Extend Security and Control from the Data Center Edge to the Core

Discover how micro-segmentation, delivered through network virtualization, provides comprehensive data center security, accelerates delivery time, and enhances the agility of your data center.
INTRODUCTION

As enterprises increasingly virtualize their physical data centers, they are discovering greater efficiency, agility, and cost-savings. Now, with a VMware NSX® powered Software-Defined Data Center (SDDC), enterprises can extend these benefits to their network as well, and realize a more powerful approach to security.

Research shows that the variety and volume of threats continue to grow. Ponemon Institute’s tenth annual Cost of Data Breach Study illustrates the seriousness of this observation. The average total cost of a data breach for companies increased 23 percent on a year-over-year basis to a whopping $3.79 million in 2015. The average cost paid for each lost or stolen record containing sensitive and confidential information increased 6 percent, jumping from $145 in 2014 to $154 in 2015.

The SDDC extends the concepts of server virtualization — abstraction, pooling and automation — to all areas of the data center including networking, security and storage. VMware NSX adds significant security benefits by enabling micro-segmentation — the ability to securely isolate networks from each other through automated finegrained security policies tied to virtual machines, allowing the wrapping of security controls around much smaller groups of resources.

Network virtualization can help your organization address three major issues you face with your network:

1. the increasing inadequacy of a perimeter-centric security strategy,
2. the delivery of networking and security services, and
3. the rigidity and lack of responsiveness to changing demands and security conditions.
If you are the chief information security officer for your company, we know you’re mindful of the constantly evolving threats, changing laws, compliance issues, and training needs of your personnel.

If you are an infrastructure architect, you care deeply about the big, operational challenges emerging across the data center, including complex, brittle, and non-scalable service integration architecture and processes, both on-and off-premise.

Whether you are an architect or a security officer, VMware NSX will help you address the challenges you are facing.

---

**Security Controls Native to Infrastructure**

The VMware NSX network virtualization platform, with native security controls, delivers for networking what VMware has already delivered for compute and storage. With VMware NSX you can create, save, delete, and restore virtual networks on demand, just as you would with server virtualization, all without reconfiguring your physical network.

What’s more, by extending data center virtualization to the network, enterprises are gaining the additional advantage of increased security, inside the data center. Traditional security solutions — whether physical or virtual — pose major challenges: perimeter-centric security, complex management, and rigid architectures which result in lengthy deployment times and inability to adapt to changing data center security requirements. This eBook illustrates how VMware NSX makes micro-segmentation a reality in order to meet these challenges — providing security teams the ability to protect the data center from within.
POWERFUL SOLUTIONS TO TODAY’S NETWORK SECURITY ISSUES

**Issue 1:** Perimeter protection is not enough to prevent breaches

Most enterprise IT professionals would agree, securing the network only at the perimeter is inadequate for today’s data centers. Modern attacks can exploit a perimeter-centric defense. Once the malware has managed to make it inside a data center, by latching onto an authorized user or by some other means, it can move easily from workload to workload within the data center. This lateral movement is possible due to a lack of sufficient internal network controls regulating server-to-server or east-west network traffic.

A stricter, micro-granular security model effectively points to the need for unique firewalling of each individual workload. Until now, this has been cost-prohibitive and operationally infeasible.
**Solution:** Micro-segmentation brings security inside the data center

VMware NSX network virtualization capabilities enable you to create entire networks in software. Along with automated fine-grained policies that are tied to the individual virtual machines they protect, this securely isolates networks from each other, delivering an inherently better security model.

VMware NSX enables the three key functions of micro-segmentation:

1. isolation (no communication across unrelated networks),

2. segmentation (controlled communication within a network), and

3. security with advanced services (tight integration with third-party security solutions). VMware NSX makes it feasible for the first time to tie flexible security policies to your virtual network, virtual machine, and operating system, providing granularity down the virtual network interface card.

Security policies are automatically applied, updated, moved and removed along with the virtual machines they protect. VMware NSX achieves this by integrating security functions into the hypervisor itself, and since the hypervisor is already distributed throughout the data center, the most robust security available for your Software-Defined Data Center is built in, not bolted on. VMware NSX prevents unauthorized network incursions from spreading laterally inside your network, piggy-backing on other workloads. By implementing security controls as virtual ‘choke points’ on the network, it enforces rules and either blocks or allows application traffic to pass through.
“Not unlike the banking industry, the k12 education space also has regulations concerned with keeping the data kept on minors’ Personally Identifiable Information (PII) safe. It’s bad if PII data is stolen from a corporation; it’s crippling if you don’t protect student data. That’s why micro-segmentation, policy-based automation and auditability with VMware NSX are critical to what we do.”

Jason Radford, Head of Operations, IlliniCloud.
**Issue 2:** Delivery time of networking and security services

Today’s data center operators are under constant pressure to respond efficiently and quickly to changing business conditions. But it’s difficult to swiftly develop, test, and deploy new applications, expand or modify existing application infrastructure, or retire legacy systems. The time and effort required to provision new networking and security services seriously limits how responsive the data center can be to meeting the needs of the organization.

**Solution:** Reduce provisioning steps, speed time to deployment

VMware NSX abstracts virtual networks from the underlying physical network, reducing the time needed to deliver multi-tier networking and security services from weeks to minutes.

Leveraging this new operational approach to networking allows you to programmatically create, provision, snapshot, delete and restore complex networks all in software. Each network is individually customizable for the workloads it supports, as well as isolated from all other virtual networks for increased security.

As a result, you can achieve faster deployment, while being flexible enough to run on top of any network hardware.
“Deploying a Software-Defined Data Center, and taking advantage of VMware NSX to overcome the barriers of traditional networking hardware, gives us a major advantage over our competitors... VMware was the right partner with the best Software-Defined Data Center portfolio, and the strongest partner ecosystem, to help us on this journey.”

Michael Mossal, CIO, JOIN Experience

See the JOIN Experience Customer Snapshot on how speed and flexibility are being experienced by VMware users right now.


**Issue 3: Rigidity and lack of responsiveness of traditional networks**

Organizations running their data centers with traditional systems are often locked into a rigid network framework and cannot respond fast enough to the changing demands and security conditions of a typical data center.

When the existing data center doesn’t easily allow for integration of third-party network and security services, changes can be slow to implement and error-prone, making them poorly suited to address fluctuating demands. This often results in degraded service and performance levels.
Solution: Adapt dynamically to changing network requirements and threat conditions

VMware NSX is the platform for advanced networking and security services. You can configure virtual networks dynamically and automatically, adding new networking and security services from an ecosystem of partners as needed. VMware NSX then allows these third-party services to share information with each other to adapt to changing threat conditions.

VMware NSX is the networking platform for the SDDC, giving you the tools to:

- **Integrate advanced functionality from leading vendors:** The industry’s leading providers of software and hardware for networking and security have integrated with VMware NSX, making it possible to meet the demands of the most sophisticated data centers.

- **Automate the delivery of network services:** VMware NSX allows cloud management platforms to automate the delivery of network services, eliminating the need to manually reconfigure physical network devices. You can then build advanced workflows to automate provisioning of networking and security including switching, routing, firewalls, and load balancing.

- **Bridge the physical and virtual parts of the data center:** VMware NSX enables you to connect your virtual networks to physical workloads and legacy VLANs, and products from VMware’s technology partners extend this capability to physical switches as well.
“VMware has ushered cloud computing into mainstream IT environments and one by one, tackled barriers to broad adoption so customers can achieve the promise of network agility, flexibility and speed. Our partnership with VMware, which brings together two best-of-breed platforms, represents one giant step towards eliminating security concerns for customers so they can safely enable business applications, securing their networks from cyber threats, and accelerating their cloud deployments.”

Lee Klarich, Senior Vice President of Product Management at Palo Alto Networks.

The Issue
Perimeter protection is not enough to prevent breaches

Adapts dynamically to changing network requirements and threat conditions

The Solution with VMware NSX
Micro-segmentation brings security inside the data center

Reduces provisioning steps, speeds time to deployment

Perimeter protection is not enough to prevent breaches

The network security issues facing IT now, and the solutions provided by VMware
CUSTOMER SNAPSHOT: ILLINICLOUD

IlliniCloud is a nonprofit consortium launched two years ago to provide state-of-the-art computing resources to K-12 education in Illinois. The IlliniCloud allows districts and individual schools to share hardware, applications, services and IT support, at a fraction of the cost of purchasing and managing these systems themselves.

In order to be successful, IlliniCloud needed to create a multi-tenant environment so that multiple organizations could access the same infrastructure. Fine grained, robust security was also a major requirement to protect each organization and its data. Finally, IlliniCloud had to reduce infrastructure costs without sacrificing important capabilities.

Network virtualization with VMware NSX was deployed in IlliniCloud’s production environment in a matter of weeks. The platform enables IlliniCloud to decouple the data center network from the underlying physical hardware to gain massive scale while simplifying network design and operations. With VMware NSX, IlliniCloud has consolidated management operations for disparate physical networks running in the data center, and manages these networks as a single logical network. The IlliniCloud team is not only virtualizing the network, but also virtualizing security and load balancing services.

Implementing VMware NSX continues to benefit IlliniCloud by providing significant cost savings. VMware NSX gives IlliniCloud flexibility in infrastructure by allowing them to choose the hardware they want, and deploy it where and when they want. It also enables deferred capital expenditures for hardware since VMware NSX can be used across the existing infrastructure.
Jason Radford, Head of Operations for IlliniCloud, said “We’re in the drive to commodity, which is the drive to reduce cost and change the economic models around things like firewalls, routing, VPN and network services. Ultimately, I want VMware NSX to replace all of my hardware firewalls and load balancers. We believe that if everything works as planned, we can cut over costs by upwards of 65% factoring in all of the hardware, maintenance and automation gained.”

The results of the IlliniCloud deployment are nothing short of amazing for students, faculty and staff. It is now estimated that each educational institution that joins the cloud can potentially cut its own annual IT spending by 30 to 50 percent, freeing up money for other important educational needs while also offering them tighter security and data protection.
CUSTOMER SNAPSHOT: JOIN EXPERIENCE

JOIN Experience is executing on a plan to become a major player in the European mobile telecom and IT services market and needs a robust, secure and agile platform to roll out world-class 4G services and cloud infrastructure.

Their solution was to build a Software-Defined Data Center featuring VMware NSX — from the ground up. For JOIN, a fully virtualized infrastructure was the best way to deliver robust and flexible services rapidly to accelerate their growth.

This infrastructure based on VMware NSX has allowed them to flexibly develop and scale new machine-to-machine (M2M), mobile virtual network operator (MVNO) and other enterprise cloud service offerings across Europe. They have overcome the limitations of traditional hardware-defined networking, including manual provisioning and operations, and high overhead costs. As a result, they’re able to respond flexibly to diverse customer demands and market dynamics across different territories.
CONCLUSION

The power to virtualize your network, with embedded security You’ve already experienced the efficiency, productivity and cost-saving benefits of virtualization in your server environment.

Now it’s time to take the next step towards the software-defined data center, and apply virtualization and micro-segmentation to the network with VMware NSX.

VMware NSX empowers chief information security officers and infrastructure architects to react quickly to prevent breaches. It facilitates faster deployment and delivers greater agility. It enables you to automate the delivery of network and security services, thereby speeding up IT’s response to rapidly changing business needs.

And with micro-segmentation, you not only have robust security measures in place to ensure isolation and segmentation of threats, you have the infrastructure to add advanced security services to secure the next-generation data center.

VMware NSX is the ideal network virtualization platform for your Software-Defined Data Center. It provides enhanced security, reduces costs, improves productivity, and accelerates IT compliance.

Learn more about the benefits of VMware NSX at vmware.com/products/nsx.