

Sponsored by: **VMware****Authors:**Brad Casemore
Matthew Marden

May 2019

Business Value Highlights**39% faster**
to respond to network problems**38% less**
unplanned downtime**48% more**
efficient IT networking staff**81% less**
staff time to support self-service requests**42% faster**
faster deployment of new network firewalls**9% higher**
developer productivity

Business Value of Software-First Networking with VMware NSX

EXECUTIVE SUMMARY

As enterprises worldwide pursue digital transformation and make software a strategic emphasis for competitive differentiation and a key enabler of business outcomes, the datacenter network must be similarly modernized and transformed through a software-first approach to network architecture, provisioning, and day-to-day management.

IDC spoke with organizations that have deployed VMware NSX as part of their efforts to implement a software-first approach to their datacenter networking infrastructures. Study participants reported making substantial gains in network security, performance, and agility with NSX. Further, interviewed VMware customers leverage virtualization, policy-based network automation, and microsegmentation with NSX to enable more efficient networking operations and capture cost efficiencies. Overall, they described positioning their networks to better support their businesses in terms of both network performance and costs in the following ways:

- » **Improving network security and performance** through microsegmentation, more robust disaster recovery (DR) operations, and lower latency
- » **Increasing network agility** through automated provisioning of network resources, including giving self-service capabilities for more users that improve business responsiveness
- » **Reducing the burden on IT networking teams** related to day-to-day operations, such as monitoring and responding to network problems
- » **Optimizing network costs** by increasing virtualization levels and allowing for cost-effective network expansion

SITUATION OVERVIEW

Given the demands of digital transformation and the rise of cloud operating models, the datacenter network has been compelled to adapt to the needs of the fast-changing and increasingly valuable application environments that it supports.

As virtualization proliferated — now followed by containers and microservices — its implications reverberated throughout the datacenter. It is universally acknowledged that traditional hardware-centric datacenter network architectures and operational practices were suited to relatively static client/server applications residing on physical servers, characterized by single tenancy and predictable north-south traffic patterns. It has become equally clear that these hardware-defined approaches to datacenter networking are unable to accommodate more dynamic virtualized and containerized applications, with their prodigious east-west (server-to-server and rack-to-rack) traffic flows and inherent elasticity.

While virtualization exposed the limitations of traditional hardware-centric networks, cloud operating models have made those limitations untenable. It is in this context that one can fully appreciate a software-first approach to networking that invests the network, architecturally and operationally, with the automated agility, flexibility, and simplicity that are essential for organizations to truly move at the speed of software. To be sure, software helps the datacenter network become an integral enabler of business outcomes rather than a siloed cost center, in software-first alignment with other facets of datacenter infrastructure as code as well as with the applications that the network supports and delivers.

VMWARE NSX AND SOFTWARE-DEFINED NETWORKING

For a long time, datacenter networks were the proverbial long poles in the tent, traditional holdovers that resisted the relentless wave of virtualization and automation. But no datacenter network is an island. It is inextricably and literally connected to datacenter compute and storage, and if the network is not significantly modernized along with the rest of the datacenter infrastructure, it becomes an encumbrance and an inhibitor to organizational agility and efficiency.

Therefore, datacenter networking has experienced a sustained burst of software-driven innovation during the past few years. Not coincidentally, the datacenter is going through a period of significant disruption as tried-and-true three-tier architectures and manual operational practices are displaced by flatter leaf-spine networks and extensive network automation including network virtualization and software-defined networking (SDN).

VMware NSX provides a network virtualization overlay (NVO) that belongs to a broader category of datacenter SDN. VMware positions NSX as a network virtualization and datacenter security platform for the software-defined datacenter (SDDC), “delivering the operational model of a virtual machine (VM) for the entire network.” With NSX, network functions (such as switching, routing, and firewalling) reside in the hypervisor and are distributed throughout the application environment. The resulting virtual network is provisioned programmatically, through logical abstractions, in a software services-only layer, and it is managed separately from the underlying physical network.

NSX is designed to enable datacenter operators to achieve network agility and security, the latter obtained through microsegmentation. NSX’s virtual network services can be provisioned through cloud management platforms using NSX APIs and deployed atop existing physical network fabrics.

A prominent use case for NSX in enterprise datacenters is providing network security for the growing wave of east-west (server-to-server) application traffic. Through microsegmentation, NSX enables enterprise IT to logically segment and isolate workloads. As a result, IT teams leverage NSX microsegmentation to define security policies for individual workloads based on dynamic security groupings, ensure containment of threats inside the datacenter through security enforcement on individual VMs, and effectively thwart lateral threat propagation within the datacenter.

NSX provides network agility through automated network provisioning and configuration management, expediting the execution of traditional manual tasks that are labor intensive and error prone. Additional automation benefits can accrue from integration of NSX with cloud management platforms such as VMware’s vRealize or OpenStack.

While security and network agility represent principal use cases for NSX within most enterprise datacenters, application and business continuity is another highly relevant use case. NSX virtualized networks allow organizations to replicate application environments with remote datacenters for disaster recovery, move applications from one datacenter to another, and manage application deployment in hybrid cloud/multicloud environments. NSX’s ability to abstract network functions from underlying network hardware makes it possible to support a variety of application continuity scenarios without having to touch the physical network.

THE BUSINESS VALUE OF NSX AND SOFTWARE-FIRST NETWORKING

Study Demographics

IDC spoke with seven organizations about their experiences with VMware NSX in connection with taking a software-first approach to building and running their networks. Interviews were in-depth in nature and focused on both the qualitative and the quantitative impact for these organizations of using VMware NSX in terms of network performance, agility, staff time requirements, and costs.

Table 1 displays the demographics of the VMware customers involved in the study in terms of total number of employees, IT staff size, number of business applications in use, total revenue, and industry verticals. These VMware customers were relatively large, with an average employee size of more than 47,000 and annual revenue of \$27.4 billion (medians of 6,640 and \$300 million, respectively). These organizations were all based in the United States and provided the experiences of various industry verticals, including the education, healthcare, insurance, retail, and technology sectors.

TABLE 1

Demographics of Interviewed Organizations		
	Average	Median
Number of employees	47,729	6,640
Number of IT staff	4,415	100
Number of business applications	898	450
Revenue per year	\$27.4 billion	\$300 million
Industries	Healthcare, higher education (2), insurance, retail, technology, primary education	

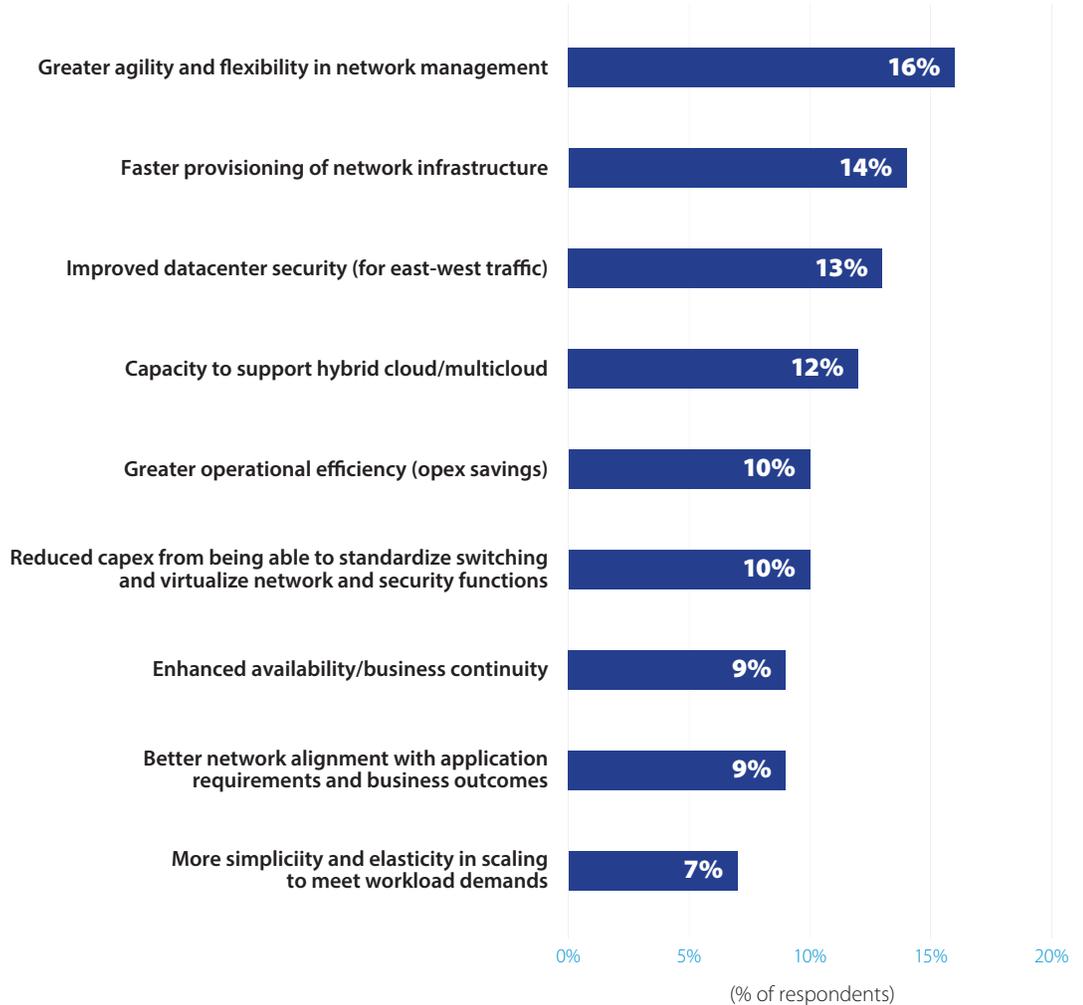
n = 7
Source: IDC, 2019

Use of VMware NSX for Software-Defined Networking

Study participants decided to deploy VMware NSX in the context of broader efforts to make their networks more responsive to business needs. For these organizations, that meant turning to software-defined practices and technologies to replace or supplement legacy technologies that too often were insufficiently robust and flexible. They described facing similar challenges in deploying networks that can keep pace with business requirements, including needing more robust network security capabilities, greater network agility, and network technologies that can be expanded cost effectively. A separate IDC survey (sponsored by VMware) of United States-based enterprise respondents confirmed that overcoming these challenges ranked among the top benefits that derive from SDN deployments in datacenter networks (see Figure 1).

FIGURE 1

Top Benefits of Datacenter SDN Deployments



n = 216

Note: This survey was sponsored by VMware and conducted by IDC.

Source: IDC's VMware Software-First Survey, September 2018

Interviewed organizations for this business value study tied their decision to deploy VMware NSX to their need to address these challenges as noted by the associated quotes:

- » **Security:** "Our main driver of going with a software-based approach with NSX was being able to microsegment our network. We looked at ways that could be accomplished without using a software-defined solution, but NSX was, by far, the best way to implement it."
- » **Agility:** "With the way that the market is changing in IT and our business need to be a lot more agile and resilient, we decided that using a software-based approach to networking with NSX would allow us to be more flexible and provide developers quicker access to resources so that they can in turn develop faster."
- » **Cost control:** "We had considered a hardware-based approach for the firewalls we needed, but the expense, the difficulty to implement, and the number of firewalls that we'd need made it really prohibitive."

At the time of the interviews, study participants were running significant volumes of network traffic on their software-defined networks that included use of VMware NSX. Most interviewed organizations had deployed VMware NSX for both a production and a disaster recovery datacenter environment to run 114 business applications on average (113 median). From a network hardware perspective, these networks counted an average of 71 network switches, 3,414 network ports, and 11 network firewalls (see Table 2).

TABLE 2

VMware NSX and Software-Defined Networking Environments		
	Average	Median
Number of datacenters	2	2
Number of sites	1,483	8
Number of internal users	41,897	931
Number of business applications	114	113
Number of network switches	71	50
Number of network ports	3,414	2,400
Number of physical firewall appliances	11	4

n = 7
Source: IDC, 2019

Quantifying the Business Value of Software-Driven Networking with VMware NSX

Study participants are realizing benefits in several areas through deployment of VMware NSX and by taking a software-first approach to networking. They have made their network environments more agile and responsive to business demand through use of automation and policy-based templates. Interviewed organizations' networks are in greater synergy with changing business requirements, in addition to being easier to manage and operate on a day-to-day basis. As discussed in this study, IDC has quantified benefits for these VMware customers in the following areas as being worth an average of \$2.17 million per interviewed organization per year (\$51,684 per 1,000 users):

- » **Reducing the cost and potential cost of operational risk** by enabling microsegmentation, improving disaster recovery operations, and ensuring higher network performance, with IDC quantifying the value of reduced impact of outages to users and the business as worth an average of \$184,000 per organization per year (\$4,329 per 1,000 users)
- » **Enabling more effective development efforts** by increasing network agility and offering self-service functionality to more development team members and other users, with IDC putting the value of higher developer productivity at an average of \$885,300 per year (\$21,131 per 1,000 users)
- » **Winning more business and increasing user productivity** by having the flexibility to better address more business opportunities and providing a better user experience, with IDC calculating that higher revenue and user productivity will be worth an average of \$306,100 per year (\$7,306 per 1,000 users)
- » **Making IT networking teams more efficient** by extending automation, templates, and policy across networking environments to reduce the volume of day-to-day work, with IDC estimating the value of IT staff time savings and productivity gains at an average of \$776,000 per year (\$18,521 per 1,000 users)
- » **Optimizing networking costs** by increasing levels of network virtualization and ensuring more effective use of existing network infrastructure capacity, with IDC projecting network-related cost savings to be worth an average of \$14,000 per organization per year (\$334 per 1,000 users)

Improved Network Security and Performance

Study participants reported substantially improving their networks' security and performance with a software-driven approach to networking based on VMware NSX. From the perspective of network security, interviewed organizations consistently cited having the ability to microsegment their networks with VMware NSX as among its most compelling functionalities. Almost all interviewed VMware customers chose VMware NSX to aid in the implementation of microsegmentation, linking the need to microsegment their networks to compliance, data protection, and other security requirements:

- » **Microsegmentation to support compliance:** *"Our primary initial use case for NSX was for microsegmenting our PCI network because when new regulations came out our systems were all on the same backbone network. Basically, we had to be able to break off any server that had the possibility of seeing credit card data from our production network traffic, and NSX made it really easy to break off those servers into their own segments."*
- » **Ensuring security through microsegmentation:** *"Microsegmentation with NSX is important to make sure that we're doing our best to ensure data protection by policing access privilege from a security standpoint. We need to make sure that we're able to protect assets within the company from a software-based standpoint as efficiently as possible."*

Beyond microsegmentation, study participants attributed running more effective and efficient disaster recovery environments to VMware NSX. They found it challenging to fluidly and consistently make the changes and configurations needed to their legacy networks to ensure that their primary and DR environments were calibrated. Automation and deeper segmentation with VMware NSX have allayed these challenges, with notably one interviewed organization explaining: *"Software-defined networking with NSX has definitely enhanced our disaster recovery position with the ability to extend our network and basically put our DR sites on the same segment. This minimizes the number of changes that need to be made if we do experience a failure and have to move our resources to our alternate site."*

Overall, these organizations have improved network performance with VMware NSX both through more robust disaster recovery operations and by optimizing use of network capacity through policy-driven traffic management. As a consequence, in addition to reducing operational risk related to data breaches and losses — which can be substantial as well as challenging to quantify — they are benefiting from reducing the frequency and duration of unplanned network outages. As shown in Table 3, this translates to fewer interruptions to core business operations and results in lower levels of productivity loss for users of applications (38% less productive time lost on average). In addition, study participants reported being able to respond in a more timely way to network problems (39% faster on average), further reducing the likelihood of experiencing major business-impacting events.

TABLE 3

Impact on Incident Response and Unplanned Downtime

	With Previous/ Other Network Environment	With VMware NSX	Difference	Change (%)
Time required to respond to network problem (hours)	2.3	1.4	0.9	39
Unplanned outages per year per organization	8.6	5.8	2.9	33
MTTR (hours)	1.4	1.1	0.3	21
Lost productive time per user per year (minutes)	18	11	7	38
Value of lost productive time per year in FTEs per organization	6.8	4.2	2.6	38

n = 7

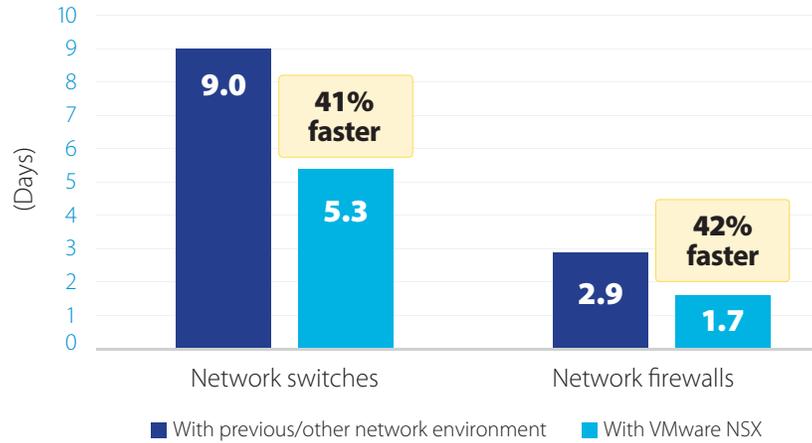
Source: IDC, 2019

Networking Agility, Self-Service, and Development Efficiencies

Study participants described leveraging VMware NSX and software-defined networking principles to increase their networks' agility. They explained that their legacy network environments struggled to provide the flexibility required to match the velocity of their business operations. As a result, their IT organizations often took too long to deploy new network equipment or provision IT resources in support of development and other business activities.

Figure 2 demonstrates the extent to which interviewed organizations have sped up deployment times for new switches and firewalls with VMware NSX, bringing down the time required by 41% and 42%, respectively. They attributed faster deployment to template-driven and automated processes that minimize manual touchpoints. One study participant described the gains it has seen in terms of adding switches to its network environment: *"The architecture we've put together with NSX and software-defined networking is much more consistent. We've been able to templatize a lot of our builds and that speeds deployment as we scale ... With NSX, we can now deploy a new switch in an hour compared with a couple of days with the previous architecture."*

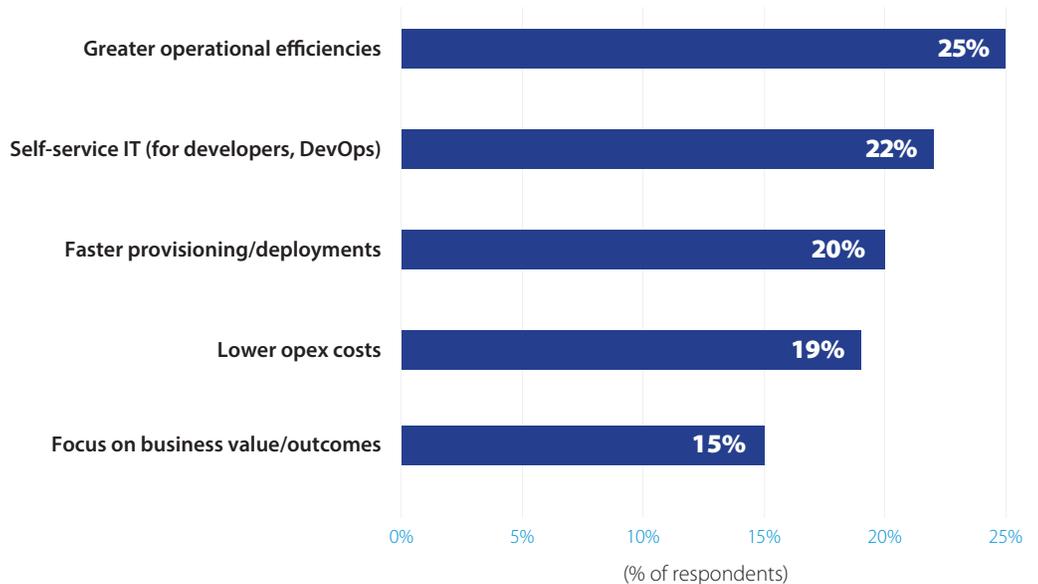
FIGURE 2
 Cost of Network Infrastructure per Organization



n = 7
 Source: IDC, 2019

Indeed, IDC found similar sentiments expressed in the separate survey of United States-based enterprise respondents referenced previously. When asked to cite the top benefits derived from implementation of network automation in the datacenter, respondents placed operational efficiencies at the top of the list, followed by self-service IT (for developers and DevOps teams) and faster provisioning and deployments (see Figure 3).

FIGURE 3
 Top Benefits of Datacenter Network Automation

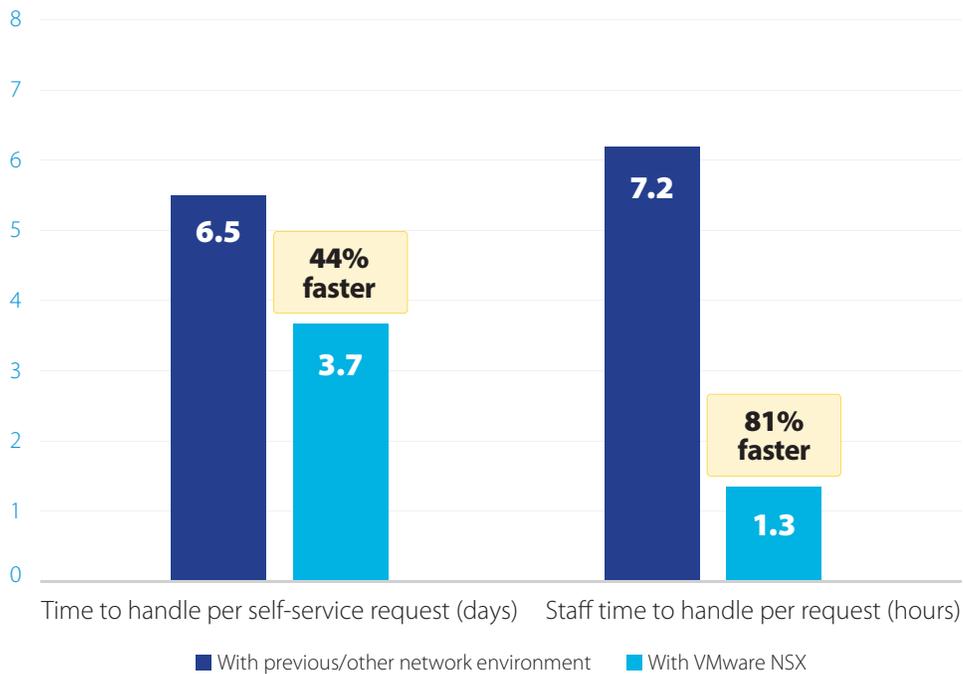


n = 216
 Note: This survey was sponsored by VMware and conducted by IDC.
 Source: IDC's VMware Software-First Survey, September 2018

Business value study participants have also made their networks more flexible and adaptable to business demand by offering greater use of self-service provisioning with VMware NSX. Self-service functionality is beneficial because it obviates friction points that legacy network infrastructures can impose on development and line-of-business teams by reducing their need to go to the IT department for network and other IT capacity. Thus teams making requests see faster fulfilment (44% faster) and IT networking teams spend substantially less time responding to such requests (81%) (see Figure 4).

FIGURE 4

Impact on Service Provisioning — Self-Service Use



n=7
Source: IDC, 2019

While various teams benefit from enhanced network agility and self-service functionality with VMware NSX, application development teams stand out as achieving compelling benefits. Development teams are increasingly called upon to deliver new applications and functionalities with greater frequency and at compressed intervals. As a result, developers require on-demand access to network and other IT resources, as well as robust network performance.

Study participants reported that taking a software-first approach to networking with VMware NSX has enabled their development teams and has sped up application development cycles (17% for new applications and 12% for new features). Overall, IDC calculates that development teams at interviewed organizations have improved their productivity levels by an average of 9%, which represents a significant increase in their value. One study participant commented on VMware NSX’s impact: *“Our development team is heavily impacted by NSX and software-defined networking. That’s the driver of going with software first for us. They save time when they are making service requests, which means that hundreds of developers are saving around 15% of their time.”*

Improved Business Operations Results

Study participants reported that moving to software-defined networking with VMware NSX has helped them ensure that their networks have the agility, flexibility, and performance needed to support their businesses. This has translated to improved business results and operational efficiencies in the form of higher employee productivity. Study participants provided examples of these types of impact:

- » **Business continuity:** *“NSX and having a software-defined network are important because we’re using them to be able to maintain our IP address space in between sites. It’s important for us to be able to run workloads both at our primary and disaster recovery sites, without having to reconfigure them or change them at all. They can technically float back and forth between the two places; in the event of a disaster recovery, you don’t have to worry about reconfiguring the applications.”*
- » **Improved competitive position through agility:** *“The most important benefit for the business of using NSX and taking a software-first approach to networking is to be as agile as possible and make changes as quickly as possible ... The way that we’ve increased our development speeds has reduced our development cycle with how fast our infrastructure can respond. It allows us to be more competitive.”*
- » **Delivering improved service levels:** *“We had a sudden need to load balance a whole bunch of applications almost overnight, because a client wanted us to, and we could do that with NSX. Another example is that we had a code push that was bad and knocked some servers offline, so we spun up others and managed to absorb the load until they could fix it — that was all done in a couple of hours with NSX.”*

Table 4 demonstrates the business-related results study participants have achieved with VMware NSX and a software-driven approach to networking. In addition to several hundred thousand dollars of additional revenue per year, almost 1,800 employees per organization have benefited from improved network performance, agility, and reliability, which translates to an almost 3% gross productivity gain for these employees.

TABLE 4

Business Productivity Benefits: Revenue and User Productivity Gains

	Per Organization	Per 1,000 Users
Higher revenue		
Additional revenue per year (\$)	300,000	7,333
Total recognized revenue per year (\$)	45,000	1,100
User productivity		
Number of users impacted	1,783	43
Gross productivity increase (%)	3	3

n = 7

Note: The IDC model assumes a 15% margin for recognizing user productivity and revenue gains.

Source: IDC, 2019

Networking Staff Efficiencies

VMware NSX has also helped study participants reduce staff time requirements for deploying, managing, and securing network environments. Study participants attributed these efficiencies to staff taking advantage of higher levels of virtualization and automation, as well as use of templates to perform network-related tasks. One organization spoke to how VMware NSX and software-based principles have simplified its network environment, thereby reducing the day-to-day burden on its IT networking team: *“Network virtualization with VMware NSX really brings intelligence very close to the application, which means that the underlying network is less complex. Because it’s less complex, it’s easier to troubleshoot and support because it’s more predictable.”*

Study participants reported achieving strong overall efficiencies for IT networking teams but noted an especially significant impact for security operations. They attributed staff time savings to VMware NSX as well as having the ability to provide much-needed functionalities such as microsegmentation that they could not have offered with their legacy network infrastructures:

- » **Efficiencies for security efforts:** *“Our team is saving a significant amount of time on firewalls — around half their time — because we’ve structured firewall management with NSX so that normal requests for changes are now automated with rules.”*
- » **Time-effective security and risk reduction:** *“NSX allows us to really segment off critical and sensitive portions of our environment... We’ve certainly made it a whole lot harder for a breach to occur with NSX. To do that work without NSX that would take more time — on an ongoing basis, we’re avoiding about one to two people.”*

Table 5 shows the overall impact of using VMware NSX and software-driven networking principles on IT networking teams. These teams are an average of 48% more efficient, highlighting the significant extent to which use of VMware NSX and software-defined networking technologies by these organizations have freed up staff capacity to take on new projects and support other initiatives.

TABLE 5

IT Networking Staff Impact				
	With Previous/ Other Network Environment	With VMware NSX	Difference	Change (%)
Equivalent time in FTEs per organization required to manage equivalent networking environments	12.1	6.3	5.8	48
Hours per 1,000 users per year	544	284	260	48

n = 7
Source: IDC, 2019

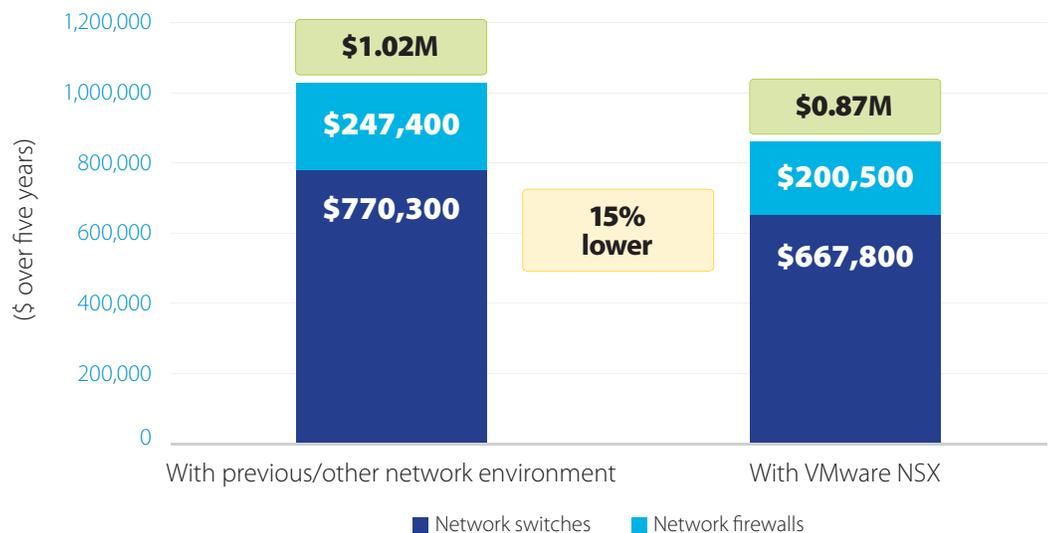
Networking Cost Efficiencies

Finally, study participants described optimizing their network environments with VMware NSX, allowing them to build and run more cost-effective networks. They have taken advantage of increased virtualization and automated segmentation to extend their networks while requiring less new network equipment. Several interviewed organizations detailed the benefits in terms of network spending:

- » **Cost-efficient network expansion:** *“As we expand our network and build out more segments, we don’t have to purchase the hardware to go along with that with SD networking and NSX. It’s just simple software changes to make those expansions.”*
- » **Cost-effective security:** *“SD networking and NSX have changed the way that we do security. Instead of having to deploy different types of hardware firewalls, we now have that ability to do microsegmentation close to the VM. This changes our future security footprint in terms of how we deploy rule sets to compute nodes.”*

As shown in Figure 5, IDC finds that study participants will incur costs related to network switch and firewall hardware that are an average of 15% lower with VMware NSX because they require fewer network switches and firewalls.

FIGURE 5
Cost of Network Infrastructure per Organization



n = 7
Source: IDC, 2019

CHALLENGES AND OPPORTUNITIES

Perhaps the most significant challenge for VMware and for many organizations that represent prospective NSX customers is the entrenched and long-established prevalence of traditional network architectures, practices, and operators that tend to be wary of change and gravitate toward the familiar and proven. Still, as this document has demonstrated both qualitatively and quantitatively, positive software-first change has come to the datacenter network, and even the most traditional of network operators cannot deny the considerable benefits and value that software-driven automation provides. Resisting the inevitable is never good practice, and network operators today are increasingly cognizant that the combination of infrastructure as code and cloud operating principles is an irreversible trend. There's only one way forward, but fortunately it offers substantially more rewards than risks.

There are competitive challenges, too, with other vendors offering software-first and software-defined networking products and technologies, but those are to be expected in any vibrant market. An additional challenge for VMware on this front is ensuring that NSX is perceived to be as relevant and valuable in the context of container-based microservices as it is for virtualized application environments.

As for the opportunities, they are compelling for VMware as well as for the organizations that adopt software-first networking as represented by NSX. The benefits and quantitative value that accrue from software-driven network automation are manifold, extending from day 0 through day 1 and beyond. Hardware will continue to provide a necessary foundation and substrate for datacenter networking, but increasingly, network operators will focus on the value that derives from the software that delivers the automated agility, efficiency, flexibility, and simplicity — all of which are essential to business outcomes within the strategic context of digital transformation.

CONCLUSION

Changing business and IT operational models, including digital transformation initiatives and the rise of cloud operating models, have put pressure on traditional approaches to datacenter networking. In short, organizations find it challenging to adapt to more dynamic virtualized and containerized application environments with hardware-based approaches to datacenter networking, and many struggle to meet demand from the business to meet ever-growing volumes of data traffic and support more agile business operations. While datacenter networks were slower than other areas of IT to adopt virtualization and software-driven innovation, the past several years has seen more organizations embracing disruption through the adoption of software-defined networking approaches and network virtualization initiatives. VMware NSX stands as a leading software-defined network virtualization and datacenter security platform to support efforts to move in the direction of software-driven datacenter networks.

This IDC study focused on efforts by organizations to take a software-first approach to datacenter networking through the use of VMware NSX. Study participants described realizing important gains in enabling their networks to better support their businesses in terms of security, performance, and agility. They explained that they have enabled their distributed business operations by making their networks more scalable and flexible and offered enhanced capabilities to developers and other business users through expanded access to self-service functionality. Further, they reported leveraging virtualization, policy-based network automation, and microsegmentation with NSX to make their networking

operations more efficient from a staff time and cost perspective. On the whole, IDC's findings show that the VMware customers interviewed for this study have made strides in ensuring that their datacenter networks can meet their current and future business needs in terms of performance, flexibility, and cost.

APPENDIX

IDC's standard ROI methodology was utilized for this project. This methodology is based on gathering data from organizations currently using VMware NSX as the foundation for the model. Based on interviews with these study participants, IDC has calculated the benefits and costs to these organizations of using VMware NSX.

IDC bases the Business Value calculations on a number of assumptions, which are summarized as follows:

- » Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For purposes of this analysis, based on the geographic locations of the interviewed organizations, IDC has used assumptions of an average fully loaded salary of \$100,000 per year for IT staff members and an average fully loaded salary of \$70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- » Downtime values are a product of the number of hours of downtime multiplied by the number of users affected.
- » The impact of unplanned downtime is quantified in terms of impaired end-user productivity and lost revenue.
- » Lost productivity is a product of downtime multiplied by burdened salary.
- » Because every hour of downtime does not equate to a lost hour of productivity or revenue generation, IDC attributes only a fraction of the result to savings. As part of our assessment, we asked each interviewed organization what fraction of downtime hours to use in calculating productivity savings and the reduction in lost revenue. IDC then taxes the revenue and user productivity gains at that rate.

Note: All numbers in this document may not be exact due to rounding.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.