A Forrester Total Economic Impact™ Study
Commissioned By
VMware

Project Director:
Henry Huang

April 2017

The Total Economic Impact™ Of VMware NSX

Cost Savings And Business Benefits Enabled By NSX

FORRESTER®

Table Of Contents

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

Executive Summary

VMware commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying NSX. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of network virtualization with NSX across the enterprise.

To better understand the benefits, costs, and risks associated with an NSX implementation, Forrester interviewed several customers with multiple years of experience using NSX. At these organizations, their networks are virtualized, with switching, routing, load balancing, and security posturing all defined with software. With these software-defined data centers running NSX, organizations gained the ability to quickly provision physical resources, optimize resource utilization, and provide security for internal network traffic.

VMware NSX is a network virtualization platform that can improve bottom-line results for organizations, by shoring up security and improving network management efficiencies across virtualized environments.

The financial assessment for a composite organization with 3,000 virtual machines, based on customer interviews, are:

- **Initial investment costs: $3.5 million.**
- **Average annual savings: $4.2 million.**
- **Three-year NPV: $5.4 million.**

Prior to deploying NSX, customers had delivered network resources through manual hardware provisioning, going through server hosts one by one. The inefficiency of this approach, however, left organizations unable to react quickly to provide the necessary resources in a timely manner. Scaling as well as security for internal network traffic, otherwise known as east-west traffic, were also clear deficiencies. Traditional network hierarchies that rely on standard perimeter defenses and reactionary patchwork internal security implementations are limited in protection for north-south data flows. Our research indicates that internal incidents are the most common source of data breaches.[1] Forrester's Zero Trust principle suggests that all data flow should be bound to some form of security policy, preferably in the form of micro-segmentation, and centrally manageable for system administrators.

Faced with the imperative to strengthen network security and be more agile, organizations have a few choices. One is to purchase additional network and security infrastructure. Another is to virtualize firewalls and implement micro-segmentation. Interviewed organizations that chose to virtualize their networks with NSX were able to save significant capital expenditure on infrastructure and security appliances, reduce operational expenditures, and improve consistent network performance, all while improving the security of internal data flows — some of which were highly regulated. Said one senior manager of enterprise cloud infrastructure, "NSX is a part of our core strategic strategy in rationalizing our infrastructure and reducing costs. We have already begun to see returns and expect it to continue delivering value going into the future."

VMWARE NSX OPTIMIZES NETWORK RESOURCES TO PROVIDE MORE WITH LESS RESOURCES

Our interviews with four existing customers and subsequent financial analysis found that a composite organization based on these interviewed organizations experienced the risk-adjusted ROI, benefits, and costs shown in Figure 1.[2]

FIGURE 1
Financial Summary Showing Three-Year Risk-Adjusted Results

ROI: 88%

Net present value (NPV): $5,382,692

Security capex savings: $6,471,480

Resource optimization with NSX: ▼ 37% hosts required

Source: Forrester Research, Inc.

- **Benefits.** The composite organization experienced the following risk-adjusted benefits that represent those experienced by the interviewed companies:

  - **Organizations looking to leverage their existing infrastructure while growing will find that NSX decreases the need for additional host server, infrastructure, and security hardware, saving $7.4 million over three years, present value (PV).** As organizations scaled on the NSX framework, they found that scaling to provide adequate compute resources for end users grew at a significantly lower rate than that of traditional networks. By improving load balancing and defining the networks by software, the composite organization was able to optimize resource utilization and avoid the hardware purchases that would have been required to achieve the throughput and security enabled by NSX. The composite organization saved $6.4 million in security hardware and $3.3 million in other hardware.

  - **Operational cost avoidance of maintaining hardware and avoiding hardware purchases yielded slightly over $1 million over three years.** Over time, the composite organization was able to scale down existing infrastructure and avoid significant hardware purchases required by business needs. Maintenance, in the form of patching, updating, administering, and reposturing security, was greatly reduced over the three-year period.

  - **System/network administration time decreased with the use of NSX, primarily from IT and security automation, saving $1.2 million over three years.** By provisioning networks virtually, using automated scripts and policies for individual network orientations, the composite organization benefited from how its administrator deployed services. Application workload provisioning, network management, and security posturing were streamlined into easier processes that were scalable, saving over 6,000 hours of administration time per year on average.

  - **End users benefited from more stable and predictable environments — especially in cases where virtualized environments were inadequate in the previous state without NSX, leading to a gain of $1.6 million over three years.** As infrastructure and use cases became more complicated, network administrators found complications in providing the right level of compute performance and availability to end users. At times, end users would experience a lack of availability or performance degradation due to the inability for admins and load balancers to change and provide resources in a timely fashion.

- **Costs.** The composite organization experienced the following risk-adjusted costs:

  - **Software licensing and support fees amounted to $5.8 million over three years.** These costs are both one-time and ongoing, reflecting perpetual socket licenses (along with additional growth in hosts) as well as yearly support and service associated with these licenses.

  - **Deployment and training costs amounted to over $275,616, primarily in the initial deployment phase.** Organizations cited a ramp-up phase of roughly two to three months for network and system administrators to acclimate to the NSX platform. They were helped greatly by professional services available from VMware and partners to promote best practices and a simplified transitionary phase.

Disclosures

The reader should be aware of the following:

- The study is commissioned by VMware and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.
- Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in VMware/NSX.
- VMware reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.
- VMware provided the customer names for the interviews but did not participate in the interviews.

TEI Framework And Methodology

INTRODUCTION

From the information provided in the interviews, Forrester has constructed a Total Economic Impact (TEI) framework for those organizations considering implementing VMware/NSX. The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision, to help organizations understand how to take advantage of specific benefits, reduce costs, and improve the overall business goals of winning, serving, and retaining customers.

APPROACH AND METHODOLOGY

Forrester took a multistep approach to evaluate the impact that VMware/NSX can have on an organization (see Figure 2). Specifically, we:

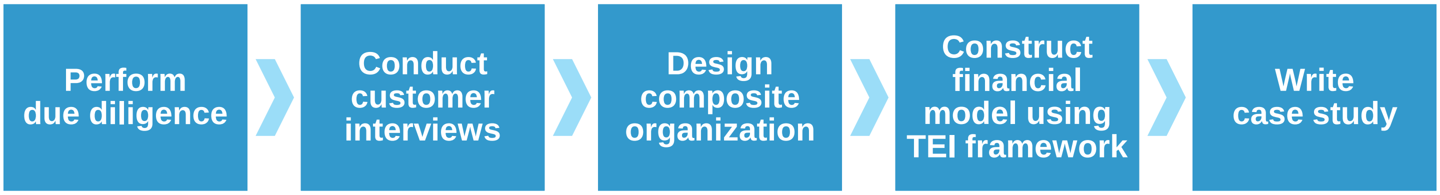
- Interviewed VMware marketing, sales, and/or consulting personnel, along with Forrester analysts, to gather data relative to NSX and the marketplace for NSX.
- Interviewed four organizations currently using VMware/NSX to obtain data with respect to costs, benefits, and risks.
- Designed a composite organization based on characteristics of the interviewed organizations.
- Constructed a financial model representative of the interviews using the TEI methodology. The financial model is populated with the cost and benefit data obtained from the interviews as applied to the composite organization.
- Risk-adjusted the financial model based on issues and concerns the interviewed organizations highlighted in interviews. Risk adjustment is a key part of the TEI methodology. While interviewed organizations provided cost and benefit estimates, some categories included a broad range of responses or had a number of outside forces that might have affected the results. For that reason, some cost and benefit totals have been risk-adjusted and are detailed in each relevant section.

Forrester employed four fundamental elements of TEI in modeling VMware/NSX's service: benefits, costs, flexibility, and risks.

Given the increasing sophistication that enterprises have regarding ROI analyses related to IT investments, Forrester's TEI methodology serves to provide a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

FIGURE 2

TEI Approach


Perform due diligence
Conduct customer interviews
Design composite organization
Construct financial model using TEI framework
Write case study

Source: Forrester Research, Inc.

Analysis

INTERVIEWED ORGANIZATIONS

For this study, Forrester conducted a total of four interviews with representatives from the following companies, which are VMware customers based in the US:

- A major US university supporting over 20,000 users on its infrastructure. It has two data centers operating with a layer 2 stretch, giving the university the flexibility to launch workloads irrespective of physical network topology. It previously operated approximately 500 host servers, which has since been shrunk to under 100 due to virtualization and NSX.
- A Fortune 500 business services organization operating with data that is regulated by bodies such as the Payment Card Industry (PCI) and FTC. This organization has leveraged NSX to manage and microsegment its virtual networks, adding control of internal east-west traffic to bolster its security stance.
- A US graduate-level educational institute with two data centers serving hundreds of virtual machines. Following the implementation of NSX, the organization was able to avoid purchases of over $600,000 in load balancers and $1 million in firewall appliances.
- An American utility company operating VMware, serving approximately 700 virtual machines. Workloads are varied and require high availability with extremely specific security policies.

> *"As our workload grew, we would constantly be building out new VLANs to accommodate the growth. Some apps had specific requirements while databases needed isolation on separate subnets using different load balancers. It became extremely complex and building on that was just inefficient. Looking to simplify that was what led us to NSX."*
>
> ~ Technologist, major university

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an associated ROI analysis that illustrates the areas financially affected. The composite organization that Forrester synthesized from these results represents an organization with the following characteristics:

- It is a US-based professional services organization that operates with significant amounts of private client data — some of which is regulated.
- It is a Fortune 500 company, with revenues in excess of $2 billion.
- It operated 300 hosts, serving nearly 3,000 virtual machines, prior to the implementation of NSX.
- A portion of its existing 300 hosts are proprietary.
- Mission-critical applications are operated across its existing virtual network.
- This organization already maintains a number of software and hardware solutions for its perimeter firewall, but it lacked interior security aside from endpoint software.

SITUATION

Prior to the deployment of NSX, the composite organization was faced with difficulties in its efforts to provide secure, segmented networks efficiently. Automation and speed-to-provision were lacking, as one interviewee stated: “Everything was done one by one — and it took days or even weeks.” End user productivity also suffered at times, from either unavailable networks or, worse, overloaded networks.

Internal network traffic was unregulated, too, meaning that the organization was unprotected from internal incidents that could potentially result in a widescale breach. Working in progressively more regulated markets, the organization had made it an imperative to make its network more secure, following the Forrester Zero Trust model to regulate internal network traffic flow. In sum, the organization needed a new virtual network solution that was modern and capable of delivering on the following key requirements:

- Centralize virtual network management.
- Improve provisioning times.
- Improve internal network security.
- Maintain or improve on current performance, following security improvements.

After researching the market and developing a business case evaluating various solutions and road maps, the composite organization chose VMware NSX and began deployment.

> *“We are a company that is tightly regulated, where workloads have to run in very specific environments accompanied by specific security policies. From that perspective, micro-segmentation and abstracting the network into software with NSX was extremely attractive to us.”*
>
> ~ Senior manager of enterprise cloud infrastructure, business services provider

RESULTS

The deployment of NSX resulted in the following at the composite organization:

- **East-west traffic flow became regulated through the micro-segmentation, forming “microperimeters,” or individually firewalled virtualized workloads, within the internal enterprise network.** With NSX, micro-segmentation and distributed firewalling provided specific policies for every tier of workload. For future considerations where tiers might be divided into sub-tiers, NSX had the capability to address those too, at an individual level. Microperimeters become individually fenced areas, limiting attack surfaces greatly and, in turn, lowering the potential costs of an actual breach. A better secured network through micro-segmentation satisfied a crucial goal for the composite without adding costly security appliances.
- **System administrators were able to improve on provisioning times due to a centralized point of management and workflow automation.** NSX improved efficiency of administrators by providing the capability to control the network regardless of physical topography while automating basic processes. Workflows improved and allowed the organization to do more without adding headcount.
- **Compute resource optimization and utilization improved.** The composite organization was able to optimize its network and increase compute utilization. Load balancing and switching was done effortlessly with NSX and allowed the

organization to provide more consistent network resource delivery. As the organization grew, this enabled the sun-setting of some proprietary servers, lowering overall operational cost.

- **NSX supported organization growth without being locked into proprietary hardware or software.** Healthy organization growth demanded additional compute resources. NSX scaled accordingly on commodity x86 servers while needing fewer servers than the existing solution. On the software side, the organization was able to integrate and connect with third-party sources easily, paving the way for future flexibility. One interviewee stated, "We appreciate the fact that VMware has a restful API — so we can integrate with other platforms and are not locked in."

> *"Having experienced rogue VMs and a rogue guest OS that took down a host made isolated workloads that much more important to us."*
>
> ~ Technologist, major university

BENEFITS

The composite organization experienced a number of quantified benefits in this case study:

- Capital expenditure avoidance with NSX in a brownfield deployment. Readers should note that greenfield deployments of NSX can result in additional capex savings by avoiding an even greater amount of hardware purchases in new data centers.

- Operational cost avoidance for decommissioned and ongoing avoided hardware purchases.

- System administrator time savings from IT and security automation.

- End user productivity gains from improved network performance and availability.

In addition to the quantified benefit categories listed above, we recommend readers to be cognizant of a benefit that we have not quantified in this study. One component of network virtualization is the increase in efficiency in network provisioning and administration. Equally important, however, is the maintenance of security for east-west data flows within the network. As previously discussed, the majority of enterprise breaches are a factor of internal activities, some malicious and some through inadvertent operations with nonmalicious intents. Studies are widely available from credible sources, such as the Ponemon Institute, and have determined the average total cost of a breach to be $4 million for enterprises globally.[3] Ponemon further calculates that the cost of data breaches has increased 29% since 2013. In favor of conservatism and being aware that organizations differ greatly in verticals and regarding the possession of sensitive data, this category has *not* been factored in ROI calculations. And while this has not been quantified, organizations should still be keenly aware of how they can be affected by the possible ramifications.

- Breaches can financially affect organizations in a number of different ways.[4] These include:

  - **Lost revenues.** Organizations may experience a loss of customer loyalty, loss of customer confidence, or an attack preventing the access of customer-facing channels. Revenue losses can be extenuating, based upon the impact of the breach.

  - **Legal settlements.** A loss of highly confidential information can increase the likelihood and the severity of the legal case. Stakeholders are not limited to the parties contained within the breached data — they may also be entities a number of degrees of connection beyond.

  - **Regulatory fines.** Highly regulated data such as healthcare information can trigger fines from governmental entities such as the Health Insurance Portability and Accountability Act (HIPAA) and the FTC.

  - **Cost of new/additional security infrastructure and implementations.** Organizations may have to make additional purchases to resolve the existing security gaps.

Capital Expenditure Avoidance With NSX

Prior to the adoption of NSX network virtualization, the composite organization noted an average compute resource utilization of 15%. While there were variances that took the utilization higher, the network resources sometimes also underperformed due to the inability of network administrators and infrastructure to adjust to changing needs. As a whole, however, the available resources were significantly underutilized. Following the implementation of NSX, the organization was able to improve utilization and enable the retirement of some legacy resources. As a brownfield implementation to augment its existing data center, NSX allowed the organization to save in capital expenditures in multiple hardware categories while accounting for growth. Additionally, the use of NSX enabled the usage of commodity servers, rather than legacy proprietary servers, bringing about further savings. The total host server purchase avoidance and reduction in the cost of servers over a three-year term yielded a PV savings of $973,964. Purchases for network infrastructure components like switches and load balancers were too reduced, attributed to the load balancing, switching, and routing capabilities of NSX. Savings for these avoided purchases yielded a PV total of $2.4 million over three years.

The composite organization started its journey for its security reposturing with a greenfield adoption — as east-west traffic, rather than just perimeter data flow, was increasingly becoming a concern for breaches — and it dictated that an additional security measure be implemented. Two choices were available to the composite organization: 1) to purchase security appliances to sit between data flows within the network or 2) to apply virtualized firewall capabilities and security policies via software-defined micro-segmentation that delineated virtual networks into smaller, more precisely controlled environments. By implementing NSX, the composite saw a significant avoidance in physical firewall appliances, totaling nearly $6.5 million, PV, over three years. In aggregate, the organization avoided capital expenditure purchases of $9 million with a brownfield data center approach and a greenfield security implementation.

Our interviews encompassed various NSX customers that had differing existing infrastructure and approaches to security. It was apparent, however, that the regulation of internal data flow was important to all of these customers, even though some operated with data that was more heavily scrutinized by regulatory bodies. Due to the varying levels of security maturity in these organizations and the amount of emphasis placed on specific data, this benefit category has been risk-adjusted down by 15%, netting a risk-adjusted three-year PV benefit of $7.6 million. See the Risks section for further detail on the application of Forrester's risk adjustments.

TABLE 1
Capital Expenditure Avoidance With NSX

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
A1	Total existing host servers with previous solution		300	330	363	399
A2	Host server growth with previous solution	Baseline: 300		30	33	36
A3	Host server growth required with NSX			19	21	23
A4	Delta in new servers required	A2-A3		11	12	14
A5	Cost per host server			$20,000	$20,000	$20,000
A6	Delta in server unit cost with existing solution versus with commodity servers on NSX			$12,000	$12,000	$12,000

A7	Host server savings with NSX	A4*(A5+A6)		$357,120	$392,832	$432,115
A8	Infrastructure purchase avoidance — switches, load balancers	Existing research		$570,000	$654,000	$654,000
A9	Security appliance purchase avoidance for east-west traffic	Existing research	$4,860,000	$648,000	$648,000	$648,000
At	Capital expenditure avoidance with NSX (brownfield deployment)	A7+A8+A9	$4,860,000	$1,575,120	$1,694,832	$1,734,115
	Risk adjustment	↓15%				
Atr	**Capital expenditure avoidance with NSX (brownfield deployment) (risk-adjusted)**		**$4,131,000**	**$1,338,852**	**$1,440,607**	**$1,473,998**

Source: Forrester Research, Inc.

Operational Cost Avoidance For Decommissioned And Avoided Hardware

The consolidation and rationalization process produced by the NSX implementation significantly reduced the cost for operational maintenance for host servers as well as associated infrastructure. This excludes the cost of security appliances, as they are considered a greenfield implementation in line with improving IT security as an overarching goal at the composite organization. The organization saw a retirement of 37% of existing servers, based in large by the improved load balancing, switching, and routing capabilities of the NSX platform. Over time, some legacy servers with specific serving capabilities were sunset and redeployed and stretched across newer commodity servers, and the organization observed similar rates of utilization improvement. Overall, it improved the utilization of host servers from 15% to 25%, while providing near-instant scalability in cases where additional compute resources were necessary. Over three years, operational costs were reduced by $1.1 million.

Interviewed organizations expressed some differences in their hardware profile prior to switching to NSX. For organizations that have a shorter hardware refresh period, fewer legacy servers are retired, resulting in a similarly reduced cost of operations from the modernized (and nonproprietary) hardware. Due to these observances, we have opted to risk-adjust this benefit category by 5%, resulting in a three-year PV of $1 million.

TABLE 2
Accelerated New Business Initiation: Processing Time Improvements Lead To Time Savings

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
B1	Servers decommissionable from previous solution		112	11	12	14
B2	Maintenance, patching, support of existing hosts	10% of server cost	$358,400	$35,712	$39,283	$43,212
B3	Maintenance, patching, upkeep of infrastructure and security appliances w/o NSX	10% of infrastructure cost	$486,000	$64,800	$64,800	$64,800

Bt	Operational cost avoidance for decommissioned and avoided hardware	B2+B3	$844,400	$100,512	$104,083	$108,012
	Risk adjustment	↓5%				
Btr	**Operational cost avoidance for decommissioned and avoided hardware (risk-adjusted)**		**$802,180**	**$95,486**	**$98,879**	**$102,611**

Source: Forrester Research, Inc.

System Admin Time Savings From IT And Security Automation

In implementing NSX across its virtualized systems, the composite organization was able to reduce its administration effort around networks, ranging in tasks from network provisioning and basic network administration to the posturing of security policies with virtualized firewalls. Across the various tasks that admins oversaw on the network, the organization saved over 6,000 hours of administration time on the centralized point of control on NSX. Translating this figure into a raw cost of administrator time resulted in a savings of nearly $1.3 million over three years. Potential adopters of NSX can realize this benefit in two ways: 1) avoiding the hiring of additional admins as the organization scales its growth or 2) reallocating existing network administrators to new tasks, including other value-add activities such as those in the public cloud and the development of improved security posturing for north-south and east-west traffic across the network. As one technologist puts it, “We would surely need a lot more people to manage the network if not for NSX.”

Forrester noted some variance between organizations interviewed, depending largely on organization maturity in network automation and existing security practices. As an example, some organizations held detailed security policies that were already enforced and, as a result, noticed slightly lower benefit realization. To reflect the lowered impact of this benefit, we have risk-adjusted it by 5%, producing a new three-year PV gain of $1.2 million.

TABLE 3
System Admin Time Savings From IT And Security Automation

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
C1	Workload provisioning automation savings in hours			2,100	2,310	2,541
C2	Network management automation savings in hours			2,520	2,772	3,049
C3	Security posturing/policy automation savings in hours			1,152	1,267	1,394
C4	Total effort reduction denoted in number of systems admin FTEs			2.9	3.2	3.5
C5	Hourly cost of systems admin, fully loaded			$81	$81	$81
Ct	Systems admin time savings from IT and security automation	(C1+C2+C3)*C5	$0	$467,532	$514,285	$565,714
	Risk adjustment	↓5%				

Ctr	**System admin time savings from IT and security automation (risk-adjusted)**		**$0**	**$444,155**	**$488,571**	**$537,428**

Source: Forrester Research, Inc.

End User Productivity Improvement

In the years prior to its adoption of VMware NSX, the composite organization provisioned networks and instances manually, which was a rather inefficient way to provide networked resources. There was a long wait for provisioning due to manual processes, and end users endured resources that had at times been underprovisioned and underperformed to expectations. Performance degradations came from a slew of factors; sometimes they were attributable to load balancers, while other times they were due to improperly set expectations from end users for system administrators. Rectifying such situations required changes, and as manual processes, these changes were not performed in the agile manner that end users required.

We calculated the periods of severe performance degradation and unavailability over three years, in the absence of NSX, and exposed approximately 11,000 hours per year that were lost by end users of the organization. With NSX, this loss was avoided, and the organization saved $1.75 million, PV, over three years.

In recognizing this benefit, Forrester understands that some organizations significantly overprovision their resources (which inadvertently raises capex costs). With overprovisioning, performance degradation can be mitigated to a degree. In observance of this possibility, this benefit has been risk-adjusted downward by 10%, resulting in a final benefit figure of $1.6 million.

TABLE 4

End User Productivity Improvement

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
D1	Active VM user usage across the enterprise, per year	4,000 VMs daily at 80% utilization	832,000	915,200	1,006,720	1,107,392
D2	Frequency of degradation occurrences with prior solution	5% of VM degrade/fail	41,600	45,760	50,336	55,370
D3	Duration of avg. performance degradation leading to lower end user productivity, in hours	1/4 hour per degrade/fail	10,400	11,440	12,584	13,842
D4	Average hourly wage of end user, fully loaded	$42/hour	$42	$42	$42	$42
Dt	End user productivity improvement	D3*D4	$436,800	$480,480	$528,528	$581,381
	Risk adjustment	↓10%				
Dtr	**End user productivity improvement (risk-adjusted)**		**$393,120**	**$432,432**	**$475,675**	**$523,243**

Source: Forrester Research, Inc.

Total Benefits

Table 5 shows the total of all benefits across the four areas listed above, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $11.4 million.

TABLE 5
Total Benefits (Risk-Adjusted)

Ref.	Benefit	Initial	Year 1	Year 2	Year 3	Total	Present Value
Atr	Capital expenditure avoidance with NSX (brownfield deployment)	$4,131,000	$1,338,852	$1,440,607	$1,473,998	$8,384,457	$7,646,159
Btr	Operational cost avoidance for decommissioned and avoided hardware	$802,180	$95,486	$98,879	$102,611	$1,099,156	$1,047,797
Ctr	System admin time savings from IT and security automation	$0	$444,155	$488,571	$537,428	$1,470,154	$1,211,333
Dtr	End user productivity improvement	$393,120	$432,432	$475,675	$523,243	$1,824,470	$1,572,480
	Total benefits (risk-adjusted)	**$5,326,300**	**$2,310,926**	**$2,503,732**	**$2,637,280**	**$12,778,238**	**$11,477,769**

Source: Forrester Research, Inc.

COSTS

The composite organization experienced a number of costs associated with the NSX solution:

- License and support costs.
- Deployment and training costs.

These represent the mix of internal and external costs experienced by the composite organization for initial planning, implementation, and ongoing maintenance associated with the solution.

License And Support Costs

The composite incurred initial perpetual NSX license costs, based upon sockets to physical CPUs. As NSX requires fewer hosts due to a higher and more optimized usage of compute resources, the licenses are only purchased for the effective number of hosts that will be serving the virtual networks. Over the course of three years, the effective license costs inclusive of the hosts added due to growth are $3.3 million. Above and beyond base license costs, organizations typically incur an ongoing cost for service and support of the NSX platform, at percentage of license costs. The total cost of both licenses and service and support was a three-year PV of $5.8 million for the composite organization. Readers should note that all costs have been calculated at list pricing.

TABLE 6
License And Support Costs

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
E1	NSX license cost		$2,630,120	$263,012	$289,313	$318,245
E2	NSX service and support		$657,530	$723,283	$729,858	$737,091
Et	License and support costs	E1+E2	$3,287,650	$986,295	$1,019,172	$1,055,336
	Risk adjustment	0%				
Etr	**License and support costs (risk-adjusted)**		**$3,287,650**	**$986,295**	**$1,019,172**	**$1,055,336**

Source: Forrester Research, Inc.

Deployment And Training Costs

In addition to the initial costs of licenses, the composite organization incurred the cost of professional services and training for its internal systems administrators. Many customers cited the benefit of professional services to accelerate implementation and production usage of NSX within two months. Adding to the one-time cost of professional services, we've accounted for additional personalized training as well as the opportunity time cost of training for system administrators, inclusive of churn that may occur. Total three-year PV costs were slightly over $277,000.

TABLE 7
Deployment And Training

Ref.	Metric	Calculation	Initial	Year 1	Year 2	Year 3
F1	VMware design and deployment of professional services		$200,000			
F2	VMware training services program		$8,250		$4,125	
F3	Cost of system admin per hour		$81	$81	$81	$81
F4	Cost of system admin training, initial	120 hours per admin, three admins	$19,440		$4,860	
F5	Cost of system admin ramp-up period	50% productivity for two months, three admins	$40,500			
Ft	Deployment and training	F1+F2+F4+F5	$268,190	$0	$8,985	$0
	Risk adjustment	0%				
Ftr	**Deployment and training (risk-adjusted)**		**$268,190**	**$0**	**$8,985**	**$0**

Source: Forrester Research, Inc.

Total Costs

Table 8 shows the total of all costs as well as associated present values (PVs), discounted at 10%. Over three years, the composite organization expects total costs to be a PV of slightly over $6 million.

TABLE 8
Total Costs (Risk-Adjusted)

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Etr	License and support costs	$3,287,650	$986,295	$1,019,172	$1,055,336	$6,348,452	$5,819,462
Ftr	Deployment and training	$268,190	$0	$8,985	$0	$277,175	$275,616
	Total costs (risk-adjusted)	**$3,555,840**	**$986,295**	**$1,028,157**	**$1,055,336**	**$6,625,627**	**$6,095,077**

Source: Forrester Research, Inc.

FLEXIBILITY

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for some future additional investment. This provides an organization with the “right” or the ability to engage in future initiatives but not the obligation to do so. There are multiple scenarios in which a customer might choose to implement NSX and later realize additional uses and business opportunities. Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A)

Interviewed clients of NSX stated that they appreciated the RESTful API provided by NSX. One interviewee stated it as a principle reason for going with NSX, as they wanted to retain the flexibility moving forward and not be locked into VMware-specific products. Of the use cases possible with the APIs, the interviewees stated specifically how development frameworks such as Java, Perl, and Python were able to leverage the NSX REST API for very specific virtual workspace provisioning and reporting.

NSX can now orchestrate the consolidation of all cloud functions deployed via cloud across NSX. As use cases and applications are released across scalable clouds, administrators have increased opportunities to orchestrate security for enterprise usage of the IT resources. Not incorporated into the base growth calculations of this study are organizations that are aggressively pursuing digital transformations, where the need for network virtualization increases. In such situations, operational costs associated with providing operationality and end user productivity can see much greater gains as the digital transformation imperative matures or is completed.

RISKS

Forrester defines two types of risk associated with our analysis: “implementation risk” and “impact risk.” Implementation risk is the risk that a proposed investment in NSX may deviate from the original or expected requirements, resulting in higher costs than anticipated. Impact risk refers to the risk that the business or technology needs of the organization may not be met by the investment in NSX, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for cost and benefit estimates. For this case study, we believe only impact risks, or the level of benefit, are the risks that are primarily associated with the adoption of NSX. Cost-level implementation risks have been calculated conservatively and are believed to require no additional adjustments.

TABLE 9
Benefit Risk Adjustments

Benefits	Adjustment
Capital expenditure avoidance with brownfield NSX implementations	↓ 15%
Operational expenditure avoidance for decommissioned and avoided hardware purchases	↓ 5%
System/network admin efficiency time savings	↓ 5%
End user productivity recovered	↓ 10%

Source: Forrester Research, Inc.

Quantitatively capturing implementation risk and impact risk by directly adjusting the financial estimates results provides more meaningful and accurate estimates and a more accurate projection of the ROI. In general, risks affect costs by raising the original estimates, and they affect benefits by reducing the original estimates. The risk-adjusted numbers should be taken as “realistic” expectations since they represent the expected values considering risk.

The following impact risks that affect benefits are identified as part of the analysis:

- Capital expenditure savings can vary for organizations that grow at different rates. Additionally, organizations that take differing stances on security readiness will realize differences in the savings realized from security and the associated infrastructure hardware purchases that might be otherwise required, thus decreasing the possible benefit for some organizations.

- Operational expenditures savings will vary between certain organizations depending on their existing infrastructure footprint. Some organizations that have progressively grown at a rapid clip will realize smaller gains on decommissioned hardware, due in part to possibly not having much hardware to decommission, although this is typically not the norm.

- System and network administrator time savings made possible by security and IT automation can depend on organizational maturity and the existing state. For instance, some organizations might have extensive scripting and tools in place for network administration. While NSX is an improvement in virtual network deployment, the degree to which it improves organizations can vary slightly.

- End user productivity savings gained from improved applications and network performance and availability can sometimes be reduced by organizations that have an overabundance of compute resources. In such situations, the resulting improvement will be decreased due to an overabundance of resources that result in reduced instances of overutilization.

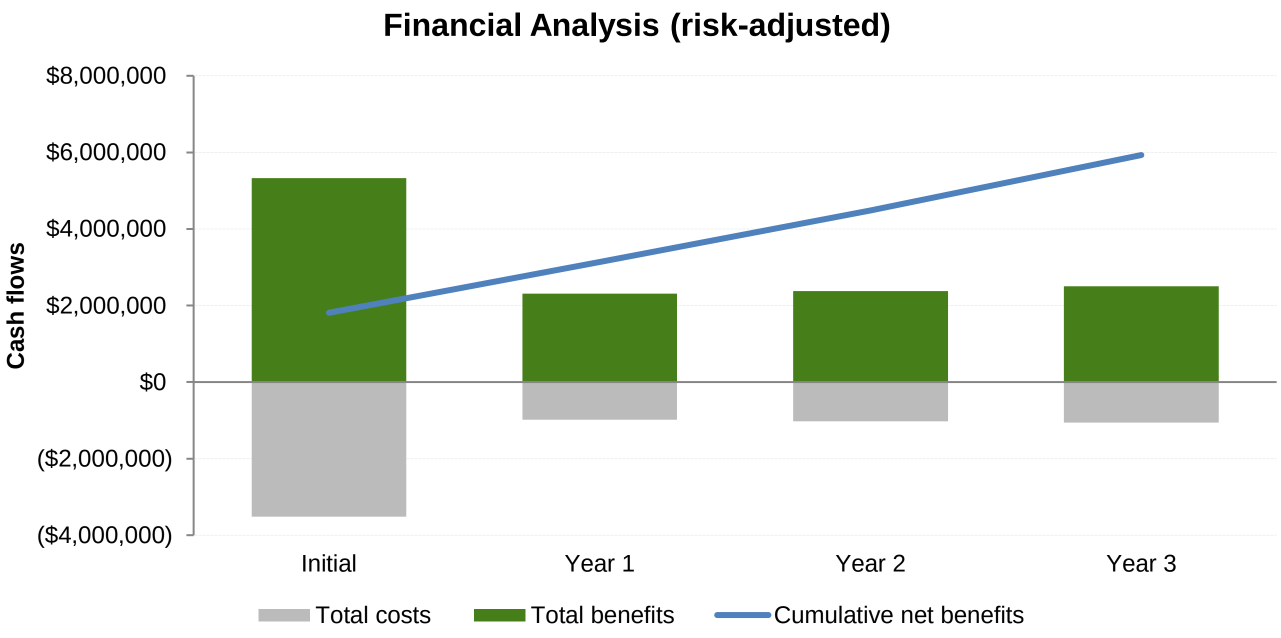
Table 9 shows the values used to adjust for risk and uncertainty in the cost and benefit estimates for the composite organization. Readers are urged to apply their own risk ranges based on their own degree of confidence in the cost and benefit estimates.

Financial Summary

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI and NPV for the composite organization's investment in NSX.

Table 10 below shows the risk-adjusted ROI and NPV values. These values are determined by applying the risk-adjustment values from Table 9 in the Risks section to the unadjusted results in each relevant cost and benefit section.

FIGURE 3
Cash Flow Chart (Risk-Adjusted)



Source: Forrester Research, Inc.

TABLE 10
Cash Flow (Risk-Adjusted)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Costs	($3,555,840)	($986,295)	($1,028,157)	($1,055,336)	($6,625,627)	($6,095,077)
Benefits	$5,326,300	$2,310,926	$2,503,732	$2,637,280	$12,778,238	$11,477,769
Net benefits	$1,770,460	$1,324,631	$1,475,576	$1,581,944	$6,152,611	$5,382,692
ROI						88%

Source: Forrester Research, Inc.

VMware NSX: Overview

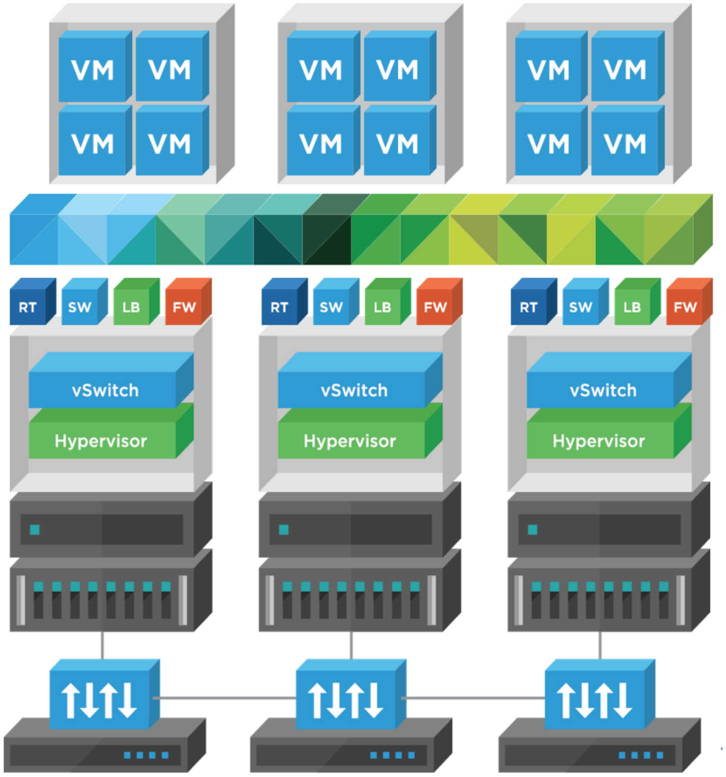
The following information is provided by VMware. Forrester has not validated any claims and does not endorse VMware or its offerings.

A fundamentally new approach to the network infrastructure is needed — one that no longer demands compromises between speed and security or between security and agility. The rules of the data center that have held businesses back from unleashing their full potential need to be rewritten to enable IT to perform without compromises. As thousands of businesses have now realized, network virtualization is that new approach.

By moving network and security services into the data center virtualization layer, network virtualization enables IT to create, snapshot, store, move, delete, and restore entire application environments with the same simplicity and speed that they now have when spinning up virtual machines. This, in turn, enables levels of security and efficiency that were previously infeasible.

VMware NSX is the network virtualization platform of the software defined data center. It takes the functionality that was formerly embedded in network hardware—such as switching, routing, and firewalling—and abstracts it to the hypervisor.

By doing this, NSX creates what can be thought of as a “network hypervisor” that is distributed throughout the data center. With it, IT is able to become an enabler of innovation for the organization, effectively saying “yes” to multiple stakeholders instead of treating their requests as competing and mutually exclusive. Not only is IT now able to provide unprecedented levels of security; it is able to do so at a speed that keeps pace with the demands of the organization. The continuity of applications, automation of manual IT processes, and critical security of the data center are all able to work in harmony with business-driven time constraints and schedules in a way that significantly reduces operational complexities and associated costs.



Distributed Stateful Firewalling

Distributed stateful firewalling, embedded in the hypervisor kernel for up to 20 Gbps of firewall capacity per hypervisor host.

Dynamic Security Policy

Security policy that is attached directly to the workload and “travels” with the workload, independent of the underlying network topology, enabling security to adapt to changes.

Cloud Management

Native integration with VMware vRealize® Automation™ and OpenStack, enabling advanced automation capabilities.

3rd Party Integration

Enhanced security and advanced networking services through an ecosystem of leading third-party vendors.

Appendix A: Total Economic Impact™ Overview

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders. TEI assists technology vendors in winning, serving, and retaining customers.

The TEI methodology consists of four components to evaluate investment value: benefits, costs, flexibility, and risks.

BENEFITS

Benefits represent the value delivered to the user organization — IT and/or business units — by the proposed product or project. Often, product or project justification exercises focus just on IT cost and cost reduction, leaving little room to analyze the effect of the technology on the entire organization. The TEI methodology and the resulting financial model place equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization. Calculation of benefit estimates involves a clear dialogue with the user organization to understand the specific value that is created. In addition, Forrester also requires that there be a clear line of accountability established between the measurement and justification of benefit estimates after the project has been completed. This ensures that benefit estimates tie back directly to the bottom line.

COSTS

Costs represent the investment necessary to capture the value, or benefits, of the proposed project. IT or the business units may incur costs in the form of fully burdened labor, subcontractors, or materials. Costs consider all the investments and expenses necessary to deliver the proposed value. In addition, the cost category within TEI captures any incremental costs over the existing environment for ongoing costs associated with the solution. All costs must be tied to the benefits that are created.

FLEXIBILITY

Within the TEI methodology, direct benefits represent one part of the investment value. While direct benefits can typically be the primary way to justify a project, Forrester believes that organizations should be able to measure the strategic value of an investment. Flexibility represents the value that can be obtained for some future additional investment building on top of the initial investment already made. For instance, an investment in an enterprisewide upgrade of an office productivity suite can potentially increase standardization (to increase efficiency) and reduce licensing costs. However, an embedded collaboration feature may translate to greater worker productivity if activated. The collaboration can only be used with additional investment in training at some future point. However, having the ability to capture that benefit has a PV that can be estimated. The flexibility component of TEI captures that value.

RISKS

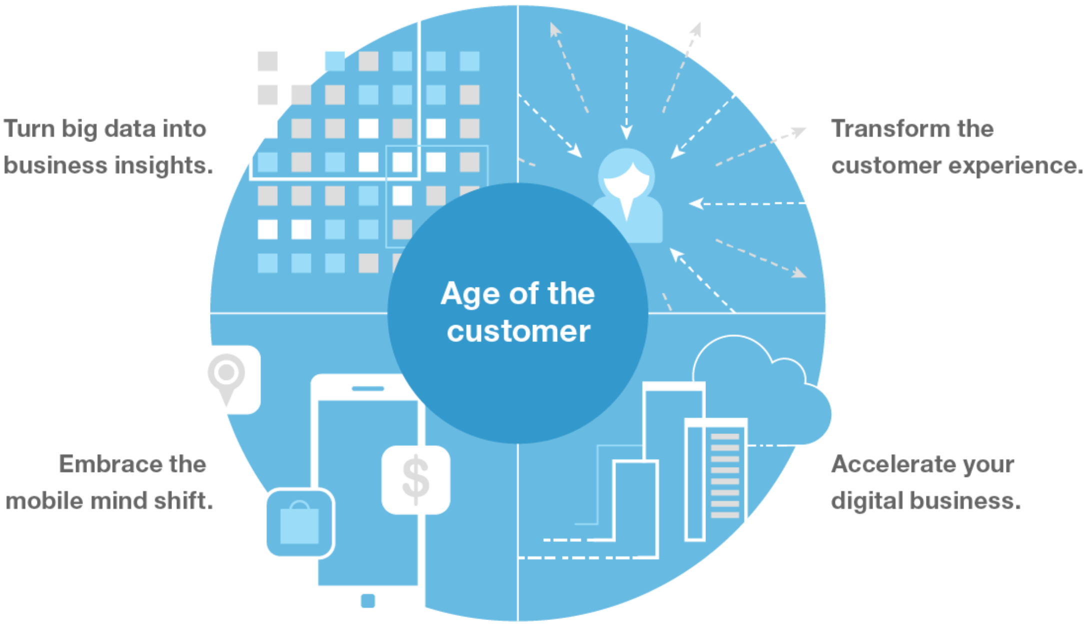
Risks measure the uncertainty of benefit and cost estimates contained within the investment. Uncertainty is measured in two ways: 1) the likelihood that the cost and benefit estimates will meet the original projections and 2) the likelihood that the estimates will be measured and tracked over time. TEI risk factors are based on a probability density function known as "triangular distribution" to the values entered. At a minimum, three values are calculated to estimate the risk factor around each cost and benefit.

Appendix B: Forrester And The Age Of The Customer

Your technology-empowered customers now know more than you do about your products and services, pricing, and reputation. Your competitors can copy or undermine the moves you take to compete. The only way to win, serve, and retain customers is to become customer-obsessed.

A customer-obsessed enterprise focuses its strategy, energy, and budget on processes that enhance knowledge of and engagement with customers and prioritizes these over maintaining traditional competitive barriers.

CMOs and CIOs must work together to create this companywide transformation.


Turn big data into business insights.
Transform the customer experience.
Age of the customer
Embrace the mobile mind shift.
Accelerate your digital business.

Forrester has a four-part blueprint for strategy in the age of the customer, including the following imperatives to help establish new competitive advantages:

Transform the customer experience to gain sustainable competitive advantage.

Accelerate your digital business with new technology strategies that fuel business growth.

Embrace the mobile mind shift by giving customers what they want, when they want it.

Turn (big) data into business insights through innovative analytics.

Appendix C: Glossary

Discount rate: The interest rate used in cash flow analysis to take into account the time value of money. Companies set their own discount rate based on their business and investment environment. Forrester assumes a yearly discount rate of 10% for this analysis. Organizations typically use discount rates between 8% and 16% based on their current environment. Readers are urged to consult their respective organizations to determine the most appropriate discount rate to use in their own environment.

Net present value (NPV): The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

Present value (PV): The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

Payback period: The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Return on investment (ROI): A measure of a project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits minus costs) by costs.

A NOTE ON CASH FLOW TABLES

The following is a note on the cash flow tables used in this study (see the example table below). The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1. Those costs are not discounted. All other cash flows in years 1 through 3 are discounted using the discount rate (shown in the Framework Assumptions section) at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations are not calculated until the summary tables are the sum of the initial investment and the discounted cash flows in each year.

Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

TABLE [EXAMPLE]
Example Table

Ref.	Metric	Calculation	Year 1	Year 2	Year 3

Source: Forrester Research, Inc.

Appendix D: Supplemental Material

Related Forrester Research

“Jump-Start Zero Trust With Forrester’s Reference Architecture,” Forrester Research, Inc., March 27, 2017

“The State Of Network Security: 2016 To 2017,” Forrester Research, Inc., January 26, 2017

“Defend Your Digital Business From Cyberattacks Using Forrester’s Zero Trust Model,” Forrester Research, Inc., November 4, 2016

“Five Steps To A Zero Trust Network,” Forrester Research, Inc., July 27, 2016

“Q&A: Six Common Questions About Software-Defined Networking,” Forrester Research, Inc., October 19, 2016

Appendix E: Endnotes

[1] Source: “The State Of Network Security: 2016 To 2017,” Forrester Research, Inc., January 26, 2017.

[2] Forrester risk-adjusts the summary financial metrics to take into account the potential uncertainty of the cost and benefit estimates. For more information, see the section on Risks.

[3] Source: “2016 Ponemon Institute Cost of a Data Breach Study: Global Analysis,” Ponemon Institute, June 15, 2016 (https://securityintelligence.com/media/2016-cost-data-breach-study/).

[4] Source: “Understanding The Business Impact And Cost Of A Breach,” Forrester Research, Inc., January 12, 2015.