# VMware NSX for Horizon

## AT A GLANCE

VMware NSX™ for Horizon® brings speed and simplicity to VDI networking. Within seconds, IT administrators can create policies that dynamically follow virtual desktops, without the need for time-consuming network provisioning. Extending security policy from the data center to the desktop and app, this joint solution also provides an extensible platform that integrates with industry-leading security solutions.

## BENEFITS

- Increase security for virtual desktops sitting amidst other data center workloads
- Simplify and accelerate administration of networking and security policy for users based on logical grouping, role, or tag
- Automatically attach policy to a desktop as it is created, following the VM irrespective of the underlying infrastructure
- Integrate with industry-leading solutions for antivirus, malware, intrusion prevention, and next-gen security services

## Networking and Security for Virtual Desktops and Apps: Fast, Easy, and Extensible

Many organizations implement desktop and application virtualization to improve client-computing security and deliver greater enterprise mobility. Centralizing desktops and applications protects data at rest, prevents unauthorized application access, and provides a more efficient way to patch, maintain and upgrade images.

However, with desktop and application virtualization, new security concerns can arise behind the data center firewall—where hundreds or even thousands of desktops reside. These desktops sit in close proximity to other users and mission-critical workloads, making them much more susceptible to malware and other attacks. These attacks can move from desktop to server, exposing a large attack surface within the data center. This "east-west" threat scenario is a common one affecting many customers today, particularly those with stringent security and compliance mandates.

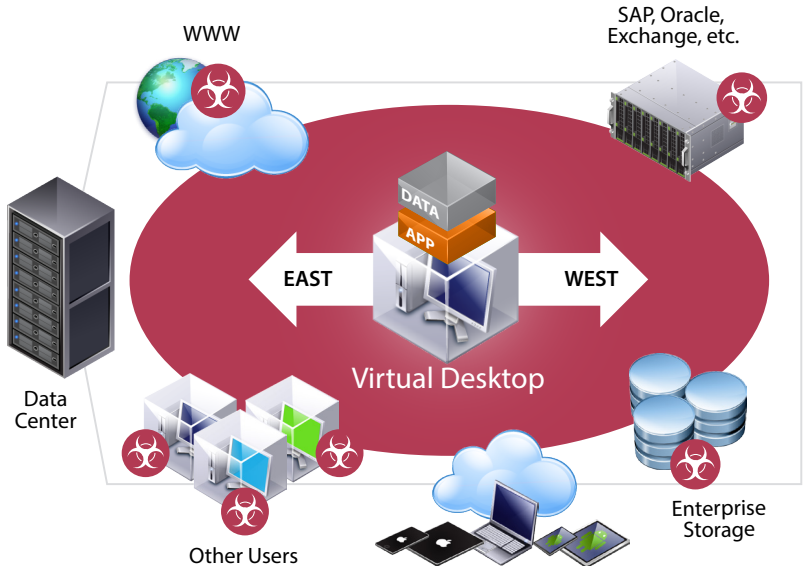


**Figure 1:** East-West Security Concerns Within the Data Center

Organizations seeking to administer networking and security policy that persistently follows users and workloads have also traditionally incurred a significant investment in a hardware-centric architecture that is CapEx-intensive, complex to operate, and slow to adapt to the typical dynamic business environment.

## VMware NSX for Horizon

VMware NSX for Horizon effectively secures east-west traffic within the data center, while ensuring that IT can quickly and easily administer networking and security policy that dynamically follows end users' virtual desktops and apps across infrastructure, devices, and locations.


**Figure 2:** NSX for Horizon Offers Fast, Easy, and Extensible VDI Networking and Security

With this solution, organizations benefit from fast and simple VDI networking and security. Within seconds, IT administrators can create policies that dynamically follow virtual desktops, without the need for time-consuming network provisioning.

Extending security policy from the data center to desktops and applications, this solution also provides an extensible platform that can integrate with the VMware ecosystem of industry-leading security partners to provide customers with defense in depth that protects the entire desktop.

## How It Works

VMware NSX for Horizon improves desktop virtualization security and helps address east-west threats by enabling administrators to define policy centrally. That policy is then distributed to the hypervisor layer within every vSphere host, and automatically attached to each virtual desktop as soon as the desktop is created. To secure virtual desktops and adjacent workloads within the data center, VMware NSX implements "micro-segmentation," giving each desktop it's own perimeter defense. This "shrink-wrapped security" uses VMware NSX distributed virtual firewalling capability to police traffic to and from each VM, eliminating unauthorized access between desktops and adjacent workloads. If the virtual desktop moves from one host to the next, or across the data center, policy will automatically follow it.

## Features and Benefits

VMware NSX for Horizon brings speed and simplicity to VDI networking with security policy that dynamically follows end users across infrastructure, devices, and locations.

### Fast and Simple VDI Networking

With VMware NSX for Horizon, administrators can create, change, and manage security policies across all virtual desktops with a few easy clicks. Security policies can be quickly mapped to user groups to speed virtual desktop onboarding. With the ability to deploy virtualized network functions (like switching, routing, firewalling, and load-balancing) administrators can build virtual networks for VDI without the need for complex VLANs, ACLs, or hardware configuration syntax.

### Automated Policy That Dynamically Follows End Users and Desktops

Administrators can set policies that dynamically adapt to the end user's computing environment, with network security services that map to the user based on role, logical grouping, desktop operating system, and more—independent of the underlying network infrastructure. Centrally administered policy is automatically attached to each desktop VM as soon as the desktop is created, so organizations can scale with confidence, with security that persistently follows the virtual desktop across the data center.

### Platform for Advanced Security

VMware NSX offers an extensible platform that can be integrated with best-in-class capabilities from an established ecosystem of security partners. By dynamically adding services, virtual desktop security can be extended from the data center to the desktop and the application. This ecosystem of partners, including Trend Micro, Intel Security, and Palo Alto Networks, offers solutions that protect the operating system, browser, email, and more—with antivirus, malware, intrusion-prevention, and next-gen security services.

## Learn More

For more information about Horizon and VMware NSX, visit the VMware Web site and follow us on Twitter.

### VMware Horizon Resources

Web: http://www.vmware.com/go/horizon

Blog: http://blogs.vmware.com/euc/

Twitter: @VMwareHorizon

### VMware NSX Resources

Web: http://www.vmware.com/go/nsx

Blog: http://blogs.vmware.com/networkvirtualization/

Twitter: @VMwareNSX

**VMware, Inc.** 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com