DevSecOps – Why Security is Coming to DevOps

With so many organizations making the move to embrace DevOps practices, we are quickly highlighting what many see as a missing piece to the puzzle: Security. As NV (Network Virtualization) and NFV (Network Function Virtualization) are rapidly growing in adoption, the ability to create programmable, repeatable security management into the development and deployment workflow has become a reality.

Dynamic, abstracted networking features such as those provided by OpenDaylight participants, Cisco ACI, VMware NSX, Nuage Networks and many others, are opening the doors to a new way to enable security to be a part of the application lifecycle management (ALM) pipeline. When we see the phrase Infrastructure-as-Code, this is precisely what is needed. Infrastructure configuration needs to extend beyond the application environment and out to the edge.

NFV: The Gateway to DevSecOps

Network virtualization isn't the end-goal for DevSecOps. It's actually only a minor portion. Enabling traffic for L2/L3 networks has been a major step in more agile practices across the data center. Both on-premises and cloud environments are already benefitting from the new ways of managing networks programmatically. Again, we have to remember that data flow is really only a small part of what NV has enabled for us.

Moving further up the stack to layers 4-7 is where NFV comes into play. From a purely operational perspective, NFV has given us the same programmatic, predictable deployment and management that we crave. Using common configuration management tools like Chef, Puppet, and Ansible for our regular data center management is now extensible to the network. This also seems like it is the raison d'être for NFV, but there is much more to the story.

NFV can be a confusing subject because it gets clouded as being L2/L3 management when it is really about managing application gateways, L4-7 firewalls, load balancers, and other such features. NFV enables the virtualization of these features and moving them closer to the workload. Since we know that

NV and NFV are Security Tools, not Networking Tools

When we take a look at NV and NFV, we have to broaden our view to the whole picture. All of the wins that are gained by creating the programmatic deployment and management seem to be mostly targeting the DevOps style of delivery. DevOps is often talked about as a way to speed application development, but when we move to the network and what we often call the DevSecOps methodology, speed and agility are only a part of the picture.

The reality is that NV and NFV are really security tools, not networking tools. Yes, that sounds odd, but let's think about what it is that NV and NFV are really creating for us.

When we enable the programmatic management of network layers, we also enable some other powerful features which include auditing for both setup and operation of our L2-L7 configurations. Knowing when and how our entire L2-L7 environments have changed is bringing great smiles to the faces of InfoSec folks all over, and with good reason.

East-West is the new Information Superhighway

Well, East-West traffic in the data center or cloud may not be a superhighway, but it will become the most traffic-heavy pathway over the next few years and beyond. As scale-out applications become the more common design pattern, more and more data will be traveling between virtualized components on behind the firewalls on nested, virtual networks.

There are stats and quotes on the amount of actual traffic that will pass in this way, but needless to say it is significant regardless of what prediction you choose to read. This is also an ability that has been accelerated by the use of NV/NFV.

Whatever the reasons we attach to how DevSecOps will become a part of the new data center and cloud practice, it is absolutely coming. The only question is how quickly we can make it part of the standard operating procedures.

Just when you thought you were behind the 8-ball with DevOps, we added a new one for you. Don't worry, this is all good stuff and it will make sense very soon. Believe me, because I'll be helping you out along the journey.

Why it is always, and never, the year of VDI, but network virtualization is here to stay

You've all heard it: The Year of VDI. It has consistently been the mantra of the launch of each calendar year since Citrix and VMware gained significant adoption during recent years. But why is it both true and false at the same time?

Desktop versus Server Virtualization

Server virtualization has taken hold in an incredible fashion. Hypervisors have become a part of every day datacenter deployments. Whatever the flavor, it is no longer necessary to justify the purchase of a products like VMware vSphere or Microsoft Hyper-V. And for those who embraced open source alternatives already, KVM, Xen and the now burgeoning OpenStack ecosystem are joining the ranks as standard step-1 products when building and scaling a datacenter.

Server virtualization just made sense. We have 24 hour workload potential because of a 24/7/365 usage scenario plus backups, failover technologies and BCP needs.

Desktop Virtualization is a good thing

The most commonly quoted reason for desktop virtualization is the cost of managing the environment. In other words, the push to move towards VDI is about policy based management of the environment. Removing or limiting the variables in desktop and application management makes the overall management and usage experience better. No arguments there.

So why hasn't it hit? One powerful reason is the commoditization of desktop hardware. It used to

cost thousands of dollars in the 70s to purchase basic desktop hardware. Throughout the 80s, 90s and 2000s the price of desktop hardware has plummeted to the point where corporate desktops are now available for $300-$500 dollars and they are amortized over 2 or 3 year cycles.

And now the CFO has their say

The impetus to use VDI save money on desktop hardware went away. We now have thin desktops that are nearly the same price as full physical desktops. There is no doubt that this has slowed the uptake of VDI in a strong way. When it comes to putting together our annual expenses, the driver has to be strong to make the shift.

Next up is the classic “Microsoft Tax”. While we may reduce the cost somewhat at the hardware layer, we are still bound to the needs of the consumer of the desktop to provide Microsoft OS and software. There is a reason why we don’t even talk about Linux on the desktop anymore. If people are ready for Linux, they will just use it. There are however millions of software consumers that require Microsoft tools. That’s just a fact.

So now that we enter 2014 and all of the analysts and pundits tout the new DaaS (Desktop-as-a-Service) revolution, we have to still be realistic about the amount of impact it will have on the overall market place. I don’t doubt that it will continue to gain footing, but nowhere near the level of adoption that server virtualization was able to produce.

A Patchwork Quilt

In my opinion, we have already gone down a parallel timeline on policy based desktop management. With Microsoft SCCM, LanDesk and a number of other imaging and application packaging tools already in many organizations, there is less of a need to make the shift towards VDI. There are great use cases for it for sure, but it will be a difficult battle to siphon away the physical desktop processes that have done us well up to now.

Patch management and application delivery can do a lot towards providing the policy based management that we are being told is the prime objective of many VDI products. I’m a big proponent for VDI myself, but I am also realistic about how much of the overall market it has already and will cut into.

So, is this the fate of network virtualization?

Network Virtualization is costly, but that’s OK

So now we have an interesting shift in the market again. Network virtualization has gone from a project in the labs of Stanford to becoming a real, market ready product with many vendors putting their chips on the table.

Not only are ASIC producers like Cisco and Juniper Networks coming forward with solutions, but VMware with their purchase and integration of Nicira to produce VMware NSX has created a significant buzz in the industry. Sprinkle in the massive commitment from open source producers with OpenFlow and Open vSwitch and there is undoubtedly a real shift coming.

2015 will be the year of Network Virtualization

In 2014 we will see a significant increase in the understanding and adoption of network virtualization tools and technologies. With the upcoming GA release of Cisco ACI and more adoption of open source solutions in the public and private cloud, we will definitely see a growth in the NV adoption.

Image source: http://blogs.vmware.com/networkvirtualization/2013/08/vmware-nsx-network-operations.html

Remember, NV isn't about reducing physical network hardware. It is about reducing the logical constraints and increasing the policy and security integration at the network layers. Server virtualization has laid the groundwork to create a perfect pairing really.

When does NV become the standard in networking deployment?

This is the real question we need to ask. As all of the analysts pore over the statistics and lay out what the landscape looks like, we as architects and systems administrators have an important task to deal with: Making NV work for us.

In my mind, network virtualization is a powerful, enabling technology. We have already come a long way in a short time in the evolution of networking. From vampire taps to the upcoming 100GBE hardware in a couple of decades is pretty impressive. Now we can fully realize the value of this hardware that we have sitting on the datacenter floor by extending it with virtualization tools and techniques that gave us exponential gains in productivity and efficiency at the server levels.

It's coming to us one way or another, so I say that we dive in and do something wondrous together.

Who's in for the ride? Count me in!

Software Defined Networking – The policy, programmability and bedlam as VMware NSX prepares for public release

These are very exciting times in virtualization as we prepare for the general availability launch of VMware NSX, the product of the Nicira integration over the past 14 months. The product received heavy focus at this year's VMworld in San Francisco, so much so that it was referred to by many as

“NSXWorld”.

I’ve been lucky enough to have some exposure to the product through a few different channels, and the product is very exciting. But with this excitement comes some trepidation by many as to how it will become a part of the customer ecosystem.

The reason that I have titled this to include the word bedlam is that there is a lot of really wild swings in opinion on the upcoming GA release, and how NSX will become a part of what we do today. Even beyond NSX, SDN in general invites some strong and often misguided opinions on either side of the argument for what it is, and why it is a forward thinking and inevitable shift in how we manage our networks.

A Key Point of NSX and SDN

The phrase SDN (Software Defined Networking) gets thrown around a lot, and sometimes incorrectly. Just like the use of the term “cloud”, there are some basic tenets that define a SDN product but the most notable is the separation of the data plane from the control plane.

This means that the underlying infrastructure and physical characteristics of networking are still present at the data plane, but the control plane is software managed, programmable and abstracted from the physical infrastructure.

What is a really big draw for this is the escape from hardware vendor lock-in. There will be more chat further down. One thing that cannot be denied is the buzz around what VMware is doing with NSX, and how much interest it is raising. The VMworld San Francisco Hands-On Labs were dominated by the HOL-SDC-1303

The Architects

There are some key people who began in Nicira and brought NSX into the VMware family through the acquisition last year. To start with, you may know folks such as Martin Casado, a significant player in the creation and growth of OpenFlow. Or perhaps you’ve heard of Bruce Davie, who among many accomplishments was involved in the architecture of a little thing called MPLS. Maybe you’ve heard of Ben Pfaff who was the lead developer on the Open vSwitch project.

The list goes on, and the people involved have a common theme. They were responsible for bringing game-changing networking technologies to the market. Nicira was a disruptive and innovative company on its own, and the merger with VMware has the potential to create a real juggernaut. This isn’t a fly-by-night operation that just hit the silicon valley with a little bit of VC money to create a marketing machine without any innovation behind it.

Policy and Programability

Possibly the most important feature of SDN is the policy management and programability of the networks through the use of SDN. By that, we mean that the deployment and management can be done through orchestration and automation to add network policy management into the deployment pipeline.

The exposure of APIs (RESTful is ideal) has become the top feature in being able to orchestrate the network features in our virtual and cloud deployment workflows.

Better Controls not Less Control

It gets tiring to hear the argument between network admins and sysadmins over who will be managing the infrastructure components as network virtualization becomes widely used. There are going to be clear delineations just as there are today. We won't have sysadmins wildly creating networks and reorganizing the topology. Just as we will not have network admins drilling down into the VM networks to change designs and policy on the fly.

If you lack the controls to manage your environment today, network virtualization will not save you from it. If anything, it will highlight that you have an issue. The goal of any NV deployment is to enhance the ability to delivery policy and features programmatically which simplifies your change control and separation of administration.

The polices are created by people, and the system applies them through orchestration and/or centralized management tools. The control lies in the fact that the policies, and the application of those policies is done using a system. That system allows for stronger controls, auditing, and logging.

The Cost

This is probably one of the biggest questions that is floating around even beyond the technical viability of the product. The truth of the situation is that it will be a non-trivial capital cost to you for running NSX in your environment. Many SMB (Small to Medium Business) customers may find themselves priced out of NSX at launch. Many SMB folks today don't even have vSphere Enterprise Plus or vCloud deployed.

Cost will be a strong factor in defining who the target customer is for VMware NSX. If bringing vCloud into your shop is already a limiter because of cost, then we can be sure that this will take some serious thought and justification. That is the capital cost side of things at least.

There is an intangible cost that comes with having, or not having a technology such as NSX in your environment. That comes with the processes and efficiency that you are able to gain by adding orchestration into your network infrastructure management.

Breaking the FUD

There are some really strong opinions for and against what is being done with NSX as it prepares for GA release. Much of the challenge from industry pundits comes as hardware vendors and ASIC providers present the case that using software abstraction creates overhead, and thus lowers the efficiency.

The truth about overhead: it exists. The real question that we have to ask ourselves is whether the challenges with overhead are outweighed by the effectiveness given with creating a singular, programmable ecosystem in which to manage your network platforms.

Is your current production workload maxing out your physical network infrastructure? If so, you need to rethink your architecture anyways. The addition of network virtualization won't be what tips the scales towards or against your infrastructure issues. Bringing NV into your environment is going to be a fundamental shift in the way you manage your networks which is the both the cause and result of what NV does for us.

Another classic that we hear is “so do we have to get rid of our physical networking gear?” Seriously?! If this is your argument then you need to back up a bit and think about what network virtualization does. If you have 700 physical ports lit up today with your bare metal infrastructure running your virtualized and physical server environment, you will need 700 after you deploy NSX.

What about Cisco being noticeably absent from the partner ecosystem diagrams during VMworld in San Francisco? The truth is that we are reading much more into it than we should. There are indications of some exciting news coming from Cisco and VMware on innovations soon, so this may just be like the Oscar speech where the actor forgot to thank the assistant director and viewers think it’s a snub.

“Network virtualization will reduce my FTE (full-time equivalent) count which could affect jobs” is another one that I’ve been hearing. This is as old an argument as the “robots will replace workers in manufacturing”. So far, automation, orchestration and virtualization of physical infrastructure hasn’t reduced jobs. In fact, it may have not just increased the number of jobs, but the quality of those available.

Are we just moving from hardware vendor lock-in to software vendor lock-in?

This is the nub of the argument. The pro-SDN camp is pushing the concept of escaping vendor lock-in. But if we are fully diving into using VMware NSX in our environment as the SDN technology of choice, aren’t we just moving to a vendor lock-in at the software side.

It’s a valid argument, but the tipping point for me, and many others is that the change in process and methodology is the real innovation that is coming with SDN. Technology is the enabler, not the goal. The goal is to fundamentally change and improve network management and deployment.

Understand the Use-Case

The core and fundamental requirement of bringing network virtualization into your environment is mapping the use-case against your business. If you are still not at a point where you are orchestrating and automating significant portions of your infrastructure, you may not gain significantly from adding NSX or any NV product into your toolkit.

The addition of NSX as an option in the virtualization world is a clear and solid step towards wider adoption of orchestrated infrastructure and abstraction of the physical infrastructure away from your network operations. You may not be hitting F5 in your browser every day looking for the GA code and price list on the VMware website, but ignoring what the release of this product means to the industry as a whole is the same as when this quote came out:

[quote]”As nice as the Apple iPhone is, it poses a real challenge to its users. Try typing a web key on a touchscreen on an Apple iPhone, that’s a real challenge. You cannot see what you type.” – BlackBerry (formerly RIM) Co-CEO Jim Balsillie, November 2007.[/quote]

Even if you don’t plan to deploy NSX at the launch, you should be ready to look at how the paradigm shift can bring your network and virtualization practices to the next level. It is as important to understand why you may not need this as understanding why you do.

Getting to Know NSX

There is one great way to start, and that is with the VMware Hands-On Labs HOL-SDC-1303 that you can do online:

Plus, there are numerous resources on NSX at the VMware Network Virtualization blog: http://blogs.vmware.com/networkvirtualization as well as lots of other resources on NSX and NV in general:

- Brad Hedlund – http://bradhedlund.com/
- Scott Lowe – http://blog.scottlowe.org/
- Network Heresy – http://networkheresy.com/
- Martin Casado's VMware blog – http://blogs.vmware.com/vmware/author/mcasado

Start there, and let's see what NSX will do for you in your organization.