VMware NSX

Helping IT move at the speed of business

"Technology continues to accelerate at an incredible pace, promising great rewards to organizations capable of seizing the initiative."

Bart Van Ark, Ph.D.
Executive Vice President, Chief Economist and Strategy Officer
The Conference Board

VMware NSX® is the network virtualization and security platform that enables VMware's cloud networking solution with a software-defined approach to networking that extends across data centers, clouds and application frameworks. With NSX, networking and security are brought closer to the application wherever it's running, from virtual machines (VMs) to containers to physical servers. Like the operational model of VMs, networks can be provisioned and managed independent of underlying hardware. NSX reproduces the entire network model in software, enabling any network topology—from simple to complex multitier networks—to be created and provisioned in seconds. Users can create multiple virtual networks with diverse requirements, leveraging a combination of the services offered via NSX or from a broad ecosystem of third-party integrations—ranging from next-generation firewalls to performance management solutions—to build inherently more agile and secure environments. These services can then be extended to a variety of endpoints within and across clouds.

Competing demands lead to compromises

Speed and agility, robust security, and high availability of applications are all critically important priorities for IT organizations to drive toward. Organizations depend so heavily on a solid application infrastructure that, increasingly, IT is the foundation enabling organizations to innovate and succeed in their digital transformation journeys. However, the rapid pace of change and shifting expectations in IT cause constantly changing priorities that often compromise effective delivery.

IT is painfully aware of the frequent tension caused by accommodating multiple stakeholders to meet these demands, often being forced to give preference to one IT priority over another. For example, speed of application deployment is often a casualty of securing that application due to the rigid complexities associated with security. Similar compromises are often made for availability of applications across environments, effectively placing IT at odds with the broader organization and vice versa.

The ultimate outcome of this constant tension and compromise has tremendous consequences for IT. In fact, it leads to serious deficiencies in multiple areas of responsibility: Organizations are unable to meet demands quickly, vulnerabilities exist across the data center and cloud environments, and overall agility is lacking.

Key benefits

- Granular security – Prevents the lateral spread of threats in the environment with micro-segmented security policy at the workload level
- Speed and agility – Reduces network provisioning time from days to seconds, and improves operational efficiency through automation
- Consistent policy and operations – Consistently manages networking and security policies independent of physical network topology across data centers, public and private clouds, and application frameworks

Unlocking the full potential of infrastructure

Most organizations have already virtualized compute components in their data centers. In addition, many organizations have also made the decision to virtualize storage, with more than 70 percent of them having already adopted or planning to adopt software-defined storage.

This abstraction of functionality from hardware into software enables organizations to quickly provision application components, move virtual systems across and between data centers, and automate critical processes. Without virtualizing switching, routing, load balancing and firewalling, the full value of the software-defined data center will remain elusive.

The fact is that organizations that possess network architectures rooted in hardware can't match the speed, agility or security of those deploying virtualized networks. The state of the organization is being held hostage by the state of the network.

A fundamentally new approach to data center networking 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 organizations back from unleashing their full potential need to be rewritten to enable IT to perform without compromises. As thousands of organizations have now realized, network virtualization is that new approach.

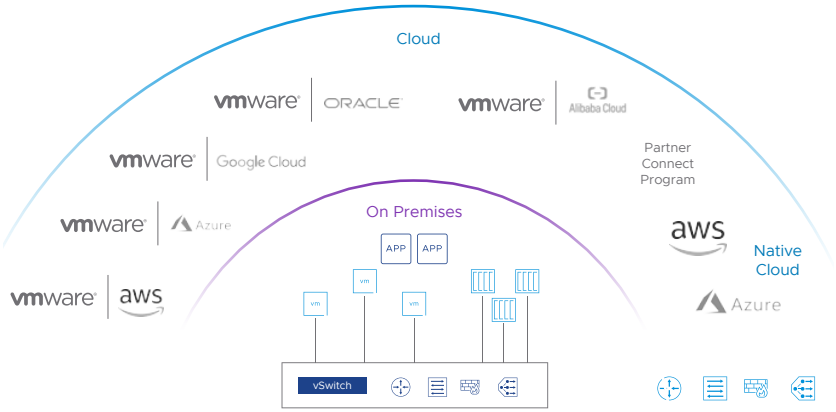

Figure 1: Consistent networking and security with NSX.

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 VMs. NSX extends common networking and security policies across heterogeneous environments and application frameworks, enabling these benefits to be realized across data centers, private and public clouds, traditional applications, and modern applications. This, in turn, enables levels of security and efficiency that have previously been operationally and financially infeasible.

Key features

- Distributed stateful firewalling – Enables stateful firewalling up to Layer 7, embedded in the hypervisor kernel, distributed across the entire environment with integration directly into cloud native, native public clouds and bare-metal hosts
- Context-aware micro-segmentation – Dynamically creates security groups and policies, and automatically updates them based on many attributes and Layer 7 application information to enable adaptive micro-segmentation policy
- Cloud management – Natively integrates with VMware vRealize® Suite, OpenStack and more, and fully supports Terraform Provider, Ansible modules, and PowerShell integration
- Third-party integration – Enhances security and advanced networking services through an ecosystem of leading third-party vendors
- Cloud native support – Supports enterprise-grade advanced networking and security across container platforms, VMs and bare-metal hosts with container network visibility
- NSX Intelligence™ – Reduces time to discover, analyze and enforce application segmentation policies without any new tools or agents to deploy; simplifies security operations with intrinsic security built into the infrastructure
- NSX Distributed IDS/IPS™ – An advanced threat detection engine purpose-built to detect lateral threat movement on east-west traffic using built-in distributed analysis and curated signature distribution

With NSX, IT can become an enabler of innovation for the organization, being able to say "yes" to multiple stakeholders at once 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 speed of business.

Intrinsic security

VMware NSX leverages unique visibility into application composition—from network communications to process-level behavior on individual workloads—granted by its built-in position in the hypervisor and other native control points on top of which applications are built. This visibility drives the automated creation of network security policies based on the intended security posture for the application. This decreases the amount of time IT/information security and application development teams spend in security review cycles.

It also enables the extension and enforcement of security policies across multi–data center and hybrid cloud environments, and grants ubiquitous control over applications built on VMs, containers and bare-metal servers. NSX Intelligence provides continuous data center–wide visibility to radically simplify and automate the process of operationalizing micro-segmentation.

NSX Distributed IDS/IPS helps achieve compliance easily, create virtual security zones, and detect lateral threat movement on east-west traffic. NSX also extends visibility and control to third-party security services, such as next-generation firewalls, intrusion prevention system (IPS)/intrusion detection system (IDS) solutions, and antivirus tools, increasing their efficacy.

NSX shifts security from a reactive add-on process to the application development lifecycle to a proactive, integrated and automated step in the lifecycle. Newly provisioned workloads automatically inherit security policies that stay with them throughout their lifecycle. When workloads are deprecated, so are their security policies, decreasing policy bloat over time and simplifying management.

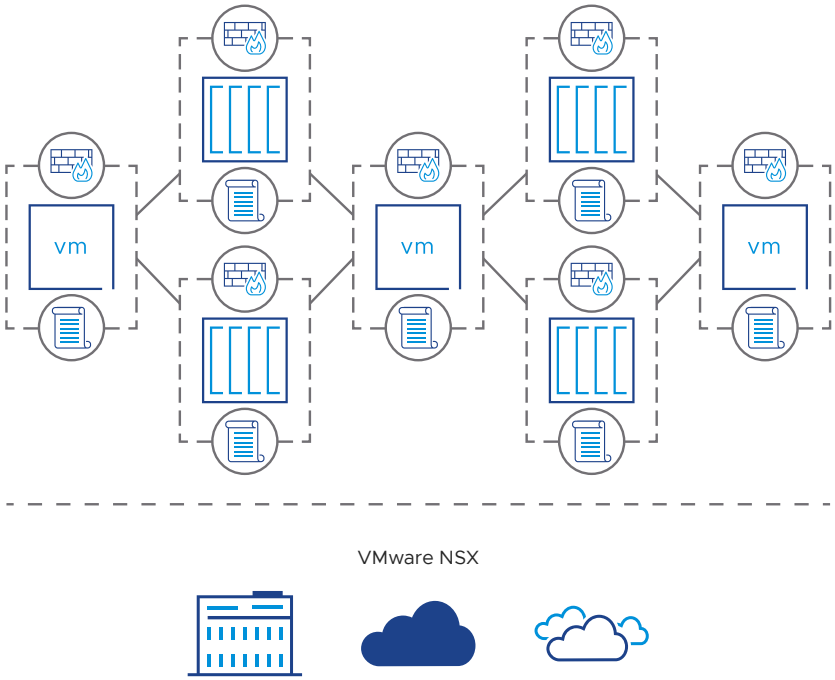

Figure 2: Enforce security at the most granular level of the data center.

Automation

As the scope pace of organizations continues to grow and accelerate, automating virtualized networking and security ensures that services and applications are created and deployed at the speed of business. By removing manual, error-prone network provisioning tasks through automation, the speed of application deployment substantially increases.

VMware NSX paired with cloud management software (for example, VMware vRealize Automation Cloud™) can manage the provisioning, deployment, operations and retirement of networking and security infrastructure and applications from a central control pane. By integrating the networking and security lifecycle into the process using tools such as Terraform and Ansible, VMware automates all infrastructure operations, and eliminates networking and security as a bottleneck in the application lifecycle.

Automation for the networking and security of both traditional (VM-based) and new (container-based) apps is made possible by extending common networking and security policies across both frameworks. Additionally, this enables the automatic deployment, mobility and retirement of applications across on-premises data centers, private clouds and public clouds.

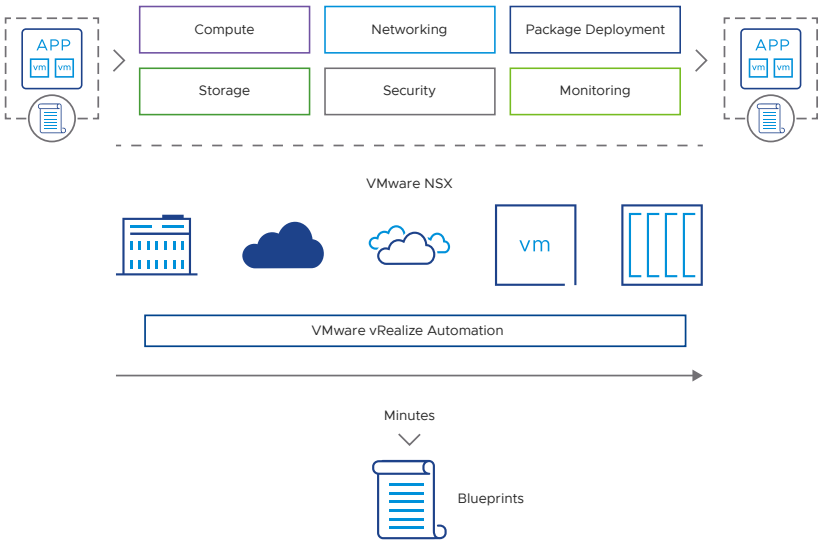

Figure 3: Rapid and repeatable deployments with automated networking and security.

Multi-cloud networking

NSX and NSX Cloud™ provide a unified networking and security model across sites, eliminating manual network configuration and achieving high operational efficiency through network automation. Network and security policies remain with the individual workload through its lifetime, simplifying policy and management in hybrid and multi-cloud environments. NSX federation enables centralized policy management across locations (on-premises and cloud), offering operational simplicity and consistent enforcement across clouds.

This also enables organizations to migrate VMs or entire data centers from one location to another with minimal or no application downtime. As a result, organizations can expedite recovery during planned migrations and unplanned outages. With network and security spanning heterogeneous environments, organizations can also leverage their resources from various physical data centers to operate as a single private cloud. This form of resource pooling with active-active data centers is called multi–data center pooling, or metro pooling.

Together, these deliver secure and seamless application mobility, making it easy to migrate to and from the cloud or between physical sites. NSX and NSX Cloud extend the same virtualized network and security platform that IT organizations use on their infrastructure into the cloud or other sites, resulting in a fast, low-touch migration process.

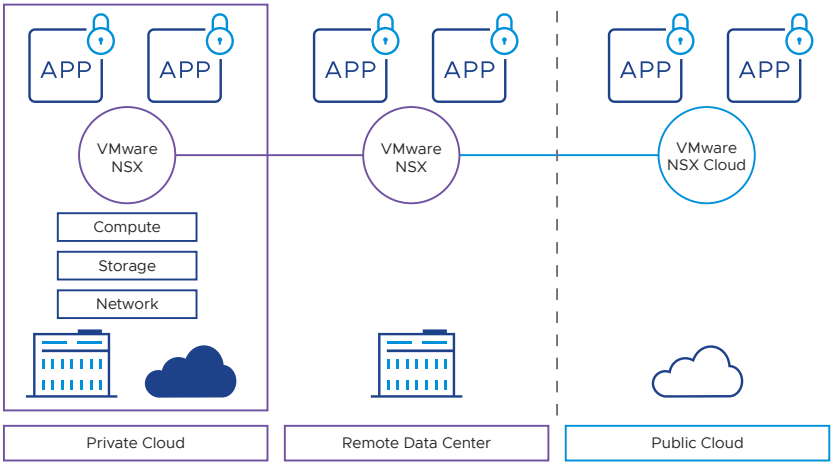

Figure 4: Get consistent networking and security across sites and clouds while reducing the impact of outages.

Networking and security for modern apps

VMware NSX integrates with new app platforms to offer networking and security functionality (such as load balancing, firewalling, switching and routing), done completely in software, and consumable in an infrastructure-as-code, API-driven fashion.

As applications become increasingly based on containers and microservices architectures, it is necessary to be able to connect and secure these new applications down to the individual workload. NSX treats containers and microservices as first-class citizens, the same as any other workload or endpoint, including the ability to do L3 networking. It can natively do container-to-container networking, as well as micro-segment down to the individual container level, enabling micro-segmentation for microservices, with policies that follow workloads as they are provisioned, changed, moved and retired.

NSX integrates with multiple application and container orchestration platforms, hypervisors and public cloud environments. It also integrates across application platforms to bring inherent, agile networking and security to new applications as they are developed.

Learn more

For more information, see the following resources:

- *VMware NSX product page*
- *VMware NSX datasheet*
- *VMware NSX Intelligence solution overview*
- *VMware NSX Distributed IDS/IPS product page*

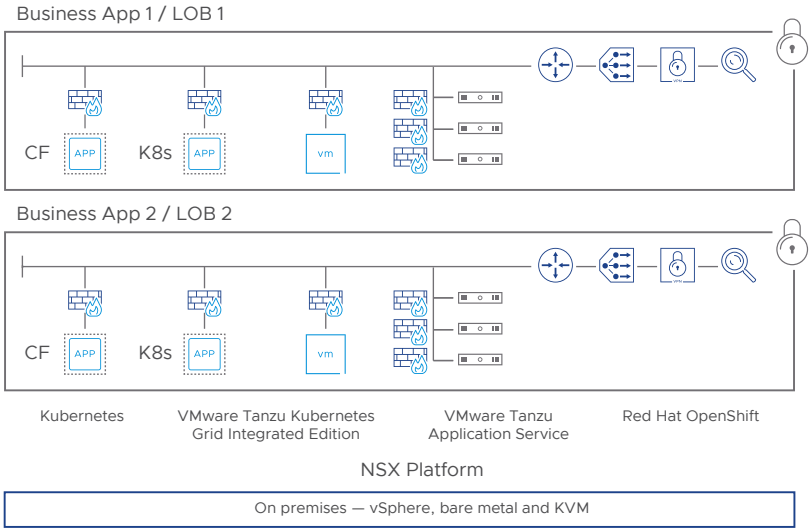

Figure 5: Bring advanced networking and security to containerized workloads across application frameworks, platforms, sites and clouds.

Accelerate business value today and set the stage for the future

Organizations that have deployed NSX find that it quickly becomes the defining factor for the success of their IT organizations and a foundational part of their data center infrastructure and multi-cloud strategies. Today, thousands of NSX customers accelerate the delivery of value to their organization, delivering some of their most sensitive and critical applications on top of fast, agile and secure virtual networks in a way that simply can't be achieved on traditional hardware-based networks.

This evolution in networking and security allows NSX customers to reap significant and immediate benefits, and also removes the time-consuming and arduous tasks that previously occupied so much of their organizational bandwidth. This, in turn, gives these organizations the latitude to consider improved organizational strategies as they plan for the future of the organization and for the necessary functions of IT to support that vision.