Network Virtualization and Security with VMware NSX

Transforming the status quo of traditional networking, and unleashing the full value of the software-defined data center.

BUSINESS CASE WHITE PAPER

vmware®

Table of Contents

Executive Summary

High-Value IT Outcomes for Software-Defined Data Centers

This VMware Business Case is for Business & IT Executives, IT Operations, IT Infrastructure, and IT Security professionals. You will learn how leading enterprises are achieving unprecedented value from network virtualization and security for their Software-Defined Data Centers (SDDCs).

Leading enterprises know that SDDCs are critical to modern IT. They are using SDDCs to help drive innovation, accelerate business velocity, establish competitive advantage, and reduce overall IT costs. They have turned to VMware for the vital pillars of their SDDC platform and approach. These enterprises use VMware NSXTM network virtualization and security in concert with VMware storage and server virtualization in a unified platform that powers their SDDCs.

With NSX, enterprises are achieving unparalleled speed, agility, and security – with orders of magnitude better economics, flexibility, and choice. Following are some of the major use cases and IT outcomes being achieved by enterprises using NSX:

- Micro-Segmentation – Firewall controls and security for East-West traffic inside the data center. Minimizes the risk and impact of data breaches. Approximately 68% CapEx savings.
- IT Automation & Orchestration – Reduces the manual effort and cycle time for network provisioning and management. Accelerates IT service delivery and time-to-market for new applications. 56-86% OpEx savings.
- IT Optimization & Refresh – Catalyst to modern leaf / spine network fabrics, bare metal switches, open networking, and other data center optimizations. 66-88% CapEx savings.
- Disaster Recovery – Cloud-scale service availability. Reduces the risk and impact of unplanned outages. OpEx savings of $690,000 to tens of millions of dollars (USD) per incident.

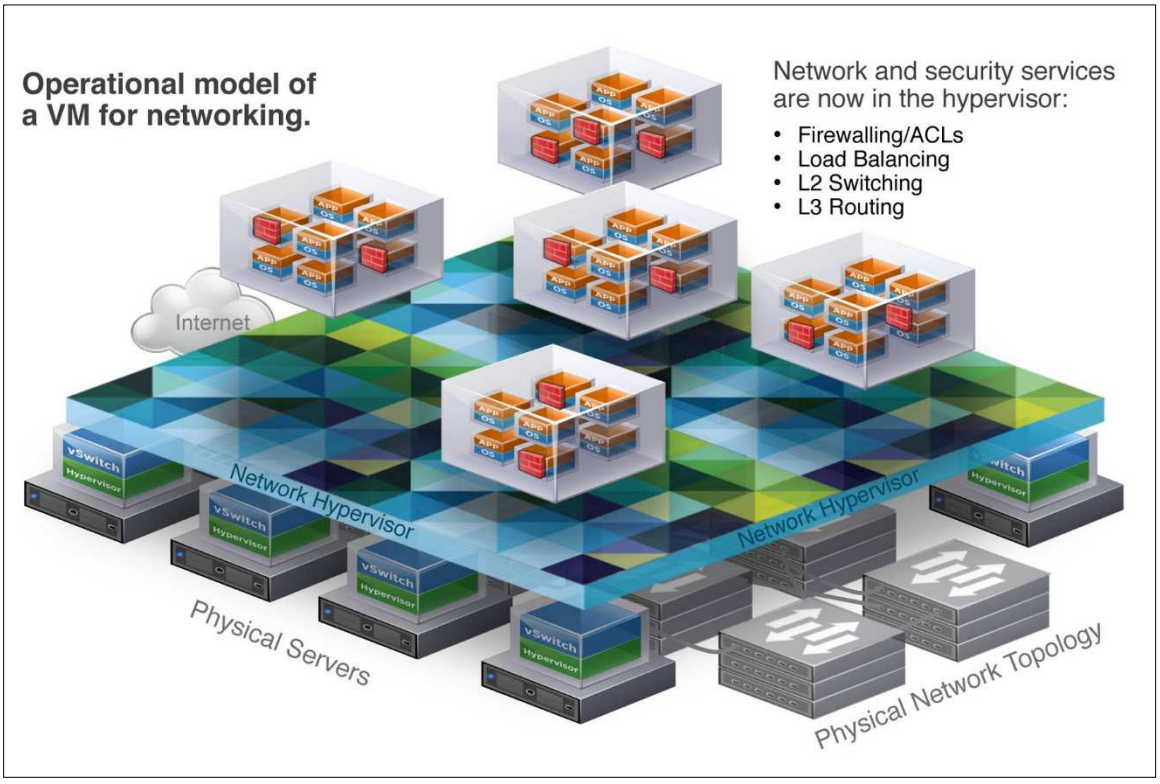
Situation Overview

Key Trends: IT Becoming Like Cloud Service Providers

The business wants IT to have the same level of speed, agility, and security as large cloud service providers, such as Amazon, Facebook, and Google. While most enterprise data centers are nowhere near the size and scale of these Web giants, they still require similar speed, agility, and economics. Amazon, Facebook, and Google have achieved these benefits by designing abstraction layers into their infrastructure. The networking elements and services are decoupled from hardware and baked into their software applications.

From an historical perspective, abstraction has been one of the fundamental enablers in computer science and software engineering. Every time we add a significant abstraction layer we accelerate innovation above and below it. Consider, for example, how operating systems, programming languages, APIs, and server virtualization have transformed information technology.

With server virtualization, the server hypervisor (an abstraction layer) reproduces attributes of an x86 physical server (e.g., CPU, RAM, Disk, NIC) in software. Think of network virtualization as the functional equivalent of a network hypervisor. NSX reproduces Layer 2 through Layer 7 networking services (e.g., switching, routing, firewalling, load balancing, VPN, access control, and QoS) in software. Enterprises use NSX to provision unique, isolated virtual networks in a matter of seconds, just like they do VMs.



Software-Defined Data Centers

In SDDC architectures, all infrastructure – including compute, storage, and networking – is virtualized, pooled, and delivered on demand. Operations and control of the data center are highly automated and standardized. Line of business (LOB), application, and Web teams deploy infrastructure instantly via self-service.

According to one recent study, SDDCs deliver a 56% reduction annually in provisioning and management operational costs.[1] The calendar days required to provision a production network for a new application including the task effort and cycle time, is reduced from 3-4 weeks to minutes. SDDCs also deliver value to the business through greater ecosystem functionality, vital innovation, and faster time-to-market.

Hybrid Cloud Computing

Enterprises are increasingly adopting hybrid clouds to speed IT service delivery at lower cost. According to a recent study, 82 percent of enterprises have a hybrid cloud strategy.[2] Hybrid clouds span on-premises private and off-premises public or private clouds. Enterprises are using hybrid clouds for data storage, auto-scaling and cloud-bursting, high availability and disaster recovery, compliance with data residency regulations, development and testing, and other use cases.

Traditional data centers are hampered by vendor-specific hardware and physical topology. Historically, these constraints have made it difficult for IT to implement hybrid clouds. Enterprises are now using NSX to bridge and build hybrid clouds, regardless of the underlying hardware. With NSX they do not have to worry about network interoperability or service provider lock-in. The resulting hybrid cloud provides unmatched business agility, dramatically simpler operations, and lower cost.

Network Virtualization

We have recently experienced a tectonic shift that has transformed networking. Enterprises are achieving seismic advances in speed, agility, and security. With orders of magnitude better economics, flexibility, and choice. Like VMs, virtual networks can be programmatically created, moved, copied, deleted, and restored – without reconfiguring the underlying physical hardware or topology.

NSX creates a complete network construct inside the virtualization layer. The virtual network can include L2 switching, L3 routing, load balancing, firewalling, VPN, ACLs, QoS, and more. Just as x86 servers became a pool of compute capacity, the physical network has become a pool of transport capacity that can be consumed and repurposed on demand.

Open Networking

IT organizations are taking advantage of the substantial price / performance benefits of open networking. The shift is being driven by the disaggregation of network hardware and software. Enterprises are replacing expensive proprietary gear with commodity bare metal switches and open source Linux network OS. The adoption of bare metal switches is also being fueled by the abstraction of network services into the virtualization layer.

In addition to the compelling CapEx savings, enterprises are also using open networking for the OpEx savings. The access, tools, and community around an open OS make it easier and more cost effective to automate, configure, monitor, troubleshoot, and add new capabilities to the network.

IT Challenges: More Speed, Agility & Security for Less

IT is experiencing a dichotomy of opposing forces: The business wants more for less. On the one hand, IT is expected to adapt to changing market demands and technology use models, drive productivity and growth, and improve quality of service. On the other hand, it is expected to consolidate and reduce cost. IT organizations are using network virtualization to successfully address both forces, just like they have with server virtualization.

Cloud service providers like Google, Facebook, and Amazon have proven that applications and services can be provisioned on-demand, and have an almost immediate impact on the business. Executive leadership is insisting that its own IT operate and perform more like these large cloud service providers. They want the same level of speed and agility for their business.

IT organizations that do not think and act like a cloud service provider are losing the confidence of business executives. As a result, the business sometimes bypasses the IT organization in order to access the infrastructure, applications, and services it needs. IT circumvention results in unwanted fragmentation that reduces the overall value of remaining corporate IT services.

Advanced Persistent Threats

While recent attacks on Target, Anthem, Home Depot, Sony, and others have each been different, they all have one characteristic in common. Once inside the data center perimeter, the attacks were able to expand laterally from server to server where sensitive data was collected and exfiltrated to the outside. These cases highlight a major weakness of modern data centers. They have limited security controls to stop advanced persistent threats (APTs) from spreading inside the perimeter.

Perimeter firewalls are necessary and effective at stopping APTs. But as recent attacks have shown, threats are still entering through legitimate access points. Once inside, they multiply from server to server and increase their prospects for doing damage. Solving this problem has been operationally infeasible. The number of physical firewalls and the complex matrix of rules required are prohibitively burdensome and expensive.

According to a recent study, in 2013 there were 63,437 confirmed security incidents, and 1,367 confirmed cases where sensitive data was compromised.[3] The total average cost of a data breach incident to companies in the United States is $5.85 million.[4] The lowest average cost globally is $1.37 million, which is in India. All other countries are somewhere in between.

As we know from widely reported data breaches, the costs can be astronomically higher. Sony Pictures Entertainment, for example, has had two data breaches in recent years. One reported June 2011, and another November 2014.[5] The 2011 breach cost Sony Pictures $171 million. Based on what we know about the 2014 breach, analysts believe the costs will likely reach $100 million.[6] The 2014 attack on Sony Pictures forced a shutdown of its entire network for days – also becoming an enormously costly disaster recovery event. Studies show that the likelihood of a material data breach involving a minimum of 10,000 records is about 22%. Given that costs can exceed $100 million, that's a risk worth preventing.

Hardware Limitations & Lock-Ins

Traditional network infrastructure has limited IT's ability to adapt and innovate in our increasingly dynamic and digital world. Workloads, even those virtualized in VMs, are tethered to physical hardware and topologies, limiting their mobility. The closed black box approach to networking – with custom OS, ASIC, CLI, and management – has further locked enterprises into incumbent hardware.

Traditional network hardware severely slows the provisioning process and limits workload placement and portability. One study found that 90% of companies are disadvantaged by the complexities of their networks – impacting when, where, and what applications and services can be deployed. On average IT makes ten changes to the corporate network in a 12-month period that require a maintenance window. The average wait for maintenance windows is 27 days each. Businesses, therefore, spend a total of 270 days or 9.6 months a year waiting for IT to deliver a new or improved service. Larger enterprises require significantly more of these changes and wait longer for maintenance windows. Of the companies surveyed, 45% report that employee productivity is adversely impacted, and 42% report business analysis is negatively affected.[7]

Error-Prone Manual Configuration

Physical networks force network administrators to perform a lot of repetitive, manual tasks on a daily basis. If a line of business or department requests a new application or service; for example, administrators need to create VLANs, map VLANs across switches and uplinks, create port groups, update service profiles, and a number of other tasks. On top of this, the configuration is often done via clunky CLIs.

Manual configuration of network infrastructure is prone to error. In fact, manual errors are the main cause of outages. Studies consistently find the largest percentage of network incidents – in the realm of 20%[8] to 32%[9] – is due to human/configuration errors. One mistake can cause a critical connectivity issue or outage that impacts business. The financial effect of an unplanned data center outage is significant. The average reported incident length is 86 minutes at a cost of $7,900 per minute. The average overall cost per incident is approximately $690,200.[10]

In terms of reach, 82% of companies experience network downtime caused by IT personnel making configuration errors. Of these, 94% reported bearing some type of loss to the business. With 80% suffering revenue losses, and 49% employee productivity loses.[11]

VMware Solution

NSX: Network Virtualization & Security for SDDCs

Leading enterprises use VMware NSX as an essential pillar of their SDDCs. These organizations view NSX as a strategic platform that addresses an extraordinary number of IT challenges and business initiatives.

NSX delivers the operational model of a VM for the network. Like server VMs, network services are programmatically provisioned and managed in software, independent of the underlying hardware and topology. NSX frees enterprises from the bonds of traditional network infrastructure.

NSX creates and provisions complex multi-tier networks in seconds - with consistent configuration and security. All of the networking elements and services – logical switches, routers, firewalls, load balancers, VPN, and workload security – inside the hypervisor.

Virtual networks use the underlying physical network as a simple IP forwarding backplane. Think of a traditional network chassis that has a backplane with sockets. Line cards connect directly to the backplane. No one makes configuration changes to the chassis backplane; it simply forwards packets between line cards. In a virtualized network, the hypervisor is like the line card and the physical network is like the backplane.

Ground-Breaking Use Cases

Enterprises are using NSX to deliver a multitude of new use cases and high-value IT outcomes – not previously possible with traditional network infrastructure. IT is also performing existing operations orders of magnitude faster and at lower cost. Enterprises can often justify the cost of NSX through a single use case. At the same time, they establish a strategic platform that automates IT and drives several additional use cases over time. Following is a discussion of the top use cases that VMware customers have in production deployments today.

Micro-Segmentation

The leading use of the NSX platform today is micro-segmentation, which dramatically transforms network security inside the data center perimeter. If a threat gets inside the network, NSX contains and blocks its lateral movement to other servers, which dramatically reduces the attack surface and risk to the business. Customers are using micro-segmentation to solve a significant problem that was operationally infeasible with traditional firewalls, and have reported doing so at approximately one-third the cost.

Micro-segmentation provides control and visibility for workloads in virtualized networks. Security is shrink-wrapped around each workload. Firewall rules are enforced at the vNIC level of each VM. In effect, this creates a separate “micro trust zone” for each workload.

NSX automatically assigns the appropriate security group and policy based on virtualization relevant context, rather than just physical topology. NSX can also dynamically change the security group and policy based on changing context, including context provided from a third party, such as a malware or vulnerability assessment solution.

NSX offers new ways of grouping VMs and applying security policy. For example, it can secure workloads based on application types, network constructs, and/or infrastructure topologies. Security policy is no longer constrained to a single distributed virtual switch or port group.

Security policies are orchestrated centrally, which reduces rule sprawl, and ensures that security is accurately and consistently applied. Further, when a VM is provisioned, moved, or deleted – its firewall rules are also added, moved, or deleted. These changes happen automatically, with no human intervention. This new level of automation dramatically reduces the operational complexity and expense of managing security policies across workloads.

With NSX, micro-segmentation is delivered through the kernel hypervisor. Each hypervisor delivers 20 Gbps of firewall throughput. The distributed nature of the firewalling provides a rapid scale-out architecture. Firewalling capacity automatically increases as additional hosts are added to the data center.

Advanced security capabilities, such as threat prevention and malware protection, are available through API-level integrations with Palo Alto Networks, Intel Security, Trend Micro, and dozens of other VMware NSX partners.

Disaster Recovery

Enterprises are using NSX as a complement to their existing disaster recovery (DR) solutions. NSX is helping them to reduce their recovery time objective (RTO) by upwards of 80%, considerably minimizing downtime and cost to the business.

Enterprises use NSX to replicate the entire network and its security environment. They periodically snapshot the network construct, along with its applications and services, and maintain it at a recover site. IT does not need to change IP addresses because the virtual network construct is decoupled from the underlying hardware and topology. The disaster recovery site is identical to the primary site, with no tradeoffs in functionality or performance. The copy sits at the recovery site in standby mode for push-button activation in the event of a disaster. Any changes made to the source network are automatically replicated to the copy at the recovery site.

Self-Service R&D Clouds

Enterprises are using NSX as their platform of choice for delivering self-service R&D clouds and other Infrastructure-as-a-Service (IaaS) initiatives. With NSX, provisioning network infrastructure is no longer a bottleneck that impacts business velocity and time to market.

NSX provisions thousands of isolated networks for development, test, and staging environments – all on the same physical infrastructure. NSX removes the manual tasks and cycle time associated with procuring, installing, and configuring traditional network infrastructure. Networks are deployed in lockstep with their workloads – as a fully audited self-service transaction. Applications quickly move through development, test, staging, and production without changes to their IP addresses.

Cloud Application Portability & Data Center Migration

NSX untethers applications and services from the physical network infrastructure, making networks as portable as VMs. With NSX, networks are virtualized in the same software switch attached to the VM. When a workload is moved (e.g., VMware vSphere® vMotion®), its network and security services automatically move with it.

Enterprises use NSX to seamlessly migrate applications from one host to another, or from one data center to another. Real world use cases include moving an application to leverage capacity at another location, complying with data residency laws, migrating to a new data center, or performing maintenance / refresh of the physical infrastructure.

Traditionally, physical network topologies and address space required IT to change IP addresses when applications were moved. In some cases, IP addresses are hardcoded into applications, which is even more costly because code changes and regression testing are required. With NSX, enterprises have the freedom to rapidly move applications without re-IPing them. These conveniences significantly reduce operational cost and improve IT agility and responsiveness.

IT Automation & Orchestration

NSX provides the operational model of a VM for networks. IT uses NSX to streamline provisioning of network services from weeks to seconds. This removes the manual effort and cycle times associated with procuring, installing, and configuring traditional network hardware.

NSX's powerful orchestration capabilities programmatically distribute network services in lock step with virtual machines. Enterprises use NSX to standardize and maintain pre-defined templates that consist of the network topologies and services. For example, a network engineer creates a template for a multi-tier application for development purposes. The environment can be provisioned to an application developer in seconds via self-service. The same can be done for QA, staging, and production environments – across multiple applications and services – with consistent configuration and security. NSX's automation capabilities reduce operational expense, accelerate time-to-market, and speed IT service delivery.

NSX also streamlines operations by consolidating configuration state and instrumentation data for all network connections – both virtual and physical. Administrators have complete operational visibility into what's occurring across the entire network infrastructure. This simplifies traffic management, monitoring, troubleshooting, and remediation.

Infrastructure Optimization & Refresh

Enterprises are using NSX to bridge and simplify data centers without disruption. NSX works with traditional multi-tier tree-type architectures and flatter next-generation fabric architectures. The result is a common platform with the same logical networking, security, and management model. Enterprises are using NSX for a number of optimization and consolidation scenarios. For example, integrating information systems following mergers and acquisitions, maximizing hardware sharing across tenants in multi-tenant clouds, and accessing islands of unused compute capacity.

If it were up to incumbent network vendors, enterprises would continue to rip-and-replace their gear every few years with increasingly expensive hardware. Fortunately, this path is no longer your only option. NSX unlocks more compelling economics and choice. Enterprises now have flexibility regarding when and how they refresh their network infrastructure. With NSX, all that is needed to deploy a SDDC is your existing physical network infrastructure.

Business Value

Functional Benefits: Speed, Agility, Security & Reliability

Minimizes Risk & Impact of Data Breaches

Leading enterprises are using micro-segmentation enabled by NSX to significantly minimize the attack surface and cost of a breach. They use micro-segmentation to isolate each workload with its own security policy, which contains threats and blocks lateral movement. With micro-segmentation threats are not able to infiltrate other applications and exfiltrate data to the outside.

Micro-segmentation helps to avoid or minimize the costs of a data breach, including engaging forensic experts, in-house investigations, loss of customers from turnover or diminished acquisition rates, providing free credit or identity monitoring subscriptions, customer communications and outsourcing hotline support, and many other costs. As noted earlier, these costs can range from several million to more than one hundred million dollars for a single data breach incident.

Speeds IT Service Delivery & Time to Market

Just as VMware server virtualization transformed the operational model of computing – VMware NSX has transformed networking. Enterprises are using NSX to provision networking with the same agility, speed, and control as VMs for computing.

With VMware, enterprises provision cloud-native or traditional applications, with full compute, storage, and network services in seconds. With NSX, application teams have full self-service provisioning. No more do they need to wait days or weeks for hardware to be procured and the network setup. Further, NSX's automation and orchestration capabilities eliminate the risk of manual configuration errors.

NSX significantly shortens the time it takes for engineering to bring new revenue-generating applications and services to market. This new level of speed and agility fuels rapid innovation and competitive advantage.

Simplifies Network Traffic Flows

The volume of server-to-server traffic generated by modern applications inside the data center continues to grow. Customers are using NSX to lessen the load of East-West traffic on the oversubscribed core. With a virtual network, VMs communicate to one another through the vSwitch or aggregation fabric. This significantly reduces East-West traffic hops, and avoids hair-pinning and core link oversubscription from convoluted traffic patterns. With NSX, enterprises avoid the expense of building up core capacity with more hardware.

Increases Service Availability

Cloud-scale data centers have few outages. Not because they have expensive, redundant high availability. But because they have flatter fabrics with equal-cost multi-path (ECMP) routing between any points on the network, rather than a collection of hierarchical hardware clusters. Simplified leaf-spine fabrics make individual links or devices inconsequential. The network can withstand multiple simultaneous device failures with no outage.

Enterprises use NSX above these fabric architectures and achieve the same high availability as cloud-scale service providers, such as Facebook, Google, and Amazon.

Improves Negotiation & Buying Leverage

Many NSX enterprise customers have continued to use their existing networking hardware. But when they refresh they now have increased negotiation and buying leverage. With NSX in place the higher value network functionality and features are delivered inside the virtualization layer. The physical infrastructure has become commoditized. Enterprises are using this market dynamic to drive down price when refreshing their network hardware with incumbent vendors.

Optimizes Use of Network Engineers

Just as virtualization transformed and simplified work for server administrators, it is now doing the same for network engineers. Network engineers appreciate NSX because they can focus more of their time on strategic initiatives that contribute to the bottom line of the business. Teams that have deployed NSX now spend more of their time on network design-level considerations. Rather than doing mundane tactical change management, network administrations are designing next-generation network fabrics and implementing software defined data centers. They are focusing on ways to make the network more resilient, scalable, and manageable.

Developing expertise in SDDCs and network virtualization is equipping network administrators and architects with the professional skills and knowledge required to succeed now and in the future.

Economic Benefits: Numerous CapEx & OpEx Savings

Micro-Segmentation CapEx Savings

Traditionally, deploying firewalls to control an increasing volume of East-West traffic inside the data center has been cost prohibitive for many enterprises. Additionally, the sheer number of devices needed and the effort required to setup and manage a complex matrix of firewall rules has made this approach operationally infeasible.

In addition to making micro-segmentation simpler and more secure – VMware NSX delivers significant CapEx and OpEx reductions for this specific use case. Looking at the capital expense alone, NSX enables enterprises to save upwards of 70% over purchasing physical firewalls for micro-segmentation. Following is an analysis of the CapEx savings for a typical enterprise that wants to use micro-segmentation for improved control of server-to-server traffic inside the data center.

Environment & Capacity	
Number of VMs	2,500
VMs per CPU	5
CPUs per server	2
Servers	250
% of VMs requiring FW controls	40%
Gbps - Average Application thoughput per host	7
Gbps - Required Firewall throughput in Gbps for all VMs	1,750
Gbps - Effective Required Firewall Throughput	700
Firewalls (20Gbps each x2 for HA)	70
Cost for Hardware	
List cost of each 20Gbps FW	$135,000
Total Hardware Firewall Cost (But Operationaly Infeasible)	$9,450,000
Cost for NSX	
NSX List Cost per CPU	*$5,995*
NSX Total Cost	*$2,997,500*
CapEx Savings with NSX	**$6,452,500**
	68%

IT Automation OpEx Reductions

Let's take a look at how enterprises are using NSX to realize significant operational cost reductions. NSX dramatically reduces the manual effort and cycle time for networking tasks, including provisioning, change/adaptation, scaling, and troubleshooting/remediation. (Cycle time accounts for delays due to requests, approvals, coordination, handoffs, logistics, downtime windows, etc.)

Network virtualization and simplified leaf/spine fabrics significantly reduce the effort and time it takes to complete network tasks. Generally, NSX reduces the effort from hours to minutes, and the cycle times from days to minutes. If you consider all of the manual tasks required to provision and manage a physical network – across development, testing, staging, and production environments – and the fact that NSX automates these, you begin to see all of the opportunities for reducing operational costs.

As the following OpEx analysis shows, NSX dramatically speeds the initial provisioning of a network into production. With traditional hardware, the associated cycle time to provision a network for a new application forces enterprises to wait 23 days. NSX reduces that to minutes – nearly a 100% reduction and massive time-to-market win. Likewise, provisioning a network for a new application takes 14 person hours or close to two days of person effort. NSX reduces that to less than 2 person hours – a substantial 87% reduction.

	Task Effort (Hours)		Cycle Time (Days)	
	Manual	**Automated - NSX**	**Manual**	**Automated - NSX**
Request & Review Network & Security Resources	1.00	0.00	1	0
Define Network & Security Environment	4.50	1.00	3	0
Determine Changes Required (Capacity Availability)	4.50	0.00	3	0
Review & Approval Process (Change Approval Board)	0.50	0.50	5	0
Change Order Scheduling	0.50	0.00	5	0
Configure the Network (VLAN, Routing)	1.00	0.00	2	0
Configure the Security (Firewall)	1.00	0.00	2	0
Configure the Load Balancer	1.00	0.00	2	0
Provision the Environment	0.30	0.30	0	0
Total	14.30	1.80	23	0
OpEx Savings with NSX	**12.50 Hours**		**23 Days**	
	87%		**100%**	

Server Asset Utilization CapEx Savings

Enterprises are also using NSX to access islands of unused compute capacity inside the data center. In traditional topologies each network cluster has its own compute capacity. IT often over provisions compute because the network re-configuration required to reach available capacity in another cluster takes too long and is prone to error. By many measures, 60% or more of a network's total compute capacity remains dormant, which is a waste of resources. Enterprises are using NSX to bridge two or more network clusters and deploy workloads to this unused capacity. As a result, they are saving upwards of 88% by using existing server capacity rather than purchasing new physical servers. The following CapEx analysis shows how much enterprise save in annual server expenses by leveraging NSX to use more of its existing compute capacity:

Environment	
Servers	250
Operational VMs	1,000
Current Effective Server Consolidation Ratio	4:1
Design Consolidation Ratio / VMs per host (determined by application performance requirements)	10:1
Annual VM growth rate	30%
VMs per year	300
Compute Asset Utilization	
Current Compute Asset Utilization	40%
Effective Utilized Server Capacity	100
Effective Dark Server Capacity (60% over-provisioned)	150
Target Compute Asset Utilization	85%
Operational VMs with current host capacity at TARGET asset utilization	2,125
Target Effective Server Consolidation Ratio	8.5:1
Effective Utilized Server Capacity at TARGET asset utilization	213
Effective Dark Server Capacity at TARGET asset utilization (15% over-provisioned)	37
Cost Without NSX	
Average Host Cost	$12,000
Annual Server cost (75 servers per year) to support growth at current compute asset utilization	$900,000
5 year server cost to support growth rate at current compute asset utilization	$4,500,000
Cost With NSX	
Years of planned annual growth, without adding host capacity	3.75
5 year server cost (total 45 servers) to support growth at TARGET asset utilization rate	$540,000
5-Year CapEx Savings with NSX	**$3,960,000**
	88%
5 year NSX Cost	**$3,995,000**
Assuming 2 CPU/server and $3,995/CPU List Price + 4 years SnS at 25%	
5 year ROI	**99%**

Price / Performance CapEx Savings

Some enterprises using NSX have gone from traditional three-tier designs (access / aggregation / core) with fixed Layer 2 boxes to two-tier (leaf / spine) designs based on Layer 3 fabrics optimized for East-West traffic. In these fabrics, the Layer 2 adjacencies, logical switching, and routing are handled by NSX. Many enterprises are replacing their proprietary hardware with lower cost infrastructure that can be procured from multiple sources for the best price / performance characteristics. Those who have gone with bare metal switches with a Linux OS installed are realizing 66% CapEx savings compared to incumbent gear.

	Cost Per Switch	# of New Switches	Total
Traditional Switch	$18,400	25	$460,000
Bare Metal Switch	$6,300	25	$157,500
	CapEx Savings with NSX		**$302,500**
			66%

Tip: Virtualize First

VMware recommends that enterprises virtualize first when they need to add network capacity. Enterprises have found that by virtualizing their workloads they can reduce the number of physical ports needed by upwards of 60%, resulting in significant CapEx savings.

Hardware Lifecycle CapEx Savings

Enterprises are using NSX to extract significantly more value from their existing network infrastructure. NSX offloads an increasing volume of East-West traffic from the network core, and extends its lifespan without having to add expensive capacity. Further, with NSX, the underlying network hardware becomes a simple IP forwarding backplane. Rather than refresh their existing networking gear at the end of accounting's depreciation cycle, enterprises are choosing to use it for longer periods of time. With this approach they only touch the hardware to add more capacity or to replace individual devices when they fail.

Enterprises not only avoid the CapEx for the hardware but also the OpEx of doing a rip-and-replace migration. Enterprises are using this strategy to free up millions of dollars from their budgets - often with upwards of 80% savings. Following is a CapEx savings analysis for an enterprise that uses its existing networking gear for a longer period of time:

Traditional Refresh Cycle

Amortization of 5 years, but refresh after 3 years.

	Year 1	Year 2	Year 3	Year 4 - Refresh	Year 5	Year 6	Year 7	Year 8 - Refresh	Total Cost Over 8 Years
Network Switches									
New	10	1.50	1.73	11.98	2.28	2.62	3.02	14.97	48
Cost	$180,000	$27,000	$31,050	$215,708	$41,064	$47,223	$54,307	$269,453	$865,804
Load Balancers									
New	15	2.25	2.59	17.98	3.42	3.94	4.53	22.45	72
Cost	$450,000	$67,500	$77,625	$539,269	$102,659	$118,058	$135,767	$673,632	$2,164,509
Firewalls									
New	30	4.50	5.18	35.95	6.84	7.87	9.05	44.91	144
Cost	$4,050,000	$607,500	$698,625	$4,853,419	$923,932	$1,062,521	$1,221,899	$6,062,684	$19,480,581
Total	$4,680,000	$702,000	$807,300	**$5,608,395**	$1,067,654	$1,227,802	$1,411,973	**$7,005,769**	**$22,510,893**

Extended Lifecycle with NSX

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7	Year 8	Total Cost Over 8 Years
Network Switches									
New	10	1.50	1.73	1.98	2.28	2.62	3.02	3.47	27
Cost	$180,000	$27,000	$31,050	$35,708	$41,064	$47,223	$54,307	$62,453	$478,804
Load Balancers									
New	15	2.25	2.59	2.98	3.42	3.94	4.53	5.20	40
Cost	$450,000	$67,500	$77,625	$89,269	$102,659	$118,058	$135,767	$156,132	$1,197,009
Firewalls									
New	30	4.50	5.18	5.95	6.84	7.87	9.05	10.41	80
Cost	$4,050,000	$607,500	$698,625	$803,419	$923,932	$1,062,521	$1,221,899	$1,405,184	$10,773,081
Total	$4,680,000	$702,000	$807,300	**$928,395**	$1,067,654	$1,227,802	$1,411,973	**$1,623,769**	**$12,448,893**
CapEx Savings with NSX				**$4,680,000**				**$5,382,000**	**$10,062,000**
				83%				**77%**	**45%**

Assumptions

Annual Growth Rate:	10%	Network Switch:	$18,000
Annual Failure Rate:	5%	Load Balancer:	$30,000
		Firewalls:	$135,000

Conclusion

Transformative Benefits & Non-Disruptive Deployment

VMware NSX has brought about a massive tectonic shift never before seen in networking – just as VMware did for compute virtualization. NSX transforms the status quo of traditional networking, and unleashes the full potential of the SDDC.

Enterprises of all sizes and across a variety of industries are using NSX to break free of the constraints and limitations of the hardware-based data center, and unlock a multitude of high-value IT outcomes. They are realizing significant benefits – including improved security, on-demand IT service delivery, faster time-to-market, new competitive differentiation, and substantial CapEx and OpEx savings.

Enterprises are using NSX for multiple use cases not previously possible with traditional data center infrastructure. As they deploy more use cases and leverage more platform capabilities, the value received increases substantially over time.

Getting Started

Join the ranks of VMware's leading enterprise customers using NSX as a strategic pillar for their SDDCs. As you've seen, enterprises are using NSX to deliver several high-value use cases. Many enterprise customers have started with micro-segmentation to secure sensitive workloads that handle PCI or PII data. After they've seen the power, they expand micro-segmentation across all workloads in their data center. After micro-segmentation is fully deployed, enterprises use the NSX platform to address a second use case, such as IT Automation, Self-Service R&D Clouds, or one of the many others we've discussed.

Ask your VMware representative or partner to demonstrate the power of NSX. Let them know which use cases and capabilities you would like to see.

References

[1] Transforming the Datacenter with VMware's Software-Defined Data Center vCloud Suite. Taneja Group.

[2] Cloud Computing Trends: 2015 State of the Cloud Survey. RightScale.

[3] 2014 Data Breach Investigation Report. Verizon.

[4] 2014 Cost of Data Breach Study: Global Analysis. Ponemon Institute.

[5] Privacy Rights Clearinghouse.

[6] Sony Breach Could Cost $100 million. Wall Street Journal.

[7] Network Agility Research 2014. Dynamic Markets.

[8] Network Agility Research 2014. Dynamic Markets.

[9] 2014 Network Barometer Report. Dimension Data.

[10] 2013 Cost of Data Center Outages. Ponemon Institute

[11] Network Agility Research 2014. Dynamic Markets.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com

 Item No: VMW7654-WP-NETWK-VIRT-SECTY-NSX-USLET-101 05/15