vmware®

GET STARTED

The Digital and Hybrid Cloud World: Are You Ready?

Network automation: Hybrid cloud management and network virtualization

Overcome Obstacles to Speed Application Delivery

Applications are the lifeblood of business. Now that users worldwide communicate, collaborate and transact through applications, many organizations are pursuing newer business models and revenue streams that require modernizing how work is done. Digital business changes how all industries operate, and the race to digital transformation drives line-of-business demands on IT to dramatically speed application delivery, becoming more agile in the process.

Many IT organizations find it difficult to provide resources to development, quality assurance (QA) and other teams faster. Often, infrastructure resources require a manual, complex deployment that negatively impacts when, where and what applications and services can be deployed—slowing time to market, productivity and revenue potential. As a result, businesses miss opportunities and cannot quickly create competitive differentiation.

Deploying today's multitier applications into highly virtualized or cloud environments can be complex. To improve day-to-day operations for development and QA teams, some IT organizations have automated the deployment of virtual machines (VMs) and multitiered application components. Even with this approach, faster component provisioning only partially solves their businesses' speed and productivity challenges because most have not addressed network or security operations.

End users still have to wait for networking and security resources that are typically still provisioned manually. IT needs to be able to author individual machines and configure them together as working applications with all of the appropriate microservices, storage, networking and security resources in a complete and automated fashion. When networking and security are done manually, it takes excessive amounts of time and introduces significant security and operational risk. With business success and brand reputation at stake, IT also must be prepared to continuously monitor ongoing operations to ensure quality of service and compliance.

Software-Defined Approach

Modern applications require a software-defined approach that leverages automation to give businesses the speed, consistency and quality needed to support ever-changing requirements. With a software-defined model, traditional businesses transform into digital businesses with greater agility. VMware's software-defined data center (SDDC) is a modern architecture for IT that helps automate the end-to-end infrastructure and application delivery process, including networking and security.

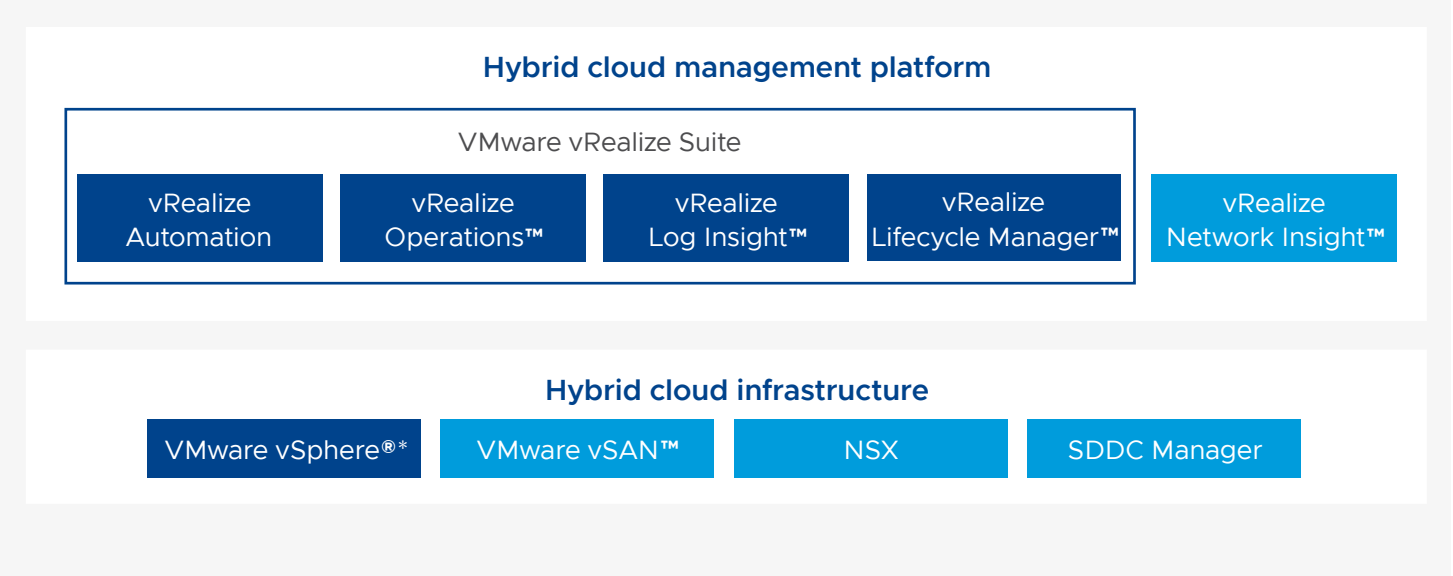
This document explores the rich integrations between two SDDC technologies that underpin VMware's software-defined approach, helping enterprises drive true business agility by overcoming obstacles to speed application delivery and ensure quality of services:

- VMware Cloud™ Automation – Consisting of on-premises VMware vRealize® Automation™ and software-as-a-service VMware Cloud Automation Services, this cloud automation solution speeds up the delivery of VM- and container-based infrastructure and application resources through a policy-based self-service portal, on premises and in the public cloud.
- VMware NSX® – This networking and security virtualization platform delivers the operational model of a VM or a container for the network by abstracting, pooling and automating networking for the SDDC and Kubernetes or PKS. Similar to VMs for compute, virtual networks are programmatically provisioned and managed independent of the underlying network hardware.

VMWARE VISION

Already the hybrid cloud leader with the SDDC portfolio and VMware Cloud, VMware gives enterprises cloud freedom and control by enabling them to run, manage, connect and secure any application across any cloud and any device in a common operating environment. VMware vRealize Automation and VMware NSX are key components of the VMware Cloud Foundation™ that drives agility for the hybrid cloud.

VMware software-defined enterprise



VMware vCloud Suite® components
*Available in Platinum

Day 1 Provisioning: Deliver Speed, Consistency and Security

Lines of business want new applications now, but traditionally, IT's application and infrastructure delivery processes have been manual and error prone, consuming huge amounts of time and often leading to configuration drift and security lapses. IT teams using enterprise-class automation from VMware can provision application environments with the underlying network and security infrastructure on Day 1 with agility, scalability and consistency. This automates the process end to end, eliminating manual tasks and long cycle times (e.g., handoffs and coordination between siloed teams), and drastically reducing wait times. Used together, VMware Cloud Automation and NSX help accelerate IT resource delivery and increase developer productivity.

Accelerate IT resource delivery

VMware Cloud Automation enables IT teams to automate the delivery and management of production-ready infrastructure and application components, whether the applications use traditional methods or rely on container services. This results in faster IT service delivery, improved IT operations, and the delivery of end-user choice with control, across heterogeneous and multi-cloud environments.

NSX enables network and security teams to dramatically reduce the amount of effort and cost to provision infrastructure, such as logical switches, routers, load balancers and distributed firewalls.

Using VMware Cloud Automation and NSX together, IT teams can model infrastructure and complete multitier application environments for developers as blueprints that include network profiles and security policies. Through native integration, VMware Cloud Automation and NSX enable IT to visually drag and drop, then dynamically build networking and security services into the blueprints, providing repeatability while reducing manual network and security administration hassles. As a result, the joint solution helps to speed infrastructure, container and application provisioning from weeks to minutes while ensuring standardized environments and avoiding configuration drift.

"Our primary objective was to improve our security posture. Our existing security solutions were not meeting some of our new and evolving business requirements, and we knew we had to move toward automated processes. The combination of VMware NSX and VMware Cloud Automation is helping us improve overall IT and security operations to reduce risk. We are also more efficient and agile with a VMware based private cloud."

DAVID SNIDER,
SENIOR DIRECTOR,
FOUNDATION ENGINEERING,
UNITEDHEALTH GROUP

The joint solution also helps address a major challenge enterprises face: provisioning workload-level security firewalls, also known as micro-segmentation, as part of the process to provision a multitier application. Generally, provisioning workload-level security is one of the last steps in provisioning an application stack, and this step alone can add days or even weeks to the overall provisioning process.

As changes occur within environments and applications, the joint solution simplifies ongoing configuration management. To change a networking configuration or security policy for a set of applications, the blueprint just needs to be updated. Any application using the updated blueprint will automatically be updated to reflect the modified configuration. Security policies also get retired with the workloads/applications to which they apply, ensuring there isn't firewall rule sprawl and that stale firewall rules don't pose security risks.

Increase developer productivity

Organizations racing to digital transformation focus on making developers hyper-productive. A crucial first step, automating the delivery of infrastructure and applications to development teams increases their ability to release applications faster and make development resources—both people and technology—more productive.

In addition to cloud-agnostic blueprints, service catalogs and governance capabilities, VMware offers API access well suited for developer-focused scenarios. With VMware Cloud Automation and NSX, IT can provide developers direct API access for compute, storage, security and networking. The ability to offer both catalog and API access to infrastructure resources means that IT can satisfy the needs of different developer preferences.

"By establishing a security policy via an automated provisioning blueprint at the front of an application's lifecycle. VMware NSX and VMware Cloud Automation give us the ability to have that security posture follow that application throughout its entire life from cradle to grave."

COBY HOLLOWAY,
VICE PRESIDENT AND
DIRECTOR, CLOUD COMPUTING,
SAIC

Day 2 Network Automation

VMware Cloud Automation provisions NSX networking and security, and allows organizations to consume these services. To meet the needs of a dynamic business environment, VMware Cloud Automation offers the ability to update configurations post-deployment.

Update configurations: Day 2 change configurations based on business needs

VMware Cloud Automation provides the ability to update NSX security applied to a VM or a container, and change network configurations for provisioned networks and VMs. Developers can request networking and security configurations specific to their needs at deployment time or update after deployment. Administrators can choose to limit the options available to developers or allow broad self-service options that developers may require for their projects. When required, a simple update to the blueprint or network profile and redeployment will update the configurations.

"[As we] deploy our next-generation NSX based software-defined data center, VMware Cloud Automation and vRealize Network Insight real-time flow analytics make it extremely easy to implement micro-segmentation security. The visibility and troubleshooting capabilities enable us to more quickly and confidently scale our NSX deployment."

BRIAN LANCASTER,
EXECUTIVE DIRECTOR,
INFORMATION MANAGEMENT,
NEBRASKA MEDICINE

Operations: Optimize and Scale Virtual Networks and Security

Beyond Day 1 app-centric network and security services provisioning, IT can also address Day 2 operations for software-defined networking and security, including the scaling of NSX deployments with vRealize Network Insight.

Plan application security and migration

Enterprises deploying NSX and vRealize Network Insight can accelerate micro-segmentation planning and deployment; plan application migration; and provide operational views to manage, scale and enable Payment Card Industry (PCI) compliance for NSX Data Center deployments.

Understanding application behavior and how different tiers communicate is a challenge but absolutely necessary to model security policies and firewall rules in an accurate and predictable fashion. Manually analyzing east-west traffic flows to design micro-segmentation with virtual distributed firewall rules can be labor intensive and error prone, potentially resulting in outages and compromised security.

Users can plan security for their applications, as well as plan an application migration to the public cloud, another data center, or a disaster recovery site using application-dependency mapping.

Together, vRealize Network Insight and NSX enable comprehensive netflow assessment and analysis to model security groups and firewall rules. vRealize Network Insight provides recommendations that make NSX micro-segmentation easier and faster to deploy.

WHY MICRO-SEGMENTATION?

Standard approaches to securing data centers emphasize strong perimeter protection to keep threats on the outside of the network. This model is ineffective for handling new types of threats occurring inside data centers. NSX delivers micro-segmentation, which assumes threats can be anywhere and probably are everywhere, and enables the deployment of granular security controls to every VM in the data center.

After deploying micro-segmentation, vRealize Network Insight can continuously monitor and audit compliance postures of the NSX distributed firewalls. Features, such as data center time machine, track all the changes for audit and compliance purposes. Users can go back in time to look at historical changes and how they impacted the security of a VM.

Optimize and troubleshoot virtual and physical networks

NSX enables IT to gain unprecedented efficiencies in mission-critical network infrastructure. It provides unparalleled application awareness, including layer 3 connectivity through logical and physical components such as routers, switches, layer 2 networks and firewalls. However, there are multiple layers, technologies and vendors involved in an SDDC network—across the overlay (virtual) and underlay (physical) network layers—so getting end-to-end visibility is essential to optimize network performance.

With NSX, vRealize Network Insight provides IT teams with converged visibility and analytics spanning physical and virtual networks. This includes integrations with most leading physical network vendors and provides out-of-the-box virtual-to-physical network topology mapping, including VM-to-VM and VXLAN views. Topology mapping coupled with log analytics across various physical network components and NSX provide deep contextual insights. This helps optimize network performance across overlay and underlay networks.

Manage and scale NSX

NSX enables IT to programmatically create, snapshot, store, move, delete and restore entire networks with the same simplicity and speed of a VM or container—delivering a level of availability unlike hardware or traditional operational approaches. However, virtual networking introduces new

constructs, and organizations struggle to grasp best practices to implement and operate VXLANs and virtual firewalls. Traditional network management tools don't provide a holistic view of the network, so troubleshooting connectivity or firewall issues in the virtual overlay can be challenging.

To manage and scale NSX, vRealize Network Insight provides an intuitive user interface (UI) and natural language search to quickly pinpoint issues and conform to best-practice guidelines. Using everyday networking and data center verbiage, administrators and operators can easily manage and troubleshoot NSX deployments without requiring a lot of additional training through a common language model. The common language model is critical to onboarding existing network and operations teams with minimal training. vRealize Network Insight also provides best-practice checks to guide users through their VXLAN and firewall implementation, and alerts them of any pitfalls in the NSX design and implementation. IT can accelerate root-cause analysis through captured and analyzed log data for NSX components, networking services and physical network components. The combined solution is essential for operationalizing and scaling NSX deployments.

Deploy Proven Solutions from a Trusted Leader

Applications are the engines powering businesses to deliver services and capture market opportunities. To deliver new and updated applications to users instantly, anywhere, anytime, from any device, IT organizations must be able to quickly build, deliver and manage all applications. Together, VMware Cloud Automation and VMware NSX deliver rapid application rollout with networking and security services, enabling IT to move at the speed of business.

The joint VMware solution helps businesses enjoy faster time to market and time to value, operational savings and productivity gains, as well as an increased competitive advantage.

"The evolution to our 3.0 cloud environment was made possible by close collaboration with our staff and our business partners, including Arkin (VMware Cloud Automation with vRealize Network Insight), which played a critical role in enabling cross-departmental visibility, delivering contextual analytics and helping layer granular security across the entire software-defined environment."

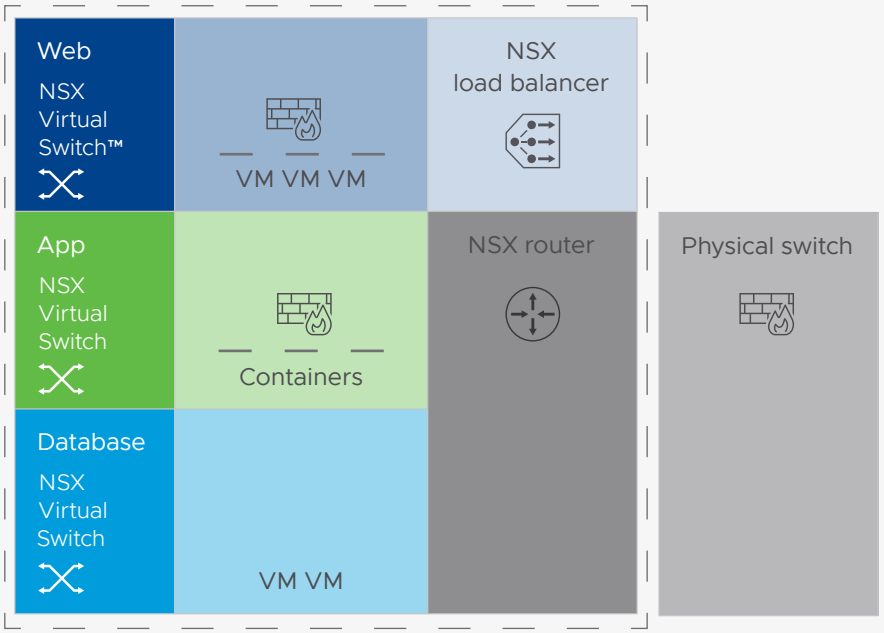
TONY MORSHED,
CTO, CALIFORNIA DEPARTMENT OF WATER RESOURCES

VMware Cloud Automation + NSX

Graphically configure and provision NSX virtual infrastructure

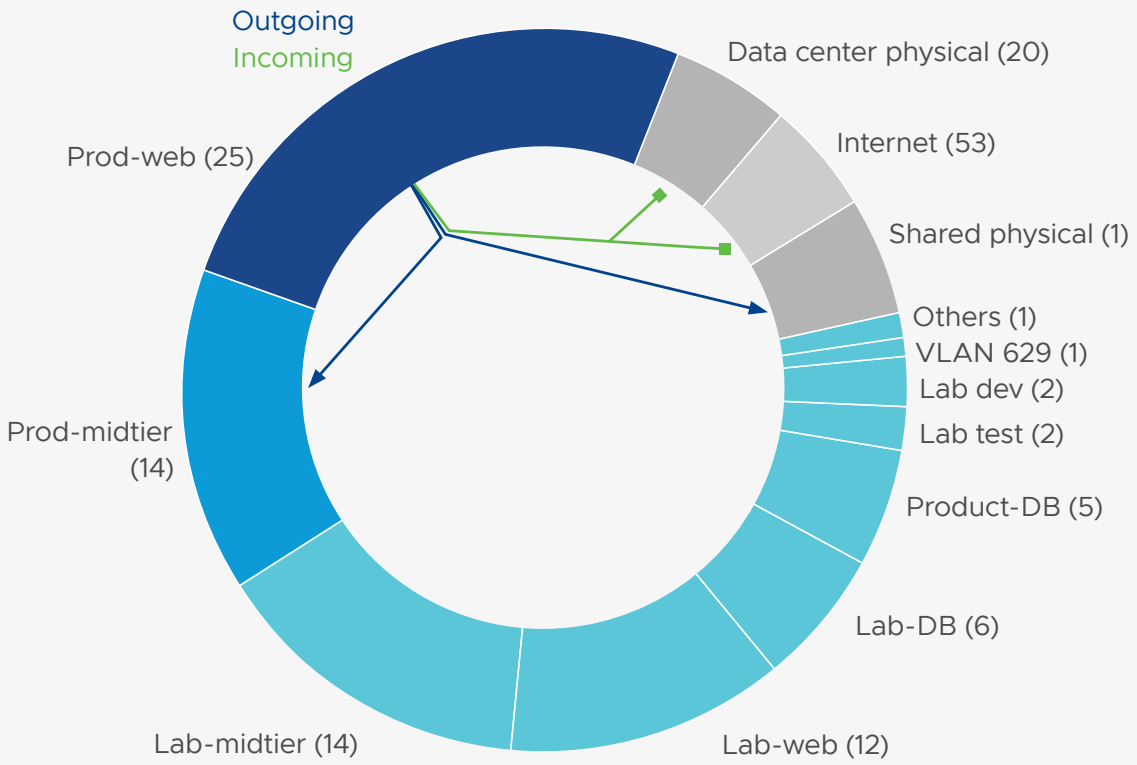
Enhance security by including firewalls and security policies as part of the app

Deliver secure, scalable and high-performing applications on demand



vRealize Network Insight + NSX

Plan application security and migration	Optimize and troubleshoot virtual and physical networks	Manage and scale NSX



Business Questions to Consider

Organizations looking to drive agility by simplifying Day 1 provisioning and Day 2 operations can begin by considering the following questions.

Q. Are you trying to improve IT efficiency and productivity, and accelerate IT service delivery to be more responsive to the business?

A. Virtualization, standardization and automation—keys to a software-defined approach—drive business and IT agility.

Q. Are you concerned about breaches that affect your reputation and brand?

A. Standardizing and simplifying network and security service provisioning can mitigate risk.

Q. Are you trying to modernize service delivery?

A. Virtualization and automation consistently reduce complexity and the time it takes to provision services while simultaneously lowering the cost of IT operations.

Q. Do you have an operational excellence initiative?

A. VMware solutions can help you quickly achieve your goals with vRealize Network Insight capabilities that also support network and security operations.

Learn More

The following resources provide additional information and insight into how VMware Cloud Automation and NSX can benefit your organization.

VMware Cloud Automation:

- On premises: vmware.com/products/vrealize-automation
- Software as a service: cloud.vmware.com/cloud-automation-services

NSX:
vmware.com/products/nsx

Join us online:

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: 250995aq-ebook-cmbu-refresh-uslet 7/19