How Australian organisations are making the business case for network virtualization and security

Australia is considered a world leader in its take-up of virtualization. CIOs have put the technology into server and desktop environments in large numbers, and the next Holy Grail has long been considered the network.

For many IT executives, network virtualization is long overdue.

"I remember when compute was virtualised in 2001," Macquarie Telecom's Group Executive, Hosting James Mystakidis said.

"I took it into production in 2004 [in a previous role] and virtualised the whole data centre, but we still had to fuss around with very complicated network pieces.

"When network virtualization finally emerged, I felt it was way overdue. I wished it had happened a lot sooner".

This kind of pent-up demand should bode well for network virtualization, and it is. Australia is already enjoying strong take-up, with the likes of the Australian Bureau of Statistics, Macquarie Telecom, Zettagrid and Global Speech Networks joining large telcos and universities as early adopters.

But unlike server and desktop virtualization, network virtualization's trajectory into Australian enterprise is far less obvious, for a couple of key reasons.

Firstly, some early use cases – and indeed the one regarded as the quickest win – is in the field of network security. Organisations have been historically unwilling to talk about the make-up of their security architectures, and to a large extent this still holds true. The result is that the most popular early business case for network virtualization is at least partially obscured from view.

In addition, server virtualization had some really settled use cases from day one. Business cases were successfully built around hardware consolidation and faster (and more automated) infrastructure provisioning, leading to deployments.

The business cases for network virtualization are more varied, and new ones continue to emerge.

A qualitative survey of Australia's early adopters commissioned by VMware shows a small sample of this variety of potential use cases for network virtualization emerging.

Known projects so far span security, automation, disaster recovery, application load balancing, network uplift and transformation.

The research also finds:

- The entry point for network virtualization into the IT environment is often unexpected, even for organisations that think they know where the quickest win is going to be.
- Cross-pollination of network virtualization into IT domains other than the one it used as a path to entry. In other words, once network virtualization is deployed, additional uses typically emerge, providing an opportunity for buyers to amortise the upfront investment and get returns more quickly.

vmware®

Server vs network virtualization

A common analogy for the value proposition presented by network virtualization is that it will do for the network what server virtualization did for compute.

That is:

- It will allow organisations to create virtual networks in software that are decoupled from the underlying network hardware; and
- These virtual networks will replicate all the features of the physical network, in the same way that a virtual machine replicates the features of a physical (hardware) server.

This analogy – repeated in the course of this research by several enterprises locally - is somewhat helpful in explaining at a very high level what network virtualization does.

However, it also oversimplifies and undersells what network virtualization is capable of enabling organisations to realise.

“Server virtualization was really mostly about consolidation, putting more workloads on fewer machines,” VMware CTO for Networking Bruce Davie said.

“With network virtualization we focus more on agility, automation, security through things like micro-segmentation and application availability or continuity through decoupling the network services from the underlying physical infrastructure.

“It’s definitely a little bit more complicated than the original value proposition for server virtualization.”

This isn’t dissuading Australian organisations from testing or putting network virtualization into production.

A survey of IT professionals by Kemp Technologies at VMware’s vForum in Sydney and Singapore last year found that between 25% and 33% of respondents plan to deploy some form of network virtualization technology in the next 12 months.

So how can you get your business case for network virtualization over the line?

In this research report we look at how other Australian organisations successfully made a business case, and the key learnings you can take from their early deployments.

The report is organised into three main sections, detailing the business cases for security, network automation, and load balancing. Each also details some of the sub-use cases that have emerged in each domain.

vmware®

THE BUSINESS CASE FOR SECURITY

- **Micro-segmentation is the quickest win for network virtualization**
- **East-west traffic flows (e.g. VM-to-VM) dominate environments**
- **Securing those flows is desirable but traditionally costly**
- **Distributed firewalls and micro-segmentation are the answer**

The business case for security

One of the major early use cases for network virtualization that has emerged in Australia is around network security.

Several sub-use cases have also emerged, including perimeter firewall replacement and securing east-west traffic flows in the data centre.

Luis Concistre, a Systems Integration Senior Advisor in Dell's Global Enterprise Technology Services division, was involved in a perimeter firewall replacement project at a major NSW university.

The project didn't start out as a firewall replacement, but in the course of scoping a different solution, the existing perimeter firewall became a potential issue.

The university's firewall was about eight years old and the number of rules it policed over time had swelled into the tens of thousands. Without knowing exactly how it operated, Concistre saw it as a risk to the success of the project he was scoping.

"We started talking about coming up with some strategy to replace the perimeter firewall," he said. "That strategy was micro-segmentation."

Rather than apply rules to all traffic coming in and out of a data centre network, micro-segmentation allows the university to attach a distributed firewall capability to individual workloads running in the data centre.

There are several advantages to this model.

Aside from de-risking a potential bottleneck to a planned program of work, as was the case for the university, the first advantage is that it allows organisations to apply what Forrester calls a Zero Trust model.

Where previously it was assumed that the best defence against attackers was good perimeter security, best practice now dictates that everything in the data centre be secured in case an attacker manages to breach the perimeter. In other words, trust nothing by securing everything.

The second advantage is that micro-segmentation secures east-west traffic flows.

Perimeter security manages north-south traffic flowing in and out of the data centre, but this accounts for an increasingly small amount of total traffic in a data centre environment.

Most IT traffic now runs east-west – that is, between applications hosted on either physical or virtual servers – so it makes sense to target security at these flows to inspect and isolate threats that attempt to move laterally between machines.

Micro-segmentation can also aid security investigations in a way that traditional networks can't.

"With absolute granularity into the network, you can take a snippet of that network, go back in time and look really deeply at what happened, down to the byte-level in an individual network packet," Zettagrid's Lead Architect Anthony Spiteri said.

"If you want to be completely safe in your network or to have total visibility after an attack, you've got to virtualise. Traditional networks don't do that just yet.

"It's another reason why security is a big play in network virtualization's future."

Several Australian firms have joined the university in adopting micro-segmentation. The common ground each has is they've adopted VMware NSX for the purpose.

A Large Telco

One of Australia's largest telcos is using micro-segmentation as an "add-on" to an existing network virtualization deployment.
The telco initially deployed network virtualization for a different purpose but, upon showing it to their security team, the instance was expanded to incorporate micro-segmentation.

vmware®

"We started by showing them all the things that we could do that they could not do," the telco's infrastructure manager said, highlighting host-based protection through a central console and the management of VM-to-VM traffic.

"We set up the discussion, they saw the benefits and then we started setting up features for them."

Australian Bureau of Statistics

The Australian Bureau of Statistics is in the process of establishing a software-defined data centre environment as part of its NextGen Infrastructure (NGI) strategy.

When complete, it is expected to act as the infrastructure for the ABS's Statistical Business Transformation Project (SBTP).

"Micro-segmentation to improve security posture is one of the major drivers" of the bureau's deployment, a spokesperson said.

Global Speech Networks

A contact centre cloud solution provider, Global Speech Networks (GSN) is taking advantage of micro-segmentation, though it is also targeting its network virtualization deployment at additional use cases.

"The security benefits that we gain from the solution associated with the distributed firewall capability are fantastic," GSN infrastructure engineer Blake Douglas said.

"Having to maintain a firewall capability on a per-VM basis was just not feasible. The segmentation and isolation capabilities that we gained from NSX allow us to deliver something that previously was not possible to our customers."

Future security business cases

Other potential use cases for micro-segmentation are continuing to emerge as network virtualization is integrated with other systems.

"For example, today you can put an AirWatch mobile device management solution onto a mobile handset and then have NSX apply security policies based on the characteristics of that mobile handset, so you can start providing micro-segmentation to mobile devices," VMware CTO for Networking Bruce Davie said.

Efforts are also underway to allow micro-segmentation to be extended to workloads that run outside the corporate network or data centre environment.

"Whether the workloads are running in a VMware hypervisor in a private data centre, or on someone else's hypervisor in a public cloud, on a mobile device or in a branch, the idea is that NSX becomes a broad networking and security layer that cuts across all different kinds of endpoints," Davie said.

Dell's Luis Concistre said that 70 percent of the conversations he has with customers on network virtualization begin with micro-segmentation.

Davie said he frequently sees micro-segmentation as the "easiest use case" to achieve a quick win on network virtualization.

"The most easily repeatable use case is where a customer has identified security or east-west traffic as the problem," he said.

"They can frequently justify the purchase, buy it, get it deployed and be in production fairly quickly."

vmware®

THE BUSINESS CASE FOR AUTOMATION

- **Streamlines network builds, configuration and management**
- **Templates create enormous time savings for engineers**
- **Make self-service configuration for customers possible**

The business case for automation (and beyond)

Though automation is considered a more heavy-lift business case for network virtualization than security, it has not stopped Australian organisations from taking the plunge.

Network virtualization makes it easier to build, configure and manage networks.

However, one of the keys to getting this business case over the line internally is the desire of the network team to embrace it.

Judging by the mix of responses uncovered in this research, broaching the topic of automating network provisioning and management functions could involve some pushback.

But there is a sense of agreement among those who go down this path that difficult conversations in this domain are worthwhile, and that first-movers will achieve significant efficiency gains.

“My colleagues and I agree and understand that there is no future in physical hardware appliances,” the infrastructure manager of a large Australian telco said.

“You will have a DevOps model consisting of very simple network hardware designs where all the complexity is handled in a virtualization layer and is automated through APIs.

“Anyone who’s telling you they don’t see any benefit [in that] I think they’re kidding themselves. This way of thinking will be gone within ten years.”

Australian infrastructure-as-a-service Zettagrid has experienced it firsthand.

“Our main network engineer was a bit standoffish to begin but it took him about five minutes to understand the power of what he was seeing,” Lead Architect Anthony Spiteri said.

“Traditionally when we deployed an availability zone, he would have had to preconfigure a couple of thousand VLANs for the zone configuration of the network. Now he configures one.”

That kind of configuration efficiency should free up time for engineers to focus on higher-level tasks like network resiliency and monitoring, according to Zettagrid’s CTO Nicki Pereira.

It also means that some configuration functions can be put into the hands of customers via self-service automation, just as IT enabled customers to spin up virtual machines on-demand when they adopted server virtualization.

Macquarie Telecom’s James Mystakidis agrees there are efficiency gains to be had.

“I remember when I ran networking teams in other businesses where I’d have a team of four-to-six engineers and they’d spend their time enabling ports, configs, routing and OSPF,” Mystakidis said.

“But using network virtualization they are able to abstract all of that and start to work from the premise that, ‘I need this asset to be on that network’ and configure it via a browser, versus having to log on to hundreds of devices and set up automation scripts.

“It’s just a night and day difference”.

VMware CTO for Networking Bruce Davie believes automation will increase work for engineers and build their expertise.

“What most people find is that once they start automating the provision of workloads and virtual networks, that their users consume more,” Davie said.

“I’ve also met people who’ve been super excited about the fact they go from being a networking specialist to someone who now understands networking and virtualization. So for many IT professionals it’s a growth opportunity.”

Dell's Luis Concistre sees about 15 percent of deployments of network virtualization begin with a business case predicated on automation.

He said that most deployments he had been involved with ran with a micro-segmentation (security) business case first, and that often led in to a supplementary network automation project.

Qualitative surveys for this research report typically found customers with both micro-segmentation and network automation in production: one created an easier path to deploy the other.

Zettagrid

Until October 2015, Zettagrid offered customers the ability to configure basic network functions – such as NAT and DHCP – for their IaaS deployments via a graphical user interface.

"What we found was customers wanted a bit more than that," Lead Architect Anthony Spiteri said.

"They wanted to be able to configure some more advanced networking services like dynamic routing, BGP and OSPF."

Spiteri said that Zettagrid had satisfied these types of configuration requests in the past manually.

But the company has a stated goal to "allow our customers to be able to control every aspect of their cloud without contacting our support desk" – and so investing in network virtualization to increase its automation sophistication made sense.

"We had some challenges around the general automation of higher-end network services for our customers," Spiteri said.

"We really wanted a way to be able to offer a fully automated and really simple solution to our customers."

Macquarie Telecom

Macquarie Telecom is using network virtualization to power Launch Cloud Extender, a tool that connects a customer's private VMware environment with Macquarie's virtual private cloud, and treats both as a single compute resource.

"The Extender gives a customer the ability to extend their network into our virtual private cloud," Group Executive, Hosting, James Mystakidis said.

Mystakidis said that virtualization also assisted in customer and workload portability between physical data centres.

"Network virtualization helps tackle some of those challenges by effectively having stateless networks that can be moved, reconfigured and controlled either by APIs or via a web browser," he said.

"It's not hard for us to pick up a customer and move them from one data centre to another because it's all virtual. There's no hard ports, networking and configuration."

A Large Telco

One of Australia's largest telcos deployed network virtualization to make it faster to implement and support workloads hosted on its internal managed infrastructure.

The success of the deployment led to an expansion of the platform to micro-segmentation.

Australian Bureau of Statistics

The ABS is in the process of establishing a software-defined data centre (SDDC) environment under its NextGen Infrastructure Program. Underpinning the deployment is a production deployment of VMware NSX.

The ABS believes that the environment will enable it to "achieve greater efficiencies while providing an agile approach to technology and application delivery."

vmware®

"We are looking to NSX as one of the components of the ABS's strategy to deliver greater agility and efficiency from our infrastructure environment," a spokesperson said.

In addition to automation, the deployment also covers micro-segmentation.

The ABS said it plans to have NextGen Infrastructure in production in the second quarter of 2016.

"We have completed the NSX design stage and are now in testing and integration stage," the spokesperson said.

Global Speech Networks

Global Speech Networks (GSN) uses network virtualization to make it easier to configure contact centre solutions for customers that leverage its cloud technology.

"In the past when we developed a customer solution, it would involve our infrastructure team scoping new hardware, configuring that new hardware and spending a lot of time preparing for the customer solution to be deployed on top of it," Infrastructure Engineer Blake Douglas said.

"With NSX [network virtualization] it allows us to accelerate that deployment because there's no longer a requirement to do a lot of physical configuration.

"We template a very complex tenant environment and then we can scale that again and again and again."

"So today when customers come to us and they want a custom solution that integrates deeply into their network, instead of having to buy physical equipment and integrating that into our environment, today we roll that out with a templated approach, driving down the total cost of ownership for our end customers, providing greater flexibility and security to them, and ultimately differentiating ourselves in the market so we can win more business," GSN CEO Max Lipovetsky added.

Lipovetsky believes that network virtualization will ultimately be thought of in the same way as server virtualization today.

"The benefits of server virtualization have been huge for us," he said.

"I think if we look back ten years from now in the same way, network virtualization will just be seen as an ordinary way of doing business and something that is readily adopted."

vmware®

THE BUSINESS CASE FOR LOAD BALANCING

- Emerging use case
- May represent value-add to an existing deployment

The business case for load balancing

It's worth briefly touching on load balancing as a third use case for network virtualization, even if it is largely dwarfed by the bigger business cases of micro-segmentation and automation.

Dell's Luis Concistre sees only about 5% of his engagements leading with load balancing, mostly because many customers "already have something to do it for them".

However, even if it isn't enough to hang a project off by itself, it could be a value-add to help get a wider network virtualization deployment over the line.

This research identified one Australian customer taking advantage of VMware NSX for load balancing purposes – Zettagrid – however it's worth pointing out they also use wide spectrum of network virtualization capabilities – including for security and network automation.

"Our customers are predominately putting web services into our virtual data centres, and they want to be able to load-balance their services," Zettagrid's Lead Architect Anthony Spiteri said.

"So the lead-in when we go and talk to customers is actually our advanced load balancing."

Bruce Davie's take

One of the big take-outs from this research is that it highlights the varied use cases that customers have found success in getting network virtualization over the line.

VMware has 700 NSX customers worldwide and over 100 already in production, including many here in Australia.

We have deployments in a diverse set of vertical industries, including healthcare, finance, retail, public sector, universities and telecommunications sectors.

Some use cases, like micro-segmentation and automation, are fairly universal; others are more niche, but this variety of use cases is a strong reason to look at your own environment and consider where network virtualization makes sense.

East-west security is often the path of least resistance for network virtualization. A small micro-segmentation project is considered one of the easier use cases if you are looking for a quick win.

There are also many gains to be had from pursuing automation, but these projects tend to have many moving parts and therefore longer lead times.

The best tip I can provide is to start small but start now.