NetEvents

APAC Press & Service Provider VIP Summit

Draft

Innovation in the Cloud & the Importance of Security

Guest Speaker: Steve Chappell, Chief Operating Officer, Wedge Networks

Manek Dubash

Good morning and welcome back. And I hope you had a fabulous dinner last night. And yes here we are again, and lovely views and everything, and there's a nice breeze out there and, anyway, it's nice and cool in here.

So welcome back to the last full session of this event. This morning we're going to be talking about lifecycle service orchestration, data centre interconnects. We're going to be talking about metro aggregation using 100 gigabit. And we're going to be talking also about innovation in the Cloud and security.

But before we get to the meat of the matter I'd just like to mention that after this afternoon's session with -- where the meetings are between press and analysts, which will be held both downstairs and in here, if you come back after those at 3.40pm this afternoon you'll be able to pick up -- the press amongst you will be able to pick up USB sticks with all the presentations and so on. There will also be bribes for you to come back - you'll get coffee and free ice cream. So do come back.

Ok, without further ado then, I'm delighted to welcome Steve Chappell, who's the Chief Operating Officer of Wedge Networks, to talk about innovation in the Cloud and the importance of security - Steve Chappell.

Innovation in the Cloud and the Importance of Security

Steve Chappell - CEO, Wedge Networks

Steve Chappell

So I'm going to talk just a little bit to start the morning. We have some great sessions this morning and a lot of really good interesting topics today and it's centred around Cloud in the future and where it's going. And hopefully I set the stage for the day and get it going.

This is fairly short - just going to talk about a little bit of things. And I'm going to focus a little bit more on the security side of it. And when you talk about Cloud security it can be quite -- there's two sides to it. And so as I start off I'll make sure I present the side that I'm going to be more talking about.

There's talking about securing the Cloud and then there's talking about security within the Cloud and using the Cloud to provide security. I'm talking about the second one more than the first one. I'm not really going to be talking about how you secure the Cloud, but more how the Cloud can be part of [our] security approach.

So with the Cloud really taking off and really expanding around the world as it has it really gives us new opportunities to rethink the way we do security. But it's more than that. It's not just giving us new opportunities to rethink how we do security. It's almost forcing to have to rethink how we do security, because just the way the networks have changed the dynamics.

And then as you have innovations like NFV and SDN these new types of technologies really gives us possibilities to do security in a different way delivered from within the Cloud that is much more effective than the way we did it before. So it really opens up the door for what we can do in the future.

So this slide is pretty simple - it's how you look at the old connectivity paradigm. And as we talked yesterday -- and I know I got to talk to several of you yesterday and I'll get to talk to quite a few more today. I talked a lot about how the old paradigm has been around for a long time.

And unfortunately -- fortunately or unfortunately I've been around long enough that I remember when we first started selling our very first Ethernet networks in the 80s. And for a couple of decades when you think of when it started, up until where we are now, the network was pretty standard.

You had file servers. You had workstations. You had a network within your office. Your data was in your office it was used amongst your employees. You could put a firewall out there. You could control what you had.

Your users, most of your employees, were working on desktops or laptops. And as a security person or an IT person you had a fairly good feel that you're controlling your network. You had a good feel around your network and you could control it.

But there is a paradigm shift. And it's happened. It's not happening - it’s happened. There is no standard network any more for most any business. Your data is anywhere. It's coming, it's going, you store it off site, you share it amongst the different companies you work with, your customers. And also the types of devices is a big part of it.

You look at this Internet of things, this 18 billion Internet of things devices out there, and they all have Ethernet ports on them and they're all part of the network. And as your employees come to work every day they all have their personal devices and as soon as they walk in the office their personal device automatically connects to the WiFi of the office. It's just what we all do.

And if they leave the office they take that device to other parts of the world, like we are here. And as soon as we are here we hook into a WiFi network. And I'm sure you're the same as me. I've got my devices here.

I have company data coming and going to me here just the same as if I was in my office back home. So there is a huge shift of the way the network looks and because of that there is a big shift of how we have to secure the network.

The other big piece of it as we look at this is -- I've got to make sure I don't miss my (inaudible). We have a report from the MEF that shows that in the next three years 70% of all the Ethernet ports sold will be in the cloud. So that's a staggering figure.

That just shows that most of the data connectivity in the future is not in enterprise - it's in the cloud - and so the way we have to think of how do we secure those devices, how do we secure our data and all the things that go with it.

This is the shortcomings of what we call the existing solutions. We had the first generation. And over the years -- it's funny, as we sit here it's -- one decade ago, so in 2005, I was one of the founders of a company called Tipping Point. We had a bolt-on box. We had a box that we sold and it was very successful.

You'd buy this box, you'd put it in your network at the perimeter and it would keep all the bad stuff from coming in and tearing up your network. And at the same time there was a lot of other technologies. You would buy -- there was multiple devices you would buy.

You could buy -- you could almost buy a device [for] almost anything you wanted to do. And you would have all these devices in your network. You'd have some at the perimeter to block the outside. You'd have some of them at the core to protect your internal data. And you would buy all these things.

[Then came some] of the first cloud-based solutions started to come out which really set the groundwork and the path for the future that we have today. This is where we're now having traffic that was being secured [in some of the] security, the anti-malware, the anti-spam data loss prevention, some of these functions were actually being serviced by a cloud.

But a lot of these first-generation cloud security products the data would leave your network and go off to their cloud to do what they do and then it would come back in.

And so while it was a good step -- and it was a very good first step. It actually turned out to be quite successful as a first way of doing it. Your data was having to go off somewhere else, be taken care of and come back.

And as you look at the way the -- some of these solutions they really just can't take care of the securities we need in the future. They can't address all the problems. But as -- of all of us that have lived through this technology industry for a few decades this is the normal evolution of the way things go.

And in this Cloud security we've had our first generations of security products come out and they've proven successful. They've shown the way it needs to go and now we're into those second, third generation of products.

Our marketing department threw in -- they had to throw in some slide that shows how security is a big problem. Everybody has got these slides of their own. This is usually one you don't need to spend a whole lot of time on because nobody will argue with you that security breaches and security is a big problem in the world today. But you always have to throw one of these slides in there just to show it.

So this is the way we look at -- we need to change the way security happens. Now, if you look at this, over here was traditional. Over there you had your endpoints, you had your employees, you had your enterprise and you had all your applications - you had your firewalls, you had your IPSs, your IDSs, you had your -- all these types of products and you had them in your enterprise, as we've talked before, then your data.

After that it went out to your service provider cloud and our into the world. That's what it was. But now the way we're going to change and you'll see things are changing now is we're moving those services from the endpoint and from the enterprise into the service provider network or the cloud network.

Same functionality and the same feature sets and the same things that we had before, but instead of having them as a hardware platform installed in your data in your enterprise we're just moving it out. And it's now being serviced externally and it's being serviced out into the cloud so it's much more effective.

Because if you look at some of these things a few of the things that have happened that have really changed it a lot of it [is to] bring your own devices. You have your iPads and your smartphones [are] these devices. You really can't -- well, you can load -- there are products like McAfees and Trend Micros that you can load on those type of devices, but really nobody does it. They really kill the performance, they're just not really effective and it's really hard to implement on those kind of devices.

So we need to change the way -- when the data is coming out of these devices we can't protect it like we used to. We have to change it up here. So basically what we're talking about in this new paradigm is we're not worrying any more about protecting the endpoints or protecting the devices. We're now concentrating on protecting the data, just the data flow that's coming out of those endpoints and devices.

If we can control and protect that, if we can take care of all the malware, we can take care of the spam, we can take care of all these other basic security functions, not even the advanced security functions, just the basic security functions -- but don't worry about the endpoints any more, worry about just the data flow.

Because as most -- all businesses, as you can see from the slide, they have all these devices, they come and go during the day, they have free WiFi for their guests and you want to make sure that your guests aren't doing something illegal while they're sitting in your network during the day.

You want to make sure employees aren't playing World of Warcraft all day or are on Facebook all day, things like that. All those things can much more easily be controlled by having the services outside of your network, so all the data that comes in and out of your company we take care of those security solutions there.

So to enable this to happen there's a few things that are happening. And the reason we didn't have this three and four and five years ago, we're now getting to it today, because some new technologies had to be developed. The first two go hand in hand.

First off, you had to have high performance. If I'm now taking this data stream coming out of a business and go and do all these security services on that data stream I've got to have the capability of doing it very fast and very efficiently. I can't slow the data down. I can't introduce latency into my data stream, so it had to be high performance.

The second one ties right into it really and this really what we're talking about - NFV. It has to be elastic, an elastic orchestration of these services. And so what I mean by that is when you have a product running that secures all your data, as that data flow increases and there are spikes in it, you need to have your security product be able to expand and actually be able to grow and support those needs.

And then as the flow goes down have the -- you can have less resources and when it's all done in NFV so now we're virtualising all these security functions. And I'll step back a minute. NFV is becoming very popular.

It's actually helping to drive the industry. And it's network function virtualisation. You're taking network functions and virtualising them. Very standard and the carriers are driving that adoption and it's happening. It is absolutely happening.

What we're talking about here is taking security functions and doing the same thing. So it's network function virtualisation, but security services, that we're now virtualising and running as a network function.

Also at the bottom here you see it needs to be embedded as a software-defined function. It's not a hardware platform. It's not something that the service provider buys and bolts in somewhere. This is just a software function that has been defined. It can be modified. It can be changed as everything is needed as you go.

And then the bottom one that's also becoming more and more important is it has to be really, really good. It has to be better than the boxes you used to buy. We need to take this new technology and be able to go beyond what the endpoint protection used to be in the past. Whether you had the Trend Micros and McAfees on the desktop it needs to be better than that.

It needs to be better than the Tipping Points of the world that we're selling these IPS boxes. It needs to be better than what we had in the past to really perform. So these type of technologies are now coming out and there's many vendors. Of course, I work with Edge, but there's many vendors that -- we're just one of the ones that are leading this path and going through it.

Also I don't know if you noticed I was wanting to kick off this morning, set the stage, and you see on my slide, 114, so as you can tell I skipped a lot of the slides in our PowerPoint. Mark didn't let me have the whole morning here. But to wrap this part up -- I know Manek and I are going to talk a little bit more about this now.

The service provider is ideally positioned to offer these services. They're in the perfect position. And as we travel around the world and as I talk to a lot of service providers it's really starting to make sense for them because the one thing they do is they have that connectivity to old enterprises.

All the data coming from the enterprises is coming into their service provider they're buying their connectivity from. So that data is now leaving that enterprise, coming into that service provider. That is the perfect point for us to have this network function virtualisation for security installed. That's where these services can be more efficiently run.

Service providers can then have the best of breed of all the different security products, the best of breed of all these functions virtualised, running, updated, monitored for thousands or hundreds of thousands of their business customers' data flows coming in.

And the businessman now doesn't have to worry about endpoint devices, how many he has as they come, as they go, as new employees start or customers, they don't have to worry about any of that because they can trust that their data, as it's leaving the data centre and going into their service provider, is being cleaned, it's being secured.

When I showed we have 114 slides this was actually our CEO, Dr Zhang, who is the chair of the security for the OCC. He has a great example and part of it is because of his background where he grew up in China and then he's moved around the world. His example on this is water.

He said 100 years ago, 150 years ago in a lot of the world people would every day get their water and boil it - it was not clean. They had to boil their water and have it ready for their consumption. But in today's world most anywhere you go [in] most of the modern world you turn on the tap and clean water comes out.

The company behind it has already perfected the water. They've already taken all the bad things out of it, they've already cleaned it and you're delivered clean water just by turning on the tap. And that's his analogy for this data. We should be able to do the same for the service providers.

When you have data and it's provided from your service provider they're providing you clean data, both coming and going. The service provider can clean it for you. They can make sure that what you're delivered is ready-to-go and clean data.

So the service provider is in that perfect spot. They're already implementing the SDN and NFV-type technologies. They already have this unique reach because they already have all the subscribers. They already have all these businesses connecting to them. And it also makes the cost for enterprise security and complexity much less for the business customers.

And for the last probably about two years I've been travelling around the world giving this story, talking to a lot of service providers, and it's really resonating. And especially -- and also talking to the enterprise customers [and] the businesses they see this as the future. They see where it's going.

And so I think that's the wrap up of this, but then I think we've got -- we're going to -- hopefully I didn't answer the questions [you're already] going to ask. I'm trying to remember what it was you're going to ask. Are we going to sit down up here? Are we sitting down up here so we can look official?

Audience Q&A

Manek Dubash

Thanks Steve.

So the first question I had -- probably don't need a mike in a room this small, do I?

So the first question I have is, this all sounds quite good, but obviously the modern enterprise doesn't all live in the cloud. It's got private cloud, it's got bits in the public cloud and we're moving towards a hybrid enterprise.

So how does that work? Because you're still in that situation then, aren't you, where you've got data going out from your private cloud up to the service provider and back down again, which is what you don't want to do.

Steve Chappell

So basically as the new style, the new paradigm for security is implemented it is going to be distributed somewhat throughout the different aspects and different security functions will be happening at different places.

You can take your very basic. Let's just say anti-malware, anti-spam, just making sure the hackers aren't getting in. That one is fairly easy to implement in multiple spots, but mainly at the core cloud. some of your more advanced functionality, your data loss prevention and some of those web content filtering things that are more specific for your business, well, then those could be more in your private cloud.

So the differentiator between a private cloud and a public cloud is not that much when your doing NFV-type functionality because it is just software. So it's very easy to spin up a resource and to start a service in a private cloud and in a public cloud and have them inter-op with each other very well.

Manek Dubash

So inter-operability implies a form of standards. What kind of standards are we talking about that are implemented here?

Steve Chappell

Well, the fortunate thing for this is we're finding we don't have to come up with very -- really new standards. It is still just Ethernet data. We're really taking the same functionality that we were doing in hardware and we were doing at the enterprise and we're just taking that a virtualising it and moving out to the private clouds or moving it out to the private clouds. And so it didn't really have to create a whole new set of standards because we're really using the same standards just a different way of delivering them.

Manek Dubash

So, all the same, I'm just thinking about the security provider model. How can I be sure, or as sure as I ever can be, that my data is being protected when it goes out into the security provider's network? What's the most reassuring thing you could say to me?

Steve Chappell

This is one of those things that will change over time as it gets adopted, because if you think about it -- and everybody in this room is in this industry and everybody here is involved in it and you see it and you've seen how it transforms.

It wasn't that long ago that it was very nervous for an enterprise to let their data leave and go to Cloud. They were like "I don't know if I dare store my data out in the Cloud". And that doesn't seem to be a concern any more. It's very common that the data is stored out in the Cloud.

We're going to show business enterprise customers this and say "you know what, I now realise that you could do -- my partner, Mr Service Provider, you can do this better than I can, you can control it better than I can and we don't have to overcome that hurdle of nervousness about the cloud because it was already overcome with other things".

Manek Dubash

Well, I don't know, I'm going to challenge you on that because there's a lot of parts of the world where people do care where their data is, particularly Germany is the obvious example, where you think, well, there's legislation and lots of other parts of the EU.

Steve Chappell

Yes. So what we're finding is -- you're exactly right. There are places -- there are countries where as an enterprise your data cannot leave your country to be stored or things like that. So in those cases it'll be -- the first steps of implementation on this will be in the private cloud.

So the enterprises instead of buying the hardware that they bought in the past they will just create their own NFV security services within their own network. And so the data is not really leaving their network.

Now, there is also -- and this is much deeper and much longer and I'm sure there's other experts here in the room know more than I. But also the service providers in those parts of the world they know the regulations and so they have to abide by, okay, if you let me have your data and I'm still within your country I have to be able to guarantee and comply that that data does not leave the country. And that's their responsibility also.

Manek Dubash

But then you're stuck in a situation where you're having to manage this stuff and actually what you wanted to do was to hand it over to [a] service provider, so you're getting the worst of both worlds.

Steve Chappell

Well, this is the sales job the service provider has to do. They really have to convince the customers. This is if the service providers want to expand their business, because there's going to be two options. The businessman can say "I'm just going to make my own private cloud, I'm going to install it there, I'll do it myself and these products are available to me just as they are available to the service provider and I'm happy with that".

It's the service provider's job to convince them, say, "no, let me do it, I can comply with all the regulations, I can guarantee you this satisfaction and that you're compatible with everything". And so they do have to sell that part of it.

Manek Dubash

So [Uday] I think a microphone is on its way to you. Sorry, did you have a question? Hold on, [got a] microphone coming to you.

Dr. Uday Lal Pai, India Telecom News

I'm Uday, India Telecom News. My question is why would a service provider invest extra funds into that especially in a situation when they're trying to cut the cost of customers and clients?

Steve Chappell

Well, what we're seeing -- and that is good because there is definitely always this capital expense how much is it going to cost as a service provider to install and to build up this whole infrastructure before I can start monetizing and getting money out of it.

So a lot of the solutions like the solution that we're providing and there's some others where we partner with the service providers, we partner within the fact that we actually will install these resources and the software without charging the service provider. We will then share -- as the revenue comes in from the customers we'll share on that revenue stream, but there's not a big upfront expense.

But also the key to this, the reason this couldn't have happened, say, even five years ago or more is you have to have the infrastructure within a service provider with VMware images. Nowadays -- today most service providers have racks and racks and racks of VMware boxes ready to go.

Now that that's already in place it's very easy for us to install our software, just say give us this image, we'll install it, you're up and running, now we'll share the revenue on that side. Because that infrastructure had to be in place before we could actually offer these services. But now it is in place. And so it's a revenue-generation model for the service providers.

Dr. Uday Lal Pai, India Telecom News

(Inaudible - microphone inaccessible).

Steve Chappell

Yes and they -- and for the most part I think the future is going to be is -- that was the trade off in the past. If you wanted to buy IPS you had to invest in millions of dollars of hardware to build this infrastructure. Then you could go to your customers and say I have this service I can offer you.

But with software-defined networking, with NFV networking it's all virtualised we can do much less -- more lower cost installation, or almost zero cost installation to some degree and then just start sharing the revenue as it comes in.

Manek Dubash

Convinced? Anyone, questions?

Are there any particular issues associated with this model that you're describing right here geographically, right here in Asia, AsiaPac?

Steve Chappell

You know, it is definitely different around the world. And one of the things that is different around the world -- and [as] many people in the room probably even have more intimate knowledge than I would of it. The amount of malware and spam that is being transmitted in just general daily use is much higher in some parts of the world than it is in other parts of the world.

And actually in this part of the world in some countries we've seen as high as 70% to 80% of the actual data is malware and spam that's just being transmitted. So there's a much higher need for it in certain countries than there are -- in certain parts of the world than there are in other parts of the world. And it's also much more -- it's more cost effective, as we talked a little bit yesterday.

If I'm a service provider and I'm in a certain geographic area and I have a few million customers and their mobile devices and they're sending data [and] they're using me as their data provider, I'm now transporting -- a large percent of the data I'm transporting throughout my network is malware and spam, because that's what is coming to the customers.

With this new technology we can take it and at the edge, as this data comes into the service provider, we can strip out the malware and spam, just throw it out. Now what they have to transport throughout their networks is clean data. And that right there can save huge amounts of just backbone usage and data usage. And we didn't change the data. All we did was take care -- get the bad stuff out as it hit the service provider.

We actually have for our company, and there's others like us -- we actually -- some of the involving markets -- and I can say that in this part of the world we have deals going in India, we have deals in Thailand, we're working on one in the Philippines right now and we are working on one here in Singapore, where it's very attractive the service providers in these markets to just clean the data before it even hits their backbone. It just frees up a lot of space.

Manek Dubash

So you're finding this area has got a big take up then?

Steve Chappell

It does. And it's also more centralised. I think we talked in one of the meetings yesterday. In a lot of the emerging countries there are some dominant service providers that play the main role in a lot of their countries. And you might have two or three or four dominant ones that handle it.

We got a report we're working on with one of our big companies in North America. And in the United States there is now a little over 20,000 services providers in the United States. Because of the way the market grew there are the big ones that everybody knows, the AT&Ts, the Verizons and all those guys, but there are over 20,000, meaning, there are so many little tiny, small service providers.

It's a harder market to get into all those in the United States as opposed to some of these other countries where there is only two or three main service providers that handle most of the data for their country. And so it's much easier to introduce this technology at that level.

Manek Dubash

And a lot of those service providers are associated in some way or have a relationship with governments, so how does that affect things?

Steve Chappell

It can affect things in some ways very positively because the governments will put restrictions on -- as we talked earlier, on data, where it can come and go. The governments can also in some markets -- and especially you'll find this more in emerging markets, where the government will help to actually fund these new technologies.

The government wants their service providers to be able to provide, as we call it, clean data. It's a [very big] benefit to their country for the data to be coming through clean. So in a lot of the emerging markets the government actually is behind it and will help give grants and funds to the service provider partners to them to pay for this installation and get it going.

Manek Dubash

OK. Any further questions? Yes, one at the back there, Gint.

Gint Atkinson, KVH

It seems like with -- the mobile network seems like a very attractive area to use this as an NFV function, especially given that the IMS core is at many providers moving into the cloud or capable to be moved into the cloud, so a really convenient place to put it right there or even further out at the edge of the backhaul network.

As you pointed out, things are a bit different in Asia, and when we factor in China and every place in APAC there is a disproportionate amount of mobile access into the Internet and gaming. So it really seems like mobile could be a very good application and not only protecting the users' experience, whether they're the content providers or game providers and the ultimate mobile users. But it seems like there's a lot of optimisations potentially in the backhaul network by cleaning out all of this dirty traffic.

Steve Chappell

Absolutely. It's interesting that the emerging markets you said -- Asia is a very good example. The infrastructure got built in a short period of time [or in] more advanced markets. In Europe maybe or in North America they've been building their infrastructure for decades.

In a lot of other countries in Asia, they just -- within the last decade they're like, we have to catch up and build something. So they didn't have the time to build it out with all these thoughts in mind. So they have more opportunity, or more holes you could almost say, that this fits perfectly in.

There's really two really big markets. As you just mentioned, it's the service providers, the backhaul, the interconnectivity between themselves and passing clean data amongst that community. The other one is -- that's really where the take up is going to be – is the small businessman.

Large enterprises are still a little hesitant. They have IT people, they have security people, they have people whose job is to secure their network and they can justify their job by saying I'm buying this equipment and I'm monitoring this technology and I'm protecting our network [and then] report every day.

It's the millions and millions of small business people that don't have that expertise. They're the ones that are perfect to just turn it over to their service provider and say "you know what, I'm paying you $100 a month for my pipe. I'd be glad to pay you an extra $50 dollars a month if you'll clean it for me, because I just don't know how. It's not my expertise. I don't have the staff. I don't have the people". That's where we're seeing the take up.

There's also a new trend. And I know this is always a little risky. Make sure my PR people back there -- they get mad at me when I say certain things. Because this is new data that we're just now getting, so it's not data that I can say, ok, here's how you can publish this, here's the source, here is where it is. This is data we're seeing as we're doing these installations.

But I see this is literally within the last -- this year, within the last three or four months, new problems are starting to arise within service provider networks that they didn't really think of ahead of time. And it's social media.

Social media is clean data. It's not that it's dirty data - it's clean. But in some networks we're now finding that over 60% of the traffic is social media. And it's now actually consuming their network. It's the business traffic that was traditionally what they were passing. And the funny thing is that it's not people sitting at home doing social media - it's people at work. How many people in their office all day have Facebook up and running? Or they have their personal device --

Manek Dubash

Everybody in marketing.

Steve Chappell

Yes, everybody in marketing. They have their personal device sitting at their desk always on Facebook or Twitter or something not realising that they're using the company's network and they're using that service provider's network to pass that data. Well, now the service providers are finding upwards of 60% of the data is social media and it's growing faster than they projected the growth of the data needs.

And so now they're starting to come to solutions. This is one that we can help with - there's others. So we can say, ok, at very, very high speeds we can see that data coming in and we can take all the social media data and segment it out. We can put it on its own path where you can control how much of your network can actually be used by Facebook.

And these are just new experiments with it. Because now they're having to determine, ok, if we take Facebook and put it on its own segment and we control it it's going to slow it down. How much can we slow it down without the customers noticing or complaining that we've slowed it down?

And so these are things that we're actually experimenting with, a few installations around the world. And that's another one, because I brought that up, because we're in Asia. It's countries -- it's developing countries that their population is using social media more than North America or the European countries.

Manek Dubash

Although, of course, they would argue there's a legitimate business use, I guess, in many cases.

Steve Chappell

Yes, absolutely.

Manek Dubash

Like in marketing departments, for example.

Steve Chappell

Yes.

Anthony Caruana - CSO Australia

Anthony Caruana, CSO Australia. Security is about trust ultimately. You've got to believe in your providers and so forth. So when you talk to your global customers, particularly with service providers, ultimately you've got to end up trusting that service provider to do the right thing.

Are we hearing service providers tell their customers we're using Wedge and using that as a selling point for that particular service provider? So, for example, if I'm a large multi-national or large company in Australia and I want to go and choose a telco to use for my mobile network, and possibly for my office network, and there's probably three or four I can go and pick from, are they actually saying "we're filtering all the traffic - we're using Wedge"? Are they using that as a positive selling point?

Steve Chappell

People are going to think that I paid you to ask that question.

Anthony Caruana

Yes, and I'm waiting.

Steve Chappell

So Wedge is our example and there's a couple of others. Because Wedge is actually one of the very cutting edge -- we're one of the very leaders in this, but there's others who are following along.

So what we're doing at a company like Wedge is we provide the capability. We have an engine that can be loaded in the service provider that can take huge amounts of data at extremely high speeds and take policy actions upon that data.

But you're exactly right. People would say well, I've never heard of Wedge. There's other companies out there. And I can name Trend Micro, McAfee, Kaspersky, Bit Offender. Everybody's heard of them. They're industry standards. Everybody trusts them. And these companies have an army of people all day that just sit there and look for threats and write filters.

So companies like Wedge we partnered with them. So all Wedge is doing is providing this high-speed platform that's virtualised that McAfee can then run on top of. So in most of the cases I can give one example, because it is one of our customers that has been running now for over a year is Bell Canada.

Bell Canada chose McAfee.

So when Bell Canada -- when a customer asks them how good is the security Bell Canada says it's McAfee, it's McAfee's latest generation of security signatures that we are actually using. Wedge is actually just the platform that allows it to analyse the data very fast and compare it against McAfee's database and take the actions that McAfee is associated with.

So you're going to find some very big -- we have some very big installations around the world. And to be honest in most of them if you said I understand you have a Wedge installation a lot of people would say, no, I haven't heard of Wedge. We have a McAfee installation or we have a Bit Defender installation when it actually was Wedge that sold it and installed it.

Manek Dubash

So you're not doing anything like Tipping Point used to do with its own analytics --

Steve Chappell

Right, what we really felt the need of for the future is we didn't need another company doing security analytics. There's companies that are really, really good at that. There's companies [that have] invested decades of manpower and engineering talent and intellectual property [of] finding these things. What Wedge -- but the downfall that they had was they couldn't do it at high speeds. They could not install it in a service provider and do multiple gigabit traffic flow at wire speed.

We provide that underpinning that's virtualised and it's an NFV application that we then just partner with those security experts. And our company in particular - and there's others like us - we now have I think nine partnerships and we're growing it.

So you're going to see as these security functions increase and there's more and more things we offer it's going to be more and more of standard industry-known companies that we've partnered with that we've just virtualised their functionality and run it on our platform.

Manek Dubash

So you're effectively taking advantage of Moore's Law, I guess, ultimately?

Steve Chappell

Yes. In some degree, yes. At Wedge our product is called -- real creative. It's called Wedge OS, Wedge Operating System. And that's the way we want to treat it. We're just the operating system. We're not the applications that are running on it. And we'll use best-of-breed applications throughout that.

Manek Dubash

Ok, good. I think we need to move on unless there's any more questions. No, OK. Well, thank you very much, Steve Chappell.

Steve Chappell

Thank you.

[End]