# The Cloud Computing News India

News And Info On Cloud Computing And Virtualization

Innovation in the Cloud & the Importance of Security

08/06/15

June 8, 2015
By admin

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 weare 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.

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 youwould 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.

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 beingserviced 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 alreadyhave 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.

**By**
**Steve Chappell, Chief Operating Officer, Wedge Networks**