NetEvents

EMEA IT Spotlight

FINAL

Keynote Presentation by

Joe Baguley, CTO and Vice President, EMEA, VMware

Yeah, so my name's Joe, I'm the CTO for VMware and EMEA. I just want to sort of tell you what that involves and what that is before we go anywhere so you understand what it is. Because some companies have 1001 CTOs it appears now and the title CTO seems to be confusing people. So I'm the CTO for a software company, so 50% of my time is chief talking officer, which is this right now, and the other 50% of my time is chief technology officer. We operate now at VMware an office of the CTO which is about 200 I think in direct line and then several hundred outside that that sits on top of now an R&D organisation that's in excess of 9000 people at VMware. VMware's become quite big.

I joined eight years ago, some of you remember me back then and even from before, and we've grown quite dramatically in that time. When I joined we were about 6000 people, we're now 24,000 people. We've gone from a couple of billion dollars to over $10 billion worth of revenue and now a market cap that puts us in the big leagues of over $80 billion. So it's an interesting space to be. The other thing is at the office of the CTO we are, at VMware, famous for innovation apparently. We keep getting voted in the top four or five most innovative companies in the world, which is quite a thing to bear as one of the four CTOs at VMware. We have a global CTO, Ray, and then three of us, one per region.

So what I wanted to share with you today was a little insight into what we're seeing going on in the marketplace with regards to application architectures and infrastructure. Then talk a little bit about security and touch on some of the stuff and some of the topics that actually we put together for Pat to talk about at RSA recently as well. So I'll take you through some of those and then we'll get into a Q&A session. So VMware's vision, very simply, has been for five or six years the same and will continue to be this until, whoever knows, which is essentially we would like our customers to be able to deliver any application from any cloud to any device.

The any cloud story has been developing quite strongly. Some of you may have noticed recently we announced with Microsoft VMware and Azure. So now there's pretty much every cloud in the world you can now run a VMware workload on and essentially achieve what we've been aiming at, which is a globally consistent operating system and a globally consistent operating model for our customers. Enabling them to have a choice between different clouds, and then obviously the ability to deliver different applications. There's a whole bunch of stuff that are about [unclear] and other things I'm not going to talk about today.

But that's not cool anymore, apparently, because if you go to any of the really cool, trendy conferences where people with much better beards and much tighter jeans than me, and much younger than me, it's all about PaaS and like serverless, right dude, isn't it? That's the thing, yeah. If you're not talking about PaaS and serverless then you're not cool apparently. Well this is where the first word in my title comes in. Now normally when I do this in different countries I translate that word, but I found out that actually it's a word that's pretty much the same in most European languages and that's chromatography.

So chromatography, some of you will remember from chemistry, if you did chemistry at school, hopefully, right? Chromatography was where you got that little liquid and you put it on the magic paper and then over a period of time that liquid split itself out into all the pretty colours or all the component parts. That's what's happening with applications and I don't think people have realised. What people think is that we re-platform stuff, that's what we've trained as an industry to do, re-platform, right?

You start off with something on a mainframe, we re-platform it to the mini-computer, to X86 and then now because we've gone through mini-computers and X86 and now cloud's the next thing. Obviously the thing to do is to re-platform everything to cloud, right? Isn't that correct? Well, unless you're government in which case you've left everything on the mainframe and then just added [accretably] other platforms to it. It's not. What's actually happening is you're not going to end up putting everything into one of these boxes.

Repeatedly I go to customers where I see them say okay, we're going to put everything in PaaS, we're going to PaaS, we're all in on PaaS, we're going to re-platform all our applications to PaaS. No, you're not, and you're not going to put everything in IaaS either, and not everything's going to be SaaS either because there's trade-offs in this stack. The higher up the stack you go the faster it is to adopt but the more sticky it is, sticky's a polite marketing word for lock-in, okay?

But essentially if you extrapolate this as a scientist to extremes if we had as one of our larger customers 3000 applications and we did those all as SaaS that might be great. Until you have to do something regarding compliance or data location or GDPR or whatever, or back-up or DR or you name it across 3000 different SaaS vendors. Or, you could go to the other extreme and run everything on the same operating system on the same box, that doesn't work either. There's a blended mix.

Just to make it a little more complicated as an industry we've added extra layers to this so now it's not just SaaS, PaaS and IaaS it's also CaaS and FaaS just to make it fun. So now you've got Infrastructure as a Service, rent a whole virtual machine, Containers as a Service, what you rent a whole virtual machine? How extravagant, I just rent parts of one. Then you've got PaaS, which is err, you dirty your hands with containers, I just turn up with an application and let the platform worry about the containers. To FaaS, which is err, you run a whole program, how extravagant, I just run a part of a program when I need to. To SaaS, which is err, you write programs? That's disgusting, I just buy them.

So when I go and talk to people now and I talk to CIOs the realisation and the dawning is that what they're not going to do is get all of their applications and put them into one of these. What they're realising is they're going to have to have a strategy for every single one of these boxes going forwards, and it's not just five boxes, folks, it's more than that, because it's 10 boxes. Because you're going to have to have answers for all of these, both on and off premises. So now it's not just one, it's 10 different destinations. What's fun is you don't take one of your applications and put it into one of these boxes. You take one of your applications and smear it across these boxes and then you take another application and smear that across the boxes and so on and so forth.

So if I give you an idea of a normal application that we're working on and deploying with our customers right now, large German car manufacturer, which is something you won't be able to say in 10 years, but that's fun. What they're doing is they are using Functions as a Service on premises with some specific OEM gateways, essentially [ZP] to IP gateways, that sit there and read stock levels, where a particular car is in the process, how many tyres they've got, et cetera, at a periodic basis.

Now obviously you don't need to monitor how many tyres you've got in a factory 30 times a second, every half an hour's fine, even every hour. But other bits, where is the car in the process, yes I need to monitor that three times a second because it's moving. So they use Functions as a Service there to periodically run different bits of code to then write some data down to an on premises SQL Server. Two boxes, stay with me.

They then have some really cool funky stuff they've written in containers, because that's the cool way to do it nowadays, guys, that does what we in the old school call ETL. Which is pull data out of that database, process it and then pushes it out to Amazon S3 which is IaaS - so that's four boxes now, folks. Where they then have Platform as a Service running in Google because they're using Cloud Foundry in Google to look at that S3 database and then build dashboards and real time stuff for management. Six boxes now.

What's great is because they've got a subset of data of what's going on in their factory in their production process in S3 now, sat publicly, they can sub-permission that. So their suppliers can now see parts of that so they can understand to do a bit more predictive in time analysis of how they're going to ship stuff into the factory. So that's six and a half boxes. That's a normal app. That's a normal app for our customers.

Now if I'd gone back 10 years and asked someone to do that they would have looked at the nasty box they had sitting in the corner that was running SAP or whatever, or

WebLogic or DB2 and gone, you're kidding me, we can't do any of that, that's impossible. Now that's normal.

Now what I want you to understand and think about is does a large perimeter firewall for their data centre make any sense at all in this model? No. So when we look at where we're going with applications, how the architecture is becoming, chromatography, the reason why I use it is because that's exactly what's happening. What used to be a big lump on a server in a data centre behind a firewall is now being smeared vertically in the stack, bits of it go to the best place for execution, FaaS, CaaS, PaaS or IaaS, et cetera. Then it's being smeared horizontally in the infrastructure, all the way out to end points, to mobile phones, to the hands of the users.

Then worse than that we now have the wonderful phenomenon of citizen developers, which is the new shadow IT, by the way. A citizen developer is someone in your management team or sales team or whoever who is now getting the data and then has realised there's some other cool thing they can get with some app on their phone that integrates them with some other piece of data somewhere else on the internet that you have no idea what it is. They then somehow link it together with an API and now they're pulling your data into someone else's cloud and giving them some really cool funky dashboard and suddenly stuff's way beyond anything you've got control over. That used to be done on Excel spreadsheets, which people kind of tried to control with locking down laptops and stuff, but now we've gone way beyond that too.

So thinking about security changes fundamentally as we go forward and there is the famous saying the network is the computer, if you remember that from Sun days. Well now we're into the application is a network and it's been said a million times by a million people but it's no more true now than ever before. It really, really is now a challenge for our customers to understand that pretty much everything they do is not about that server in a data centre. So it's why for the last four, five years at VMware we've been working on edge technologies distributed, integrated software defined networks, software defined storage. Essentially building a distributable platform that will run anywhere.

So now for our customers I can provide them with a software defined data centre - here comes the marketing slide, just warning people. I will as we do, that's not the only one - we have been building what I call an operating system for data centres, which is now an operating system for clouds, which is something that gives you globally consistent operations at every point in this chain. So whether you're doing it in a public cloud such as AWS or IBM or VMware or VMware Cloud on AWS or Azure it's exactly the same operations model, the same security model, the same network with NSX that you're doing at the edge, that you're doing it in your core data centres.

So whether you're building new style applications, old style applications, cloud-native applications, twelve-factor applications, microservices, it doesn't really matter. The platform that it sits on is a consistent infrastructure.

So now - I'll give you the perfect example. We deal with retailers a lot, a lot of our edge work actually has been driven by two main, I suppose there's two main industries have been the early drivers of edge. Military and retail. So military want to push more and more technology to the edge, retail have realised that they need to do more and more in their stores. You can add on to that telcos pushing technology out through the network, et cetera, which has really come as a much later phase and a whole bunch of other things. But really they drove it for me.

Retail was a great one, I'm not going to talk about military apart from we do it for submarines and helicopters and things. But the retail one was great because with retail the people that run branch infrastructure usually are nothing to do with the IT department, which is part of the biggest problem, okay?

If you go to an average retailer today and go and stand and look at the store infrastructure, I'd hate to call it the server room because it isn't, it's a [22U9U] whatever it is, rack stuffed under some manager's desk at the back. In there there's a massive old Cisco router that someone's paying thousands of pounds a month to maintain probably. There's kit with Compaq written on it, to give you an idea of how old it is. There's a particular box there which has a flashing light on it and a machine that goes ping that runs their point of sale system that no one knows what it does but we just have to keep it and look after it.

So when you go to that team that manages that infrastructure, as one of our retailers did, it was brilliant, they said yeah, what we're doing is we're rolling out a new application and we want to put three containers in every store. No word of a lie the guy from the store team said, what size are the boxes? Thinking they meant plastic containers, all right, and I'm not making this up. Because that's how detached they were from, not reality but from where and how things were being built.

What I'm providing, what we're looking at now, is they will drop into that store instead a hyper-converged piece of infrastructure which may be very small, it might be two in 200ths, [supermicro read] 200ths with a Raspberry Pi stuck on top of it for the SAN witness. Not a lot of money. In there will be the ability to run VMs, to run desktops for the management, to run containers. Also there'll be a virtualised SD1 Endpoint, so we don't worry about that either, it's one self-contained box. These things already exist, we're delivering them for a lot of people.

But what that means is actually it's not about infrastructure, it's about applications. So as an application developer I can now sit at the top and go right, I'd like to develop my application. I'm going to have some VMs in this blueprint that are deployed over here in this cloud, I'm going to have some access to some data services over there in that cloud, I'm going to put two VMs in every single one of our data centres and we're going to have five containers spun up in every store. API, click, next, next, go, done. That's the point.

So when we look at consistent infrastructure and ultimately consistent operations what you're aiming for is a consistent developer experience. So really if you get the bottom line of where we're at at VMware right now it is providing that globally consistent infrastructure that then provides a globally consistent operations model that then provides a consistent developer experience. But at the same time if we're developing applications differently, then security becomes very different very fast too. As I alluded to before the way we think about security has to change, and it has to change dramatically.

So what's wrong with security? Well, the first thing that's wrong with security is this hyper-focus on security threats. We seem to be absolutely focused on chasing down threats. We organise everything we do as an industry into two major buckets, right? So either reactive, this is all about firefighting, anti-malware, host intrusion prevention, endpoint detection and response, et cetera. Then there's proactive, which is fire prevention, hardening, patching, segmentation, app control, encryption, two-factor, all those kind of things that we should be doing.

If you look at the focus in budget, response, effort, time in most security organisations it kind of looks like this. The bulk of our investment is - and this is also in time and innovation - is predominantly focused on the reactive. We're hyper-focused, we chase threats. We are underinvested in preventative, this is for most organisations and as an industry, and even from an innovation standpoint it's like we've been standing still for the last decade. Patching's patching, process whitelisting, encryption, this hasn't experienced a wave of innovation in the last 10 years, it's just sort of best practice and people and process, it's not actually moved on.

80% of enterprise IT's investment in security goes into reactive, 72% of current venture capital investment in security start-ups is in reactive security model stuff. However, what has the biggest impact on reducing risk is to flip it, as I think you all probably realise and I don't need to tell you as we go through this model. Dollar for dollar we have a far greater impact when reducing risk with preventative measures than we do with reactive ones. I think everyone knows that, whether it's medicine, whether it's anything.

In fact we're not the only ones saying so. It's not often I stand up and quote Gartner but today I'm going to. When you look at essentially the Gartner framework for protecting workloads they stack ranked all the controls you could apply to a protected workload in order of how much risk it addresses. The items that address the most risk? All preventative. As we know, an ounce of prevention is worth a pound of cure. This is exactly where we're underinvested.

However, all this stuff that claims to be application aware typically isn't. You come from a security industry that thinks application aware is oh, we do deep packet inspection. That's not application aware, that's I can look at a header. I don't know what that packet's doing or where it's going, okay. You would be hard pressed to find, at a security show you'd be hard pressed to find a security product on the show floor that doesn't claim to be application aware.

You see, it doesn't translate to what actually composes this application. If you think about what I just said, the previous piece, application awareness is about how an application is composed, how it interacts with the infrastructure. Its typology, its intended behaviour. That's what's needed, not just protocol analysers on a network link.

So on our perimeters at the moment we dissect traffic going to the internet to gain some kind of application context, but that's not sufficient to solve the problem inside our environment. This is like having a city and saying you're going to prevent fraud by inspecting people as they walk down the street on certain checkpoints. Okay, it's not going to happen. It might've happened in medieval times when we had walls around our city and everybody who came in and out of the city we could check. But now our society doesn't work like that.

So we see acts of security theatre in the physical world all the time that I know all of you laugh at as we go through various bits of our journeys. But how much security theatre do you see in IT? How much times do you think people are missing the forest for the trees by looking at this? Understanding an application means I have to see the whole thing, not just that small part of it.

The other thing here is your most important security product won't be a security product. So if you go and ask any large enterprise how many server vendors they have they'll tell you two, right? Maybe three. Why two? To keep them each honest, I use HP and Dell. How many networking vendors do you have? Well, we're mainly Cisco but we've got a bit of Palo Alto or whatever coming in just to keep them honest. How many security vendors do you have? Well, on average about 100, usually more like 150 or something. Is that right? I mean look at it, this is the security NASCAR slide as it stands right now for our industry. It's so small that I can't read it standing here, so I don't know how any of you guys are coping but you can have a look later on when [we send the deck out].

These are the security products we use to protect our critical applications and data. The big problem isn't that there are too many products to choose from, no I've not got a problem with that. It's that there's too many products to manage and reconcile. The average organisation uses between 50 to 100 of these products, that's 100 products to deploy and manage, that's 100 different policies and policy boundaries to reconcile, and policy management is one of the biggest problems when it comes to security. The security of applications and data are hurt far more by misconfiguration and misalignment of 100 different applications than by something that we didn't do. It's complexity that kills us and it's complexity that is the weakness for our organisations.

But what if solving some of these problems didn't involve adding more products? More agents, more appliances? What if it leveraged what we already own? What if it opened the opportunity to get rid of a tonne of these products? This brings us to, really, the greatest security opportunity before us which is to leverage cloud and virtual infrastructure as an industry rather than simply securing cloud and virtual infrastructure.

We marvel as an industry about how the cloud, both private and public, has given us unique properties like elasticity, automobility, simplicity. We've used these properties to change how we build, deliver and manage our applications as you saw me talk about earlier. But it's time to start looking at the capabilities of the platform for security as well. What we're doing is we're doing everything in a new sexy way around software defined data centres, but what we're doing is we're applying old security principles and old security rules to that model. If I see another security vendor coming out trying to install agents in VMs I think I'm going to kill myself, right? It's not the way to do things, okay?

What we can do here is we can give visibility and control without more agents. No more appliances and without bolt on controls. So our focus at VMware has been on leveraging the virtual infrastructure to dramatically reduce the attack surface, and by doing so use our position to provide you with a clear understanding of the applications running on top of us. It's all about its intent, and to lock it down to ensure good rather than chase bad to make security intrinsic rather than bolt on. That's more than embedding just our old controls into a switch, that would be simply integrated security.

What we're doing, integrated security makes security distributed service within the platform, it rethinks the model of leveraging the power of the cloud to secure the cloud. If the law of gravity no longer applies don't define yourself by it. We've changed the rules with cloud, we've changed the rules with virtualised infrastructure, we've changed the rules with virtualised networking, we've changed the rules with virtualised storage. We need to change the rules about how we do security. So what does this shift in thinking look like?

Well let's consider how this would change something as basic as a firewall, right? We all understand enterprise firewalls hopefully. But using the principles I laid out and the unique properties of virtualisation you end up with something that you don't add to your environment, you already have it, it is your environment. You now use this new distributed service provided by your environment to see your infrastructure through the lens of the applications running on top of it.

What you do is through the application you understand what known good is. I know all the components of my application. Through machine learning I can understand what those components do, how they talk to each other. By collecting similar components and information on similar components from all of our customers and 50 million VMs worldwide I can do unbelievable understanding of how things behave. Then what I can do is I can start to say things such as, hang on a second, that thing there is talking to a box it never talked to before. That thing there is encrypting its file system, it's never encrypted its file system before.

I can spot, from understanding how and what normally communicates with each other, I get to a world of known good. That world of known good means that both the network level and at the post level I can understand an application and apply policy. Not just in isolation.

A known good is the difference between golf and tennis. If you're playing golf it's very different to playing tennis, right? Hopefully you've worked that one out by this age, okay? Now tennis, what you're doing is you're playing against different opponents on a weekly basis and those opponents can hit the ball at you in thousands of different ways, millions if you consider all the possible trajectories, spin, et cetera, of that ball. So you can spend your life perfecting the ability to deal with and respond to a rapidly changing threat.

Known good is the opposite, that's like playing golf. Where I stand in relation to the ball never changes. I can tune that to my own liking and I'm continually practising how I perfectly hit that ball every single time. Because I know the parameters of the world I live in. I might move to a different golf course and learn different golf courses, but ultimately I'm working off a base of known good. It's a very, very different way of thinking. So it's because we understand this, both at the host and the network level that we can do this. Somehow my [unclear] - no okay, there we go.

So in this model because what we're doing is we're putting security into the hypervisor, security monitoring and management into the hypervisor, then connecting those hypervisors to all the other hypervisors. Then understanding the network, the security, the compute. Because what we're in is a unique position. As a hypervisor I see everything, okay? Because I am the virtual world that everything lives in, so I see every piece of network traffic but also I see every piece of storage traffic. I see every piece of memory traffic, I see every CPU traffic, I see everything. So I am in what we call that Goldilocks Zone for security to understand what's going on. So we know the host because [we booted it].

More importantly we're outside the host because we're not stuck inside an OS and more importantly we're everywhere, we are a distributed service. We're running the network, we're running the storage, we're running the compute, we're running across multiple clouds. We can apply a policy that stays and lives with an operating system, with a host, with a guest no matter where that ends up in the infrastructure.

In the old world if I took a VM and wanted to move it from one data centre to another that was a nightmare of networking security. I'd have to tell the network to remove the VM and they'd scream at you about trunk ports and PIX firewall rules and all this other kind of stuff. In this world I drag and drop the VM from one cloud to another, its security goes with it, its networking goes with it, its policy stays with it, I don't have to do anything.

More importantly we sit holistically with global machine learning and learn from all the hosts. This comes together into what we call a service defined or service driven firewall. So an enterprise firewall makes sense for north/south traffic, all right, where we've defined perimeters and users going to the internet and [comms] and extend beyond our applications. But it's the wrong tool for the job inside our environments. [Unclear] to understand the [compound] position, topology and intended behaviour of our application will lock them down. [Lease] privilege for your entire application, for everything that does.

This is an internal firewall, it's an east/west firewall as well as a north/south firewall. But it's not a firewall, it's intrinsic in what we're doing in the system. It's not just taking north/south concepts and sticking them inside the firewall or inside our hypervisor either. It's leveraging the unique capabilities of the cloud to make it even better than we possibly could be. So, what do we need to do? As an industry we need to drive and invest in prevention.

We had a customer who spoke at RSA for us in the keynote and she was a bit bolder and she said fire your security team and don't hire them back until they've built an application. Which was kind of interesting, it was a bit strung, but I'm not going to say that myself is the best way to do it. But while you're at it make your application teams visit the SOC, security operations centre, and see what a challenge it is to secure the attacks based on what they've built. Okay.

I mean the prevention one's pretty obvious, right? Do I buy and spend loads more money on firemen or do I work on making houses a little less flammable? It's not difficult to understand. Focus on applications. This is probably for me, as a technologist and an architect, the biggest shift. Applications were something we ran on top of the infrastructure that we secured, right? Now it's different. Applications are what we're all about. Applications are bigger and more complex than ever before. Applications are what we secure, the infrastructure should not be something we have to worry about. The infrastructure should be there to support securing applications not the other way around.

So when you're looking at those, now the security vendors or the security world, think about how many of them are talking about securing infrastructure. For us, we need to make security intrinsic, built into absolutely everything that we do. Built into the hypervisor, built into the network, built into the compute, built into the storage. So no VMware is not a security vendor, we don't sell security software. What we do is we make sure that security is in everything that we do with our platform and we make sure that we enable others to add security features on top of that. With that, that's my 20 minutes up and I'll thank you very much and I think I'm going to head over there and sit down and have a chat with Joel. Thank you.

[Applause]

Keynote interview with Joe Baguley & Joel Stradling, Research Director at GlobalData

&

Audience Q&A

Joel Stradling

Okay, thank you very much Joe for that fantastic presentation. My name's Joel Stradling, I'm a research director at GlobalData and for the next 20 minutes I will be interviewing Joe on the presentation he just made. Also, this is a chance for the audience to ask any questions. So there doesn't have to be a strict structure to this, if somebody has a question please feel free to ask it. I'll be quite happy to get the ball rolling as listening to you I formulated some questions and some thoughts going on there. So if we could focus in on that concept of the application becoming a network, or…

Joe Baguley

Yeah.

Joel Stradling

…the application is a network.

So does that mean that now the responsibility for having a secure app running lies with the developer? The independent software vendor? In the new world of very rapid and continuous updates, DevOps style, where does the responsibility sit now with those applications running for those enterprises? Is it the telecom operator? Is it the ISV that has to build it in? Or is it a virtualising company expert such as VMware?

Joe Baguley

I think when you look at it, if you want to sort of wind back again it's the changing role of the CISO, right, so the Chief Information Security Officer and they're moving from the role of previous dictatorship. So the CISO was the dictator, right? To now they're moving much more to sort of a spiritual and religious leader, does that make sense? Because what they're looking at now is they're audience is far, far broader than ever before. Rewind it was CISO right, we lock down the servers, we lock down the desktops and we're done and let's just watch everything and hope nothing goes wrong and the creep has been going for a long time.

So where does security responsibility lie? Of course it lies with developers, but training developers to do security is pretty hard, to be honest, and getting them to think about that. So what you have to do is you have to enable them to develop it in an environment that's inherently intrinsically secure. Now we did that before, right. So if you look at most of the problems we have with security breaches it's because developers didn't worry about security because what they deployed was going to run in a secure environment, right? I'm going to write my app, it's going to run behind a firewall so I'm good, I don't have to worry about security.

What I want to do now is say okay, well you want to develop, are you going to develop on a secure platform so you don't have to worry too much about security because it's going to be secure, inherently, wherever that bit ends up. Because I'm going to put in place all the controls and policy toolsets to do that. So it's an interesting evolution of where it goes. It sort of started with - I mentioned operating system for data centres. That was a dawning moment for us when we realised that what we were actually building was that and so we were looking at an entire data centre as a machine.

When as a team - we assembled people from across the industry that had experience with building large distributed systems, whether it's distributed apps, distributed whatever. We had people from Google, people from eBay, et cetera. Sort of eight years ago we built this team that looked at an entire data centre as one. That was where we realised we needed software to fine networking. We didn't do virtualised networking just to upset the networking industry, we did it because we were building this operating system, same with storage, et cetera. That model has just expanded to be multi data centre, multi cloud, multi endpoint now but it's built on that solid base.

Joel Stradling

Okay, thank you and the next question I had was around the security monitoring. So looking at my notes here is VMware has massive experience with hypervisors and that is a sweet spot, that's your space, you've really managed to own that space. With the security monitoring comes a response to an incident happening and I think you mentioned it briefly when you had one slide with, there was the mobile up there on the left hand side and the app running, something weird happens. What happens next? Could you just talk a little bit about the response? I think you said shut down, but…

Joe Baguley

Well it's not just shut down, that's the point. So what we can do, because we are a controlling, because - we, [inverted] - because in this model you are controlling the entire operating system for the entire app the responses are myriad. So the options I've got are huge. I can instantly dynamically firewall or quarantine a whole bunch of application servers in one go. So the response might be right, let's just lock these down. We'll leave them running but we'll lock them down.

It might be no, suspend them, I can pause every single server or I can move it to somewhere else. Or it could be I'm going to encrypt all traffic between my servers and I'm going to do that by clicking a mouse. Or I'm going to stop exposing certain sections of an application to a certain subset of a bunch of endpoints and applications and users.

My favourite is we, when we first started doing software defined networking the last people I thought were going to buy software defined networking were governments and security services. Because they're all about air gaps and they're all about it's got to be - they were the first and they're our biggest consumer of this. Why? Well I'll tell you, there's one government now that sets up an environment, their production environment, and it gets hacked two or three times a day by other government actors or whoever, and we'll discuss that in another panel. What do they do? This is great. They instantly clone their entire production environment. They start a new one up and start running their systems on that and they leave the old one running and watch the people attack it and learn.

Joel Stradling

Is that a digital twin? Is that the same thing?

Joe Baguley

Yeah.

Joel Stradling

Or [slightly different]?

Joe Baguley

Yeah, but they instantly twin it. Because everything defined in software, networking, storage, compute, the whole thing, they can instantly twin that entire environment, leave the hacker attacking that twinned environment and then their production environment moves on. It's really cool. There is no way you could do that with traditional networking, physical networking, in any way.

So this is what I'm on about. It's this total different way of - we're doing all these other things differently because of cloud, we can do so much differently with security with cloud but people aren't realising it yet.

Joel Stradling

Okay great, thank you. That sort of addresses more around the technical side of things that I had and I think the other area I was interested in exploring further is around organisational. So you presented there how enterprises currently think where there is a lot of spend on the reactive side, less on the preventative. One of your recommendations is invest more in preventative and that's understood. Then there was the far more dramatic example you shared of fire your security team…

Joe Baguley

Wasn't mine, it was a customer's, yeah.

Joel Stradling

…ask them to build an app. A bit more dramatic. So yes, somewhere hopefully there's a middle road in there.

But really in your conversations with enterprise or with government, because we are going to look at critical infrastructure in the next debate. So there's enterprise and there's government and utilities, national utilities, critical infrastructure.

Joe Baguley

Well you've got telcos which is the worst of both.

Joel Stradling

The telcos as well, okay, we'll get into that one too on the debate, as we will have a telco on the panel. So we'll look forward to that one. But, yeah, that, we can include that in this next question too. How can you lead these companies from, you know, to that end game? They are here where they are today, they can't change in the next six months. They can't chuck out all that legacy stuff and - so what's the discussion? What's the conversation with them really to prod them in that direction?

Joe Baguley

So there's a famous law on the internet which is every argument on the internet will eventually end up with someone calling someone else a Nazi, all right? So someone quoted that but then called it Baguley's law about five years ago at VMworld because I said that every conversation about technology ends up being a conversation about people and process. We've done it now, in less than an hour.

We had to invent a service called OTS at VM which is Operational Transformation Services. We had to invent services offering - and I'm not advertising here, I'm just saying it's a symptom - because we were going into an organisation and going let's rewind, forget security, let's just talk about updating data centres. We were going in saying well, you've virtualised your servers, we can now virtualise your storage and your networking.

That's still going on. We've still got companies that are going well hang on, the networking team's different to the server team, which is different to the storage team and they don't talk to each other and bada-bada-bada. It's okay to actually, you've got to get them all together into a new service team that talks together about networking and security and everything together in one. So you change your operations model and you change your organisation around the services, the platforms, the infrastructure that you're providing.

So when you look at it you go into most companies and you see an organisation that is built based around their infrastructure. But it's based around their infrastructure from 15 years ago and it's creaking at the seams because all these new ways of doing things are there and it doesn't fit the model that they built 15 years ago for the network team, the storage team, the security team.

So for us that's been possibly, and continues to be, the biggest challenge. Is that operational transformation and you have to look at something completely different. The car industry is one that I work with quite closely and it's brilliant. One of my friends who works in the automotive industry told me that much like there's another [law] where you can tell the organisation [to show up] the software company by its product offerings, right? What he also said is that you can also tell the org chart of a car company by looking at the dashboard, and you can. You go in and you see there's oh, look the air conditioning people don't talk to the car stereo people that don't talk to the navigation people that don't talk, and so on. You can see that.

If you look at Tesla, completely different because they look at the whole system as a different thing. They're not fighting an old org chart. So that's a brilliant, for me, kind of summary or what's going on in the industry, is these companies are looking at everything through their old org chart, not going to work.

Joel Stradling

Yeah, that really does tie, or attune, or align closely with just the studies we have done internally is that that transformation process begins with an organisational change and if you don't have buy-in from the executive team to the managers throughout those projects fail. They crumble and fall in the middle.

So we have five minutes before the panel debate is to begin, much as I would like to keep asking Joe questions, because I have more, each time he answers another three spring up. But that wouldn't be fair. Are there any questions, please, from the audience? Now is the opportunity to get that question in.

Joe Baguley

It's too early.

Jan Guldentops

I'll bite the bullet. Anyway, I am Jan Guldentops from BA Test Labs.

But it's the ultimate lock in story, isn't it?

Joe Baguley

Why is that? Who, why, where, how?

Jan Guldentops

Which you presented. Is VMware going for to be the new IBM?

Joe Baguley

Not necessarily. So it's an interesting one. So always people will say oh, well this is a good question, it's the ultimate lock in story, buy into VMware's lock in story. You can build pretty much the same thing with open source components if you wanted to, and we're surrounded by open standards. So there's an open standard called OVFTool where you can take all your virtual machines and move them to a different VM. We're based on standards such as Kubernetes as a control plane. We're based on standards such as OpenStack, there's an OpenStack version of this you can do. You can build this all - what I'm talking about here is nothing's inherent, really, to what we do at VMware.

There's bits and pieces and features, yes, such as NSX, that we're doing uniquely within our hypervisor. vSAN, for example, which our storage tool is uniquely within our hypervisor. But I think the principles go much broader than that, but yeah, people buy into our ecosystem, I would say. But actually what's interesting is people come into our platform because it gives them openness and choice. If I look at what we've done at VMware historically our success comes from the fact that we introduce choice.

I came in with a hypervisor that allowed people to run on any hardware they like and at the same time I support any virtual machine that you like and the fact I support DOS 6.22 which even Microsoft don't support that far back, right, and I have customers running that. At the same time we're consistently looking at it from an API-led lens which is why our heavy investment in acquiring Heptio and Kubernetes, et cetera, so we can make sure that going forward will be a much more API driven world in that context.

So I would, of course, argue that it's not lock in. There's always benefits to coming and using our platform, but I'm not looking to lock people in. The last thing I want is hostages, because they don't make really nice customers. I want customers that come back to us time and time again because the value we provide in our software is so great. I want customers to do that because they feel that they can switch off that platform easily if they want to, and they do. They come to our platform because they know with

OVF and other things they can switch to a different platform. So for me I want customers, not hostages. There's other companies that have hostages, we don't.

Jan Guldentops

Just one small follow up question. So the biggest competitor to this, I can imagine, is Red Hat, isn't it? Or IBM I should say, now [unclear].

Joe Baguley

No, honestly not really and I'm not saying that to be dismissive. So yeah, Red Hat have a hypervisor in KVM. Red Hat have the OpenStack and…

Jan Guldentops

CloudForms.

Joe Baguley

Sorry?

Jan Guldentops

CloudForms.

Joe Baguley

We can talk about that in a minute. They have CloudForms, they have OpenShift. Yeah, yeah so they have all the pieces for it, yeah. But no I wouldn't necessarily identify them as our prime competitor in this space, I don't think there is one. I think it's a world that's very, very grey. I love the fact that our industry always likes to find a two horse race, we always like to find the good guy and the bad guy and the reality is there isn't anymore. It's coopertition.

I've got Satya Nadella and Michael Dell and Pat Gelsinger standing on stage last week talking about us all going to market together with a whole bunch of other stuff. At the same time we're going to market with Amazon and we're going to market with IBM and we're about to announce some stuff at Red Hat Summit this week as well. There's people running things on best place to run OpenShift is on SDDC. So it's much more cooperative than that. So I don't think - keep searching for that two horse race, but it's not there I'm afraid, sorry. Some of my best friends are the CTOs of their companies.

Joel Stradling

Are there any more questions, please?

Steve Broadhead

Steve Broadhead, Broadband Testing - all right, morning Joe. We'll leave the security questions until the next debate.

Joe Baguley

Next panel, yeah.

Steve Broadhead

But it's just, you're talking about VMware and obviously [I run] VMware from 1837, all right? When you very nicely gave me loads of free software to run in the labs. But let's say in two years' time, even, how are you going to define what VMware is as a company? What, how are you going to describe VMware in two years' time?

Joe Baguley

I think it's the same way that the slide that I used at the start there, which is the ability for our customers to run any application on any cloud and deliver it to any device. That's really it, that story of globally consistent operations, globally consistent infrastructure, is very important. I mean our hypervisor is a small percentage of our revenue now as a company, so that's fairly public. We are much more now around cloud management software, we're the number one player in cloud management. But, again, not many people know that because they still think we're the company that has hypervisors.

We're the number one [sole] vendor in SD1 with VeloCloud, two times clear of the nearest vendor but people don't realise that. We're number one in a whole bunch of markets, hyper diversion infrastructure we wipe the board there. But you're right, it's this kind of what is VMware, I think it's an entirely different company to the company of 2010/2011. Totally and utterly different. The culture's still the same, but the products have evolved dramatically, and very successfully. I mean we're very, very proud of the success that we've had and we've got great plans going forwards. We've announced the thing with Microsoft recently, we've got obviously VMware Cloud on Azure, VMware Cloud on AWS. All these different products means that customers get more choice.

So one thing I've noticed is that I'm having conversations now with CIOs that are strategic, as a strategic vendor, as one of their top two or three. Which eight years ago I wasn't, I was down here as someone in the data centre. So yeah, certainly. I think the most underrated part of VMware that people miss all the time is our WorkSpace One digital workspace piece. What we do there with our Endpoint Management AirWatch, user management delivery, et cetera, is truly game changing and puts us ahead of our competitors in that space by, in the last 18 months, by a clear head.

But again people don't often, unless they specifically analyse a report in that space don't notice that market, but it's big and it's going to be transformative. Because we've learnt a lot there that I can take now into IoT and edge and a whole bunch of other different places that people don't realise. My favourite stat is we - if you see those Coke machines, you know those freestyle Coke machines where you get to choose your own thing? Every single one of those is managed by VMware. You wouldn't have thought that eight years ago. So it's odd, but it's fun.

Joel Stradling

That kind of just sums up what I said about what is VMware now.

Joe Baguley

Yeah, we're lots of things.

Joel Stradling

Okay, thank you very much indeed Joe, for that.

[Applause]

[end]