# Networking (R)Evolution

## Virtualization is vital for a real SDDC

Remco Bruijn
Solutions Architect

Martijn Smit
NSX Specialist SE
@smitmartijn

# VMware's Integrated Architecture

## Any Device

VMware Workspace ONE™ | Desktop | Mobile | Identity

## Any Application

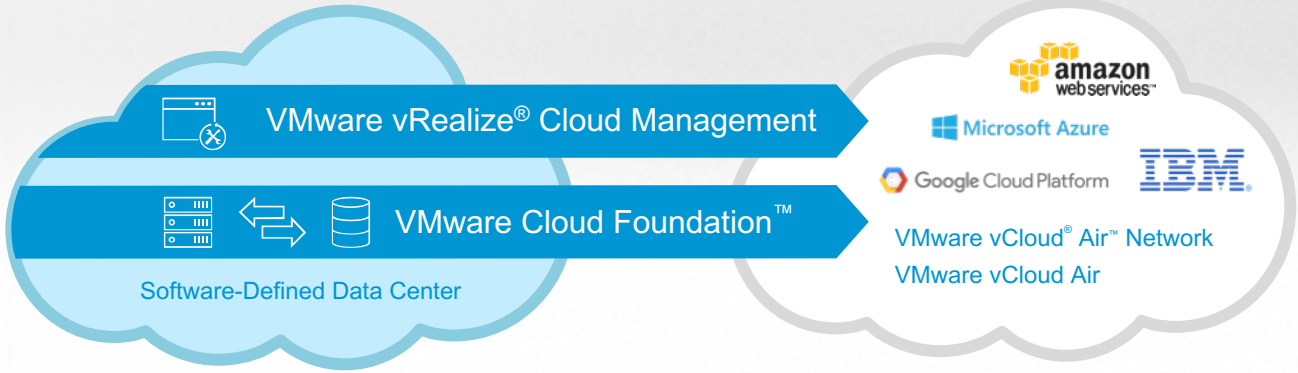

Traditional Apps | Cloud-Native Apps | SaaS Apps

## Any Cloud

### VMware Cross-Cloud Architecture™

Private Cloud | Hybrid Cloud | Public Cloud

VMware Cross-Cloud Services™



# What is Software-Defined Data Center (SDDC)?

## Software


- Compute
- Storage
- Network

- Intelligence in software
- Operational model of VM for data center
- Automated provisioning and configuration

*Data center virtualization layer*

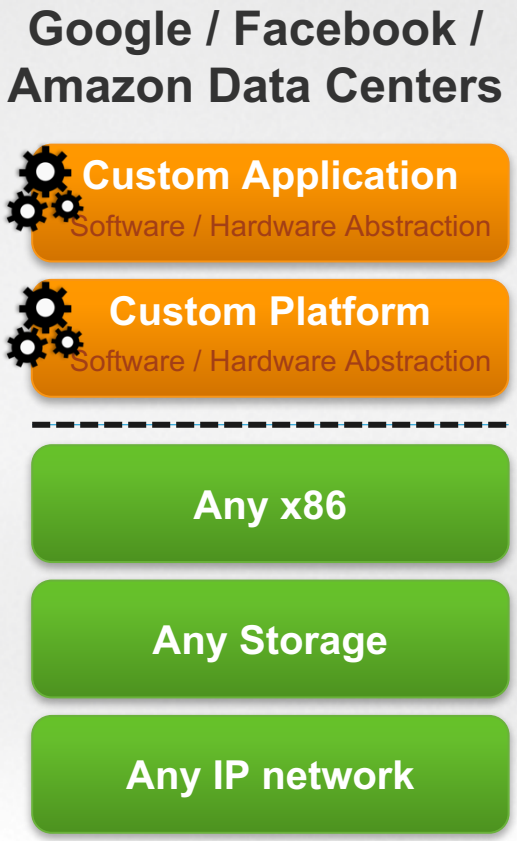
## Hardware

- Compute
- Storage
- Network

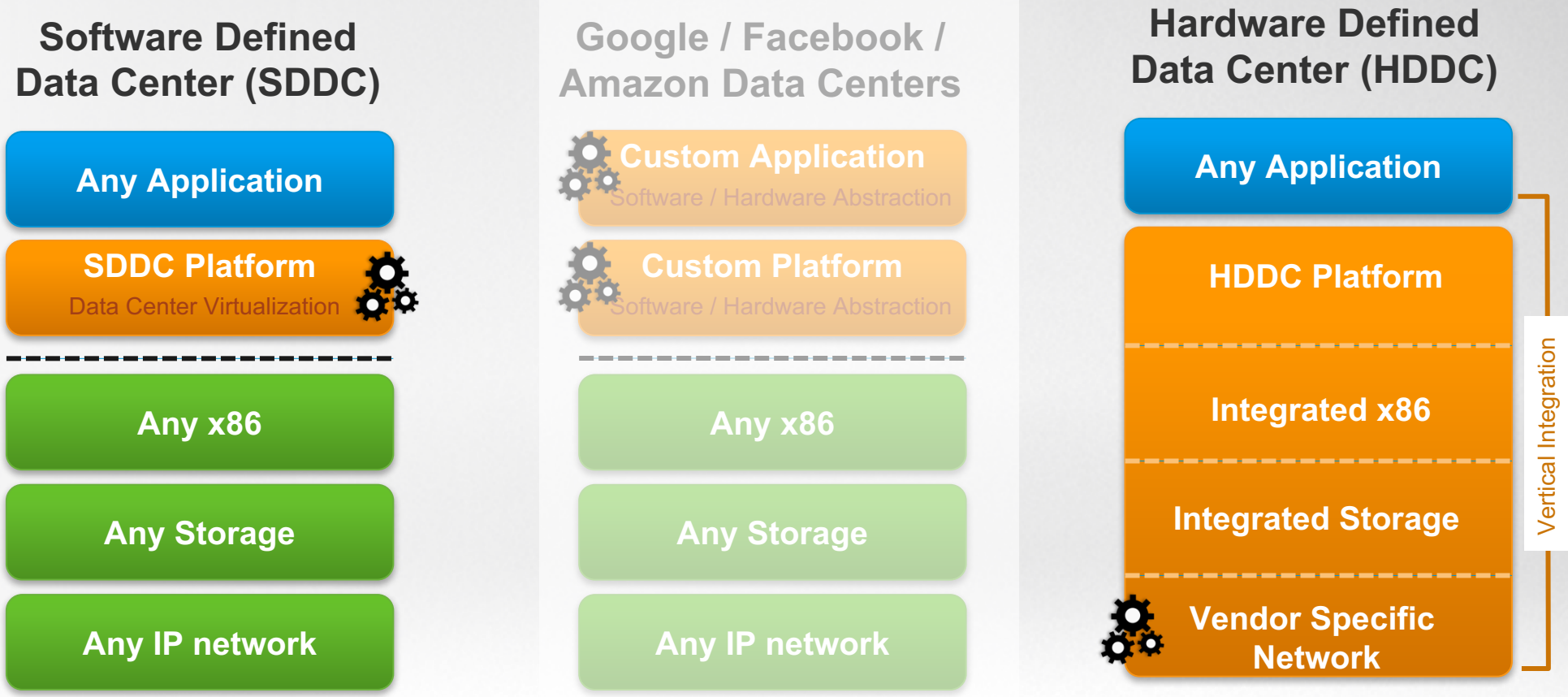
- Pooled compute, network, and storage capacity
- Vendor independent, best price/performance/service
- Simplified configuration and management

vmware®

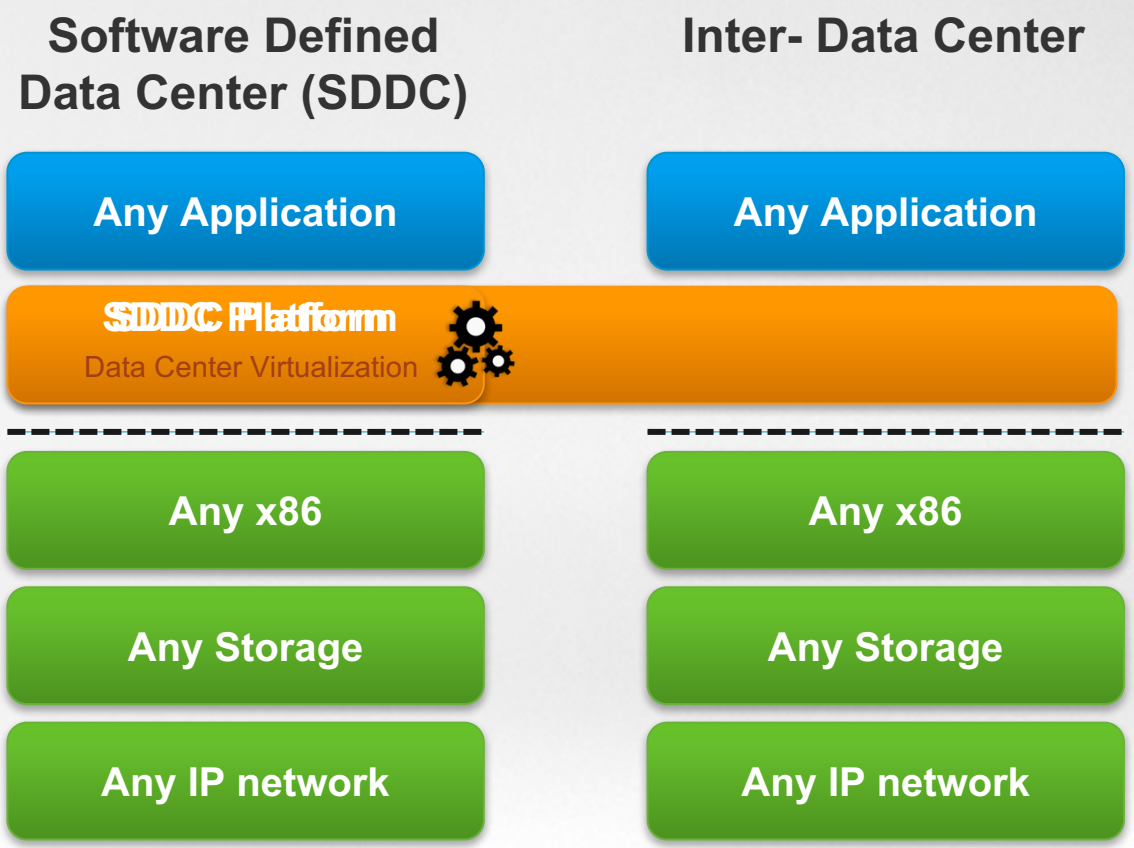
# The approach taken by the most agile & efficient data centers is SDDC



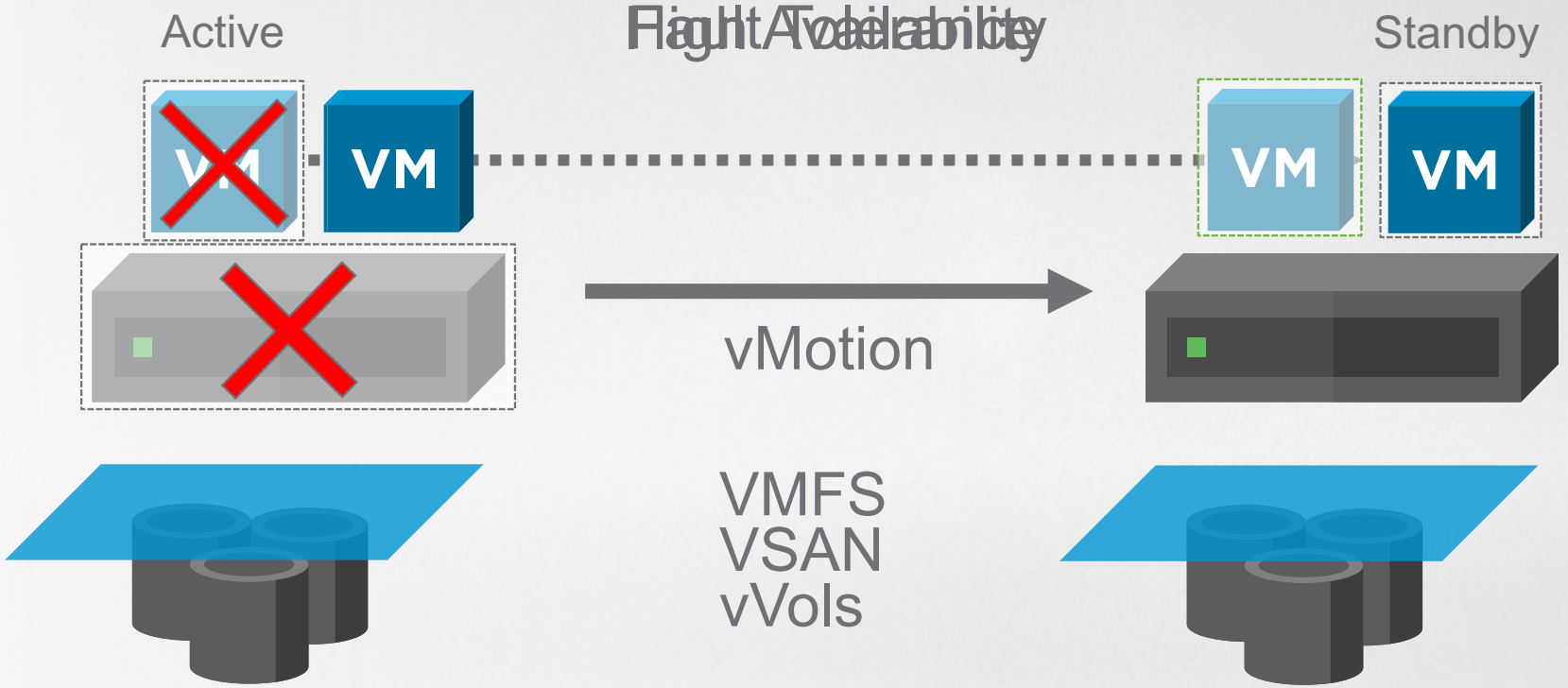
# What do you believe will be the future of data center design?



# SDDC Within, Between and Across Data Centers



# VMware Journey

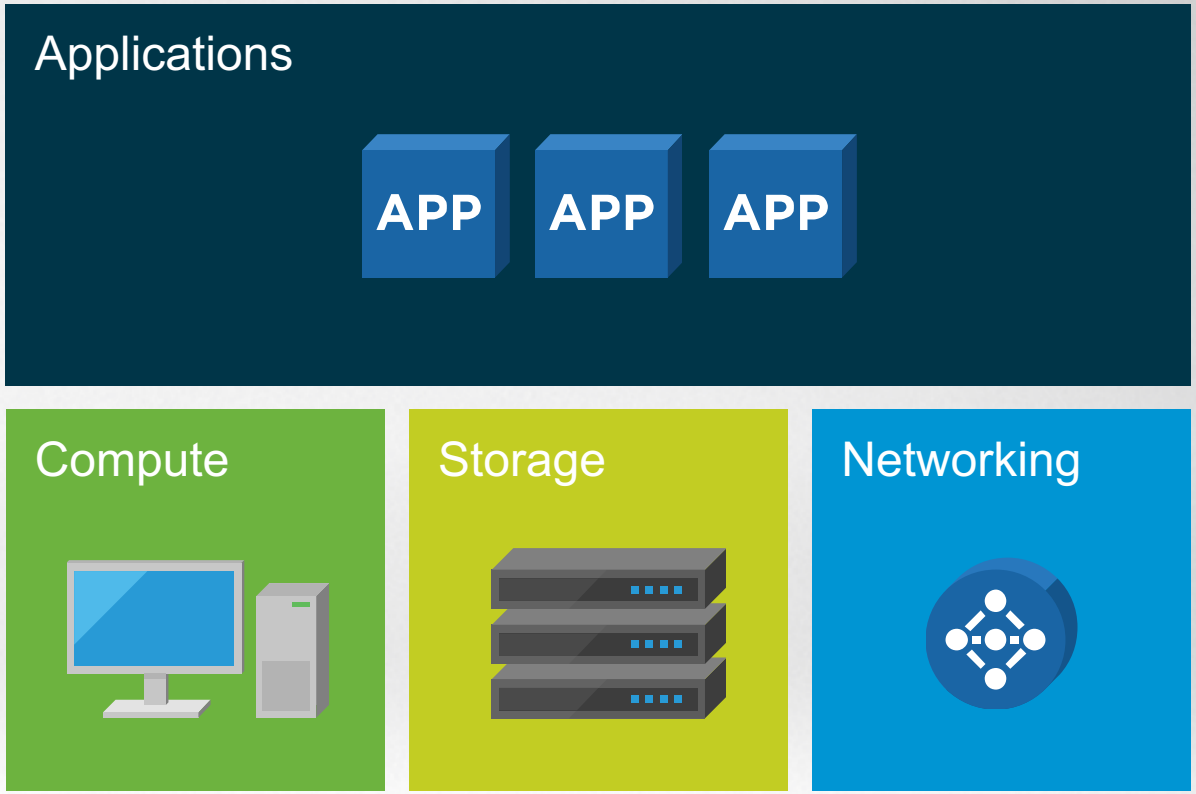


# So...what's the problem?

Over the past decade, a lot of virtualization innovation has happened in the data center and in clouds across software, compute, and storage.

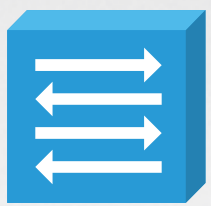
**Networking has lagged behind and is still hardware based, expensive, inflexible, and risk-prone.**

- You can't keep up with the pace of business
- You can't secure the data center
- You can't support this new app-driven world

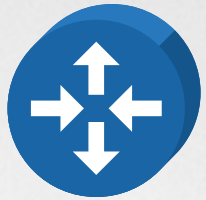


# NSX Services

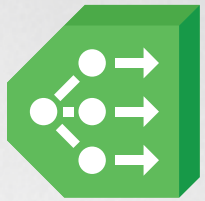
NSX Platform



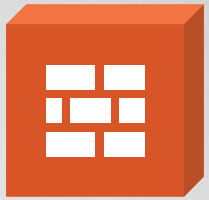
In-Kernel Switching



In-Kernel Routing



In-Kernel Load Balancing



In-Kernel Firewalling

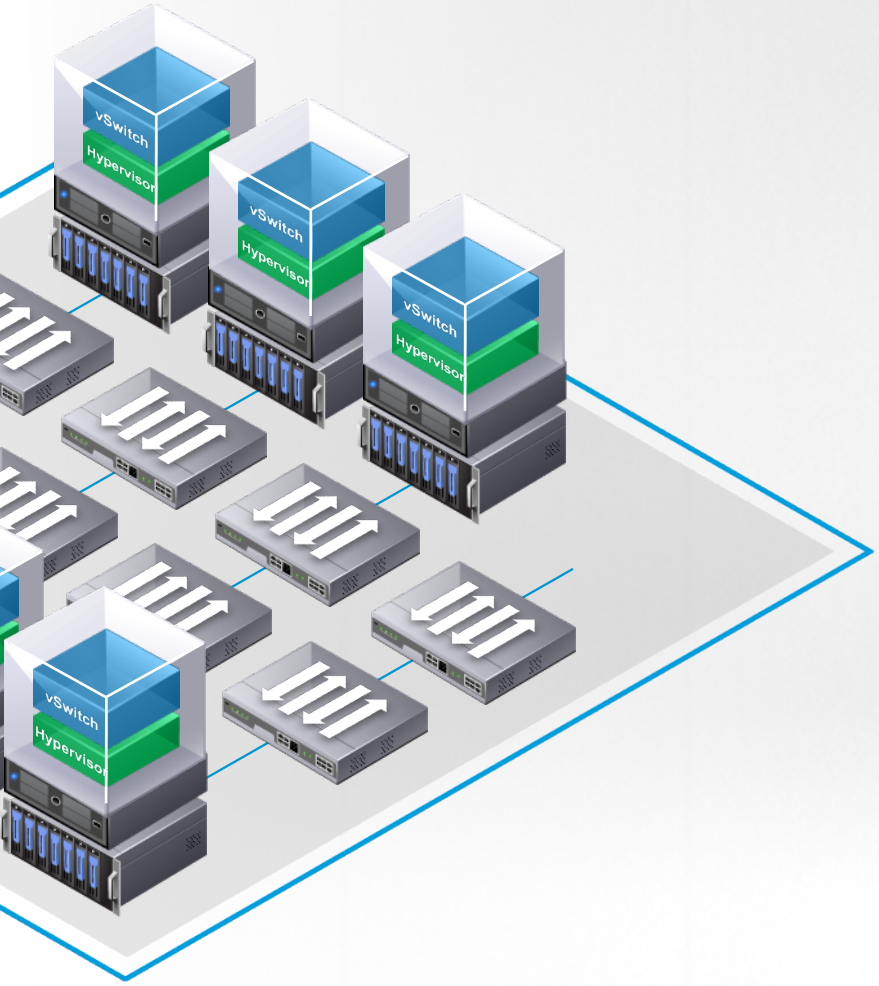

Connectivity to Physical Networks

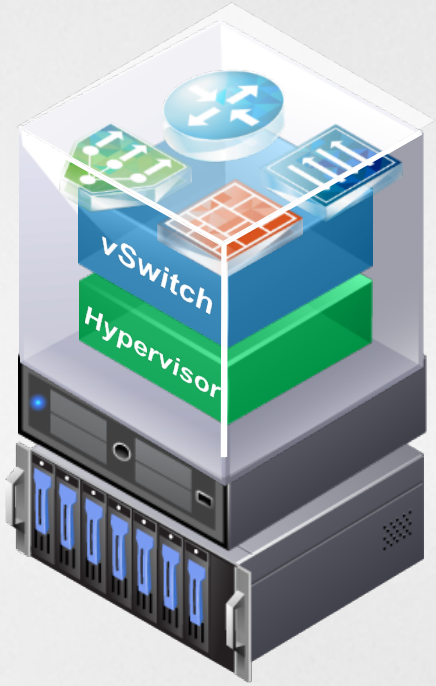

VPN (IPsec, SSLVPN, L2VPN)

3rd Party Service Insertion


Open API (Automation)

# The Power of Distributed Services




Routing

Load Balancing

Switching

Firewalling/ACLs

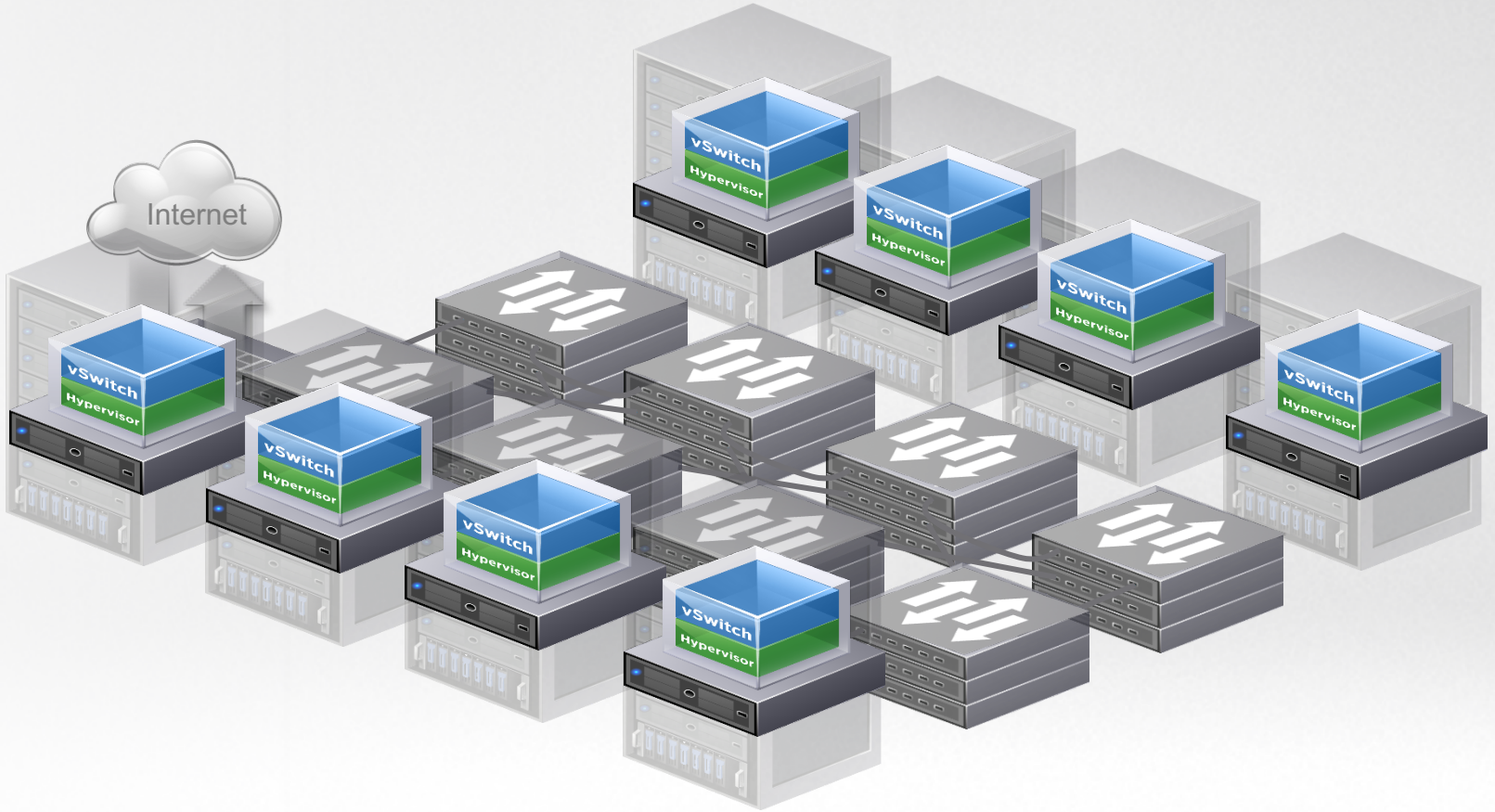
- High throughput / low latency
- East-west firewalling
- Native platform capability

vmware®

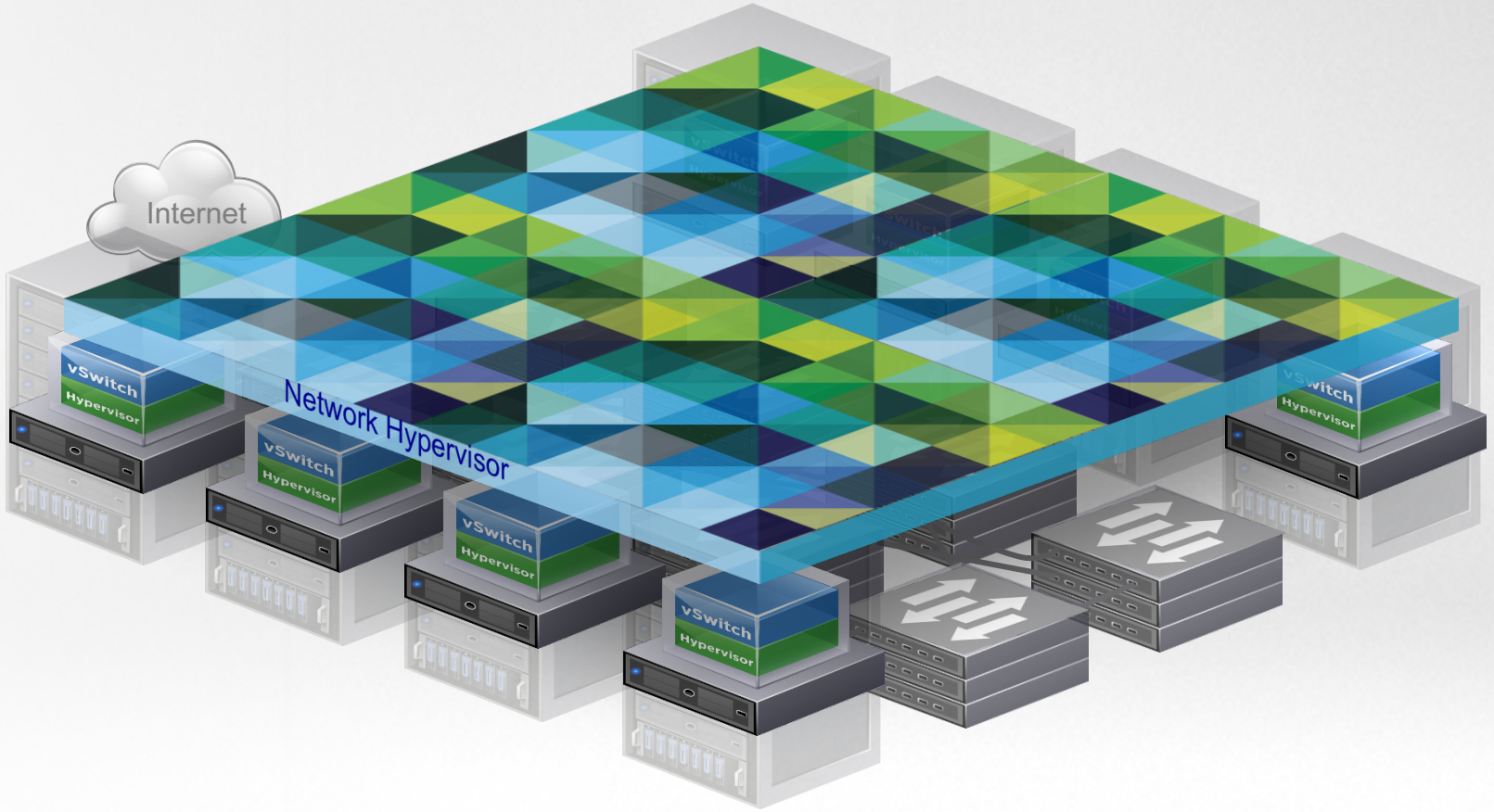
# Your Typical Datacenter


vmware®

# NSX Virtual Networking Components



# The “Network Hypervisor”



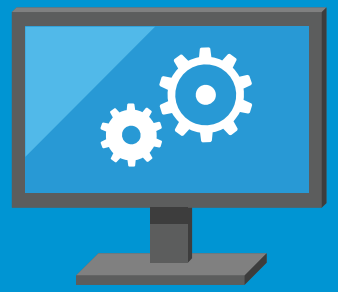



vmware®

# Our “Three Pillars”

Security

IT Automation



Application Continuity

vmware

# Security

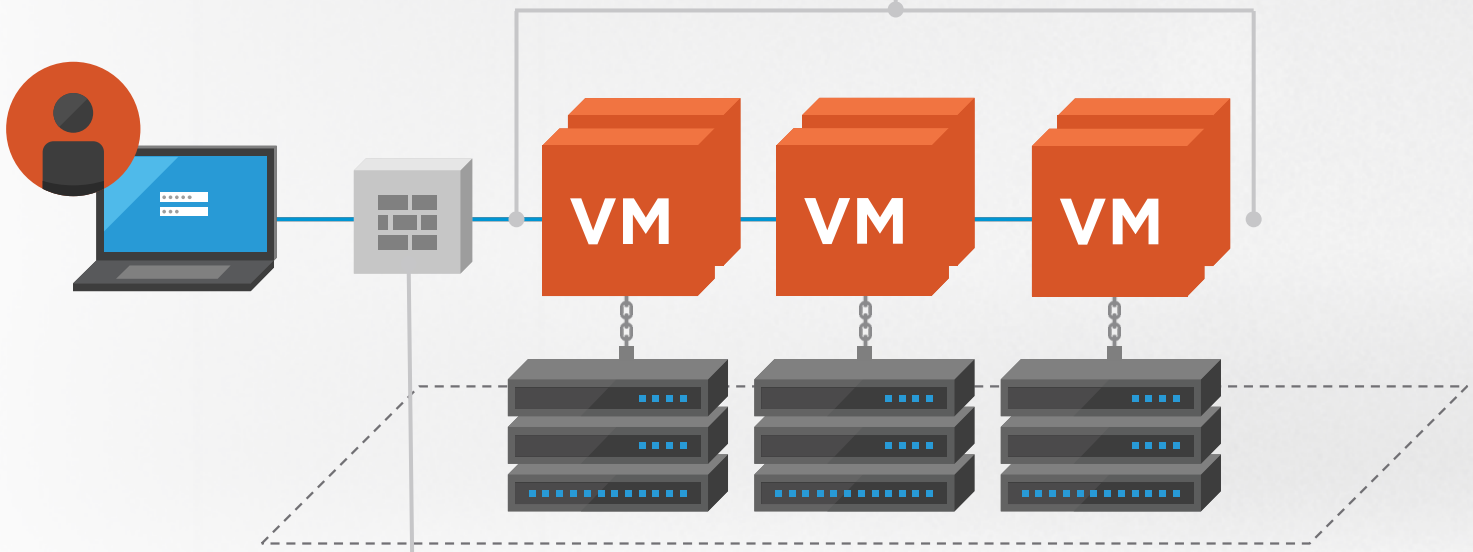
## Micro-segmentation

# Our security realities

**Unrestricted lateral spread:**
Inability to secure the DC interior

**20% of investment**

Focused on internal controls…
**resulting in lack of visibility and control**

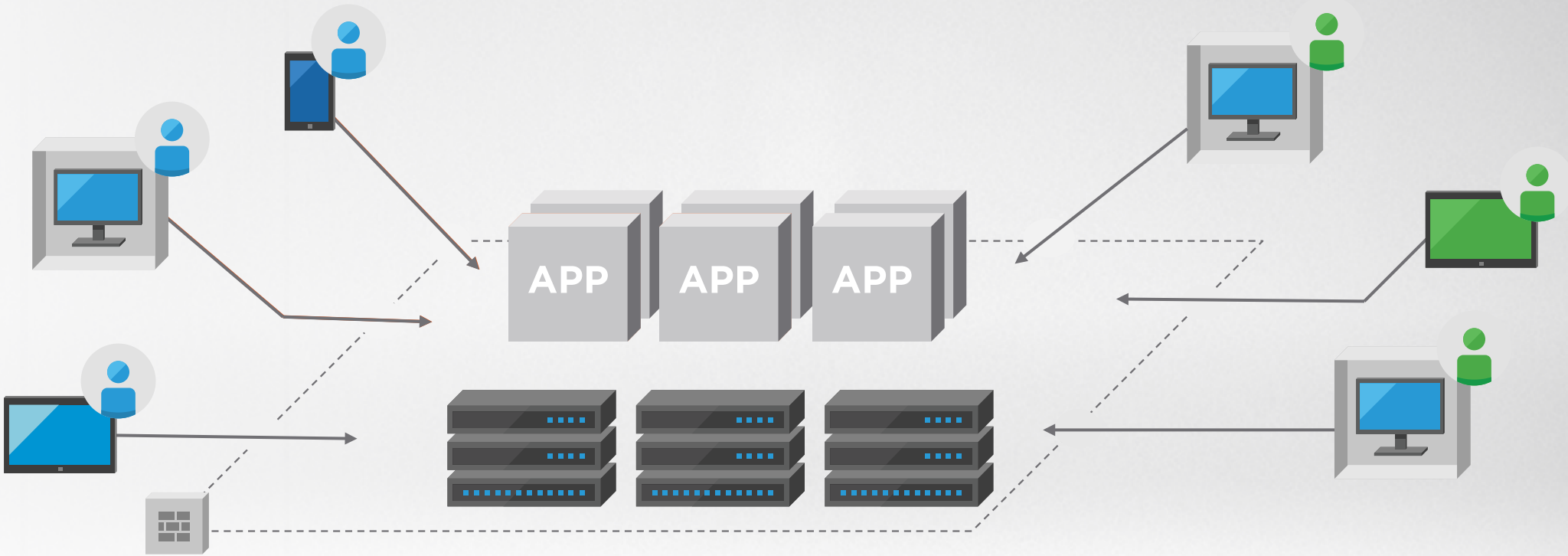



**80% of investment**

Focused on preventing intrusion

# Our security realities

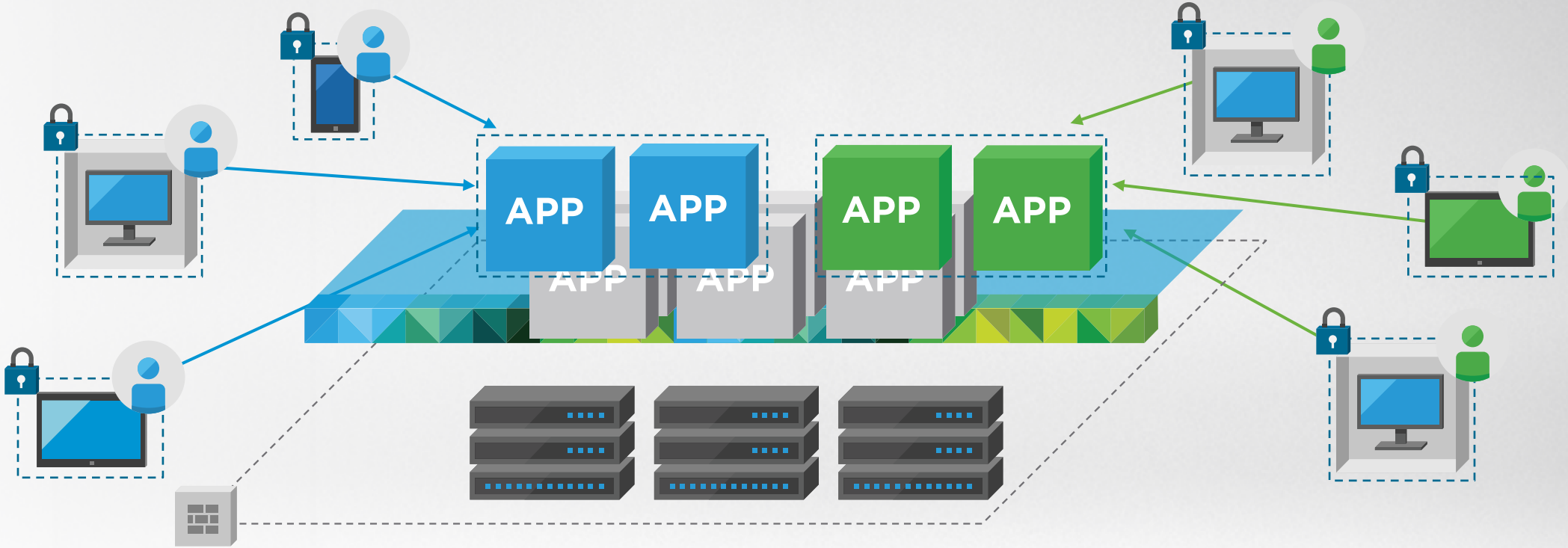
## Unchecked end user access creates significant risks inside the data center



# What if you could…

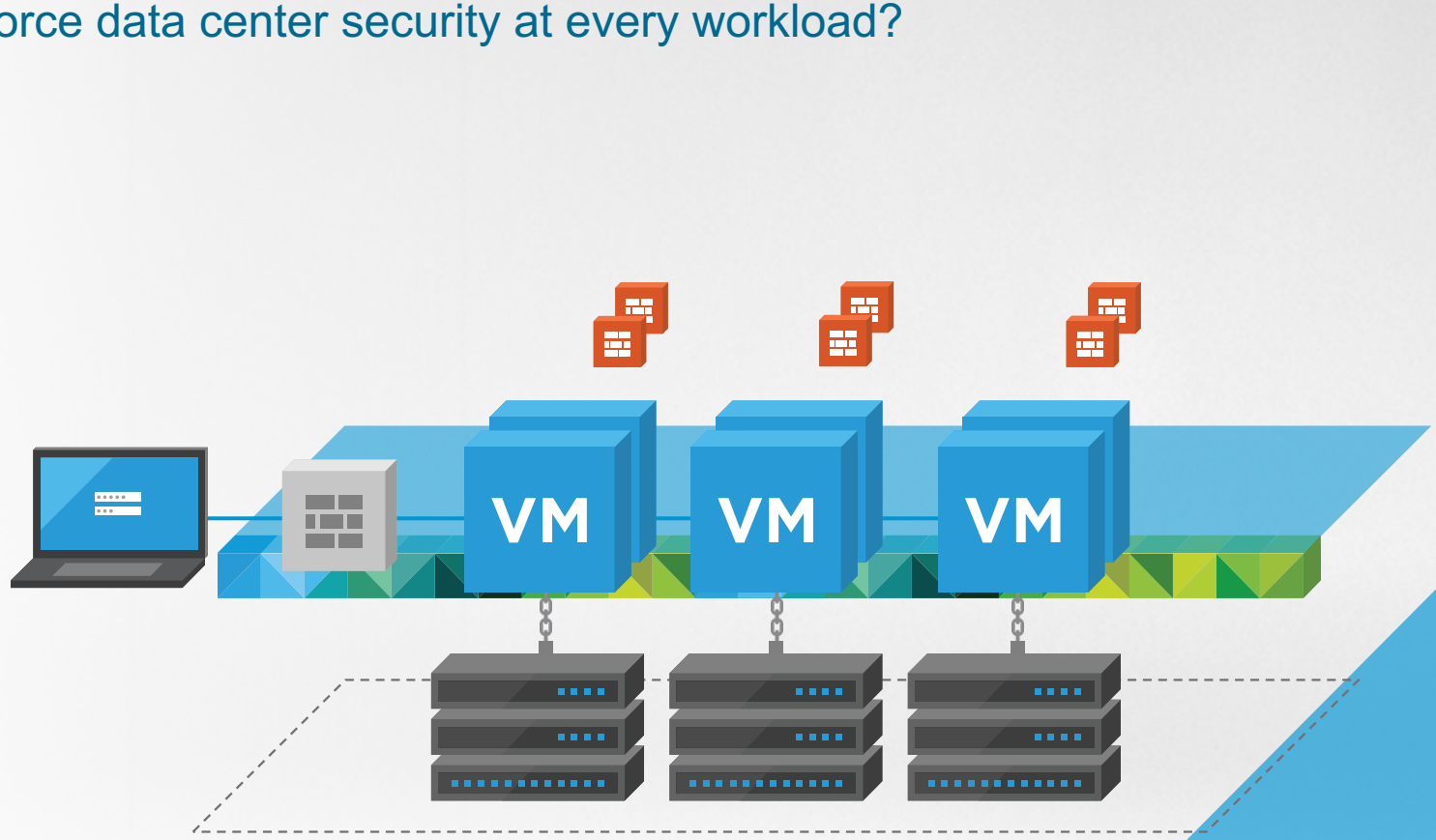
Provide granular end user security?

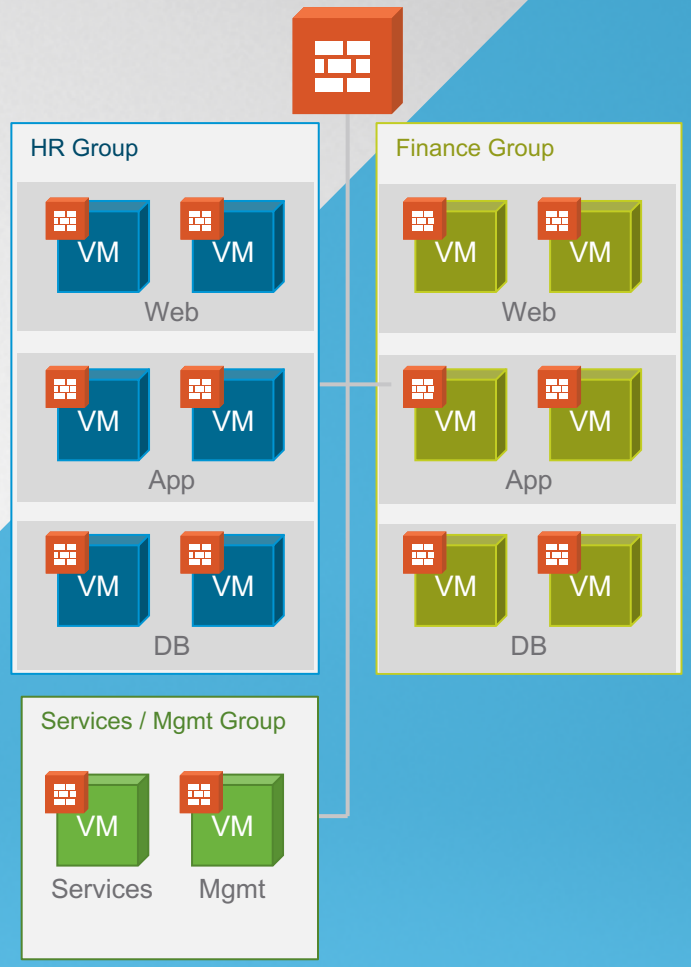
**Who you are** | **Where you are** | **What device you're on**



# What if you could…

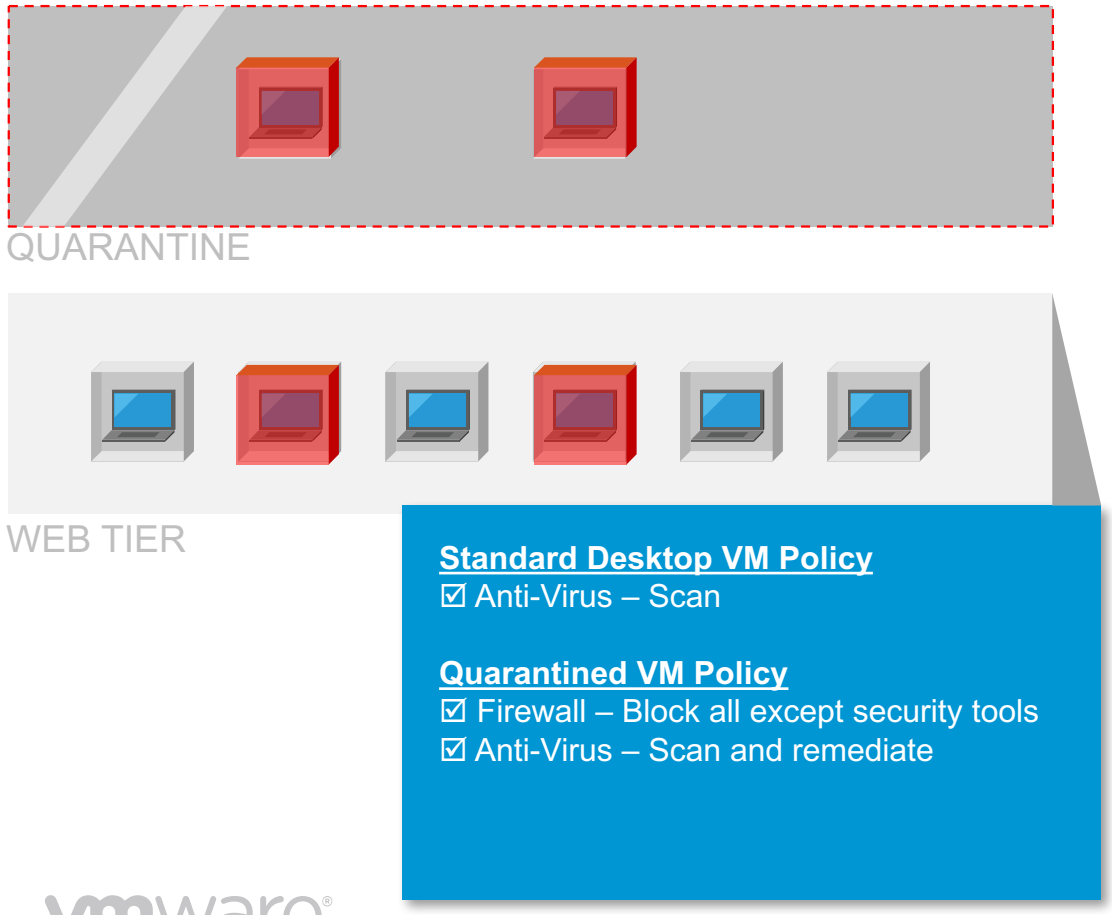
## Enforce data center security at every workload?



# Dynamic Isolation

## Automated security response




### Quarantine of Compromised Systems

Quickly and dynamically isolate security risks using existing security tools.

### Automated Remediation

Automate responses to known security events to take corrective course of action or collect forensics data.

### Dynamic Service Chaining

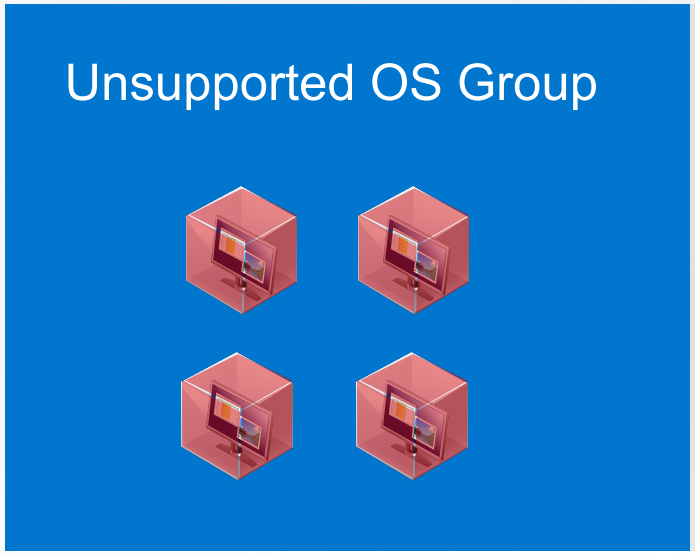
Share context between securtiy controls so that one control can trigger a response from another dynamically.

# Intelligent Grouping for Unsupported Operating Systems

## Situation

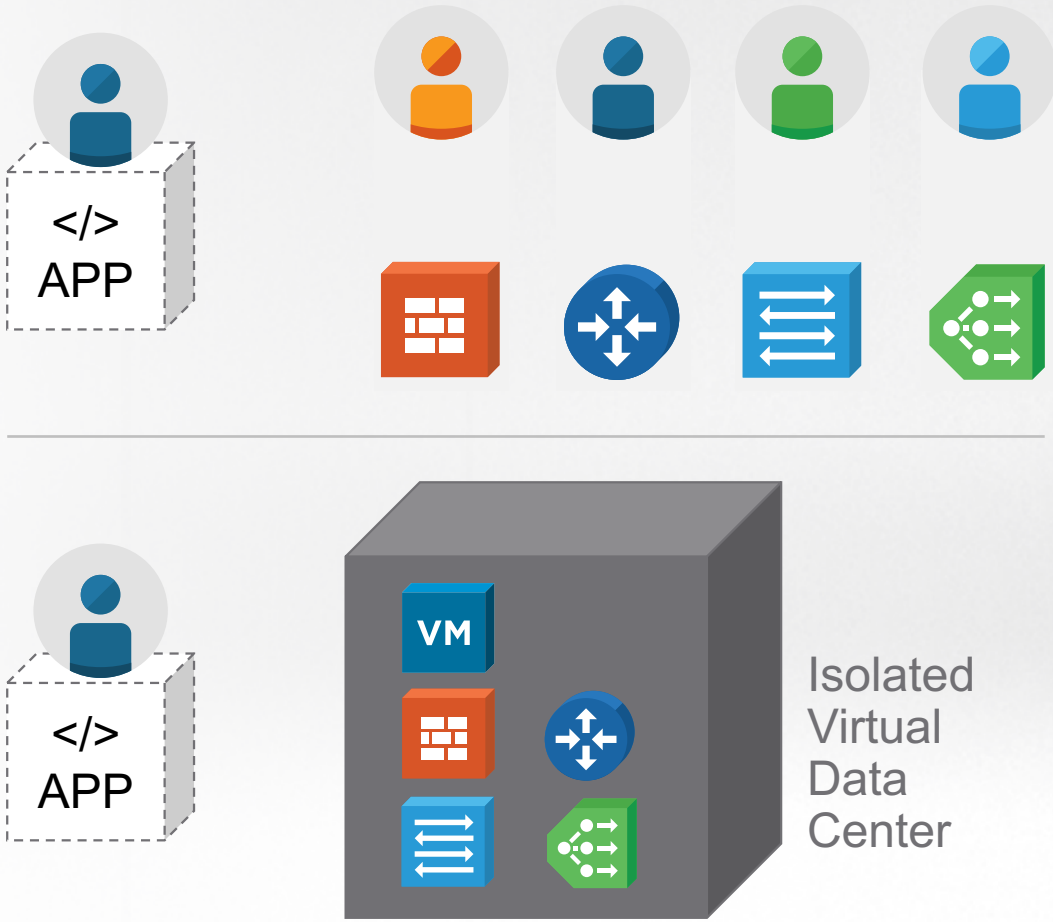
OS no longer supported on several systems

These systems need policy which restricts access to only email servers




# Delegation of Infrastructure

## Delegation of LB/FW/NAT management without risk




### Independent Data Centers

Application owners have access to their own environments in a safe virtual data center without spillover effects into the rest of the data center.

### Access to Infrastructure

Ability to grant control of individual network constructs, including access to unlimited virtual routers, switches, firewalls, and load balancers without any additional hardware cost

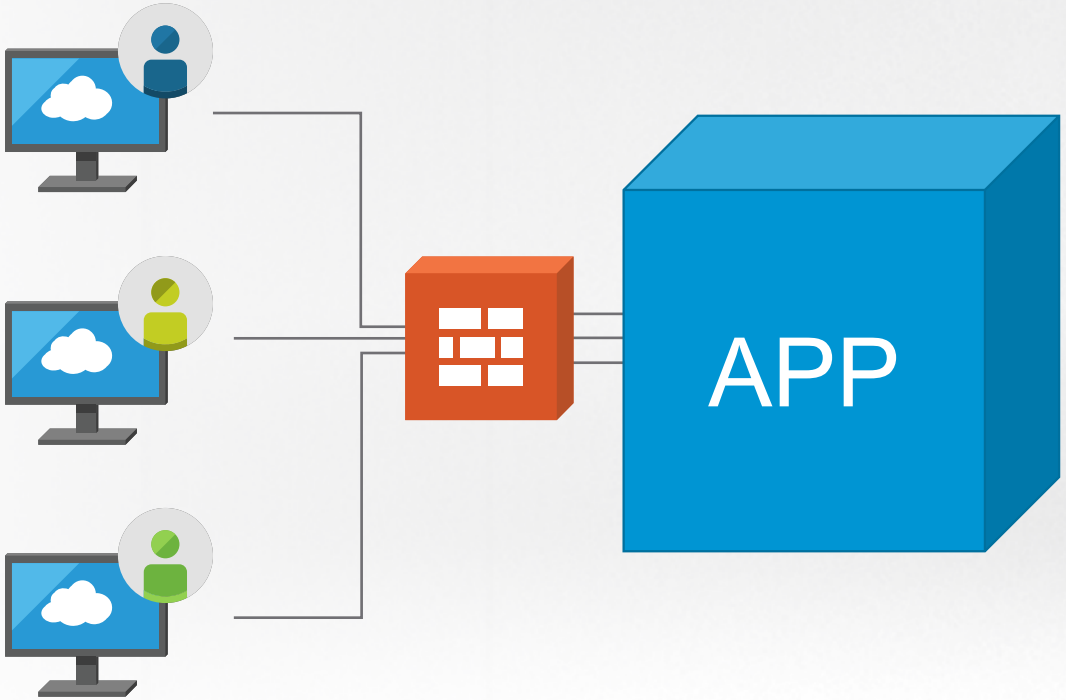
### Application Migration

Ability to migrate applications to production environments in seconds with no impact to production

vmware

# External Access to App Infra

Granting temporary or permanent VPN access to vendors,




## Secure Access

Safely grant a vendor, contractor, offshore developer, or support team direct access to their application

## Access to Infrastructure

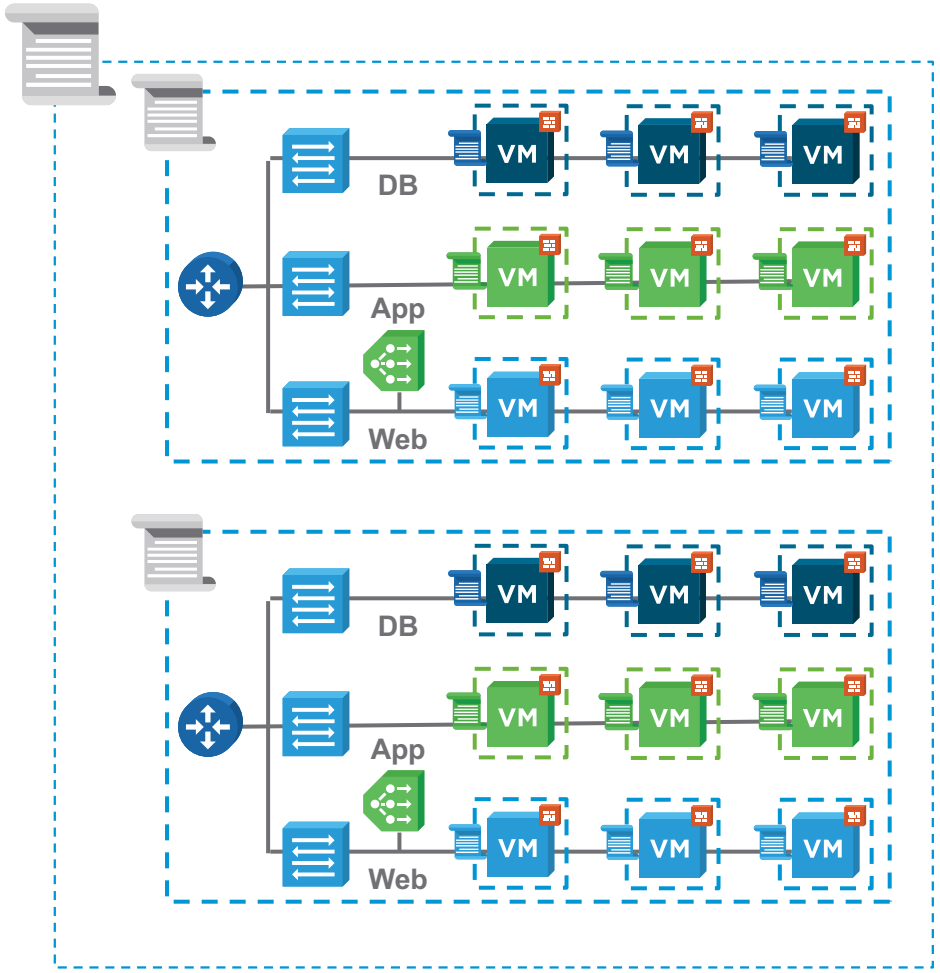
Ability to grant control of individual network constructs, including access to unlimited virtual routers, switches, firewalls, and load balancers without any additional hardware cost

## Application Migration

Ability to migrate applications to production environments in seconds with no impact to production

vmware®

# Collapsed DMZ




## Increased east-west security

Distributed firewalling provides segmentation and isolation to satisfy compliance requirements

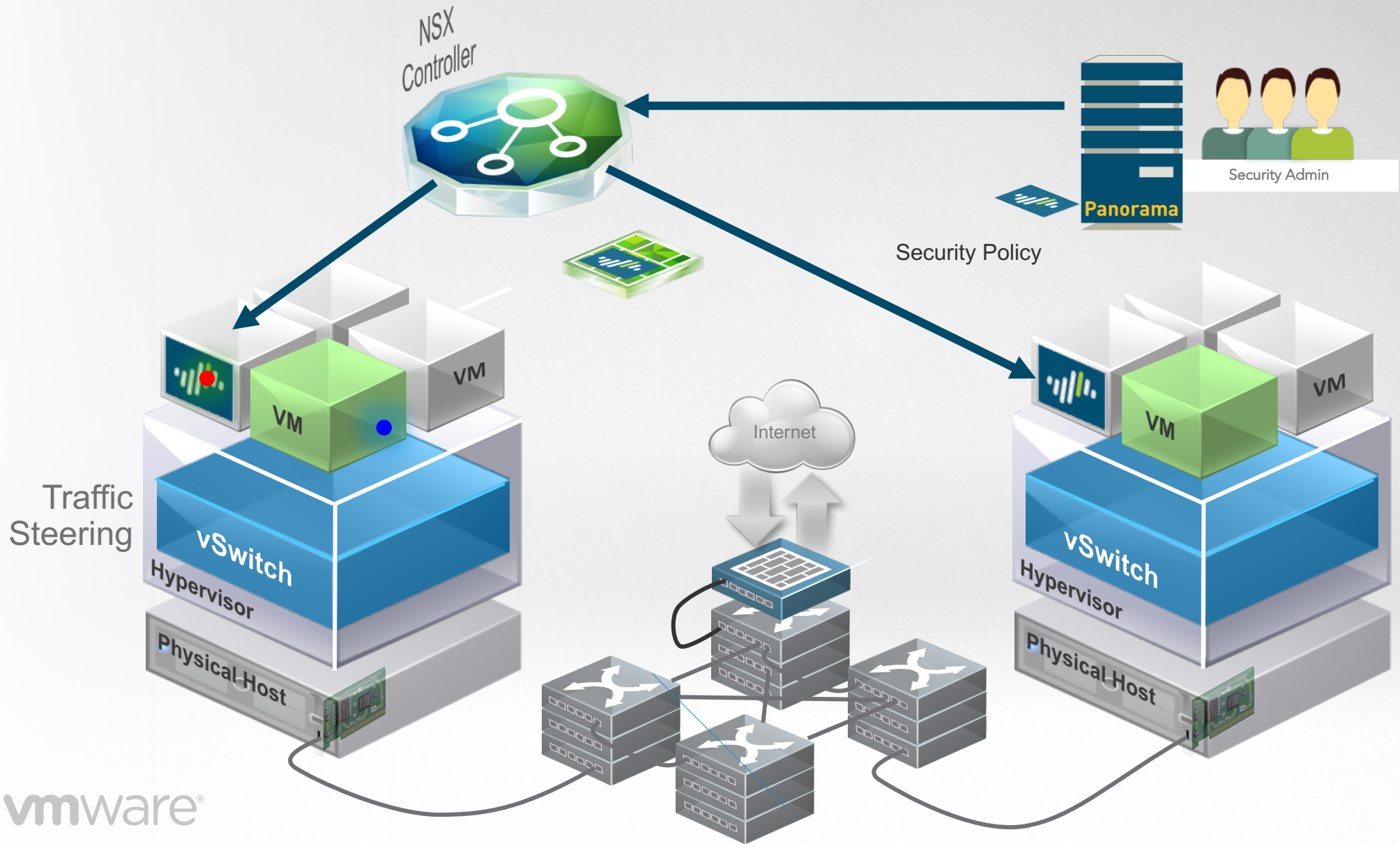
## Lower cost - Fewer devices

Consolidation of security zones is possible while maintaining a rigorous security posture

## Automation of Security

Security partner solutions, such as Palo Alto's Wildfire, can provide cloud based forensic analysis and automated response

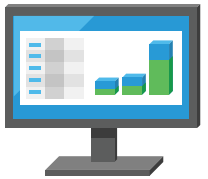
# Advanced Security (IDS/IPS) Insertion – Example: Palo Alto Networks NGFW

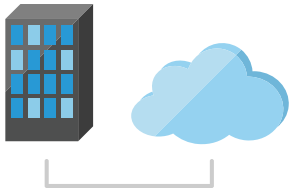



vmware

# NSX Partner Ecosystem

| Application delivery services | Security | Visibility & operations | Physical to cloud |
|---|---|---|---|






















vmware

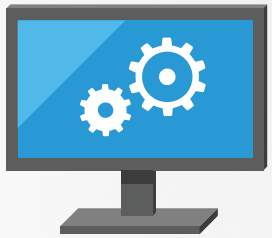
# IT Automation

## Speed and Agility

# Automated App Deployment

## Multi-tier app deployments with networking and security

Cloud Management Platform



APIs
Roll Your Own




Application Workloads

Virtual Network Infrastructure

Physical Network Infrastructure

### Deploy and Configure NSX

Provides the functionality for the network and security components to be deployed.

### Deploy Cloud Management Platform

vRA or Openstack enabled network automation.

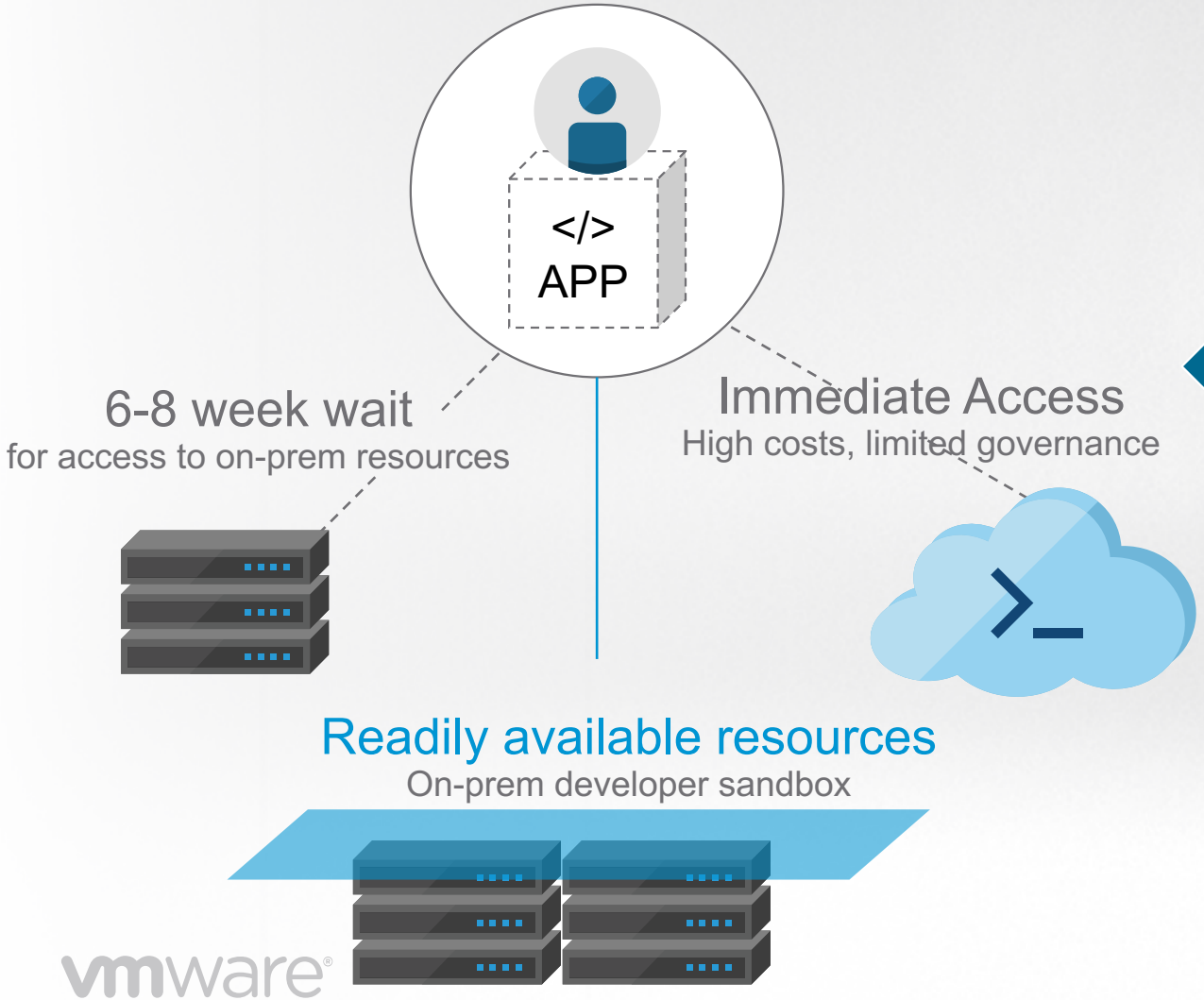
### Configure Application Blueprints

Enable self-service catalog based on known application configurations

vmware

# Self-service Dev Sandbox

Facilitate innovation with a public cloud experience




## Network Virtualization Platform

Provides the functionality for the network and security components to be deployed.

## Cloud Management
vRA / Openstack

Automated provisioning of isolated application pods.
Initiation portal for requesting applications and services

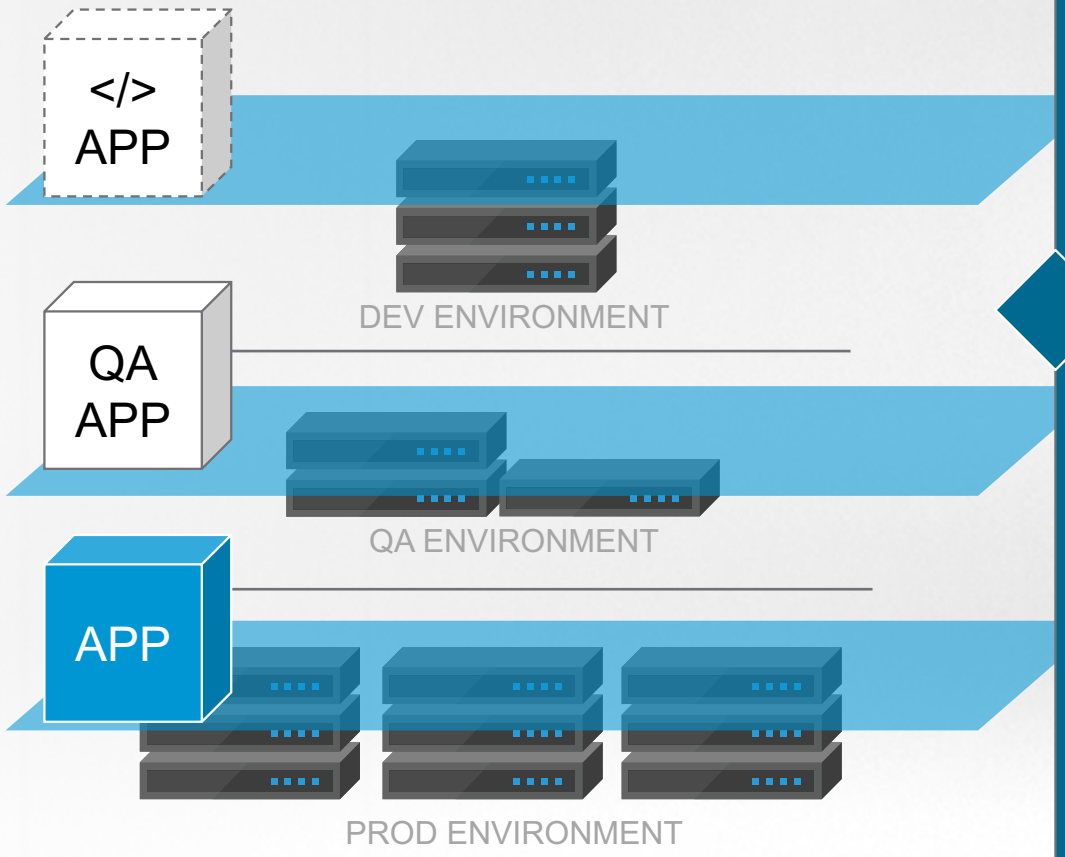
## Developer Sandboxes

Aggregate multiple sandbox templates as a self-service catalog for developers
Consistent Dev/Test/Prod Environments

vmware

# Development Lifecycle

## Consistent Test / Dev / Production Environments




### Independent Data Centers

Each application gets its own logical network topology on its own separate VXLANs/DLRs while still allowing access to external dependencies

### Identical Dev/Test/Prod

Networking and security environments that can be copied as the application evolves

### Snapshot Environments

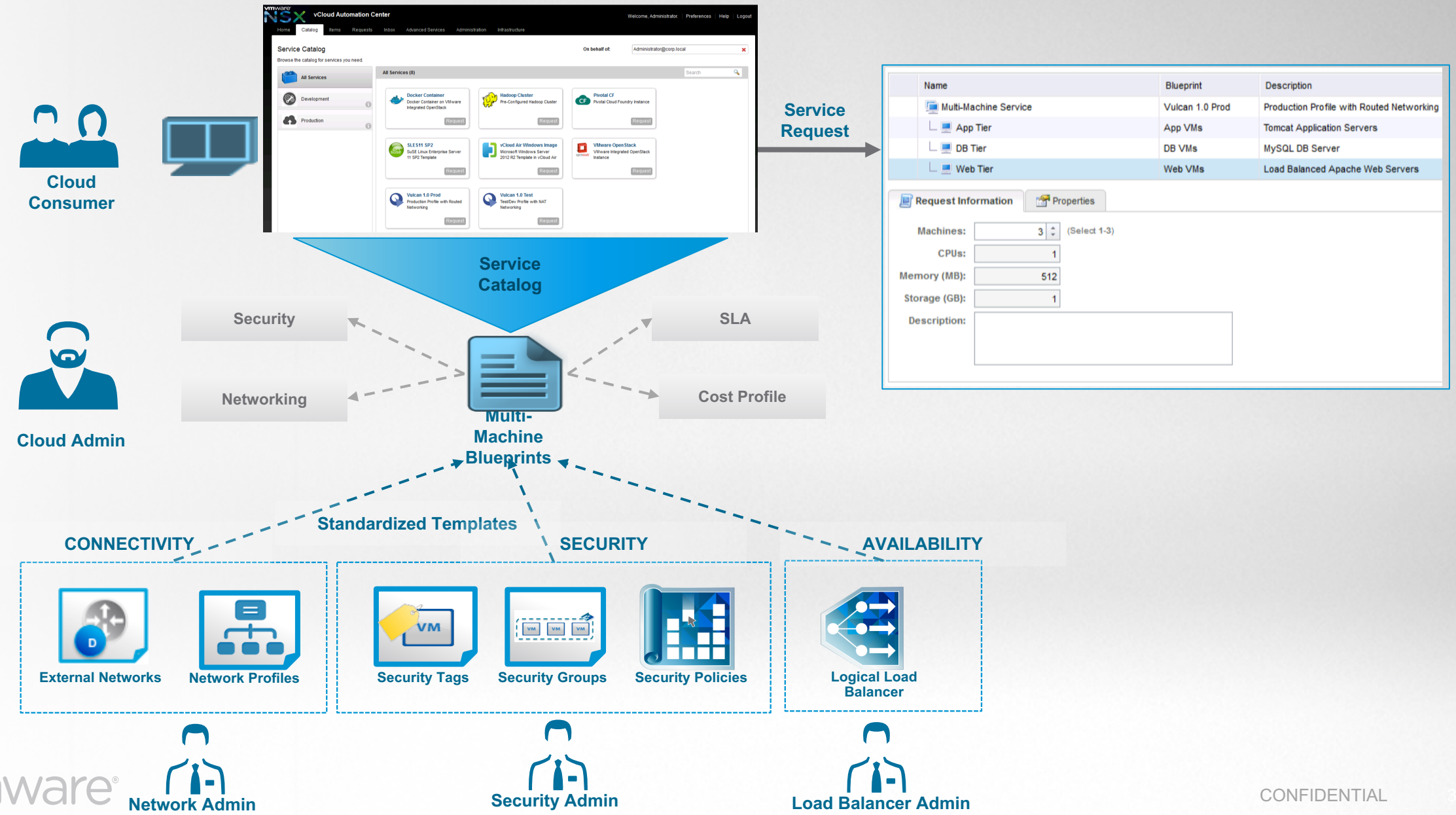
Enabling developers to roll back infrastructure configurations to a previous step in the lifecycle to debug applications

vmware

# Integrate Dev, Test and Prod environment into single infrastructure


- No communication path between different tenants
- Separate dev, test and production environments over single physical network
- Independent of hardware
- Overlapping IP addressing can be used

# Self Service IT

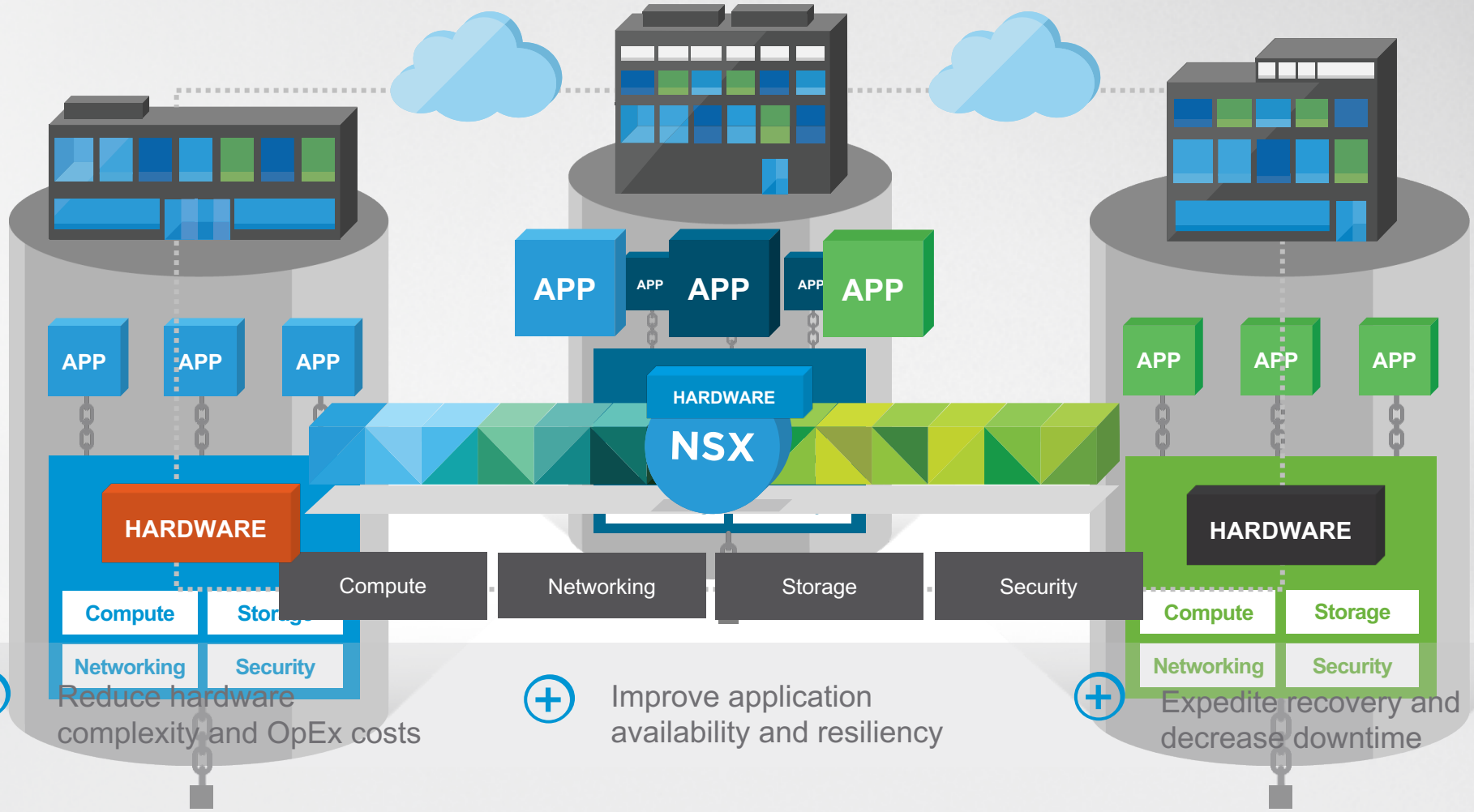


vmware

# Application Continuity

## Disaster Recovery

# Enabling Data Centers Anywhere



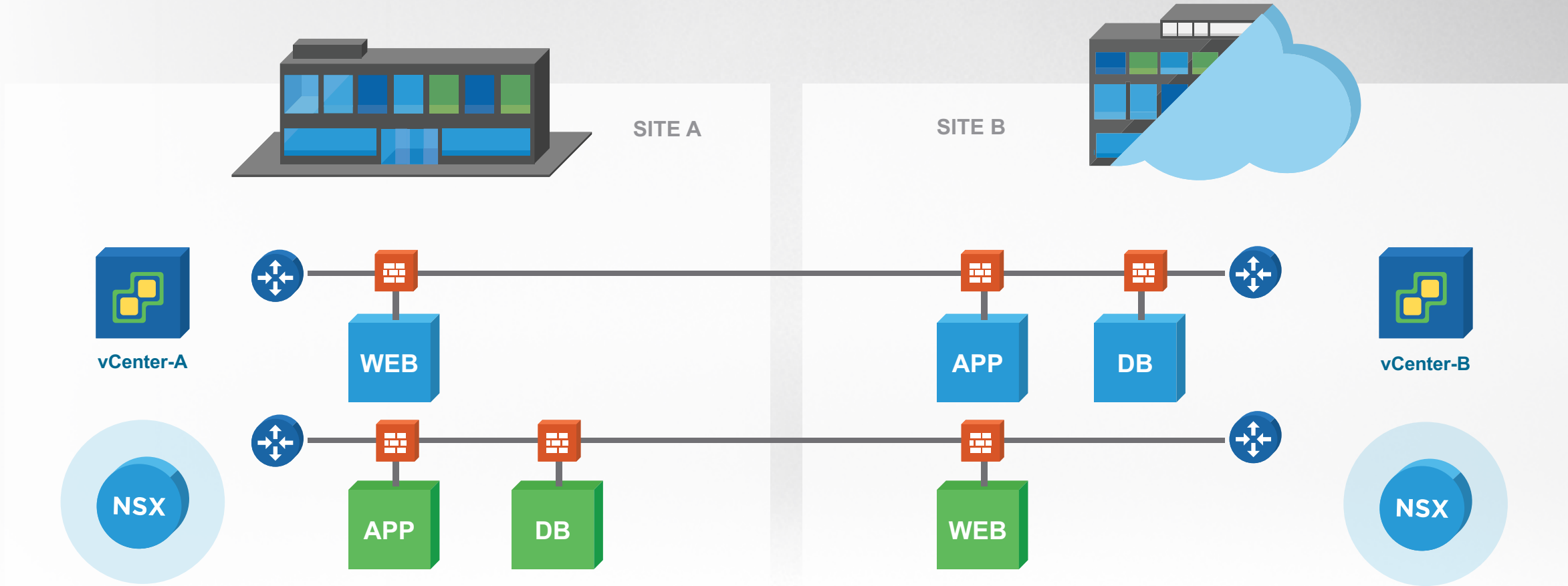

Reduce hardware complexity and OpEx costs

Improve application availability and resiliency

Expedite recovery and decrease downtime

# Application anywhere

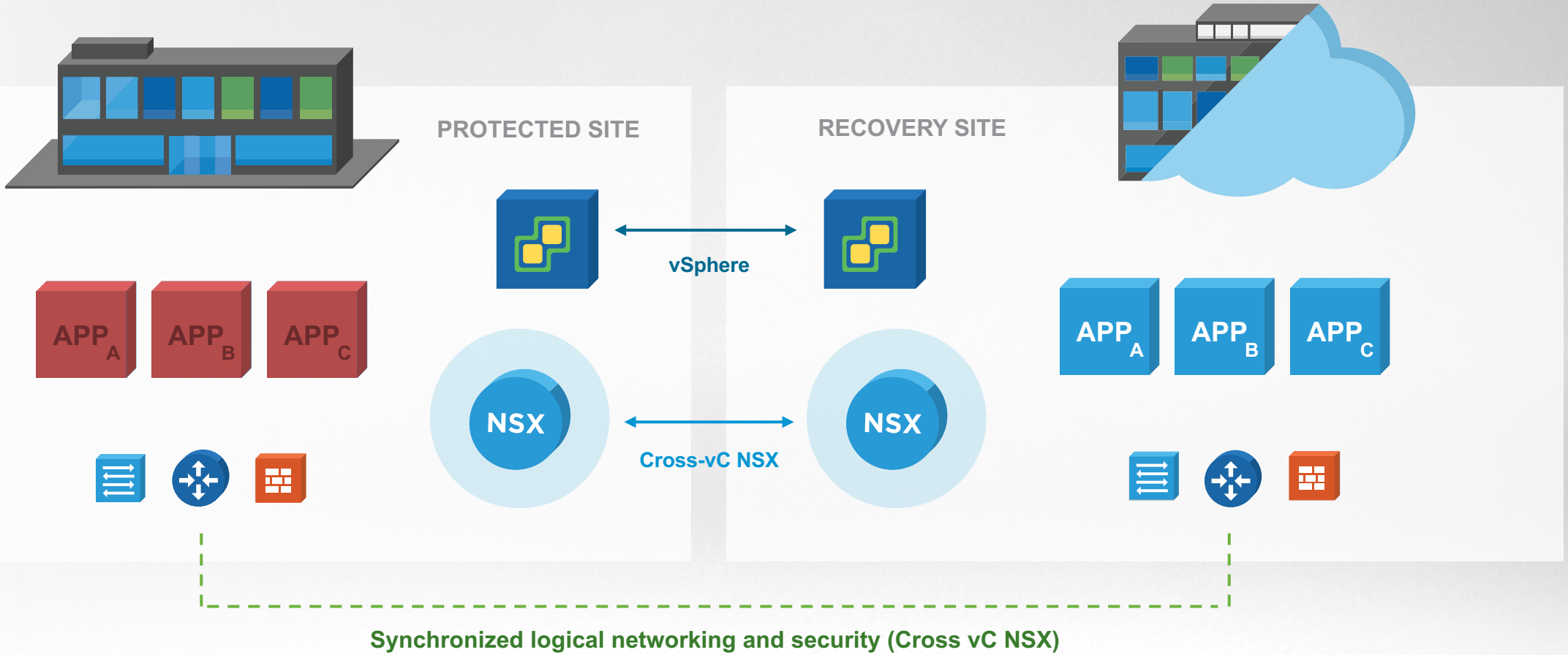
## Unified, seamless, and resilient networking and security infrastructure to run your applications




vmware

# Disaster recovery

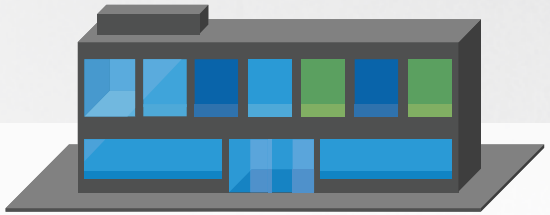
## Synchronize applications, networking, and security across locations to reduce recovery time



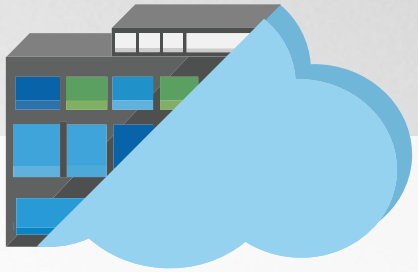

vmware

# Workload mobility

## Simplify how you move existing workloads across locations



SITE A



SITE B

vCenter-A

vCenter-B

NSX

VM VM

VMware

192.168.96.1

vMotion

Hot or cold migration

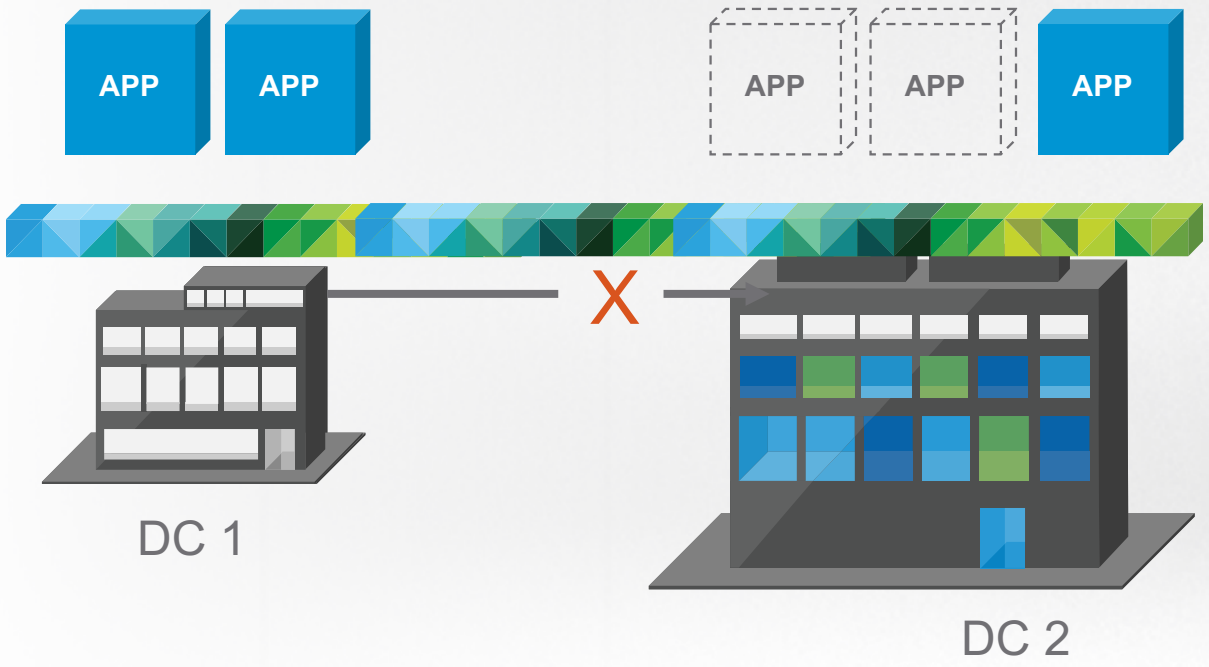
VM

VMware

NSX

vmware

# Mergers and Acquisitions




## IAAS with Network Virtualization

Provides a platform that allows the logical network topology of the acquired company to be reproduced within the virtual space

## Non Disruptive Migration

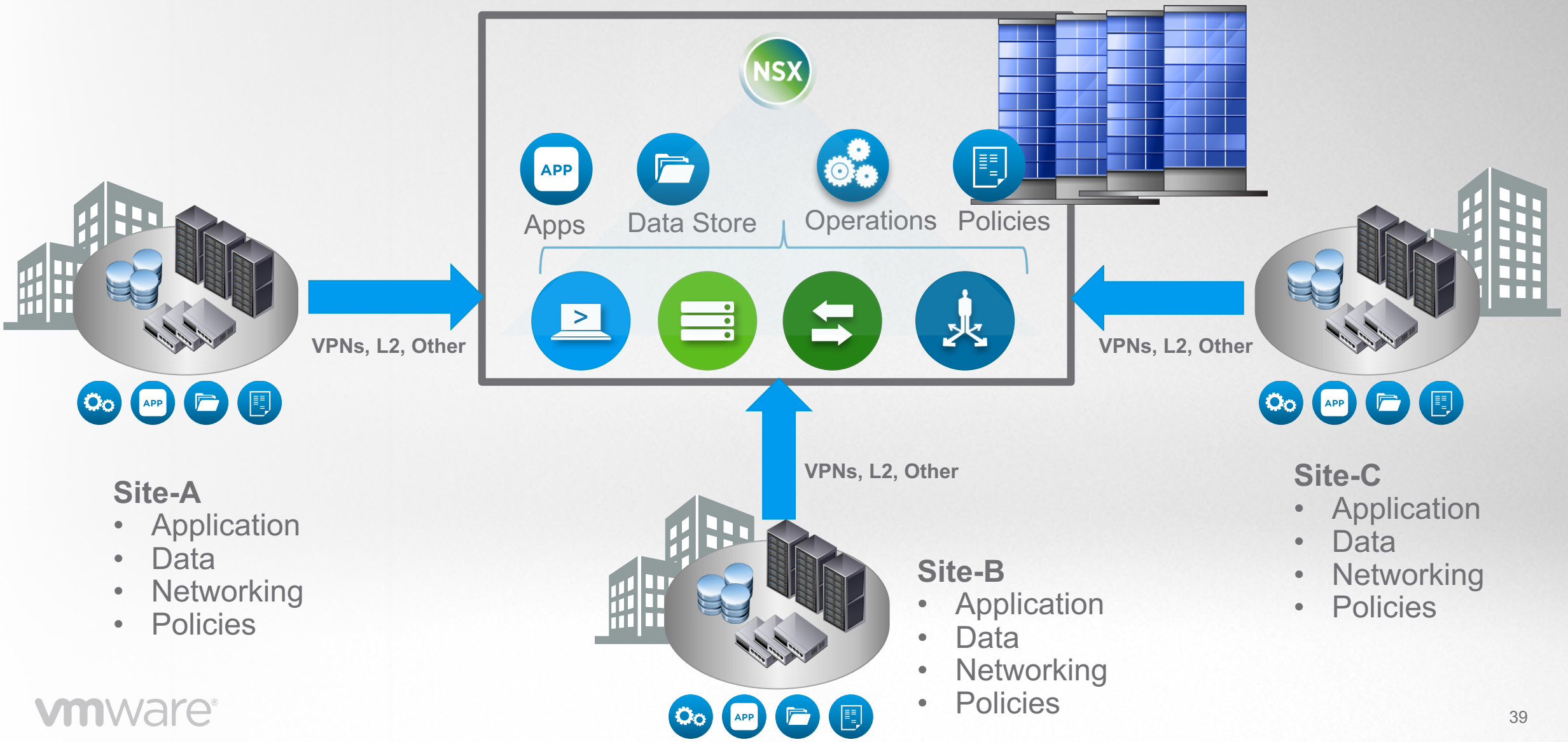
While VMs and applications are migrated, the new virtualized version of the acquired network is maintained and operated by that companies existing network team

## Rapid DC Consolidation

The acquired companies applications and networking topology is absorbed much more quickly than if it needed to be re-architected as part of the migration

vmware®

# DC Consolidation/Migration




**Site-A**
- Application
- Data
- Networking
- Policies

**Site-B**
- Application
- Data
- Networking
- Policies

**Site-C**
- Application
- Data
- Networking
- Policies

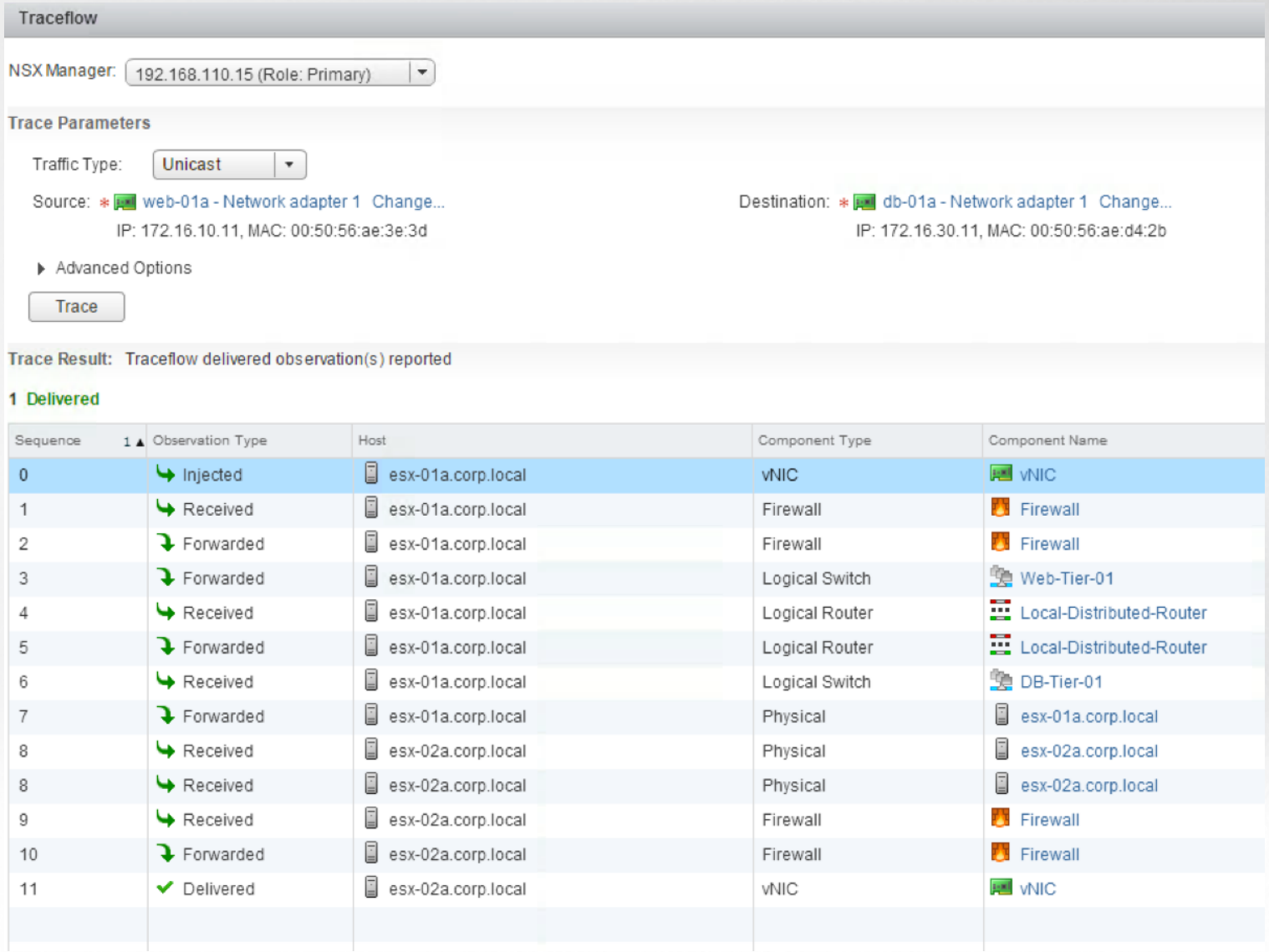
vmware

# Operations

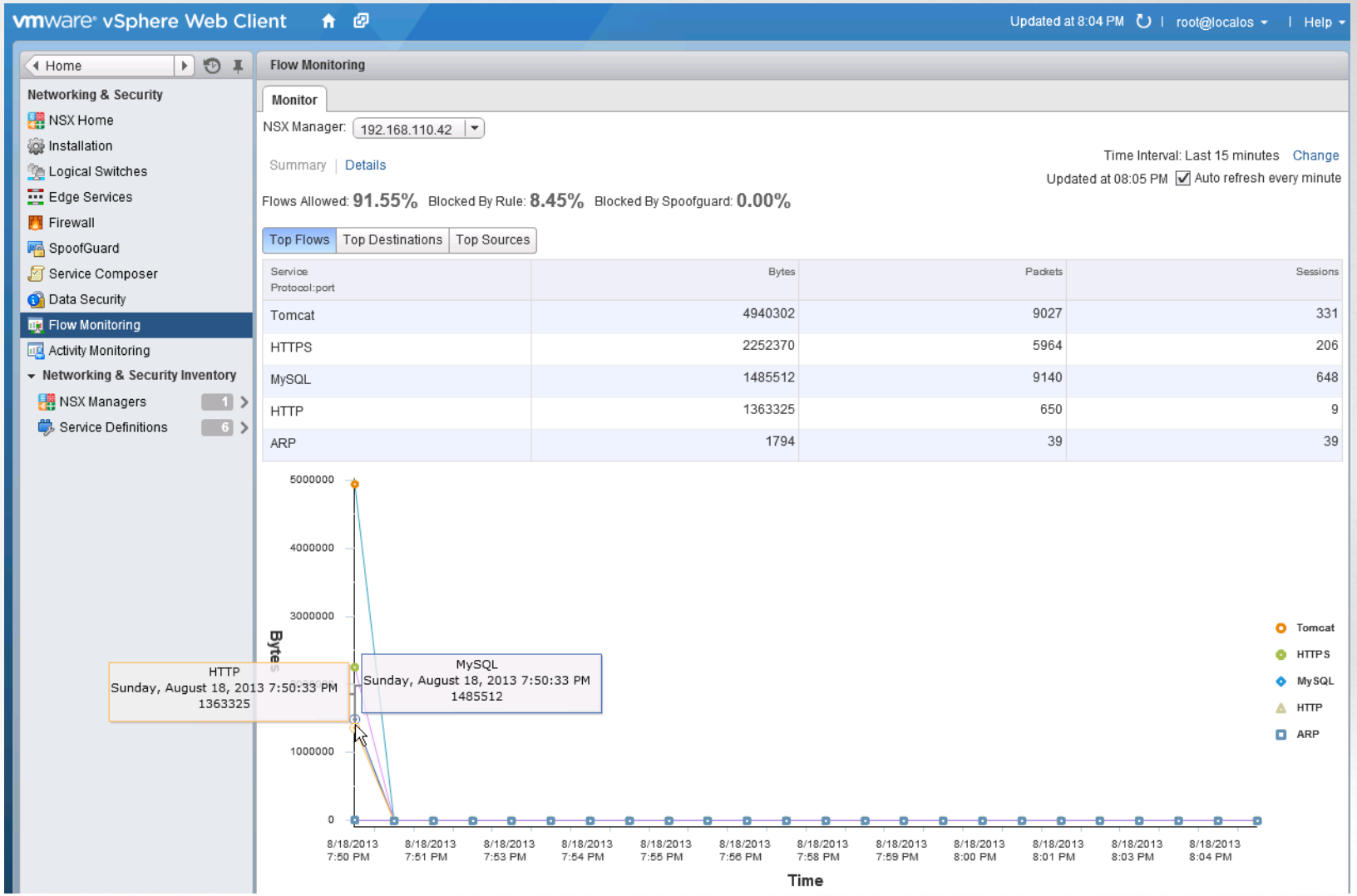
## Managing & troubleshooting

# NSX native operations capabilities

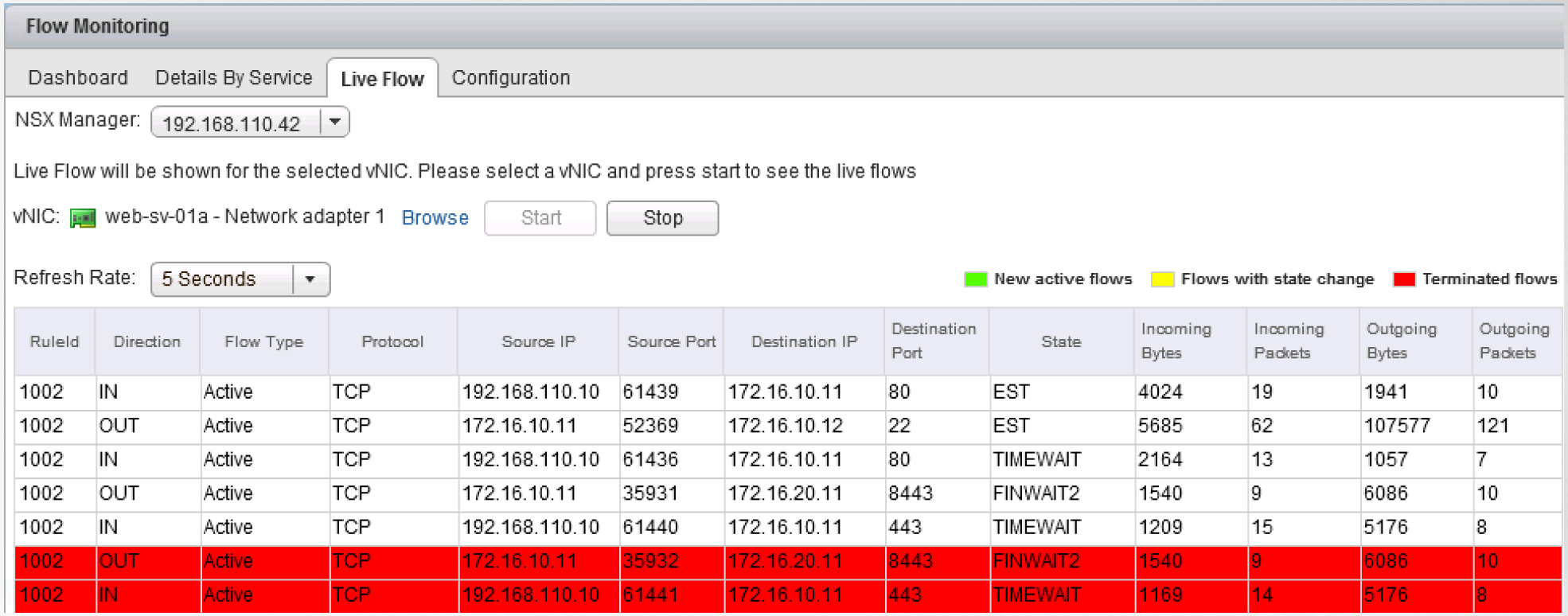
# NSX Operation Tools – Traceflow



# NSX Operation Tools – Flow Monitoring



# NSX Operation Tools – Live Flows



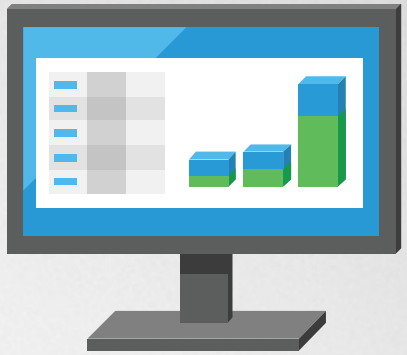

| RuleId | Direction | Flow Type | Protocol | Source IP | Source Port | Destination IP | Destination Port | State | Incoming Bytes | Incoming Packets | Outgoing Bytes | Outgoing Packets |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1002 | IN | Active | TCP | 192.168.110.10 | 61439 | 172.16.10.11 | 80 | EST | 4024 | 19 | 1941 | 10 |
| 1002 | OUT | Active | TCP | 172.16.10.11 | 52369 | 172.16.10.12 | 22 | EST | 5685 | 62 | 107577 | 121 |
| 1002 | IN | Active | TCP | 192.168.110.10 | 61436 | 172.16.10.11 | 80 | TIMEWAIT | 2164 | 13 | 1057 | 7 |
| 1002 | OUT | Active | TCP | 172.16.10.11 | 35931 | 172.16.20.11 | 8443 | FINWAIT2 | 1540 | 9 | 6086 | 10 |
| 1002 | IN | Active | TCP | 192.168.110.10 | 61440 | 172.16.10.11 | 443 | TIMEWAIT | 1209 | 15 | 5176 | 8 |
| 1002 | OUT | Active | TCP | 172.16.10.11 | 35932 | 172.16.20.11 | 8443 | FINWAIT2 | 1540 | 9 | 6086 | 10 |
| 1002 | IN | Active | TCP | 192.168.110.10 | 61441 | 172.16.10.11 | 443 | TIMEWAIT | 1169 | 14 | 5176 | 8 |

# vRealize Network Insight

## Transformative Operations for NSX based Software-Defined Data Center

Plan Micro-segmentation Deployment and Ensure Compliance

Optimize Network Performance with $360^0$ Visibility & Analytics



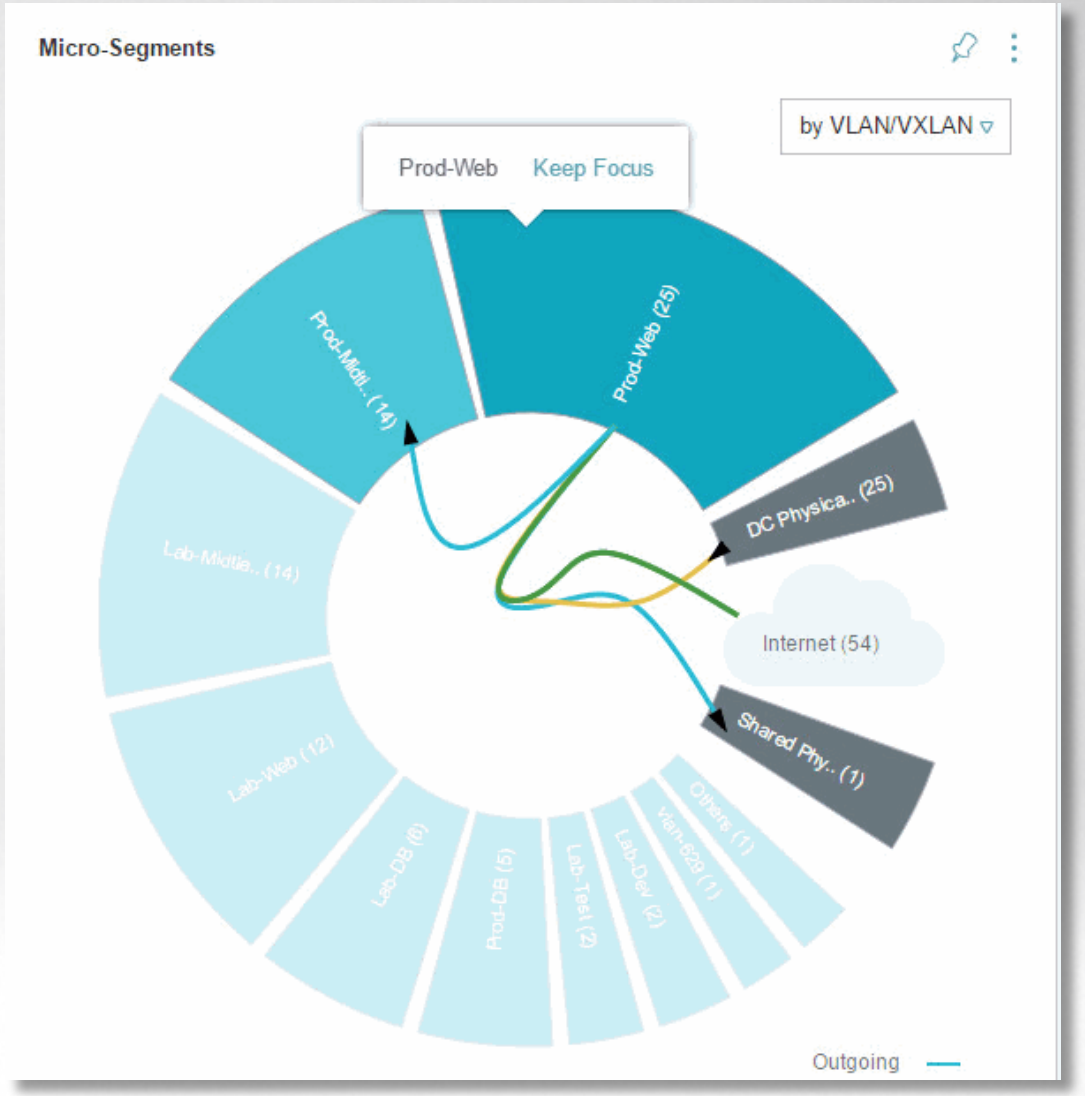
Ensure Best Practices, Health and Availability of NSX Deployment

Across Virtual, Physical and Cloud

vmware®

# Security Policy Automation – Micro-Segmentation

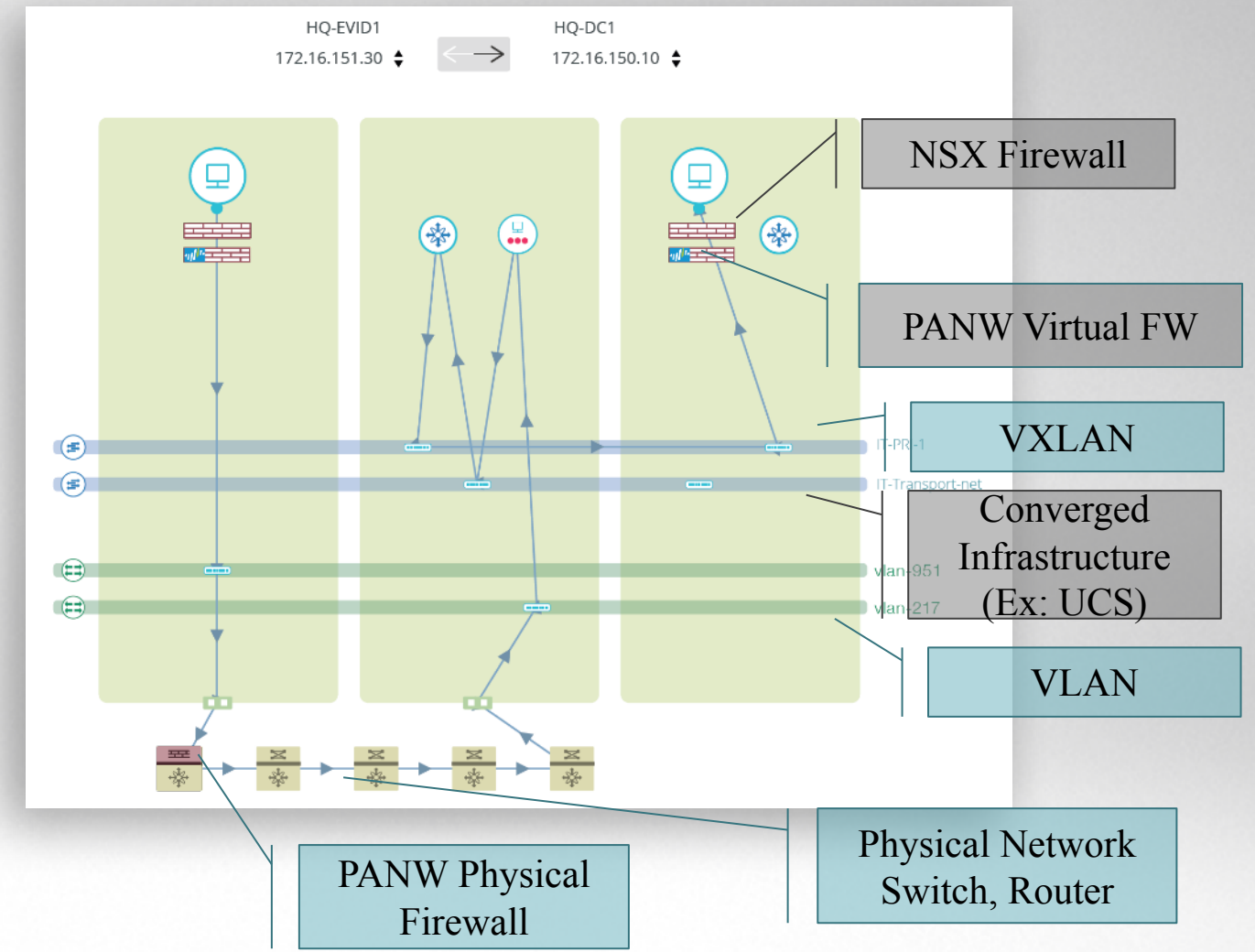
- Discover vCenter and NSX constructs (folders, clusters, vlans, security tags)
- Automated Security Groupings Based on vCenter and NSX Constructs, Workload Characteristics, Ports, Common Services
- Recommended Security Policies / Firewall Rules (Zero-Trust Model)
- See Network Traffic Per Host, Per VM
- Export as CSV



# Data Paths Across Overlay And Underlay

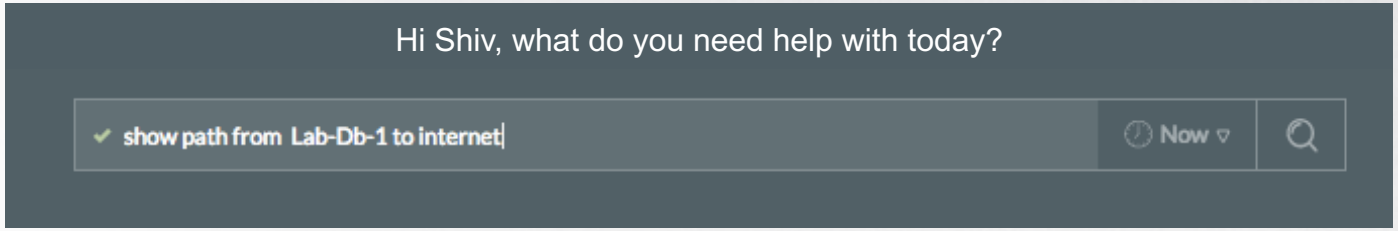
**Connectivity Graphs**

- VM to VM, VM to Physical, VM to Internet
- Hop-by-Hop Path across Overlay (LDRs, Edge Gateways) and Underlay (Physical VDCs & VRFs). See V-To-P Boundary
- Correlated Problems And Performance Metrics Across Virtual and Physical
- See Effective Firewall Rules and Security Policies across NSX and PANW in Service-Chained Environment

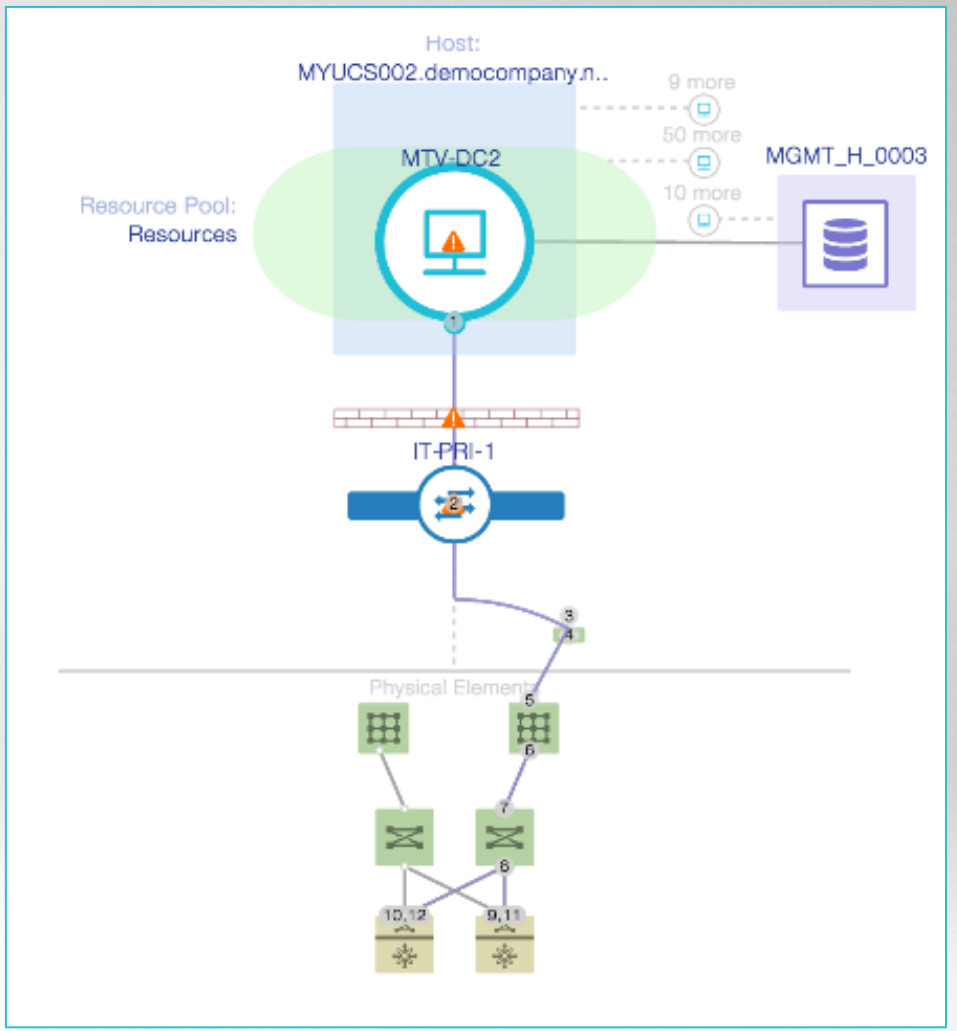



vmware

# Simple & Contextual Search




- Single pane of glass between virtual & physical
- Google-like search for ease of use
- Time aware search (go back in time)
- Fewer clicks to find and identify issues
- Simplified interface, reduce learning curve across admin teams

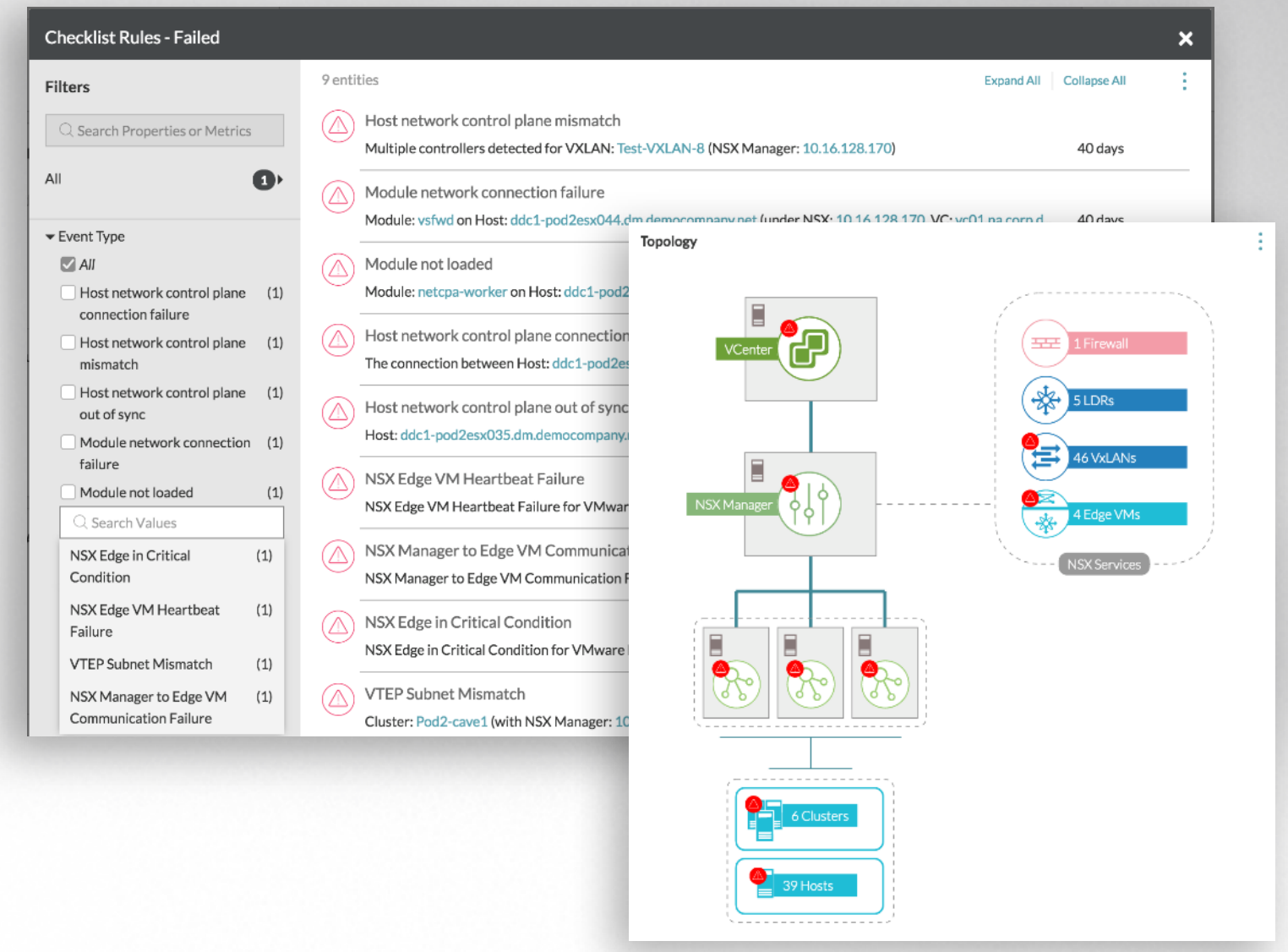



vmware

# NSX Infra Monitoring & Best Practices Checks (80+)

## Configuration, Health and Consistency Validation

- VTEP Level Misconfigurations
- VTEPS – Underlay Mapping Checks
- Netcpa Health
- Hosts Version Validation
- LDR and Edge Config Issues
- Routing Misconfigurations/ Issues between LDR, Edge and Physical Routers

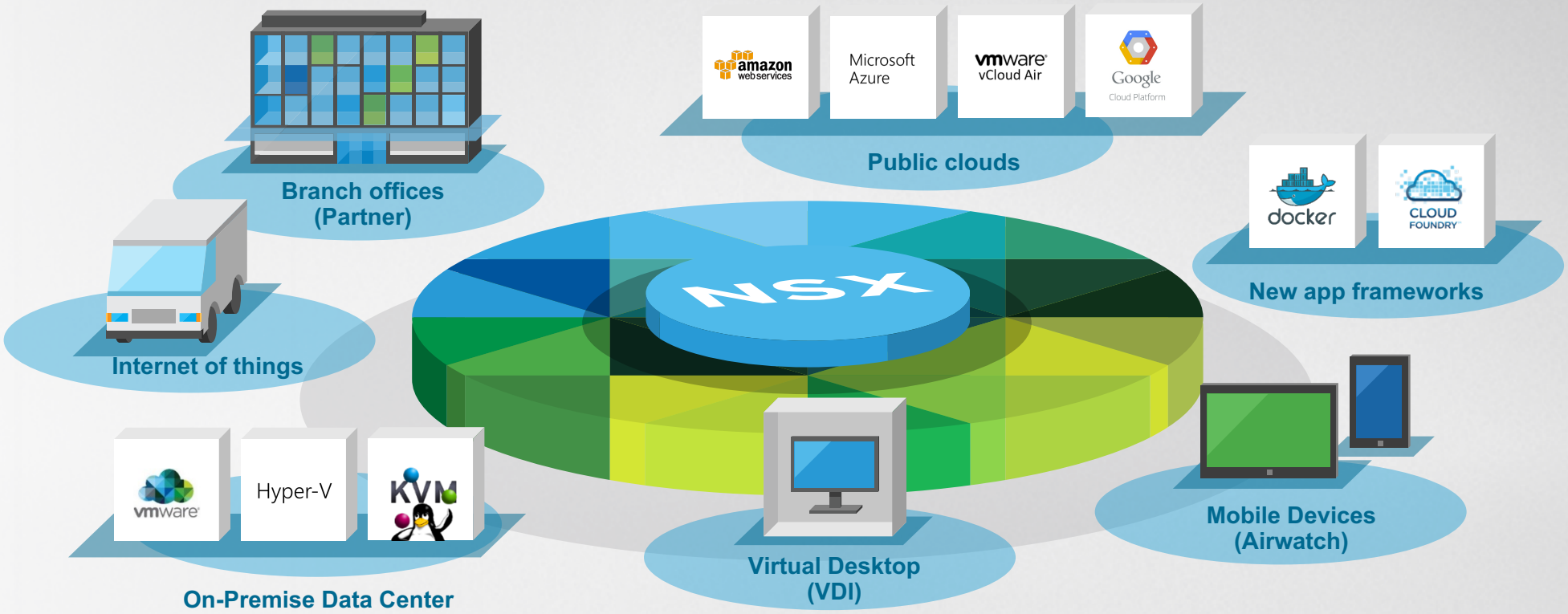


vmware

# Next Generation

## Clouds & Containers

# NSX Vision: Driving NSX Everywhere




**Automation**

IT at the Speed of Business

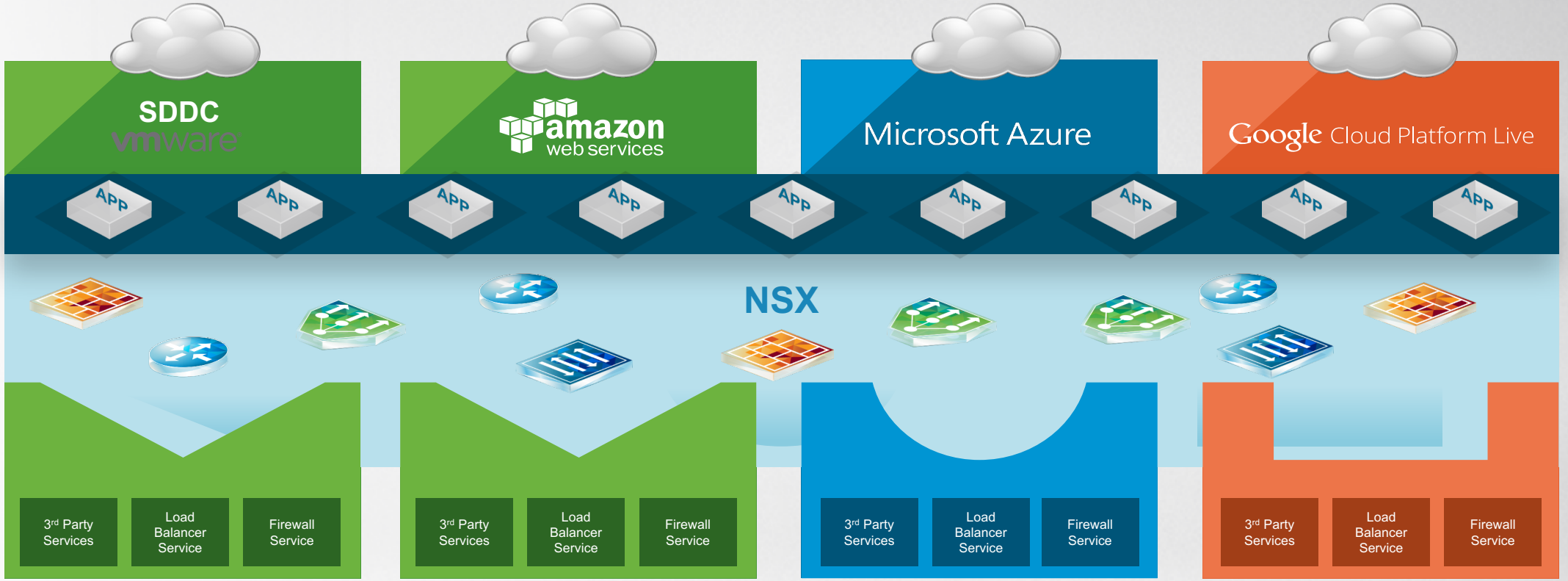
**Security**

Inherently Secure Infrastructure

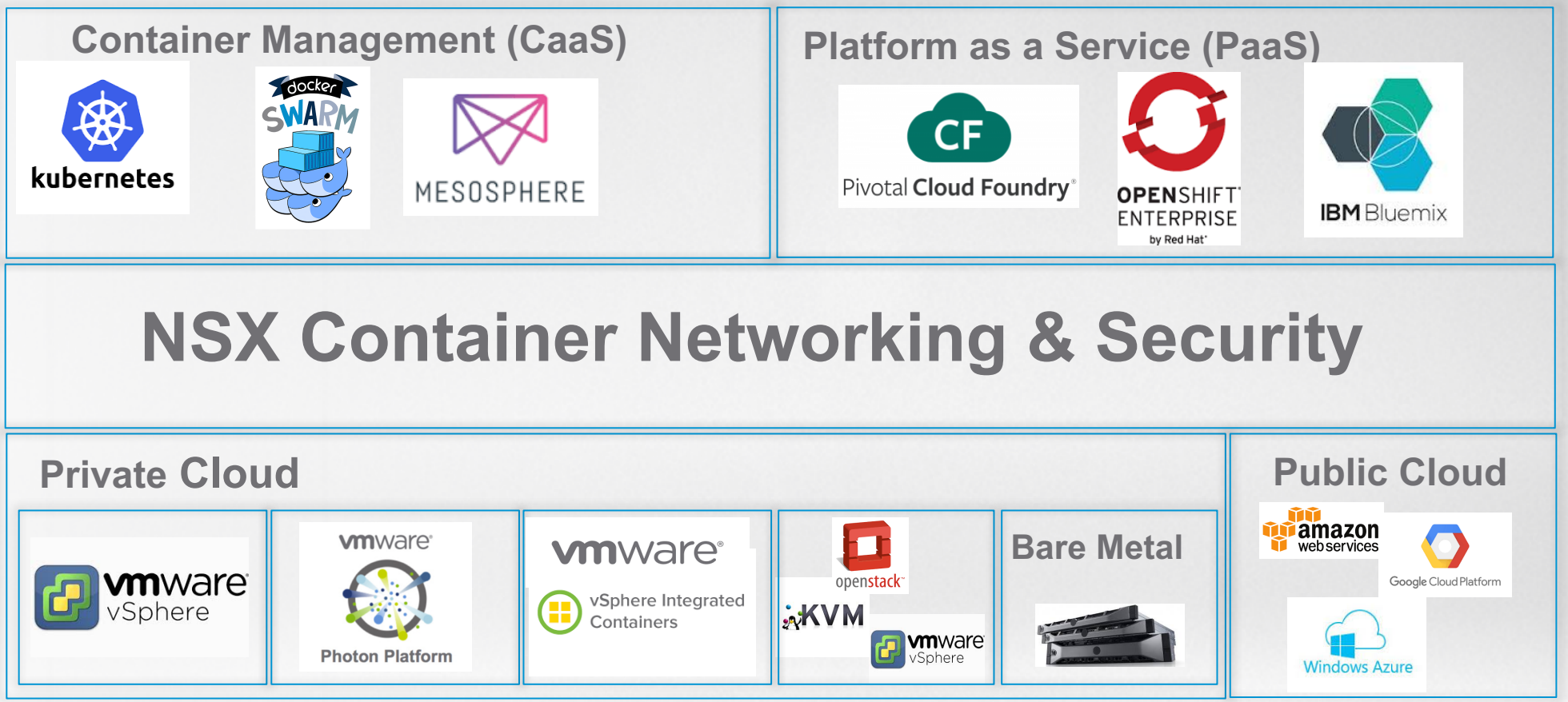
**Application Continuity**

Data Center Anywhere

# VMware Cross-Cloud Services



# NSX with Containers & CNA



vmware®

# Thank You!