The Business Value of Networking and Lateral Security for VMware Cloud Foundation

Vijay Bhagavath
Research Vice President,
Cloud and Datacenter Networks, IDC

Matthew Marden
Research Vice President,
Business Value Strategy Practice, IDC

Table of Contents

CLICK ANY HEADING TO NAVIGATE DIRECTLY TO THAT PAGE.

Executive Summary . . . 3

Business Value Highlights . . . 3

Situation Overview . . . 4

Networking and Lateral Security Solutions for VMware Cloud Foundation . . . 5

The Business Value of Networking and Lateral Security in VCF . . . 6

Study Demographics . . . 6

Choice and Use of Networking and Lateral Security for VCF . . . 7

Business Value and Quantified Benefits of VMware NSX and VMware vDefend . . . 9

Networking Efficiencies and Cost Benefits . . . 11

Security Benefits and Efficiencies . . . 14

Agility and Development Benefits . . . 16

Benefits of Reduced Operational Risk . . . 18

Business Benefits . . . 20

ROI Summary . . . 20

Challenges/Opportunities . . . 21

Conclusion . . . 22

Appendix 1: Methodology . . . 23

Appendix 2: Quantified Benefits of Use of VMware NSX and VMware vDefend Solutions . . . 25

Appendix 3: Supplemental Data . . . 26

About the IDC Analysts . . . 28

Executive Summary

VMware NSX Network Virtualization (NSX) and VMware vDefend Distributed Firewall (vDefend) are critical components of the VMware Cloud Foundation (VCF) private cloud platform. This platform implements a best-in-class software-defined infrastructure (SDI) for modern application architectures such as Kubernetes/containers, VMs, application programming interfaces, and application microservices.

VMware NSX and VMware vDefend for VCF offer a comprehensive suite of tools and resources for rapid and efficient business application development.

IDC assessed the impact of using VMware NSX and VMware vDefend (collectively networking and lateral security for VCF) by interviewing organizations about their experiences. Study participants reported achieving significant value through networking and security staff efficiencies, cost savings, and improved capabilities.

In addition to these direct benefits, interviewed VMware customers reported benefiting from enhanced agility, scalability, and performance in support of their business operations.

Based on these interviews with current users of networking and lateral security for VCF, IDC projects that they will realize benefits worth an annual average of $1.24 million per datacenter ($16.0 million per organization) by:

- Providing more efficient and cost-effective networking in private cloud environments
- Improving private cloud security capabilities and reducing security-related risk
- Enabling development teams to react more readily to business needs
- Reducing operational risk associated with network and other IT outages
- Achieving better business outcomes by more readily addressing opportunities and delivering high-quality services and products to customers

Click highlights for related content in this document.

BUSINESS VALUE HIGHLIGHTS

610%
three-year return on investment

6-month
payback on investment

25%
IT network management efficiencies

70%
infrastructure and direct cost savings

35%
IT security team efficiencies

>11x
more east-west network traffic secured

6%
higher developer productivity

$1.96 million
higher revenue per organization per year

Situation Overview

Network modernization is crucial for enabling private cloud environments as part of an enterprise's digital transformation journey, which requires reimagining how large, complex, and global-scale enterprise datacenters are architected and life cycles are managed.

Transitioning to a modern software-defined infrastructure brings challenges around ensuring security, resiliency, manageability, peak application performance, and cost-efficiencies. This occurs when full-stack enterprise applications are implemented as a distributed set of virtualized and containerized workloads that span private cloud environments across in-house and third-party cloud datacenters.

This is when a production-ready SDI platform such as VMware Cloud Foundation comes in. VMware Cloud Foundation is a flagship platform of Broadcom's software portfolio that offers a full suite of software-defined services for computing, storage, network, and security, plus day 0–2+ cloud management capabilities.

Enterprise IT and business leaders we have spoken with point out the need to work with a production-ready software-defined infrastructure platform for building private clouds — ideally from a single vendor, versus a cobbled-up mesh of products from point vendors. Based on unified modern infrastructure, private clouds run with a true cloud operating model, deliver cloud experience for developers, and are protected with strong security and resilience.

While virtualized networking and computing bring elastic scale to private and hybrid cloud datacenters, virtualized and distributed security and full-stack observability features help organizations mitigate threat vulnerabilities and costly application outages while ensuring compliance with industry-specific and regulatory requirements.

In summary, IDC views software-defined infrastructure as integral to accelerating enterprise digital transformation and datacenter modernization initiatives. It enables IT teams to effectively build and manage cloud-scale applications, driving superior business outcomes.

Networking and Lateral Security Solutions for VMware Cloud Foundation

This IDC Business Value paper focuses on VMware NSX Network Virtualization and VMware vDefend Distributed Firewall, two critical components of VCF private cloud software. These technologies largely provide the technology functions underlying networking and lateral security for VCF.

NSX is a core component of the VCF software stack, purchasable only through the VCF SKU. vDefend is an add-on offering to VCF via the vDefend Firewall SKU or via the vDefend Firewall with advanced threat prevention SKU.

NSX Network Virtualization is an industry-unique software-defined networking (SDN) technology in VCF that offers the following key value propositions to enterprise buyers:

- **Simplicity and scale benefits of the cloud operating model** for traditional and modern applications running in private and hybrid cloud datacenters
- **End-to-end automation and deep visibility** for simplifying and accelerating network operations and optimization
- **Robust ransomware defense and simplified disaster recovery capabilities** for ensuring application availability despite cyberattacks and datacenter outages
- **Improved compute infrastructure utilization, reduced carbon emissions, and cost savings** (space, HVAC, power, infrastructure), with meaningful reduction in datacenter footprint
- **Network acceleration capabilities** for accelerating datacenter network throughput for high-performance generative AI (GenAI) clusters, where network performance can be tuned specifically for AI traffic and workload profiles

VMware vDefend Distributed Firewall is a software-defined Layer 7 firewall for securing VM, container, and bare metal workloads.

Key features include:

- **Stateful firewalling with IDS/IPS, sandboxing, and NTA/NDR —** delivered as software and distributed to each host
- **Comprehensive visibility and insight into applications and flows,** with policy automation integrated into the workload life cycle and enabling micro-segmentation at scale
- **Distributed firewalling capability at each host for scaling out the security architecture** to enable security operations teams to block the lateral movement of attack vectors, drive faster forensics, and automate IT security policies in a simpler operational model
- **Securing applications on corporate networks against known malicious IP addresses on the internet,** such as botnet masters (the list of malicious IP addresses is dynamically updated from the VMware global threat intelligence network)
- **Defense against known and unknown threats with threat prevention or advanced threat prevention add-ons for full-stack security —** firewalling, IDS/IPS, sandbox, NTA, NDR, and encrypted traffic monitoring

The Business Value of Networking and Lateral Security in VCF

Study Demographics

IDC conducted in-depth interviews with eight organizations about their experiences using VMware NSX and VMware vDefend solutions for VCF. Interviewers sought to understand the unique benefits of the NSX and vDefend solutions, as well as the combined value of using both solutions.

As shown in **Table 1** (next page), study participants had an enterprise-level profile with 52,900 employees and $32.25 billion in annual revenue on average (medians of 5,500 employees and $1.43 billion in annual revenue). They provided experiences with networking and lateral security for VCF solutions from organizations from both North America and Europe, the Middle East, and Africa, as well as a mix of industry verticals, including higher education (2), government, healthcare, legal, manufacturing, software, and telecommunications.

TABLE 1

Demographics of Interviewed Organizations

	Average	Median
Number of employees	52,900	5,500
Number of IT staff	5,621	275
Number of business applications	1,817	850
Annual revenue	$32.25B	$1.43B
Countries	United States (4), United Kingdom, Germany, Sweden, Switzerland	
Industries	Government, healthcare, higher education (2), legal, manufacturing, software, telecommunications	

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Choice and Use of Networking and Lateral Security for VCF

Study participants provided details about their reasons for choosing VMware NSX and VMware vDefend solutions that focused on their ability to maintain continuity with their broader VMware environments as well as strong networking and security functionalities. They realized that they needed an approach to providing networking and security capabilities to their organizations that would scale cost effectively and provide greater overall functionality. With VMware NSX and VMware vDefend, they perceived an opportunity to both achieve these objectives individually for their networking and security environments and take advantage of beneficial synergies from using the networking and security solutions.

Interviewed VMware customers described their considerations:

Integrated approach to security and networking:

"VMware Cloud Foundation offers a unique approach that brings us closer to the actual servers, so the security gets wrapped around actual servers instead of being at the edge — things are more integrated."

Ability to micro-segment within datacenters:

"We chose VMware Cloud Foundation because we preferred to go with vSAN and all the VCF solutions because we want to micro-segment to add a lot of security inside the datacenter … We cannot rely on perimeter security only. We also have to secure the datacenter, and we now have one stack that fits all our needs."

Speed of deployment, maintaining control with software-defined datacenter (SDDC):

"We chose VMware Cloud Foundation for fast deployment for our software developers, giving them the newest and best services to keep them inside our datacenter, and not putting them out into the wild cloud world … We are saving money by not putting it in the public cloud with a software-defined datacenter."

Price and availability of skilled resources:

"We chose VMware Cloud Foundation primarily for two reasons, which were price and availability of experienced resources. We have a global footprint but a primary operating location. We need to pick products where we can get at least semi-skilled people, and VMware gave us that."

Table 2 provides information about study participants' extensive use of VMware NSX and VMware vDefend solutions. Interviewed VMware customers reported supporting an average of 13 datacenters and 332 sites, demonstrating how they are using VMware NSX and VMware vDefend to run their distributed IT and business operations. The scale of their use is also evident in the average 44,986 employees who rely on IT services and an average of 61% of revenue running networking and lateral security for VCF.

TABLE 2

Use of VMware NSX and VMware vDefend by Interviewed Organizations

	Average	Median
Number of datacenters	13	3
Number of sites	332	5
Number of physical servers	586	132
Number of VMs/cloud VMs	15,094	1,775
Number of applications	1,377	700
Number of users of applications	44,986	2,000
Percentage of revenue supported	61%	80%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Business Value and Quantified Benefits of VMware NSX and VMware vDefend

Study participants reported achieving significant value through the use of VMware NSX Network Virtualization and vDefend Distributed Firewall solutions. Individually, the use of these solutions has enabled study participants to make their networking and security operations more efficient, robust, and cost effective. Combined, VMware NSX and VMware vDefend solutions have established more agile, secure, and high-performing IT foundations for their business operations.

Interviewed VMware customers gave specific examples of the critical impact in areas such as security, development, and business agility and performance:

Security of data, development team enablement:

"The number 1 value for us of VMware NSX and VMware vDefend is safe data and keeping that reputation. Next would be faster deployment for our 2,000 developers. Previously, to give a developer some resources, it took 2–3 weeks to provide the network infrastructure that we can now provide in minutes."

Enhanced security and ease of management:

"Security is the main benefit of VMware vDefend, but also the ease of manageability. Instead of having manual configurations on all the different switches and firewalls … We are also building on top of that to automate all those different pipelines, so it also helps with our automation going forward."

Significantly improved visibility into traffic and security:

"The biggest IT-related benefit of VMware NSX and VMware vDefend is visibility. It's much easier for us to see what everything's doing and understand the traffic flows, the patterns, the irregularities, where it's rare from a security perspective that massively helps us out … It's dramatically different."

Meet customer-driven security requirements:

"Security is a big thing right now, and our clients ask about how we ensure security, including questionnaires that ask about very specific topics. Networking and lateral security in VCF has allowed us to meet these goals and do it in an efficient way compared with other solutions, and it has simplified things for us."

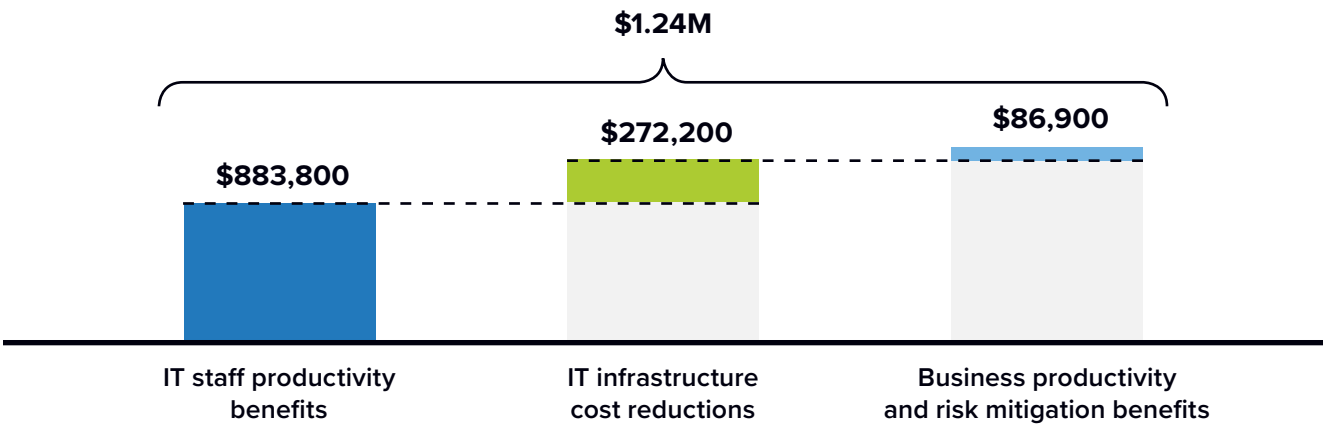
Based on interviews with customers using VMware NSX and VMware vDefend, IDC calculates that they will realize average annual benefits per datacenter worth $1.24 million ($16.0 million per organization) in the following areas:

- **IT staff productivity benefits:**
  Study participants make core IT teams, including development, networking, and security teams, significantly more effective. Networking and security teams require substantially less time to handle day-to-day activities, while development teams deliver significant value in support of business operations. IDC puts the value of staff efficiencies and productivity gains at an annual average of $883,800 per datacenter ($11.38 million per organization).
- **IT infrastructure cost reductions:**
  Study participants minimize their network infrastructure requirements through greater virtualization and consolidate their security point solutions, allowing them to significantly reduce direct costs. On average, IDC estimates that they will realize average annual cost savings of $272,200 per datacenter ($3.50 million per organization).
- **Business productivity and risk mitigation benefits:**
  Study participants minimize the operational impact of unplanned outages and enable business teams to better address opportunities with timely and high-quality services and solutions. IDC calculates that they will capture net productivity and revenue gains worth an annual average of $86,900 per datacenter ($1.12 million per organization).

FIGURE 1

Average Annual Benefits per Datacenter

($)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

For an accessible version of the data in this figure, see Figure 1 Supplemental Data in Appendix 3.

Networking Efficiencies and Cost Benefits

Study participants reported achieving significant networking-related staff and cost benefits from establishing SDDCs characterized by high virtualization with the VMware NSX Network Virtualization solution. Most frequently, they compared the positively enhanced visibility, agility, and automation available with VMware NSX with those of their legacy networking environments. The automation of responsibilities such as provisioning and troubleshooting means that less staff time must be dedicated on a day-to-day basis to running their networking environments. It creates simpler and less complex networking environments.

Interviewed VMware customers commented on how the use of VMware NSX has enabled their network infrastructure teams to perform more efficiently:

Automation speeds up IT-related activities:

"We have removed almost everything in terms of low-level tasks for the technicians with VMware NSX … This automation saves a lot of time for the network team and the server team."

Platform for consolidated and integrated IT team support:

"In our VMware NSX environments, we can leverage a single team who can build everything for me from compute, networking, security, etc., and take that through all our compliance, change control, etc., and achieve that much quicker and easier."

Substantial overall team efficiencies:

"We have the ability to work with more servers with fewer people with VMware NSX … Everything is automated today, so we only need a networking team of two compared with 14 previously — we moved those team members to other areas."

Shift staff focus from day-to-day operations:

"The biggest value of VMware NSX is the time savings, allowing our staff to learn about future technologies and learn about other things, instead of having to focus on operational matters."

Table 3 (next page) presents IDC's findings on the impact of using VMware NSX Network Virtualization on day-to-day network infrastructure team activities. On average, study participants reported a 25% efficiency increase for these teams, which frees up significant amounts of staff time to work on more complex network management activities or support other IT and business initiatives.

TABLE 3

Networking Team Efficiencies

Average per Organization	Before/Without VMware NSX and VMware vDefend	With VMware NSX and VMware vDefend	Difference	Improvement
Equivalent FTEs required for same workloads	19.8	14.7	5.1	25%
Value of equivalent FTE time required ($ per organization per year)	**$1.98M**	**$1.47M**	**$501,700**	**25%**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Interviewed VMware customers also reported a substantial reduction in their direct network infrastructure costs through the use of NSX Network Virtualization solutions. They benefit from creating a completely SDN overlay, which limits their need to purchase and run additional network hardware.

Further, by building a 100% SDN environment, they can establish an operational cost model for their network environments and move away from more expensive and time-consuming purchasing cycles. Interviewed VMware customers provided examples of these infrastructure efficiencies:

Network hardware cost savings:

"We've avoided hardware costs with VMware NSX because we don't need to invest as much in network switches — we're saving probably between $1 million and $2 million per year, which pays for VMware NSX."

Benefit of investing cost savings:

"We can invest the money we'd be paying to other cloud providers in hardware, people, support, and services. We're saving millions of dollars a year that we are now saving into ourselves."

Significantly lower power use:

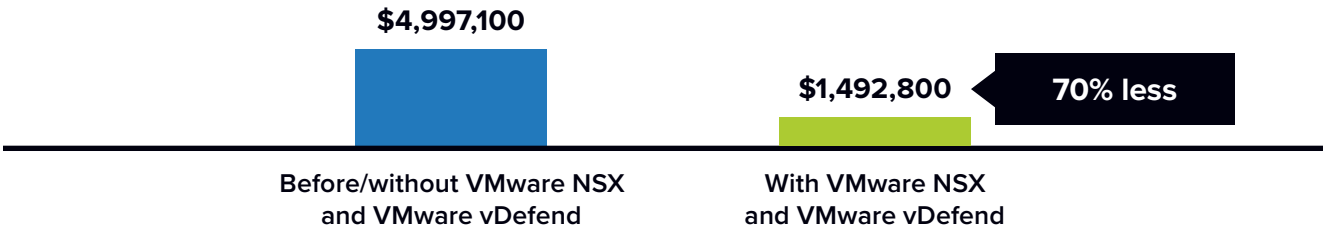
"VMware NSX is supporting our sustainability objectives because we have so much less footprint. The electricity usage is much less compared with the full bare metal set that we had before. We've reduced power use by at least 80%."

As shown in **Figure 2,** study participants have leveraged VMware NSX Network Virtualization to establish much more cost-effective network infrastructure environments. On average, they reported lowering their direct costs by 70%, thereby saving around $3.5 million per organization per year.

FIGURE 2

Average Annual Network Infrastructure Costs

(Annualized cost per organization ($))



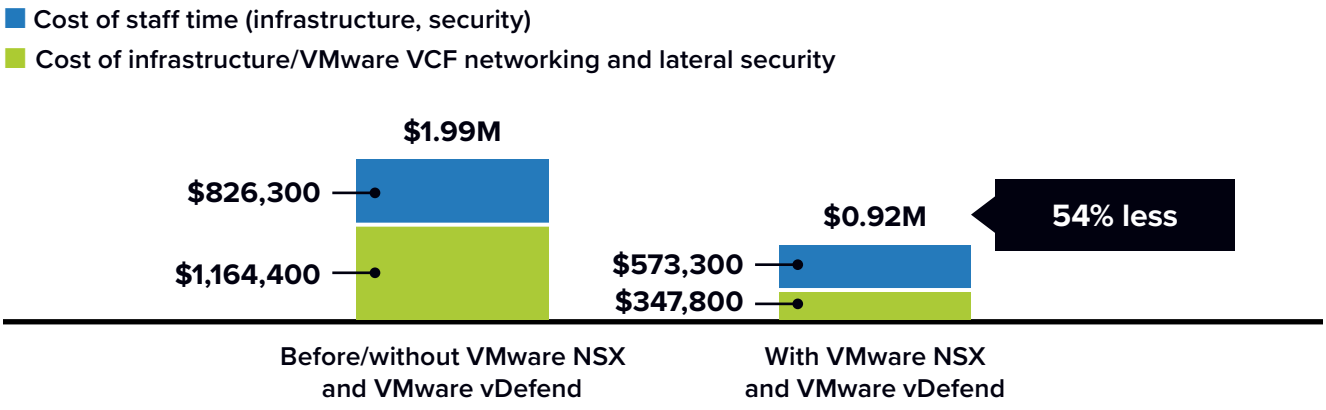
n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

These staff and infrastructure savings and efficiencies ensure that study participants can support their businesses with more cost-effective networking and security services. As shown in **Figure 3,** IDC calculates that they will save an average of 54% over three years in these two areas of cost, allowing them to save an average of more than $1 million per year per datacenter.

FIGURE 3

Three-Year Cost of Operations

(Three-year cost per datacenter ($))



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

For an accessible version of the data in this figure, see Figure 3 Supplemental Data in Appendix 3.

Security Benefits and Efficiencies

Study participants consistently reported achieving much-improved security outcomes with VMware vDefend Distributed Firewall solutions. They explained that embedded security functionality allows them to more readily identify threats and provide more comprehensive security capabilities for data and traffic coming into and moving across their networking and IT environments.

Study participants provided specific examples of how their security capabilities have improved with VMware vDefend solutions:

Much improved east-west traffic security capabilities:

"VMware vDefend has really been transformative in terms of security, certainly for the east-west firewall capabilities within micro-segmentation … Now, we have that real granular per VM control that really enhances our security."

Improved visibility drives more robust security:

"There has been a huge improvement in terms of security with VMware vDefend Distributed Firewall because we can see everything that was difficult to see in the past."

Robust security zones:

"VMware vDefend has helped us a lot in securing within the different security zones we have. Before, we had different security zones, but within that security zone, everything was open, and it was hard to keep track of flows."

Ease of segmentation with existing infrastructure:

"VMware vDefend helps with security because of the speed to be able to segment devices. We can do it much more quickly with no additional hardware."

Single view of security for all workloads:

"With VMware vDefend, we have one pane of glass to check 10 different environments, so we can see exactly where the problem is. We can see all workloads, so we can see everything now. It also provides segmentation of the people on the security team, including the security operation center and our operation team."

Allow for retirement of much more expensive physical hardware:

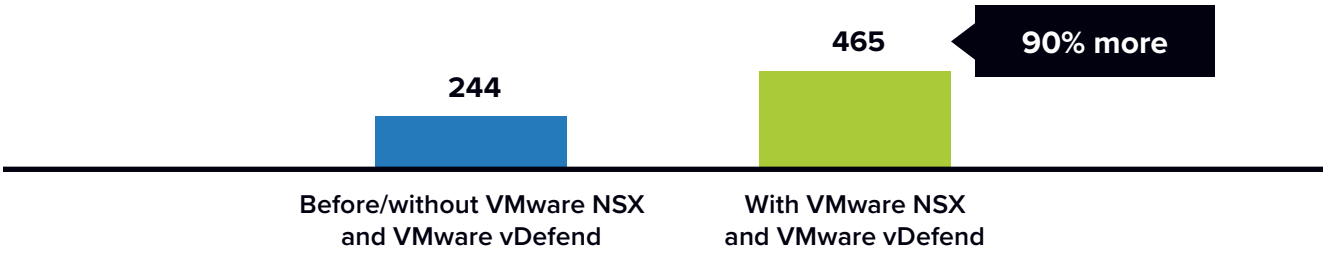
"VMware NSX and VMware vDefend will replace our physical firewalls when they are end of life. We pay more for those than VMware NSX and VMware vDefend by several times."

Figure 4 (next page) demonstrates how study participants have used VMware vDefend to establish and maintain better security controls through increased network segmentation. On average, they reported nearly doubling the number of network segments they maintain, reflecting their ability to apply unique and more granular security policies across employees, customers, and other third parties that access their private cloud network environments.

FIGURE 4

Impact on Network Segmentation

(Number of network segments per organization)



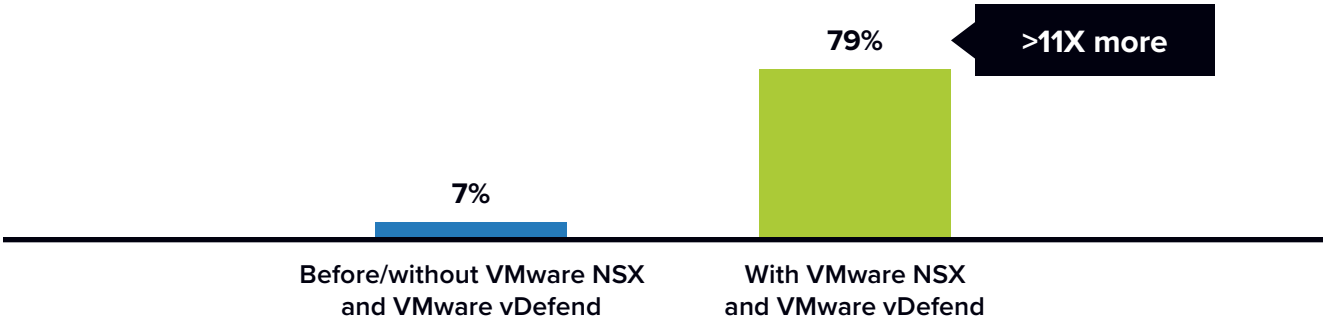
n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Figure 5 provides a key example of how VMware vDefend use has provided study participants with an important security capability that they largely lacked prior to deployment. For many organizations, east-west network traffic, or the flow of data and information within an organization's networking environment, is too often a relative blind spot. This means that if a security threat penetrates external firewalls, organizations have found it challenging to isolate and address as it moves across their internal networking environments. As shown in Figure 5, interviewed VMware customers have gone from securing very little of their east-west network traffic (7% on average) to securing a significant majority of network traffic (79% on average). This increase in coverage of more than 11 times reflects a significant and impactful gain for study participants in security capabilities. It helps them to limit the risk and potential damage associated with traffic flowing across their internal networks.

FIGURE 5

Impact on East-West Network Security

(Percentage of east-west traffic secured)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

These enhanced security capabilities of VMware vDefend Distributed Firewall alongside broader automation and virtualization benefits ensure that security teams perform more efficiently and effectively. One study participant spoke about how centralized management and having a single pane of glass ensures security operational efficiencies: *"VMware vDefend gives us centralized management of our firewalls, so we can leverage a single pane of glass rather than managing individual servers. This makes it easier to manage, and we need less staff time to manage — 12 staff members are saving around 15% each."* As shown in **Table 4**, interviewed VMware customers reported average efficiencies of 35% for their security teams from the use of VMware vDefend, which not only limits the amount of staff time devoted to day-to-day activities but also helps them ensure and apply the benefits from enhanced security functionality already discussed.

TABLE 4

Security Team Efficiencies

Average per Organization	Before/Without VMware NSX and VMware vDefend	With VMware NSX and VMware vDefend	Difference	Improvement
Equivalent FTEs required for same workloads	21.8	14.1	7.7	35%
Value of equivalent FTE time required ($ per organization per year)	**$2.18M**	**$1.41M**	**$766,700**	**35%**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Agility and Development Benefits

Study participants linked their use of VMwareNSX and VMware vDefend solutions to significant benefits in terms of agility and development team capabilities. They rely on their development teams to provide employees and customers with updated and new software functionality. They thus must try to minimize the extent to which network, security, and other infrastructure create friction that impairs development processes.

Interviewed VMware customers noted that they now have access to functionalities that help them move more smoothly through development processes as their teams seek to access networking, security, and other IT capacities to build, test, and deploy new applications and features.

In particular, study participants cited self-service access to capacity as especially impactful, alongside the overall ease of providing additional capacity and thus establishing needed testing and deployment environments:

Development operational efficiencies:

"Our developers are roughly 20% more productive with VMware Cloud Foundation because they can do all their own provisioning and don't have to wait for infrastructure … Now, we are using DevOps methods for the infrastructure management team. The networking engineers have become more cloud engineers in that they can also do a little bit of programming and a little bit of security."

Improvement in time to implement:

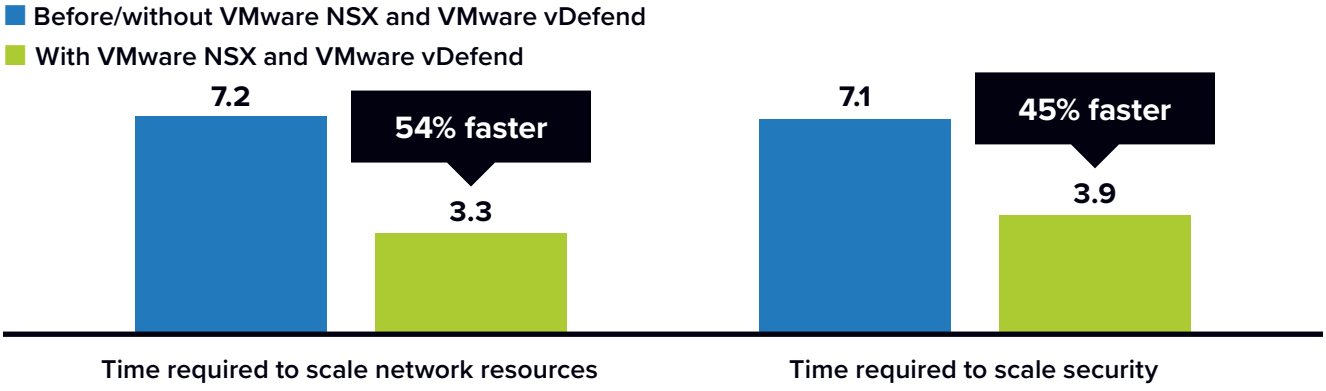
"VMware Cloud Foundation really supports our business with speed to implementation. For example, if our development teams need to deploy a new application but aren't sure about the infrastructure, VCF allows them to quickly put the application in, model the traffic, and then make decisions about the firewall rules required, all with the click of a button."

Figure 6 demonstrates how VMware NSX and VMware vDefend solutions enable study participants to readily scale networking and security capacity as needed by development and business operations. On average, interviewed VMware customers reported requiring 54% less time to provide new networking resources and 45% less time to extend security to a new environment, which is a key factor in speeding up development processes and scaling business operations to meet customer demand.

FIGURE 6

Impact on Agility

(Number of days)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

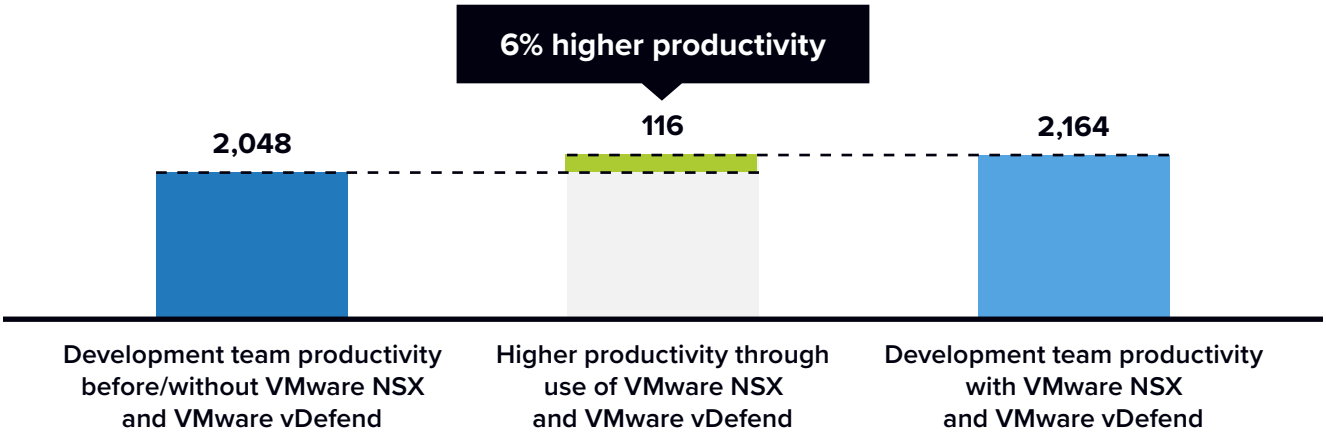
For an accessible version of the data in this figure, see Figure 6 Supplemental Data in Appendix 3.

Figure 7 reflects the significant value that study participants are achieving through the use of VMware NSX and VMware vDefend in terms of enabling their development teams. They have large development teams overall that consist of traditional development, DevOps, and even line-of-business developers who benefit from much-enhanced access to network and security capacity. As shown, IDC calculates that these teams — over 2,000 developers strong on average — will see average productivity gains of 6% with VMware NSX and VMware vDefend solutions.

FIGURE 7

Impact on Development Team Productivity

(Equivalent productivity, FTEs per organization)



n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

For an accessible version of the data in this figure, see Figure 7 Supplemental Data in Appendix 3.

Benefits of Reduced Operational Risk

Study participants must minimize the direct risk associated with security events and find ways to ensure operational continuity. Disruptions to applications and services caused by infrastructure problems can create significant operational friction for employees and even customers. When this happens, employees struggle to perform at their regular levels and communications with customers may be impaired.

Interviewed VMware customers consistently noted that they have reduced the frequency and impact of unplanned outages through centralized management, increased visibility into performance, and robust problem redressal.

Significant reduction in risk:

"With VMware NSX and VMware vDefend, we have visibility into what's going on in the datacenter and also the IPs that are dropping traffic and so on. This means that we know what's happening on the network and the real traffic, and what are the real threats. There is a huge improvement in terms of security with VMware."

Reduce business impact of unplanned outages:

"VMware NSX and VMware vDefend definitely change the number of unplanned downtime events because all of our infrastructure is managed from a centralized location."

Table 5 displays IDC's findings on the impact of using VMware NSX and VMware vDefend solutions on unplanned downtime for study participants. As shown, interviewed VMware customers reported reducing the frequency of unplanned outages by an average of 58%. This contributes to their ability to reduce the overall impact of unplanned outages on employee productivity by an average of 43%, which IDC quantifies as ensuring higher employee productivity levels worth an average of $1.02 million per organization per year.

TABLE 5

Impact on Unplanned Downtime

Average per Organization	Before/Without VMware NSX and VMware vDefend	With VMware NSX and VMware vDefend	Difference	Improvement
Number of unplanned outages per year	7.0	2.9	4.1	58%
Productivity loss in hours per user per year	1.2	0.7	0.5	43%
Productivity loss per year in FTEs per organization	34.0	19.4	14.6	43%
Value of lost productivity time per organization per year	**$2.38M**	**$1.36M**	**$1.02M**	**43%**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Business Benefits

Study participants reported that they ultimately run their businesses with greater flexibility and confidence with VMware NSX and vDefend solutions, which help them address customer demand and meet customer expectations. With VMware NSX and VMware vDefend, they can move faster when opportunities present themselves, ensure high-quality services, and minimize operational and reputational risk associated with potential security incidents. One interviewed VMware customer explained: *"In terms of scaling to meet business demand, that's roughly 70% faster with VMware NSX and VMware vDefend; network resources and security now take a few weeks where before it would take a couple of months."* For interviewed VMware customers, this type of ability to move faster helps win new customers and speed up revenue recognition.

As shown in **Table 6,** IDC's analysis shows that study participants are achieving important incremental business gains through the use of VMware NSX and VMware vDefend solutions. IDC estimates that they will capture average revenue gains of $1.96 million per year ($152,000 per datacenter), further demonstrating the value of their investment in VMware NSX and VMware vDefend solutions.

TABLE 6

Business Impact, Use of VMware NSX and VMware vDefend Solutions

	Per Organization	Per Datacenter
Higher revenue per year	$1.96M	$152,000
Assumed operating margin	15%	15%
Higher net revenue per year	$293,500	$22,800

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

ROI Summary

Table 7 (next page) provides IDC's analysis of the net benefits and costs for study participants of deploying and using VMware NSX and VMware vDefend solutions. IDC puts the discounted three-year benefits that they will achieve at an average of $37.85 million per organization ($2.94 million per datacenter) in networking staff and cost efficiencies, security staff and cost efficiencies, development productivity gains, reduced operational risk, and higher net revenue. These benefits compare with average three-year discounted investment costs of $5.33 million per organization ($0.41 million per datacenter). These benefits and investment costs would yield an average three-year ROI of 610% and enable interviewed VMware customers to break even on their investment in an average of six months.

TABLE 7

ROI Analysis

	Three-Year Average per Organization	Three-Year Average per Datacenter
Benefit (discounted)	$37.85M	$2.94M
Investment (discounted)	$5.33M	$0.41M
Net present value	$32.51M	$2.52M
ROI (NPV/investment)	610%	610%
Payback	6 months	6 months
Discount factor	12%	12%

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Challenges/Opportunities

While software-defined networking and security have meaningfully evolved over the past decade, IDC views scalability, performance consistency, robust security, multi-vendor interoperability, and resiliency as key challenges for SDI technologies.

IDC sees the ongoing operational challenges of adopting SDI technologies as opportunities for VMware's NSX Network Virtualization and vDefend Distributed Firewall capabilities to strategically benefit from new feature sets and platform capabilities that would differentiate VMware Cloud Foundation, broadly, from an assortment of point-product approaches to implementing SDI technologies.

Feature set differentiation is timely, as new secular growth drivers, such as GenAI and multicloud networking, are starting to meaningfully ramp up across industry verticals, as gauged from IDC's primary research with enterprise IT decision-makers.

For example, IT operational metrics in VMware NSX and VMware vDefend, in particular, could be significantly enhanced by "LLM training" and the VCF platform–generated data sets along with remediation and performance improvement approaches used by ITOps teams. This is to offer a conversational Q&A UI to IT and business decision-makers for natural language and visual interactions with a GenAI app that interfaces with the VCF private cloud platform. VMware could monetize this GenAI application as a value-added feature for IT practitioners.

Staying in lockstep with the hyperscalers to ensure that private and hybrid cloud operational model and user experience is at or above par versus product and user experience innovations in public cloud frameworks needs to be a top priority for Broadcom/VMware. This is to stay ahead of its competitors and grow IT mindshare and wallet share as midmarket and large enterprises worldwide accelerate their application modernization and digital transformation journeys.

Conclusion

The transition to a modern SDDC has become a pivotal element of many enterprises' digital transformation journeys. VMware Cloud Foundation has emerged as a comprehensive solution offering a suite of software-defined services for computing, storage, network, and security alongside cloud management capabilities. This integrated approach can help organizations address challenges around security, resiliency, manageability, and cost-efficiency in deploying distributed virtualized and containerized workloads across private and public cloud environments.

This IDC Business Value study articulates the substantial business value that organizations can achieve by adopting VMware NSX and vDefend solutions within the VMware Cloud Foundation platform. The findings underscore the importance of a modern SDI in accelerating digital transformation and datacenter modernization initiatives, enabling enterprises to build and manage cloud-scale applications more effectively and drive superior business outcomes. Interviewed VMware customers identified significant benefits they are achieving through their use of VMware NSX and VMware vDefend, including networking and security staff efficiencies, cost savings, and improved capabilities, projecting average annual benefits of $1.24 million per datacenter, which would result in a strong average three-year ROI of 610%.

Appendix 1: Methodology

IDC's standard Business Value/ROI methodology was utilized for this project. This methodology is based on gathering data from organizations currently using VMware NSX Network Virtualization and vDefend lateral security solutions as the foundation for the model.

Based on interviews with organizations using VMware NSX and VMware vDefend, IDC performed a three-step process to calculate the ROI and payback period:

1. **Gathered quantitative benefit information during the interviews using a before-and-after assessment of the impact of using VMware NSX and VMware vDefend.** In this study, the benefits included cost savings, IT staff and development team efficiencies and productivity gains, reduced costs associated with risk, and higher revenue.
2. **Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using VMware NSX and VMware vDefend and can include additional costs related to migrations, planning, consulting, and staff or user training.
3. **Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of networking and lateral security in VCF over three years. ROI is the ratio of the net present value and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI 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 manager productivity savings. For this analysis, 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 per year for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).

- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- IDC applies a net margin assumption (15%) for gross revenue gains attributed to interviewed organizations' use of VMware NSX and VMware vDefend, which results in the net revenue calculations applied to IDC's model.
- Because VMware NSX and VMware vDefend require a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC prorates the benefits monthly and then subtracts the deployment time from the first-year savings.

Appendix 2: Quantified Benefits of Use of VMware NSX and VMware vDefend Solutions

Table 8 provides details about the average annual value that study participants attributed to their use of VMware NSX and VMware vDefend solutions, which IDC calculates will equal $16.0 million per year over three years.

TABLE 8

Average Annual Benefits

Category of Value	Average Quantitative Benefit	Calculated Average Annual Value*
IT infrastructure cost reductions	70% average cost savings, $3.50M in savings per year	$3.50M
Network infrastructure team efficiencies	25% average efficiencies, worth 5.0 FTEs, $100,000 salary assumption	$428,600
Security team efficiencies	35% average efficiencies, worth 7.7 FTEs, $100,000 salary assumption	$655,000
Troubleshooting team efficiencies	31% average efficiencies, worth 4.8 FTEs, $100,000 salary assumption	$414,000
Development team productivity gains	6% average productivity gain, worth 116 FTEs, $100,000 salary assumption	$9.88M
Higher user productivity, downtime	43% less unplanned downtime, worth 0.5 hours of higher productivity per user, 14.5 FTEs per org, $70,000 salary assumption	$868,200
Higher net revenue	$1.96M higher revenue per year, 15% margin assumption	$250,800
Total average annual benefits per organization	**$16.0M**	

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

* Data includes 5.2 months, deployment time in year 1.

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

Appendix 3: Supplemental Data

This appendix provides an accessible version of the data for the complex figures in this document. Click "Return to original figure" below each table to get back to the original data figure.

FIGURE 1 SUPPLEMENTAL DATA

Average Annual Benefits per Datacenter

	Average Annual Benefits per Datacenter ($)
IT staff productivity benefits	$883,800
IT infrastructure cost reductions	$272,200
Business productivity and risk mitigation benefits	$86,900
Total	**$1.24M**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Return to original figure

FIGURE 3 SUPPLEMENTAL DATA

Three-Year Cost of Operations

	Cost of Infrastructure/ VMware VCF Networking and Lateral Security	Cost of Staff Time (Infrastructure, Security)
Before/without VMware NSX and VMware vDefend	$1,164,400	$826,300
With VMware NSX and VMware vDefend	$347,800	$573,300
Total	**$1.99M**	**$0.92 (54% less)**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Return to original figure

Appendix 3: Supplemental Data (continued)

FIGURE 6 SUPPLEMENTAL DATA

Impact on Agility

	Before/Without VMware NSX and VMware vDefend	With VMware NSX and VMware vDefend
Time required to scale network resources	7.2	3.3
Time required to scale security	7.1	3.9
Difference	**54% faster**	**45% faster**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Return to original figure

FIGURE 7 SUPPLEMENTAL DATA

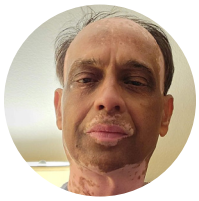
Impact on Development Team Productivity

	Equivalent Productivity, FTEs per Organization
Development team productivity before/without VMware NSX and VMware vDefend	2048 FTEs
Development team productivity with VMware NSX and VMware vDefend	2164 FTEs
Higher productivity through use of VMware NSX and VMware vDefend	116 FTEs
Difference	**6% higher productivity**

n = 8; Source: IDC Business Value In-Depth Interviews, January 2024

Return to original figure

About the IDC Analysts



Vijay Bhagavath
Research Vice President, Cloud and Datacenter Networks, IDC

Vijay Bhagavath is IDC's Research Vice President, Cloud and Datacenter Networks. He provides actionable thought leadership and pragmatic insights on cloud and datacenter networking markets and technologies. Vijay has a deep understanding of the overall networking market, technologies, product road maps, competitive differentiation, and deployment strategies, enabling him to provide insightful commentary and guidance for vendors, cloud providers, enterprise IT buyers, and practitioners.

More about Vijay Bhagavath

Matthew Marden
Research Vice President, Business Value Strategy Practice, IDC

Matthew is responsible for carrying out custom business value research engagements and consulting projects for clients in a number of technology areas with a focus on determining the return on investment of their use of enterprise technologies. Matthew's research often analyzes how organizations are leveraging investment in digital technology solutions and initiatives to create value through efficiencies and business enablement.

More about Matthew Marden

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.

IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

idc.com @idc @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. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.