VMware vRealize Network Insight

VMware vRealize® Network Insight™ delivers intelligent operations for software-defined networking and security. It helps customers build an optimized, highly available, and secure network infrastructure across multi-cloud environments. It accelerates micro-segmentation planning and deployment, enables visibility across virtual and physical networks, and provides operational views to manage and scale VMware NSX deployments.

This document provides a step-by-step guide focused on the key capabilities and benefits gained throughout a typical one- to two-week deployment.

Solving the virtual and physical network puzzle
When it comes to managing, troubleshooting, and securing the network, many network administrators face a puzzling, and frustrating, visibility gap across the virtual and physical network. vRealize Network Insight can help you with the following use cases.

Plan application security and migration:
• Accelerate micro-segmentation deployment
• Troubleshoot security for the software-defined data center (SDDC), native AWS, and hybrid applications
• Minimize business risk during application migration

Optimize and troubleshoot virtual and physical networks:
• Reduce mean time to resolution for application connectivity issues
• Optimize application performance by eliminating network bottlenecks
• Audit network and security changes over time

Manage and scale NSX:
• Scale across multiple NSX Managers
• Boost uptime by proactively detecting misconfiguration errors
• Ensure compliance for NSX

KEY BENEFITS
• Accelerate micro-segmentation planning and deployment
• Audit changes to the security posture and ensure compliance
• Troubleshoot quickly across virtual and physical network and security infrastructure
• Manage and scale VMware NSX® deployments with confidence
• Manage network and security across private and public clouds consistently

LEARN MORE ABOUT vREALIZE NETWORK INSIGHT
• Read the datasheet
• Take it for a test-drive
• Watch the video overview

WATCH USE CASE OVERVIEW VIDEOS
• Plan security
• 360-degree visibility
• NSX operations
Phase 1: Enable infrastructure components access and define networks

Step 1: Connect vRealize Network Insight to vCenter and NSX Manager™

Key benefits
- Gain visibility into all VMware vCenter® objects and performance metrics
- Discover all NSX security groups, firewall rules, virtual networks, and infrastructure components

Step 2: Enable IPFIX (NetFlow) on devices

Key benefits
- Gain visibility into all intra- and inter-host traffic for firewall policy planning (micro-segmentation) and flow monitoring
- Extend visibility into application flows that include bare-metal servers and devices supporting NetFlow versions 5, 7, and 9, and IPFIX
- Analyze flows that are blocked, protected, and unprotected by the NSX Distributed Firewall

Step 3: Add network and security data sources (read only: SSH/SNMP/HTTPS)

Key benefits
- Collect configuration and performance data from physical and virtual network devices; vRealize Network Insight stitches together this information for a single, end-to-end view of your data center
- Get support for physical devices (firewalls, switches, routers, servers) and virtual devices (VMware vSphere®, NSX Controller™, NSX Edge™ gateway, partner firewall vendors)
- Gain support for VMware Cloud™ on AWS, AWS, and VMware® Enterprise PKS
Step 4: Define network segment ranges

Key benefits
- Specify data center public IPs as non-Internet IPs while tagging flows and micro-segmentation
- Get a more accurate view of true North-South and East-West traffic for security planning and flow visualization
- Add in VMware Cloud on AWS and AWS security groups, subnets, virtual machines (VMs), and flows

Phase 2: Verify connectivity and plan security
Step 1: Perform path analysis

Key benefits
- Test app-to-app connectivity with easy-to-use, Google-like searches to verify all virtual and physical network devices were discovered and are being managed
- Get a dynamic topology map based on application flow to easily pinpoint networking and security issues
- Save any of the searches for customizable alerts
- Troubleshoot VM-to-VM connectivity for VMs on premises, on VMware Cloud on AWS, on AWS, or across multiple clouds
Step 2: Create application groups

**Key benefits**
- Plan security and migration, and troubleshoot connectivity in an application-centric manner by pulling in application definitions from ServiceNow or using regular expressions for app-tier VM names
- Use applications that are purely on-premises, public, or hybrid
- Perform custom alerts and/or pin boards that can easily be shared and searched against; if any component of the application group has issues, vRealize Network Insight will be aware and update the topology map and/or alert as configured

Step 3: Review recommended micro-segmentation firewall rules

**Key benefits**
- Since Day 0, vRealize Network Insight has been analyzing all East-West and North-South flows in the data center. As a result, a very precise firewall micro-segmentation allowlist policy is developed for review and export to NSX Manager
- vRealize Network Insight recommended firewall groups and rules are based on actual traffic flows observed.
- AWS security group rules can also be determined using AWS flow data.
Phase 3: Perform a best practice check, and implement data center timeline and alerting

Step 1: Perform an NSX best practice check

Key benefits
- Get an easy-to-read summary of NSX related issues and alerts against dozens of VMware’s networking and security best practices
- Easily remediate identified issues with provided recommendations
- Automatically detect configuration errors in mismatch segment ID, IPset definitions, and so on

Step 2: Implement a network and security data center timeline

Key benefits
- The network and security timeline provides the ability to look at the configured state of the data center at a particular time in the past and a bird’s-eye view of events that were detected across a selected time range.
- From the time range option, you can select the time range of the timeline that you want to view.
- A small gray horizontal bar denotes an event, and a small red horizontal bar denotes a problem.
Step 3: Set up custom alerting events and severity levels

Key benefits
- In addition to pre-defined system-level events, user-defined events enable custom-alerting capabilities by using any of the vRealize Network Insight searches as an event type. Users can define specific application, device, security, or network alerts based on their monitoring needs.
- The event is triggered when search results change or when no results are returned. If the event is marked as a problem, a severity designation will be associated.
- Events may also be created and monitored for AWS entities such as EC2 instances, VPC, security groups, and tags.

Step 4: Use pins to custom define a dashboard

Key benefits
- Every pane within vRealize Network Insight is available to be added to custom pin boards for easy access to network, security, and device information.
- A pin board can be defined for a specific critical application where a single dashboard can provide end-to-end connectivity, device metrics, problem alerts, and so on.
- Application owners, NOC users, and SOC users gain visibility with read-only access via a secure URL.