. It means if you are providing healthcare services, so either you're a doctor or medical doctor or a dentist, storing your health record information, they have to be compliant with HIPAA. And then as an insurance carrier, healthcare insurance carrier, we have to comply for HIPAA. And so there's a lot of security requirements that sum up to HIPAA compliance.

But just being HIPAA compliant doesn't mean there won't be data breaches. Actually I look at HIPAA as being the lowest common denominator. And organisations won't survive just by HIPAA compliance. And that's going to be a major factor for healthcare.

Bob Metcalfe

I'm a customer of Delta Dental, by the way, at the University of Texas, which has a really good football team, especially compared to Oklahoma. As we say in Austin, OU sucks.

Could I add a second thought? Would you mind? I'm sorry. So there's the security one. But then there's the relating to adoption of clouds. There's the problem which I think this meeting has gathered to address directly, which is there are now four, five, six, seven, eight, nine, ten flavours of cloud. And so you have to choose which one you're going to use. And then there's, as we heard in the previous session, the danger of getting locked in by using too many of their special features. So I think that's the second cloud problem is the one we're working on here, which is how to generate a standard, standards-based cloud.

Casey Quillin

Do you have an opinion on which cloud wins ultimately, or two? Is it hybrid and public?

Bob Metcalfe

It's going to take a very long time. Since the top, well, Amazon is killing it. So it'll take a very long time to get Amazon to adopt a standards-based open cloud, I bet. But if we work hard and we're lucky, eventually they'll offer some sort of open cloud wrapper. It's like all the computer vendors switch from SNA and DECnet and all those other proprietary protocols. Eventually they had to go to TCP/IP I think the same is likely to happen here.

Casey Quillin

Okay. We'll come back to security, because that's a big topic. But I was thinking, as end users or customers of these trends or technologies, we want our applications to exist out there because we want to be able to access them from everywhere we go. But we also demand that that access and that user experience is very similar to what it's like when our server's down the hall. So I would turn to Eric and say how do we scale the infrastructure to be able to do that and use things like validation and testing to optimise that experience.

Eric Hutchinson

Okay. So the root challenge today, so quite interesting because Casey just expanded the scope dramatically over remarks, talking about the Internet of all Things. That's everything. We were trying to deal with the Internet of Things, which is a big enough challenge. We have conversations with service providers who are trying to support these technologies today.

And it's interesting that when we were talking to the CTO of a major wireless carrier, the comment they made was at present our current processes, equipment and systems enable us to be ready to test the internet of a thing, because the background they come from is testing things like smart devices to the nth degree. Test the performance to the ultimate level, and that's been a very large-scale investment in people, processes and equipment. We now need to switch to millions and billions of devices being connected, enabled by the cloud technologies. You wouldn't be able to all of that data without it. So the cost per item, per connected sensor, has got to be very low.

So it's all about developing new software processes, new automation processes and reducing the cost of people in those test and validation processes. So DevOps, agile developments, that's what we're working on. So we're constantly pushing this, everything going into virtual. And really the only way that you'll get to the nirvana of being able to validate the security, the linking and the optimization of all the connected sensors themselves is to have a cloud test service, otherwise the people developing the different things, they need to validate and test that before they're connected.

We at very early stage of being able to enable this and roll this out today. As Bob's saying, we're beginning quite a long journey. And as Jeff Schmitz said in his opening remarks, we've still got 600 different fire hose connectors. So let's hope the cloud won't take that long to deal with.

Casey Quillin

Right. If you think about what your company does, the scope of what – an amazing job in what they do, being able to test and validate systems that are ultimately changing so quickly is amazing to me. But if you think about all these trends coming down the pipe, how do you decide what you're going to develop – because you have to build these things beforehand. You now have to decide what technologies seem

meaningful, but also you have to be ahead of that curve and have testing before that. So how do you go about finding that?

Eric Hutchinson

Well you've got to keep close to the strategic thinkers in the industry. And quite often you're being close to the chip developers. They're often looking ten years out of where the world's going. We're dealing with a narrower time horizon of having test systems, validation systems two to three years out. So being connected with those developments and just interacting with everybody in the industry and the way they're thinking about the way the technologies go.

That's not to say we don't find it hard to make the right bets because not all technologies, not all solutions come to fruition and become a big market. And that's where balancing the cost of innovation and speed of innovation against ultimate revenue is the challenge. And again, you hit it right on the head, if you don't adapt, then you'll die. So we're going through a massive adaption phase.

Casey Quillin

Yes. Paul, continuing on the same vein, how do we provision the needed equipment or infrastructure in the cloud in order to make this possible? And how do we scale it? And how do we ultimately secure it?

Paul McNamara

Yes. I think one of the big trends that we're seeing, when the cloud first started, there were really a small number of massive datacentres that were bolted on to the end of the network. And so data would transit the network to get to the cloud. I think the really big trend that we're seeing now is the network itself is becoming much more cloudlike. And so operators are transitioning from traditional black box infrastructures towards cloudlike infrastructures, where you'll see the rise of brand-new kinds of network functions that really do lead to what some people are calling programmable network, the ability for applications to control the behaviour of the network through APIs.

And so I think that's a really exciting trend that's going to lead to a big wave of innovation. And of course leads to a whole set of challenges that we need to focus on in terms of how do we deliver these new kinds of network functions and make sure that the network remains as robust and reliable as it's always been? How do we ensure security around both data and the processes of workloads and things of that sort?

And all of these things I think have been, you could say, reasonably well addressed in the cloud world. A few years ago the debate had always been can horizontal systems ever be as reliable as vertically scaled systems? And in fact what you saw was horizontal systems became much more reliable than vertically scaled systems. So I think the same sort of philosophies now are starting to move into the network.

Casey Quillin

Okay. So getting back to security a little bit and the topic that we or Bob said is what's really of interest here - which flavour of cloud and where do we end up. Maybe if we go back to Hari and go down the panel. If each of you could talk a little bit about what you see as the security challenges specifically and maybe some remedies and that you are aware of, from your perspective, maybe the top two flavours of the cloud at this point.

Hari Makkala

Sure. From an enterprise perspective, I don't think it's possible for an enterprise to say we're only private cloud type only. I think for the next five years to whenever, whichever model we're going to settle, it's going to be a hybrid cloud requirement. And cost is going to be primary driver there. But I think we'll have to balance it with security.

From a security perspective, I think definitely no argument, especially the large security, large cloud outfits. And much better security than a single enterprise can ever afford because you have a lot more security professionals and investments that are happening in large-scale clouds. But then it's going to be what is it that you're willing to put on the cloud. And as a healthcare organisation, protecting personal health information becomes the number-one priority for us. So even if we wanted to take, can the consumers? And the customers that we support are willing for us to put the data in the cloud, especially given the cloud could – their data could be stored anywhere, right. It could be stored in other countries because we're mirroring information and data across continents. So there are a lot of regulations still putting fences around what information could be stored on the cloud and not.

Casey Quillin

Right. Just one question. So you had mentioned also at breakfast and then just moments ago about compliance not being enough. So what do you look at? What do most people start out with? And how does where they start with looking at securing affect where they are now and where they end up?

Hari Makkala

So there are four top reasons today. The number one is compliance. Number two is best practice. Third is financial cost of data breach. And the fourth is brand reputation. And years ago I worked in financial services, where this was the same pattern. These were number one through four. But financial services changed that. Now the top two are how to avoid financial cost or from the data breaches and then second is brand reputation.

So healthcare and retail organisations, you'll see the transition to that because compliance has been a longstanding driver for securing sensitive data. But you can't survive that way. I think the threat behaviours that we're seeing are a lot more advanced and they are very persistent. And I think the earlier panel discussed a lot

about what kind of sophistication that we're seeing. And honestly, compliance cannot – is not evolving fast enough to set the requirements for security.

So I expect, especially in healthcare and any industry, as to take the lead from a security perspective, if you're going to deal with personal identifiable information, PII, PCI or PHI, your strategy has to be security-driven. How are you going to protect from those hackers and not just the compliance requirements? And it's going to take years for compliance to ever create something that's more adaptable with threats, because threats are changing every few months. And they're changing very fast and becoming sophisticated.

Casey Quillin

Yes. It's really a moving target. Bob, so how do you look at, maybe from a network perspective, maybe add a little more colour on security and the two top flavours of cloud.

Bob Metcalfe

So wonder about this. So innovation and standardisation are, in some way of thinking, opposites. And you don't want to standardise too often. You don't want to standardise too soon. So here's all this talk about security, and I get a sense that security is not a solved problem yet. So when doing the OpenCloud Connect standards, it seems like we're going to be limited by security technology. We could make the mistake of standardising too soon in that area until we begin to have some solutions that we can then use as the basis of standards.

So that's a wondering about the pace of development of this standardised platform. Will we be limited because we don't quite yet know how to secure it? Would you agree we don't?

Hari Makkala

Absolutely. I think as the leading factor is always going to be innovation for customer experience, for any consumer market. But right behind that, there is no reason why security can't be an innovative factor as well. And I see that chasing right behind.

Bob Metcalfe

Having sold a lot of networks in my day, I have noticed over the years that customers, even when you have security products, customers don't often buy them or use them. So even if we had solutions maybe, what's that about? Why don't you buy our securitisations?

Hari Makkala

Very good question. See I think one – here is another fundamental thing that a lot of the enterprises are – you'll see them shifting is that tools will come and go. It's having the process, having more the capabilities that you want to have to defend yourself,

right. Like if you look at the regular warfare, you have areas that you have to be prepared on the sea, on the ground and on the air. Right? And it doesn't matter the technology and the type, air defence mechanisms have changed. That's how I think this approach to security will also change is that you need to have a strong process in place, but the tools are going to come and go.

Because if you look at the market with security tools, it's very unsettled. Just in end point detection and response tools, and we're evaluating right now, even in the [Gartner] support, there are like 19 tools. They're all competing because they're all going after it from different vantage perspectives. So we're having to deal with it by picking two or three to come up with that comprehensive solution.

So I think it's too early for the security solutions to settle. But you'll see enterprises, especially that are going towards hybrid cloud or private clouds or total clouds, trying to have that security spread.

Eric Hutchinson

Yes. It's really interesting because if you just go across the water to the security show this week, you'll see hundreds of people with different security solutions all competing and vying and saying how they're better than somebody else. Then you get the other guys saying none can do it. And the truth is that you get 10,000 new threats today and the firewall guys maybe have got 40% of them incorporated into their next release by the end of the week or two weeks and 80% a month later.

So enterprises find it really difficult to deal with because they rely on buying the firewall. I think the only way that the world will increase security levels is with the global threats database and enabling that distribution back to everybody through a cloud service. Ultimately that's where we've got to go. So again it comes down to data analytics, predictive analysis of traffic to identify threats before they've hit you. At the moment we find them, we write protections, we incorporate those protections and then we're starting to look at bad traffic and building protection for that. But you need to be more proactive.

So the cloud itself will become an enabler of enhancing security. From a commercial perspective, it's got to be that the cost of attack gets too expensive. So can is the classic warfare balance, is the cost of defence higher than the cost of attack and vice versa?

Casey Quillin

Right. The economics are on the side of the hacker, and they always have been. And that's the challenge, making it less effective economically for them to try to break in.

Eric Hutchinson

Yes. The only one that's outside that is state type of warfare because the cost element is not quite the same dynamic there.

Paul McNamara

Yes. But I very much agree with Bob's sentiment that we need to find a way to let innovation lead in this, in the field of security. The bad guys are innovating at a very, very rapid rate. And so the good guys need to be able to keep pace. And there is that paradox that if we lock down our approach too quickly, we could starve off the flow of capital to a lot of the innovative solutions.

And we're seeing there's a lot of really interesting things going on out there. Work on [links containers] with setting up perimeters that are policy-based is I think really interesting. There's a lot of people who are now looking at the blockchain as potentially a new way of thinking about security. So many of you may be familiar with Bitcoin, which is a cyber currency. It realise on this technology called the blockchain. And the basic idea is that with currency as an asset class, we're very, very careful when we transfer from one person to another and we have systems in place to make sure that that transfer happens in a very secure way.

With some of the cyber currencies, what they've said is can we create a way of doing that through a distributed consensus protocol rather than using banks and things like that. Well it turn out you can apply that same thinking to other classes of assets. It's not just currency. It could also be exchanges of data in the network could be thought of in the same way.

So there's a lot of really fundamental sort of innovation going on out there. And I think as we start to scale the network as we go to 50 billion connected devices, as all sorts of new classes of data moving around the network, we've really got to find a better security protocol, because today what we're doing is, I'd say, barely working, I think.

Eric Hutchinson

Yes. I agree. We see far too much validation testing to comply with standards or de facto standards in security, when the truth is that does nothing for you. It just ticks the boxes, makes everybody feel good. And so we're looking to generate much, much more realistic tests all the time. And that's really what the industry needs is keep that validation going. And the last thing we want to do from a security perspective is build the Maginot line, which is a huge amount of investment, and you just drive around.

Casey Quillin

And it just gets pushed somewhere else. Yes. I notice we're about five minutes, so we want to open up for questions you all might have. Are there other questions?

Unidentified Questioner

Okay. My question is more or less related to the acquisition of health data. If you go around here, many people are using these smart bands. They're using smart watches. Everybody is collecting a huge amount of personal data related to his behaviour, blood pressure, his weight, the heart beat. Even glucose measurements are already in it. But when I feel some disease, I have to go to the doctor. He starts from the

beginning, so they start their own investigations. Where at the same time if you have the right configuration in the cloud, the whole analysis is done and in fact the doctor gets a proposal, this guy has that and that disease and this is the way he should fix it.

To what extent does all this discussion about security and privacy block the next step in using the medical data that is generated and effectively available already? Do you understand the question or not?

Paul McNamara

So it's an interesting question. So you can imagine ways of using network analytics that could be interesting from an application standpoint. In other words, my application could consumer some network analytics that says, hey, this particular group of end users is having a really bad experience. Let's move the workload somewhere else or do something like that. And so you can envision all sorts of benefits. But then you also have to consider, well, as soon as we start exposing metadata to third party applications, have we made the privacy issues and order of magnitude worse and can the bad guys exploit that metadata in a way that individuals were not even contemplating?

So I think it's a very complex subject. I think we have to find the right way of approaching it. I'm not sure we're ready to just say let's expose all metadata to all commerce, because I think there's serious externalities that happen when you do that.

Hari Makkala

But if you look to the healthcare initiative from Apple and also the investigations on the [Castrona] Institute in Sweden, they see that there's a lot of advantages if you can process that data. And if you can reduce the cost of medical support, you can increase the average life of the inhabitants. You can make life much better. There must be a smart solution by making the data separate from the person who acquired it, something like that. It can't be that hard.

Eric Hutchinson

So at danger of moving to areas of philosophy, who owns your health data, who owns your body, a lot of the work that's done on population study is based upon aggregation of large amounts of health data, is immensely valuable. And the benefits that come from that open data analysis to all of us in the population probably outweigh some of the concerns we have about privacy. And locking it down to privacy around individuals can probably be dealt with and you could still get the benefits from the analysis of them metadata at the population level.

And as the population changes in age profile and the disease profiles, this type of study can reduce the cost of healthcare and enable preventative medicine to be much more effective so that we don't spend huge amounts of money trying to fix problems that probably are unfixable by the time you're trying to treat people. So I think there's a debate about the benefits outweighing the downside.

Hari Makkala

Yes. I agree. I think no doubt there are a lot of benefits for correlating information, doing big data analytics and all that when you capture that information. But how do you balance that with – and the concern is not just how do we keep the bad guys away. How could we make sure that the information, through big data analytics, is not misused? Could that impact individual's credit in the future or insurance or employment status? So I think the question that we need to ask ourselves is how much is that going – we're going to let influence the social engineering.

Casey Quillin

And that's a really big topic. We could probably spend an hour just on that. I think we have time for one more question.

Jean Baptiste Su – Forbes

Yes. Jean Baptiste Su with Forbes. So perhaps a question to you, Bob, but please, anyone can actually jump in. Bob, as a former investor and now a professor on innovation, have you seen that the cloud and the mobile revolution that we're seeing now has accelerated innovation or actually created some more junk and things like that? Or did it really accelerate true innovation, cloud and mobility, Bob?

Bob Metcalfe

Well there's a kind of snobbery in the investment area that social mobile cloud is a not real innovation. Like Facebook was a huge hit and now everyone's trying to do the next Facebook, and is that really true innovation? But that's snobbery, I think. I think the social mobile cloud explosion is exploring every nook and cranny of this platform that we have, this internet platform that we have. We're now exploring every nook and cranny. Eventually all the nooks and crannies will be explored and then we'll, as investors, we'll move on to the next fruitful platform. Hopefully the output of OCC will be such a platform that will open up a bunch of new nooks and crannies for innovators to explore.

Meanwhile, the National Academy of Engineering has 14 grand challenges, which are not getting the amount of attention that they should. Maybe that was the point you were trying to raise, how these 14 grand challenges, like solving energy and infectious diseases and cancer and so on. Maybe we should be putting more of our innovation and investment dollars into those instead. I think that will probably happen in time.

Casey Quillin

Thanks. I think we're at the end of our time. I wanted to thank the panel, not only for their depth of knowledge and expertise, but they've been very courteous, very helpful, made my job very easy this time. So thank you all very much. I appreciate it. And I thank you.

[End]