

# Real security in the virtual environment

*Date: Fri, 01/28/2011 - 14:17*

Virtualization in the data center has moved from a "new paradigm" to a vital strategic and critical component of the enterprise infrastructure. As organizations reap the benefits of virtualizing segments of the data center, they often overlook the next key step – securing data across the entire environment



Stuart Hatto, Solutions Architect, HP TippingPoint EMEA, HP

Networking

Virtualized environments and their applications are subject to many of the same threats as traditional data centers, but they replace fixed hardware infrastructure with a dynamic allocation of resources – demanding a whole new way of thinking for the security administrator. For example, many virtual machines (VM) are hosted on a single server, so one security breach can have a far wider impact. So IT and security managers must look for new ways to stay secure and protect their applications and assets.

Simon Leech's role at HP TippingPoint puts him at the leading edge of IT security, and the evolving challenges of virtualization. We asked him to share his insights into the key issues when the virtual environment and to highlight the most prevalent security weak spots in current virtualization architectures. What threats are most likely to exploit these weak spots? What sort of harm can we expect from them? Above all, what can be done to minimize their likelihood, and their impact?

## **Presentation by Stuart Hatto, Solutions Architect, HP TippingPoint EMEA, HP Networking, at NetEvents EMEA Press Summit, Istanbul**

It's going to be a really quick presentation. I had loads of product slides, but I was told you hate product pictures. There you go. So what I want to talk about is real world security but in a virtual environment. And try and give you an idea of some of the issues that your customers, you readers are going to see in terms of securing, when they go headlong into virtualisation because of all the cost savings, the rationalisation that gives them. So I'm going to talk about some of the issues that perhaps they need to consider and perhaps you can help them consider.

Gartner in 2010, beginning of 2010 did a Exec survey, over 1,500 CIOs and virtualisation is their number one priority, and that displaced business intelligence which had been in that top position for the last five years. So its clear in the CIOs mind that rationalisation by virtualisation is very key. There are cost savings to be made, and so uppermost.

And in terms of CP workload, 50% of workloads by 2012 will be virtualised. So I think that's fairly considerable when you consider that right now probably somewhere around 16%. And what's going to happen is that as people rush into virtualisation they'll forget every lesson they ever learnt in terms of security. So, virtual data centres are complex.

A visionary, more gift with words than me, once say today's data centre is incapable of handling the complexity in the management of the virtual machine environment.

Thank you for your words John. He said that yesterday.

Now, when you provision a new virtual machine it happens instantly. You don't know where that virtual machine is going to end up you have no idea where the server is. And so you could be faced with a situation where maybe you've got a PCI application in a bounded PCI zone that a QSA has said its fine, it adheres to PCI. And then it ends up on a server running an external web application that could be compromised quite easily. So again, the security boundaries have been blurred there.

And people just aren't thinking about it.

Security of the applications in the virtual machines is paramount. Why should it be any different just because it's virtualised? Why is that host any different now? Just because you're running exchange in a virtual machine why is the security any different than when you run it on a physical host? Clearly its not.

And I talk a little bit about patching, patching in most enterprises is at best patchy.

But when you put them into a virtualised environment that patchy patching cycle becomes even more important. If you think about a virtual machine, which you have fully patched, it has all the security patches installed on it and then you roll that VM back to some snapshot that security has gone, its something else that needs to be thought about.

So let's go through what a virtual data centre looks like, look at the components, look at the threats that might be there and some of the challenges, and some of the things to think about when you are securing those.

So let's talk first of all about Hypervisor Security. The Hypervisor is mission critical, it's clear. You've moved from a physical host that would break, have power supply issues, have disc

issues to a situation now where you have a Hypervisor running on a physical host that's now hosting 30, 60 virtual machines all of those are mission critical.

But the Hypervisor itself is software, it has bugs. There are theoretical, theoretical at the moment, attacks for VMware's vSphere Hypervisor things like Blue Pill for example, that could attack that Hypervisor. And when we see other security companies going down the route of virtual IPS's they can't secure the Hypervisor with a virtual IPS that runs on the same Hypervisor as the Hypervisor you are trying to secure. It's just not possible.

And what we are seeing in terms of virtual IPS's is actually those companies are delivering virtual appliances. They are not delivering an integrated solution integrated into the virtualised environment. All they are delivering is an appliance in the same way that somebody would deliver an exchange appliance or it's just another thing to provision.

Hypervisor security patches have to be immediate. Remember its mission critical, its running mission critical applications. So the Hypervisor security has to be maintained at all times. And so when there are patches available from VMware for example, you have to patch immediately. So that brings it the issues of mobility of the virtual machines while you patch, but also issues of, if I can't patch immediately how do I protect the Hypervisor while I'm buying time to patch it? So that's a physical world IPS probably, or physical world fire walling.

Think about host-to-host threats. Why, again I have to keep saying this don't forget security just because your host's are now running in a virtual environment. If a host was capable of being compromised when it was running on a physical server it's just as capable of being compromised in a virtual world. There's nothing to stop that. And once you have a virtual server that's compromised it can then attack all other virtual servers.

Now it's just not economical to deploy physical IPSs in front of every single bare metal Hypervisor, economically it's not viable. So you need some kind of other solution. And the other thing not to forget is your going to need some kind of virtual machine to host security because if we have an attack vector on, I don't know, Windows 2008 server and we can compromise Windows 2008 server, maybe from 2008 server I can then compromise the Hypervisor underneath. Okay, so again remember that theoretical threat at the moment, but that threat is real.

And then of course we've got virtual machine to virtual machine threats. You've got 30 physical hosts down into one virtual server or one physical host running 30 virtual servers now. If one of those servers gets compromised now the games over, because now pretty much every server running on that virtual host -- or sorry, every virtual host running on that physical server is now fair game.

And a physical IPS and physical controls, physical network inspection controls, can't help you because that traffic is invisible to physical controls. It goes between virtual machines on the Hypervisor itself. So maybe think about that as well, how do we secure that interim machine traffic?

And then mobility brings with it its own problems. If we have a VMotion environment, and we move a physical machine or move a virtual host to a remote data centre for DR purposes or whatever, any security solution that you've deployed has to move with it. It's got to move with it. You've got to have a situation where whatever we have here in our active data centre is the same in the redundancy site, okay the security has to be maintained. So whatever solution you have has to be VMotion capable.

And again physical IP options there, you could use them but again they are tending to now be cost prohibitive because you're collapsing this whole data centre where we could have put one or two IPSs in front of the data centre, now we are having to think about securing each individual host.

So let's look at where we might, or some possible solutions to some of this visibility gap that we've got here. If you think about Hypervisor security, I've already talked about the virtual IPS and it can't help. Virtual IPS solutions can't secure the Hypervisor it's running on.

So there is only one solution. Remember Hypervisor's, 40,000 lines of code, you can't install third party firewalls on there you can't install third party host intrusion prevention on there. It's a lock-down operating system. So your only option for securing a Hypervisor is a physical IPS, so securing the data centre at a physical level.

And of course it's a TippingPoint IPS platform up there on the top right, but it could be any IPS platform. You have to have that physicality there.

In terms of host-to-host threats well again you need some kind of physical IPS, there has to be physicality there. You cannot put host intrusion prevention on the Hypervisor. You cannot put fire walling on the Hypervisor, and so there has to be some kind of physical IPS. So you've got to have a mix of physical IPSs. You still will need a mix of physical IPSs and virtual capability.

In terms of VM to VM threats we are seeing a lot of interesting solutions here. And I don't want to discredit any of the solutions, but I also want to give you things to think about. You know, I'm sure many of you with your laptops open today, apart from those with MACS, have probably got some kind of host intrusion prevention, probably got some kind of antivirus, almost certainly running some kind of firewall.

You know the impact that has on the performance of that PC, from the day you got it out of the box to the day you put those software packages on there.

If you put host intrusion prevention on every virtual machine in the environment you've got two problems. One of scalability, you've not got 10,000, 20,000 each with host intrusion prevention that has to be managed. You've also got an issue of nondeterministic performance. You typically don't put host intrusion prevention on servers, so now it's fair game.

Firewalls don't help you, because firewalls all they do is say I'm going to allow all traffic on port 80 into my machine. They don't help. And antivirus does help clearly, but again it has an impact on the performance of the host and it's a non-deterministic impact. So you need to think about how you secure VM to VM traffic. Clearly, I am stood here from TippingPoint so there are ways of doing that.

And in terms of mobility this is quite a difficult solution to fix, because when your moving hosts around or when your moving physical hosts, the whole host and all of its virtual hosts, moving to another data centre for example with VMotion, as I said the security has to follow it. You don't want to have to intervene from a security point of view to actually set up new policies. So you want something that's seamless and easy to administer.

So, hopefully that's given you some ideas of things that you need in terms of security the virtual world. It can't just be done with software, and it can't just be done with physical IPSs. There has got to be some kind of combination of both.

And within that combination of both, if you're going to chose something that integrates with VMware for example, make sure it integrates at the API level. As I said integrating as if it was an appliance isn't going to work. Virtualised appliances, IPS appliances just will not work. They are okay for low-throughput, low-bandwidth requirements, and their okay if you don't really care about the Hypervisor environment itself. But typically virtual IPSs are not going to fix this problem.

So you need something that's fully integrated with the VMsafe APIs. I'm picking on VMware specifically here, because the other virtualisation vendors don't have open APIs. It's actually quite difficult for anybody to integrate with them at the moment.

In terms of management, do you really want another management console in your environment? You've got virtual centre so why not integrate with that? So maybe your customers want to think about an integration point there as well. Make things simple, they already understand vCentre, so give them something that's a snap-in, a plug-in to vCentre, something they already understand and are familiar with the management.

Possibly chose a partner that's a member of the VMware Alliance. I think that's always good, you've always got guaranteed support there at least. And look for products that are certified for VMware that's certified VMware ready [like that]. I'm sure I am preaching to the converted here.

So in terms of TippingPoint, this is my only product slide, we do have all of that clearly. We have a virtual IPS, well actually we don't have a virtual IPS, don't want to make an announcement but we probably will have one. We have a VMsafe API compatible plug-in called vController, it's a kernel shim. That allows us to inspect intra-host machines, Intra-VM Traffic. And also we can secure the physical world as you've heard over the last two days from conversations with myself and my colleagues.

So the solutions are there, just need to make your customers think that just because they are vitalising security doesn't go away. In fact they've actually probably increased their security problems. And people are seriously just forgetting about security.

Previously it was dead easy, you could say I know that server is running [at] exchange, it usually said exchange on the front of it. Well now you have no idea. You can't point to any server in a data centre and say what's running on it, you just can't. And they could move at any point. So security is paramount. And security actually is quite challenging and complex now.

So I said it was going to be nice and snappy. Don't know whether we've got any questions. You can try.

**Dean Bublely - Moderator**

Okay, any questions? Looks like you're going to have an easy afternoon.

**Simon Leech**

I got away with that didn't I?

**Dean Bublely - Moderator**

Indeed, thank you very much.

**Simon Leech**

Thank you.

<http://www.telecomkh.com/en/business-communications/news/data-center/hewlett-packard/netevents-emea-press-summit-istanbul/2692>