FORRESTER®

VMware NSX Distributed Firewall Enables A Major US City To Secure Its Most Important Networks, Workloads, And Information While Reducing Infrastructure Costs And Burden On Personnel

As organizations prioritize digital transformation initiatives, many are finding that legacy network architectures are holding them back. To support new business models, private and public cloud adoption, containers, and an explosion in connected devices, modern networks must support interoperability across data centers, multiple clouds, branch locations, and edge devices. Applications now run at every point on this spectrum, and they are critical to businesses' ability to win in hyper-competitive marketplaces. Yet, even as organizational success has become more dependent on this new architecture and the amount of data flowing across connections has increased, many organizations still lack a unified approach to management, automation, and security.

VMware NSX is a full-stack network virtualization and network security platform that uses a software-defined approach to extend networking and security across data centers, clouds, and application frameworks.

To better understand the benefits, costs, and risks associated with a VMware NSX investment, VMware commissioned Forrester Consulting to interview several representatives and conduct a Total Economic Impact™ (TEI) study.[1] For the purposes of this Total Economic Impact™ Spotlight, Forrester interviewed an additional representative from a city government with experience using VMware NSX with the following characteristics:

- The interviewee's title is Network Administration Specialist.
- The interviewed city government has been using NSX for just over three years after considering solutions other than VMware NSX.
- The city has a budget of just over $1 billion USD annually and 1,500 employees.

Magnified for this city government organization, VMware NSX Distributed Firewall enables the city to maintain zero-trust and micro-segmentation capabilities in the datacenter while maximizing current investments in infrastructure and personnel skills. Security rules can be applied at scale, faster, and more efficiently than before leveraging fewer resources and supporting a more robust security posture.

> **"NSX [Distributed Firewall] makes it easier for us to sleep at night because it makes securing workloads a repeatable programmatic process. There is no longer anxiety in being told we need to secure things for compliance reasons."**
>
> *Network administration specialist, city government*

Avoided infrastructure purchasing for interviewed organization

$553,680-$630,000

READ THE FULL STUDY

INVESTMENT DRIVERS

The interviewed city government adopted VMware NSX Distributed Firewall for the following reasons:

- **The need to secure "thousands" of VMs.** The interviewee told Forrester that thousands of VMs needed to be secured across all of the city's workloads. The interviewee continued: "we had to put separate firewalls at different locations to segment off certain networks and then start extending different networks with VLANs. While securing everything is possible this way, operationally it becomes very time intensive."
- **Limited personnel capacity.** Despite the need to secure the city's VMs and workloads, there were simply not enough IT personnel to do the job. The interviewee further noted that a lack of standardization across network security firewall configuration among the network engineers added additional around audits to demonstrate compliance amid several security approaches.
- **The need for "easy" PCI compliance.** PCI compliance was top of mind for the city's interviewee. The organization needed a single, repeatable process to ensure network security and compliance was needed amid increasing requirements and audit frequency.

NSX INVESTMENT OBJECTIVES

The interviewees' organizations chose to invest in NSX Distributed Firewall for the following reasons:

- **Infrastructure avoidance in a brownfield deployment.** The interviewee noted that compared with competitive solutions investigated, VMware NSX Distributed Firewall allowed the city to leverage already purchased host, security, and network infrastructure without a significant need for additional investments, as was the case with several other options.
- **"Out of the box" improvements to visibility and security.** While prior to the investment in NSX, the city lacked visibility into network traffic. With NSX Distributed Firewall, the interviewee highlighted the significant improvements in this area, noting: "NSX allows you to see all of the traffic in your virtual environment, every host that you have virtually, and the ability to do application modeling, where we can see all the traffic around a particular host. It helps us secure the "crown jewels" of our organization quickly. We can start modeling traffic and NSX will suggest firewall rules to stop certain types of traffic."
- **Functionality that improves staff productivity.** By providing a consistent, repeatable programmatic process for securing workloads, the interviewee noted that any network engineer can work within NSX faster and more efficiency than on prior processes, providing faster and better security with less individual effort. "It's all done the same way. And if somebody leaves our organization, someone else can come in tomorrow and do the same job. All they have to do is follow that processes that VMware and NSX lay out for us," the interviewee summarized.

KEY RESULTS

Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Capital expenditure avoidance of over $600,000 annually.** The interviewee noted that capital expenditure was avoided through a micro-segmentation strategy on VMware NSX through avoidable security appliance purchases, networking equipment purchasing, and commodity hardware viability. Based on Forrester's modeling and the specifics of the interviewed city government, this benefit is worth over $600,000 annually in avoided cost.
- **Operational cost avoidance for decommissioned and avoided hardware of over 2.5 FTEs.** Based on Forrester's model, the organization can offset approximately $370,000

in personnel costs over three years from avoidable infrastructure maintenance on VMware NSX. This represents just over 2.5 FTEs assuming a $140,000 average loaded salary.

- **Systems admin time savings from IT and security automation.** The interviewee told Forrester about reduced burden on their limited staff to manage network security: “It’s just a huge operational benefit to us because of how quickly we can start zero trusting our network segments versus the traditional way with private VLANs, or firewalls in different locations, or moving segments around, or even taking larger network segments and then taking hosts out of those and putting those in a smaller segment for security. With NSX to do that at the vNIC level with automatic tagging and dynamic inclusion and it can be done programmatically, much faster, and at scale.” Based on Forrester’s TEI model and the interviewed city government, nearly $550,000 annually in personnel hours are avoidable in this domain. The interviewee noted that much of this reclaimed time is purposed to learning new skills and/or technologies to prepare for the future: “This is a huge benefit when it comes to time savings because of what we can do with that time. I'm learning some Kubernetes right now and building some clusters. I'm getting a lot deeper with my Python skills. But these things would not be able to happen without the ability to programmatically do the things we can do in NSX.”
- **End-user experience improvements.** Prior to an investment in NSX, interviewees' IT organizations frequently provisioned resources that underperformed because of the inexact and manual process with which the companies allocated them. Rectifying performance issues took time, forcing end users to work with suboptimal resources and hampering productivity. VMware NSX enabled administrators to quickly provision resources able to support end user workflows. The interviewee highlighted NSX’s ability to quickly model impacts on individual applications or workloads as a major benefit in support the city’s end-users.

[Unquantified benefits]

- **Improved relationship with information security personnel.** The interviewee spoke to an improved relationship with their security team resulting from standardization on VMware NSX Distributed Firewall, summarizing: “We have a much better relationship with the security team. They trust in the tools that we’re using because they’re seeing the value in those tools. When we give them information, they know where in the chain of custody that information came from. And not only is the security team aware of what we can do on the zero-trust side, they actively help us to figure out how we can do more. This is a huge benefit because once you have a good relationship with your security team and can agree on mutual goals, it really opens up the door to a lot more conversations on some of the things that we can do together as a team.”
- **Support for cloud migrations.** Despite supporting an on-premises VMware and NSX deployment, the interviewee summarized optimism for future migrations to public clouds given VMware’s inroads with several major public clouds: “What if we decide six months from now we want to go to the cloud? We’ve built this great environment with NSX. Well, we have a multitude of public cloud options. Each one of those clouds has an implementation of NSX that we can leverage our rules, and more importantly our personnel skills for. It's no problem because once it goes up to the cloud, that same policy enforcement that we’ve built continues to be applied.”

TOTAL ECONOMIC IMPACT ANALYSIS

For more information, download the full study: "The Total Economic Impact™ Of VMware NSX," a commissioned study conducted by Forrester Consulting on behalf of VMware, May 2020.

STUDY FINDINGS

Forrester interviewed seven representatives at organizations with experience using the NSX and combined the results into a three-year composite organization financial analysis. Risk-adjusted present value (PV) quantified benefits for the composite organization include:

- Capital expenditure avoidance for server and network hardware with NSX totaling $6,459,422.
- Operational cost avoidance for decommissioned and avoided hardware totaling $741,336.
- System administrator time savings from IT and security automation totaling $3,160,044.
- End user productivity improvements totaling $1,572,469.

Return on investment (ROI)

95%

Net present value (NPV)

$5.8 million

Appendix A: Endnotes

[1] 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.

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 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. 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.
- VMware provided the customer names for the interview(s) but did not participate in the interviews.

ABOUT TEI

Total Economic Impact™ (TEI) 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. The TEI methodology consists of four components to evaluate investment value: benefits, costs, risks, and flexibility.

© Forrester Research, Inc. All rights reserved. Forrester is a registered trademark of Forrester Research, Inc.


FORRESTER®