

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



VMware Cross-Cloud Architecture™

Private Cloud

Hybrid Cloud

Public Cloud

VMware Cross-Cloud Services™

Any Cloud



VMware vRealize® Cloud Management



Software-Defined Data Center



Microsoft Azure



Google Cloud Platform

VMware vCloud® Air™ Network
VMware vCloud Air

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

Hardware



- Compute
- Storage
- Network



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

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

**Google / Facebook /
Amazon Data Centers**

 **Custom Application**
Software / Hardware Abstraction

 **Custom Platform**
Software / Hardware Abstraction

Any x86

Any Storage

Any IP network

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

Software Defined Data Center (SDDC)

Any Application

SDDC Platform

Data Center Virtualization



Any x86

Any Storage

Any IP network

Google / Facebook / Amazon Data Centers

Custom Application

Software / Hardware Abstraction

Custom Platform

Software / Hardware Abstraction

Any x86

Any Storage

Any IP network

Hardware Defined Data Center (HDDC)

Any Application

HDDC Platform

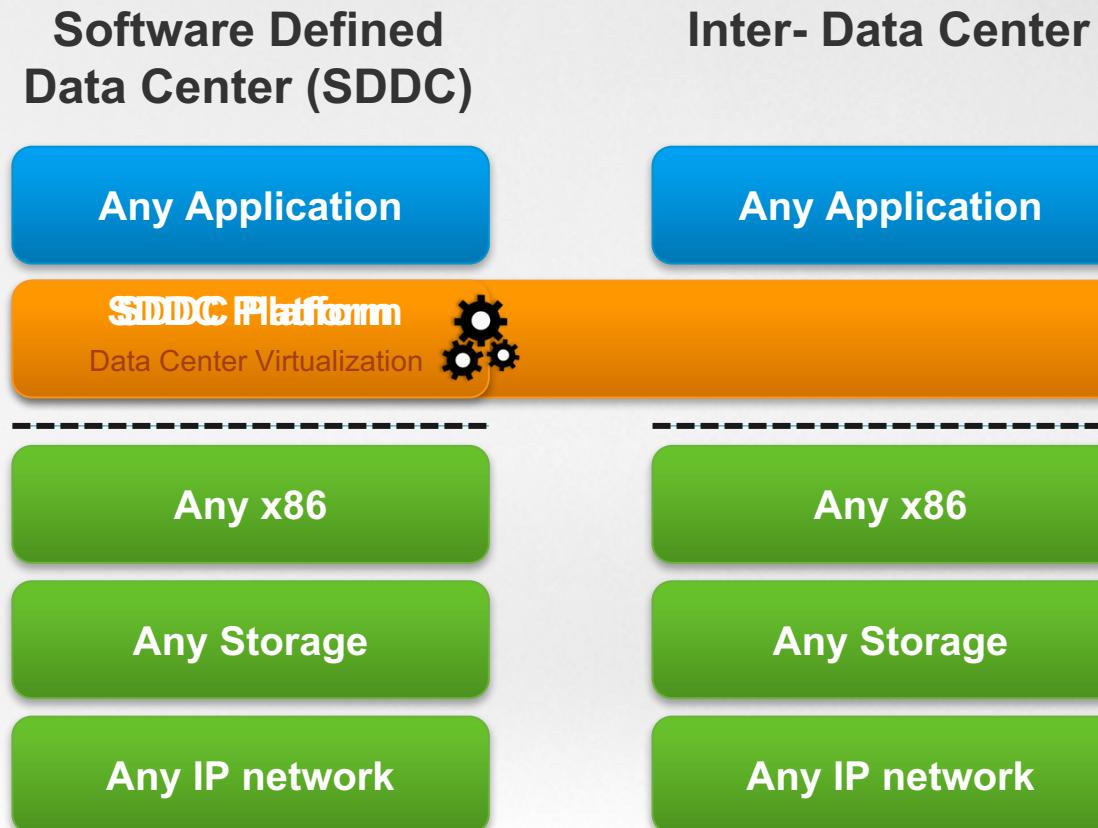
Integrated x86

Integrated Storage

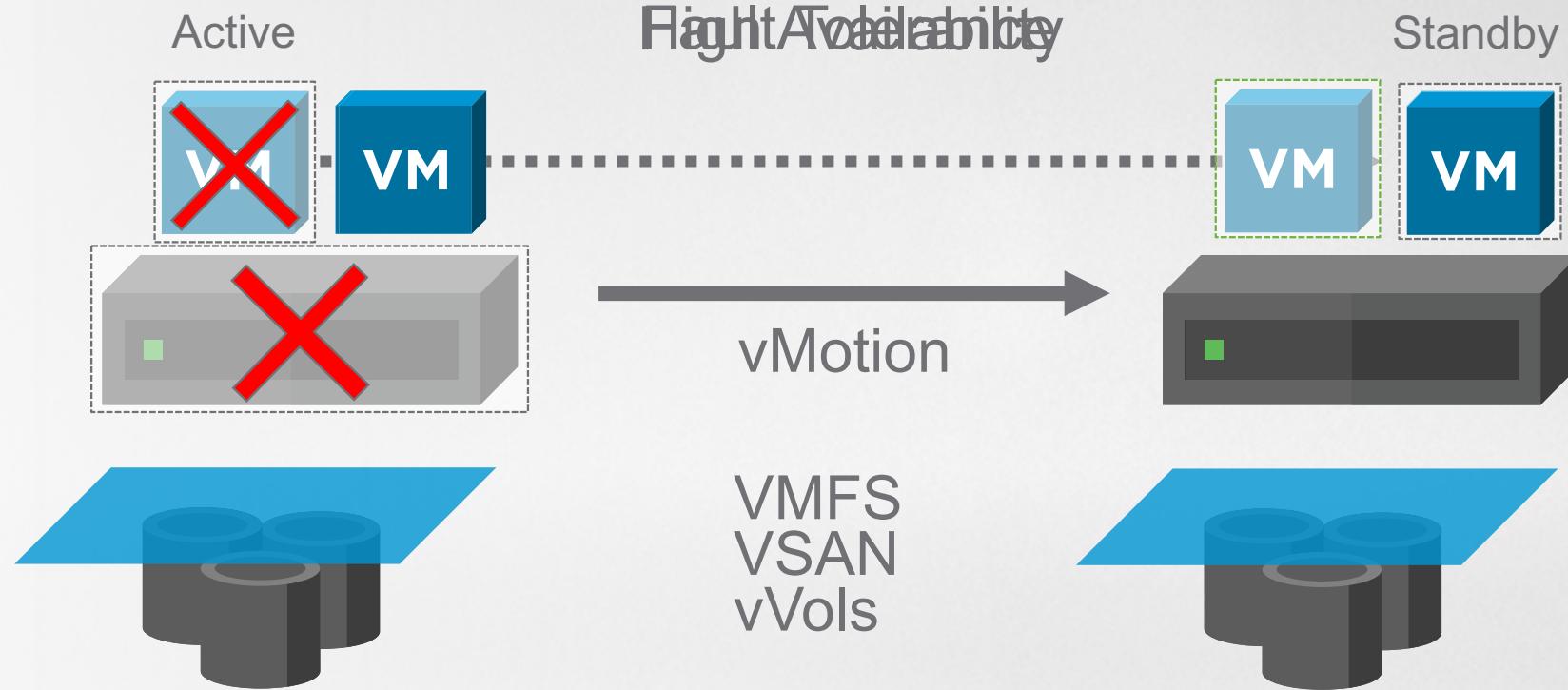
Vendor Specific Network

Vertical Integration

SDDC Within, Between and Across Data Centers



VMware Journey

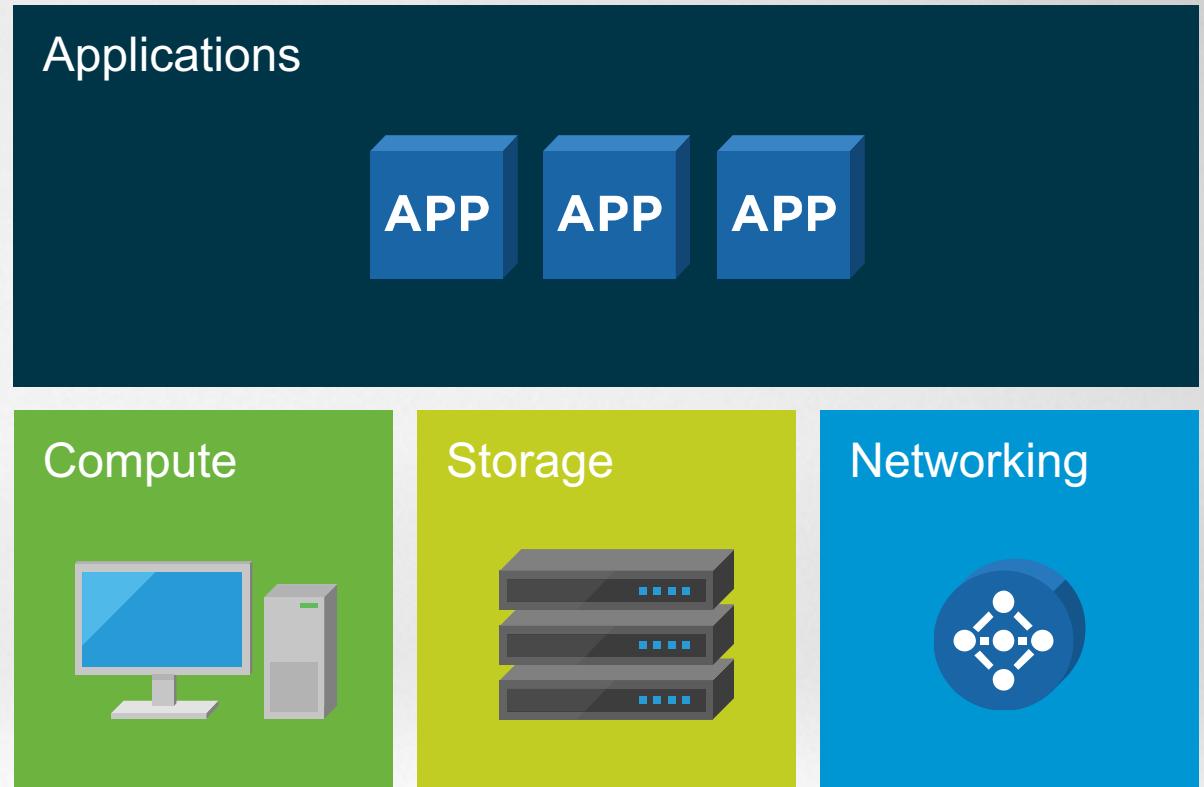


So...what's the problem?

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.

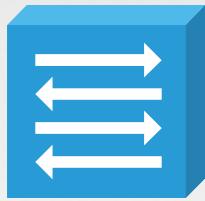
- You can't keep up with the pace of business
- You can't secure the data center
- You can't support this new app-driven world



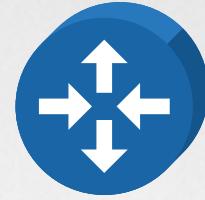
NSX Services



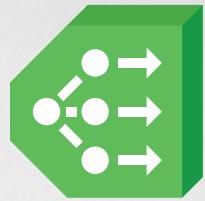
NSX Platform



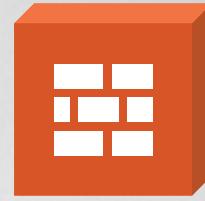
In-Kernel
Switching



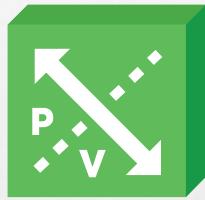
In-Kernel
Routing



In-Kernel
Load Balancing



In-Kernel
Firewalling



Connectivity
to Physical
Networks



VPN (IPsec,
SSLVPN,
L2VPN)

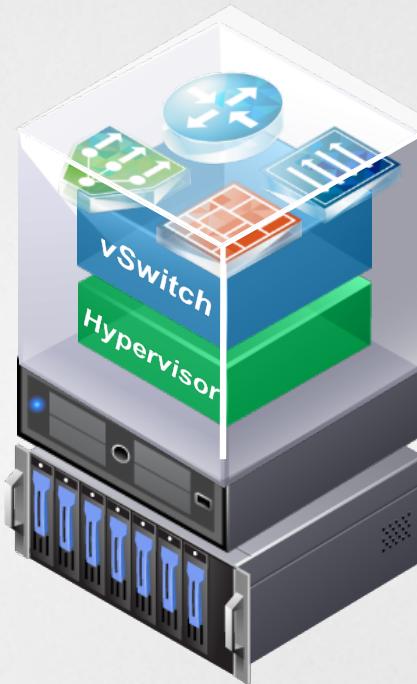
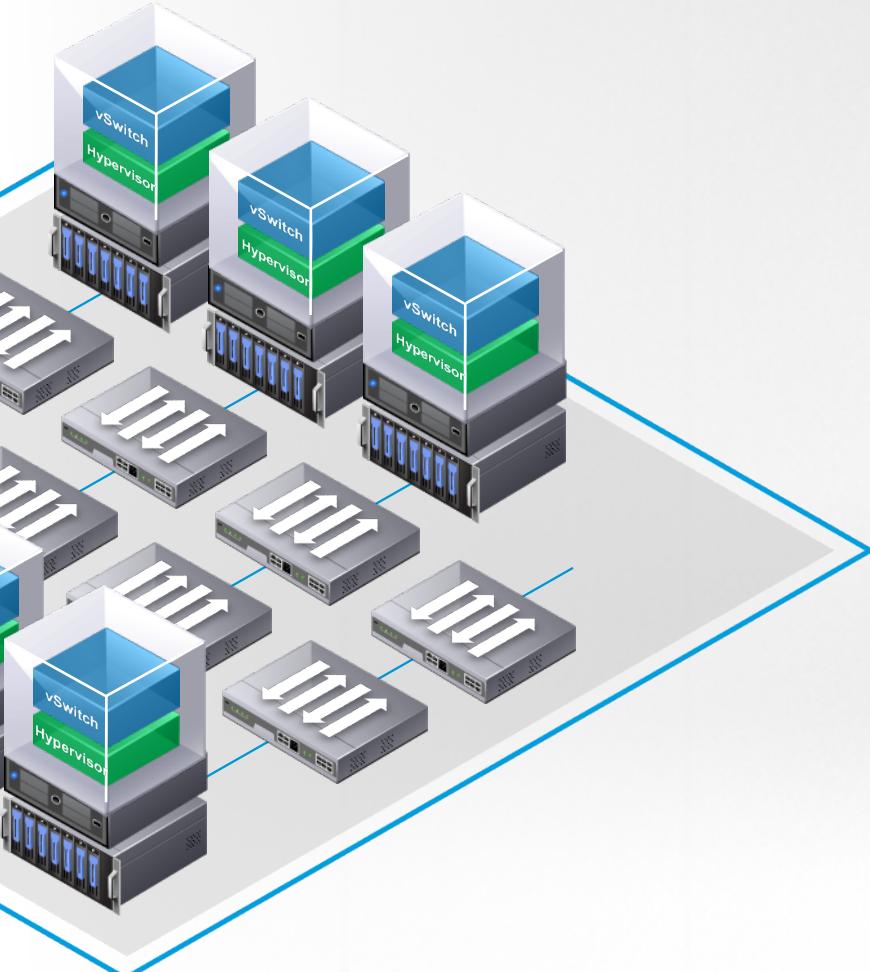


3rd Party
Service
Insertion



Open API
(Automation)

The Power of Distributed Services



Routing

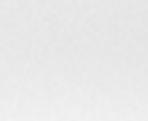


Load Balancing



vSwitch
Hypervisor

Routing



Load Balancing



Switching

High throughput / low latency

East-west firewalling

Firewalling/ACLs

Native platform capability

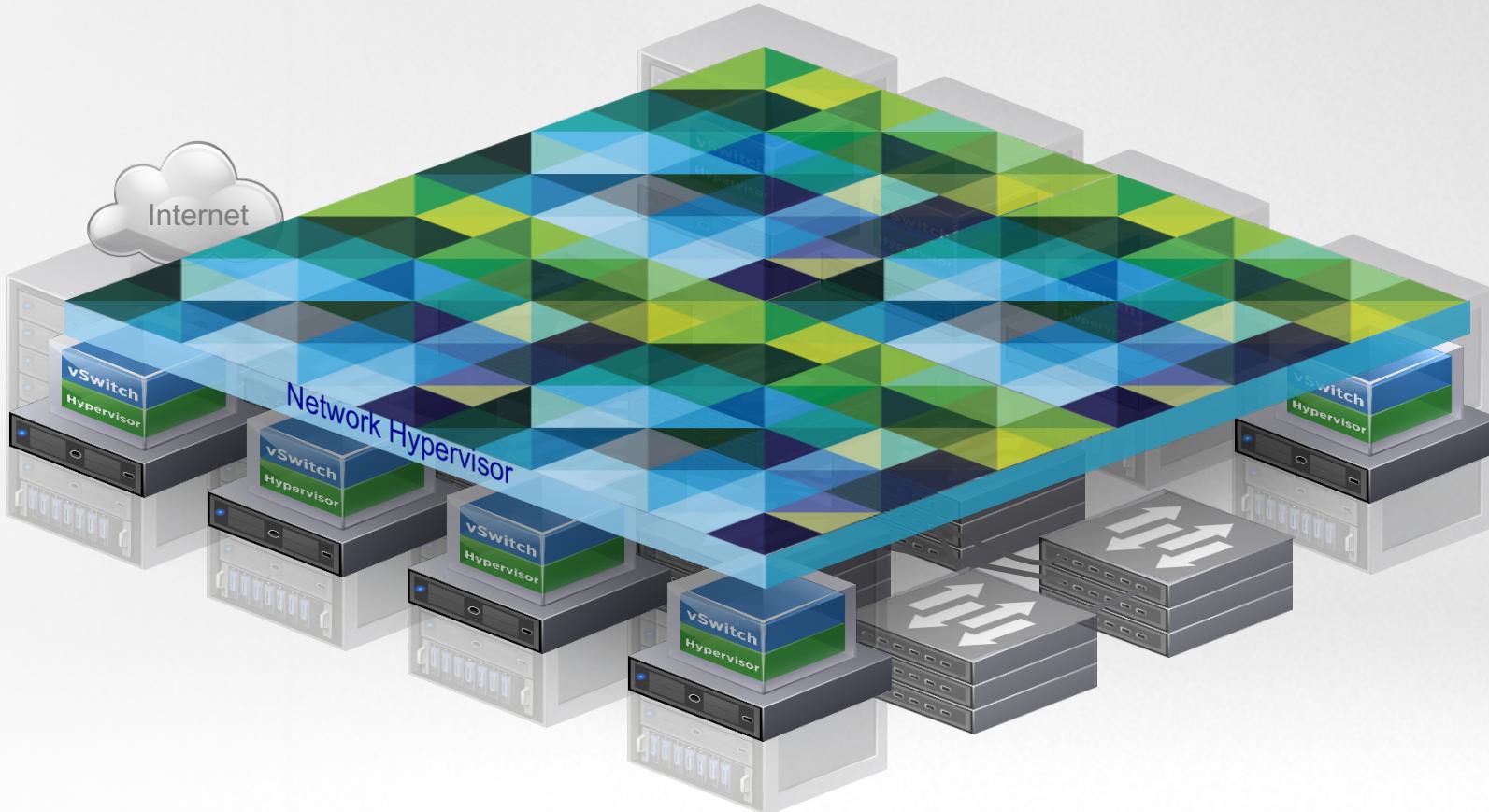
Your Typical Datacenter



NSX Virtual Networking Components



The “Network Hypervisor”



Our “Three Pillars”

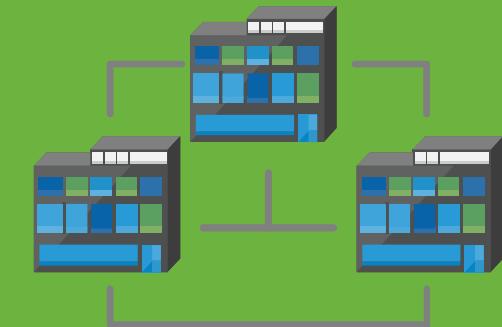
Security



IT Automation



Application
Continuity





Security

Micro-segmentation





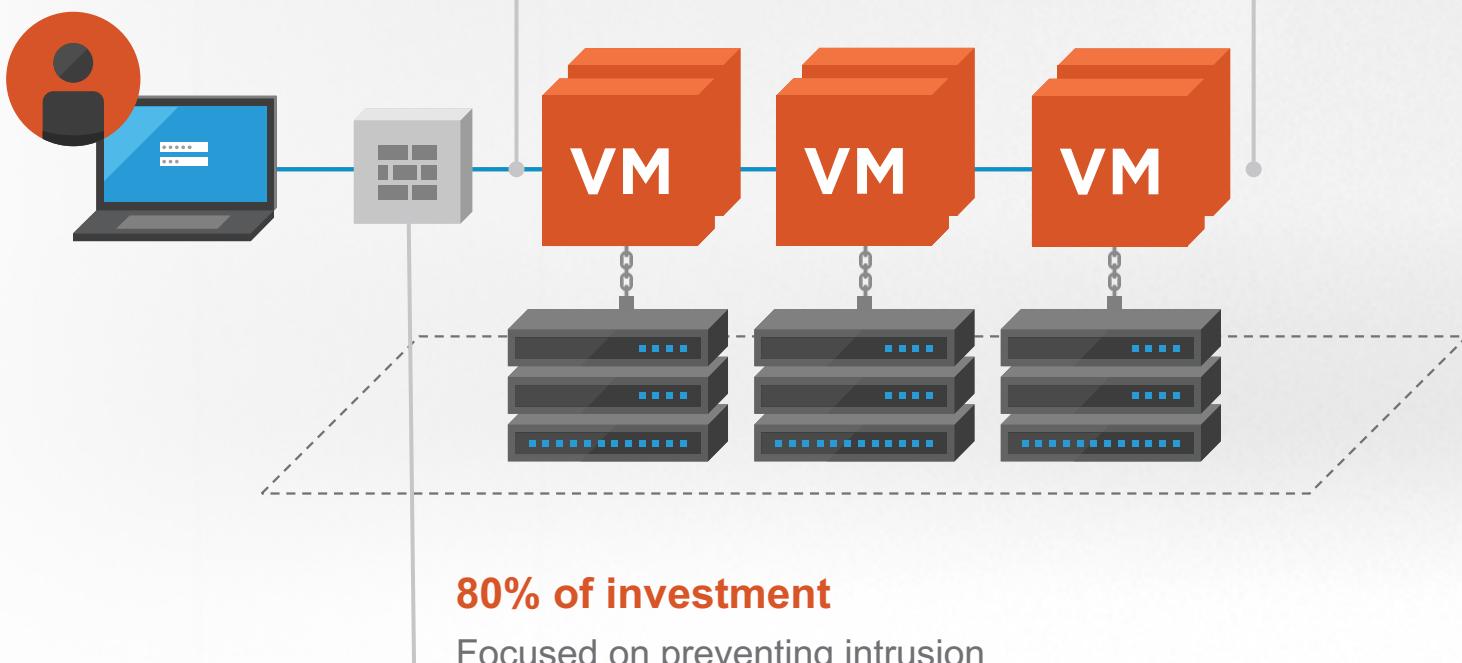
Our security realities

Unrestricted lateral spread:

Inability to secure the DC interior

20% of investment

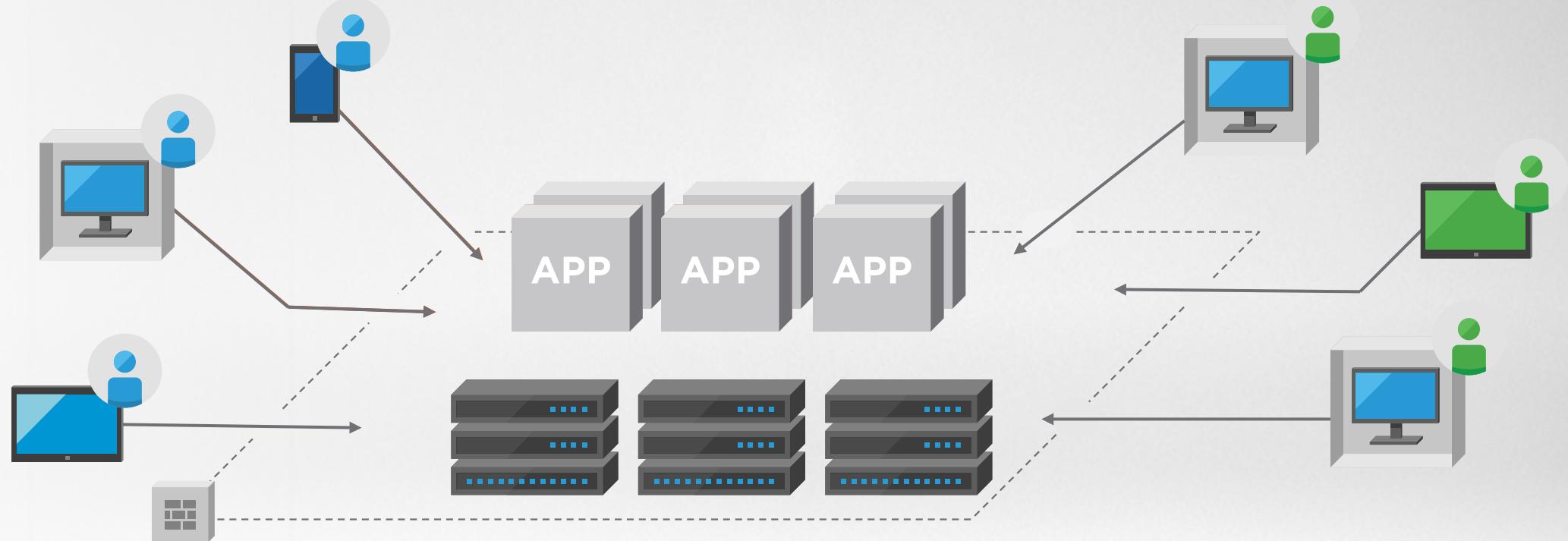
Focused on internal controls...
resulting in lack of visibility and control





Our security realities

Unchecked end user access creates significant risks inside the data center





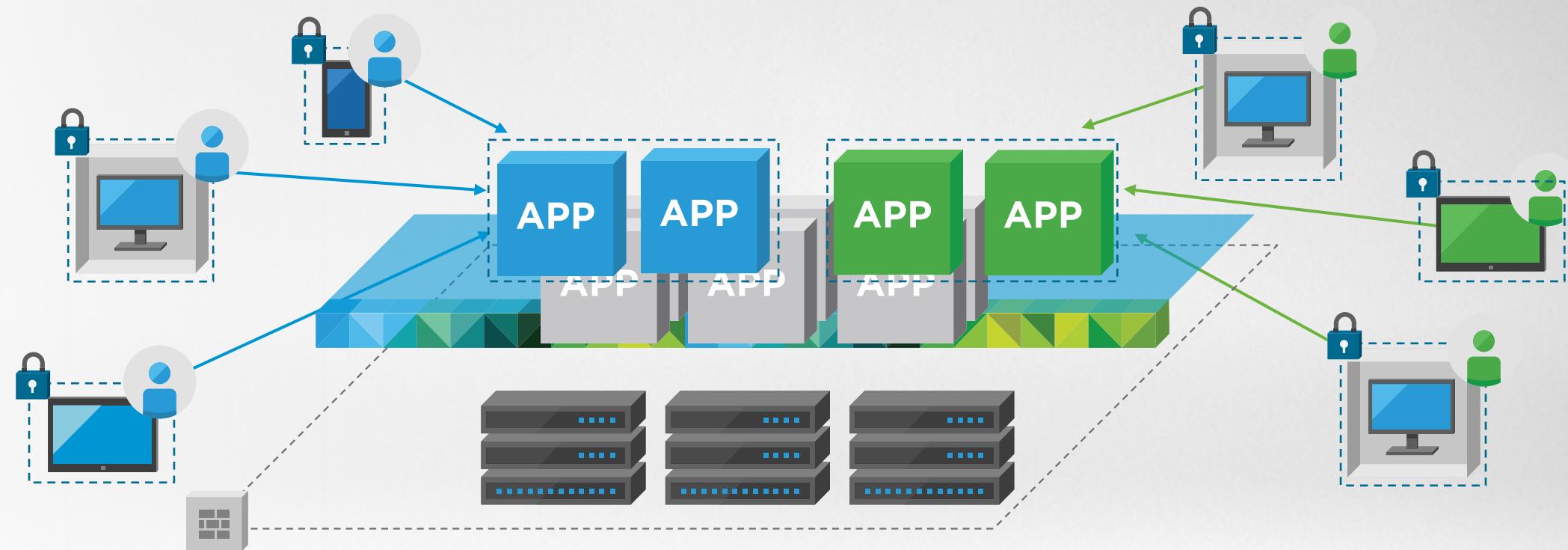
What if you could...

Provide granular end user security?

Who you are

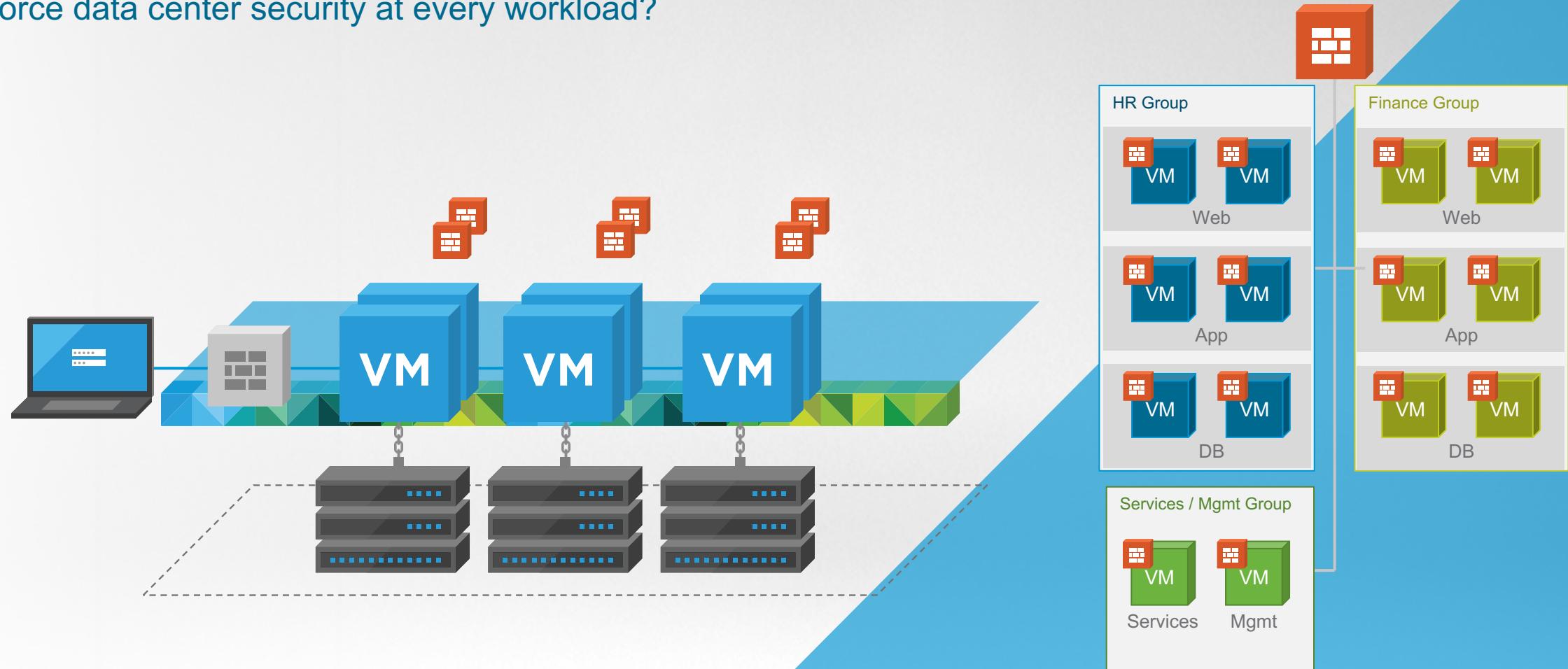
Where you are

What device
you're on



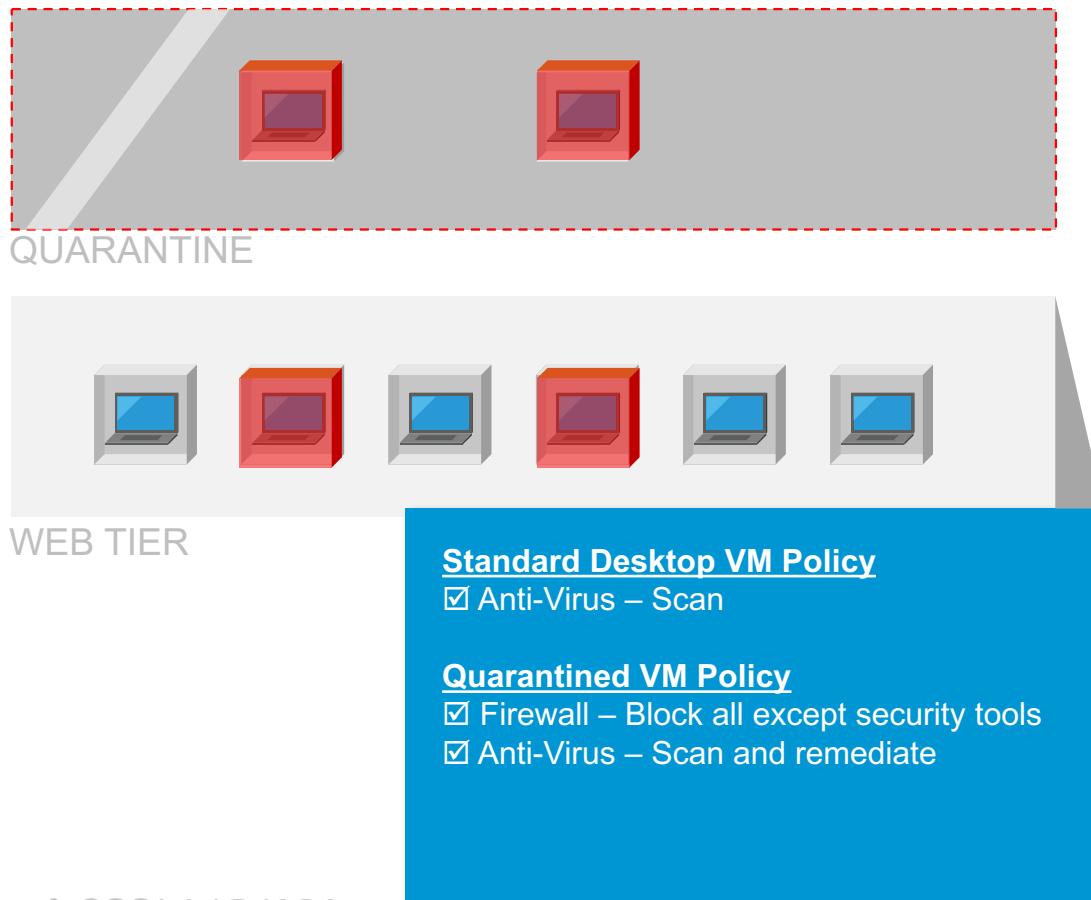
What if you could...

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

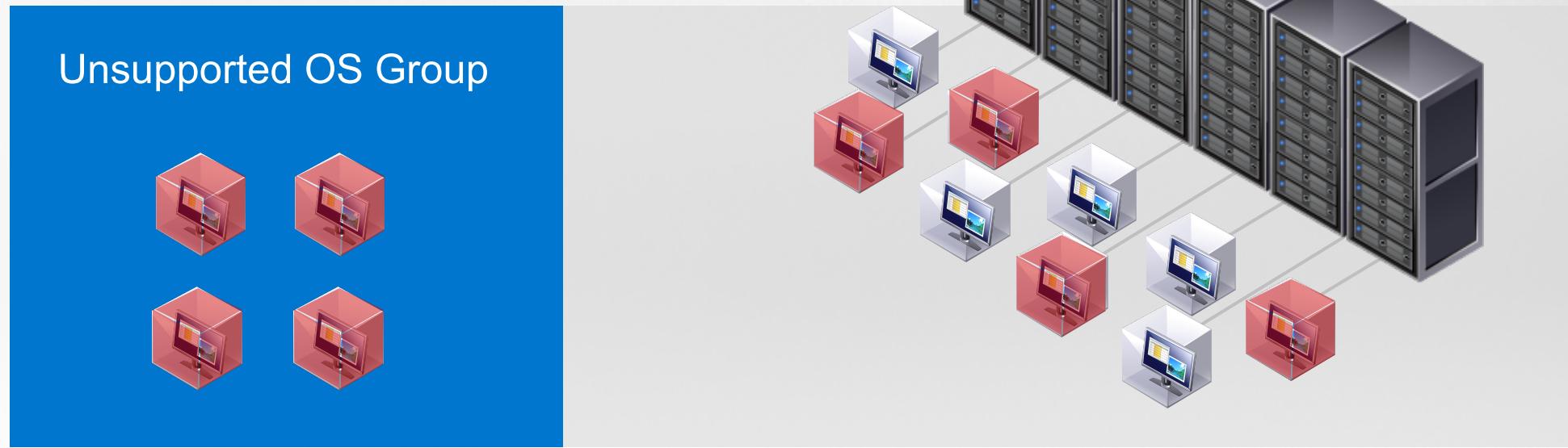
Share context between security controls so that one control can trigger a response from another dynamically.

Intelligent Grouping for Unsupported Operating Systems

Situation

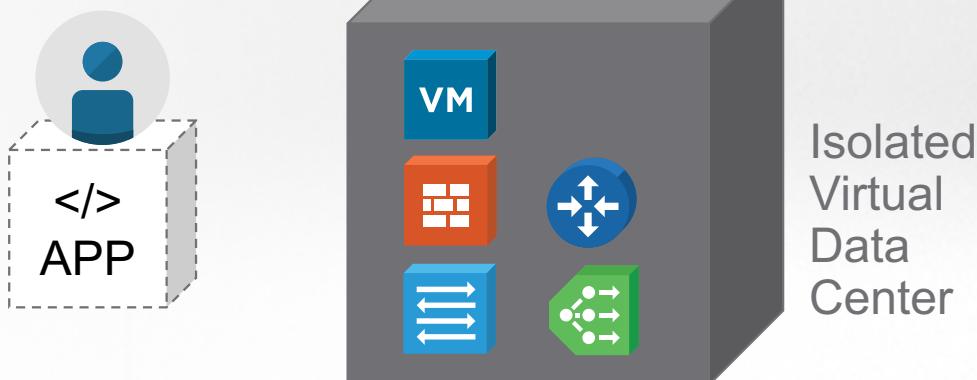
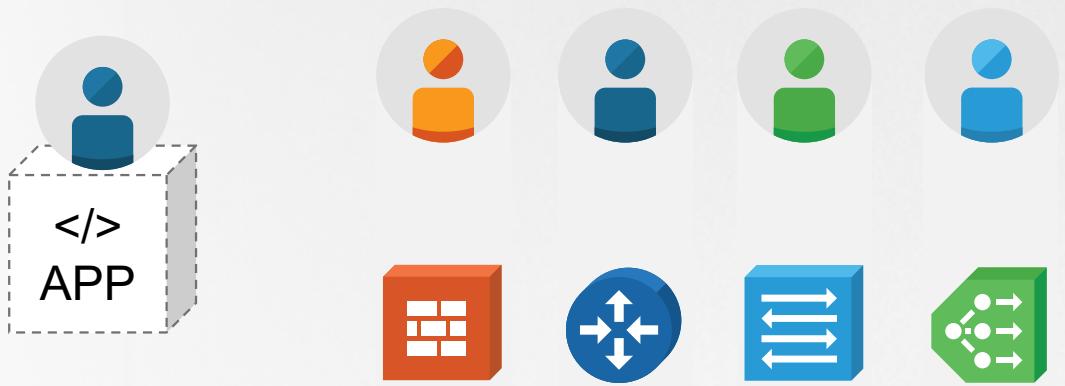
OS no longer supported on several systems

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

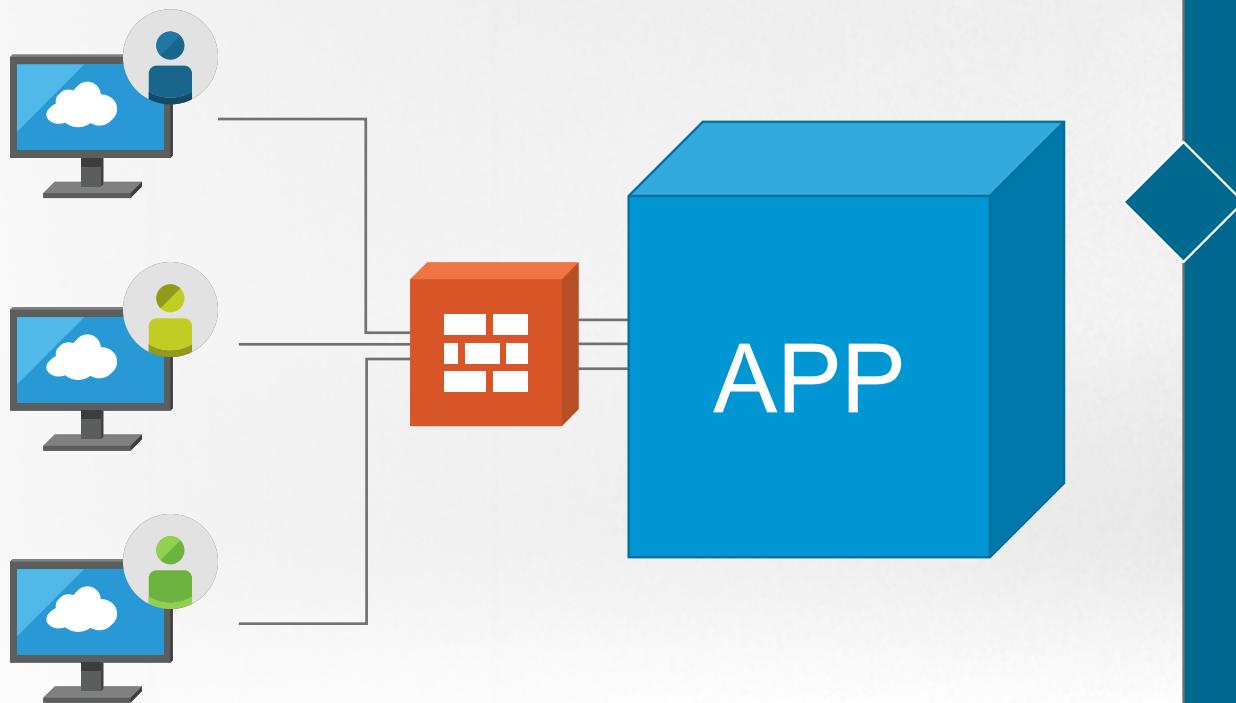
Ability to grant control of individual network constructs, including access to unlimited virtual routers, switches, firewalls, and load balancers without any additional hardware cost

Application Migration

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

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

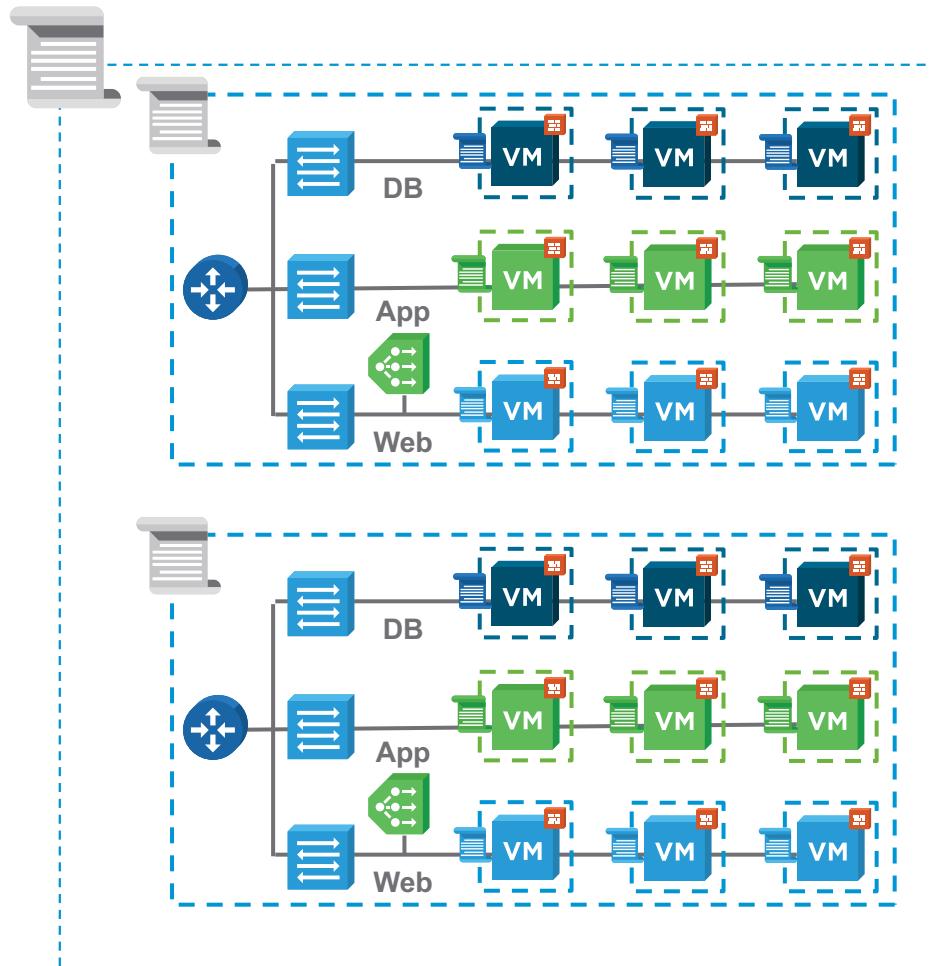
Access to Infrastructure

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

Collapsed DMZ



Increased east-west security

Distributed firewalling provides segmentation and isolation to satisfy compliance requirements

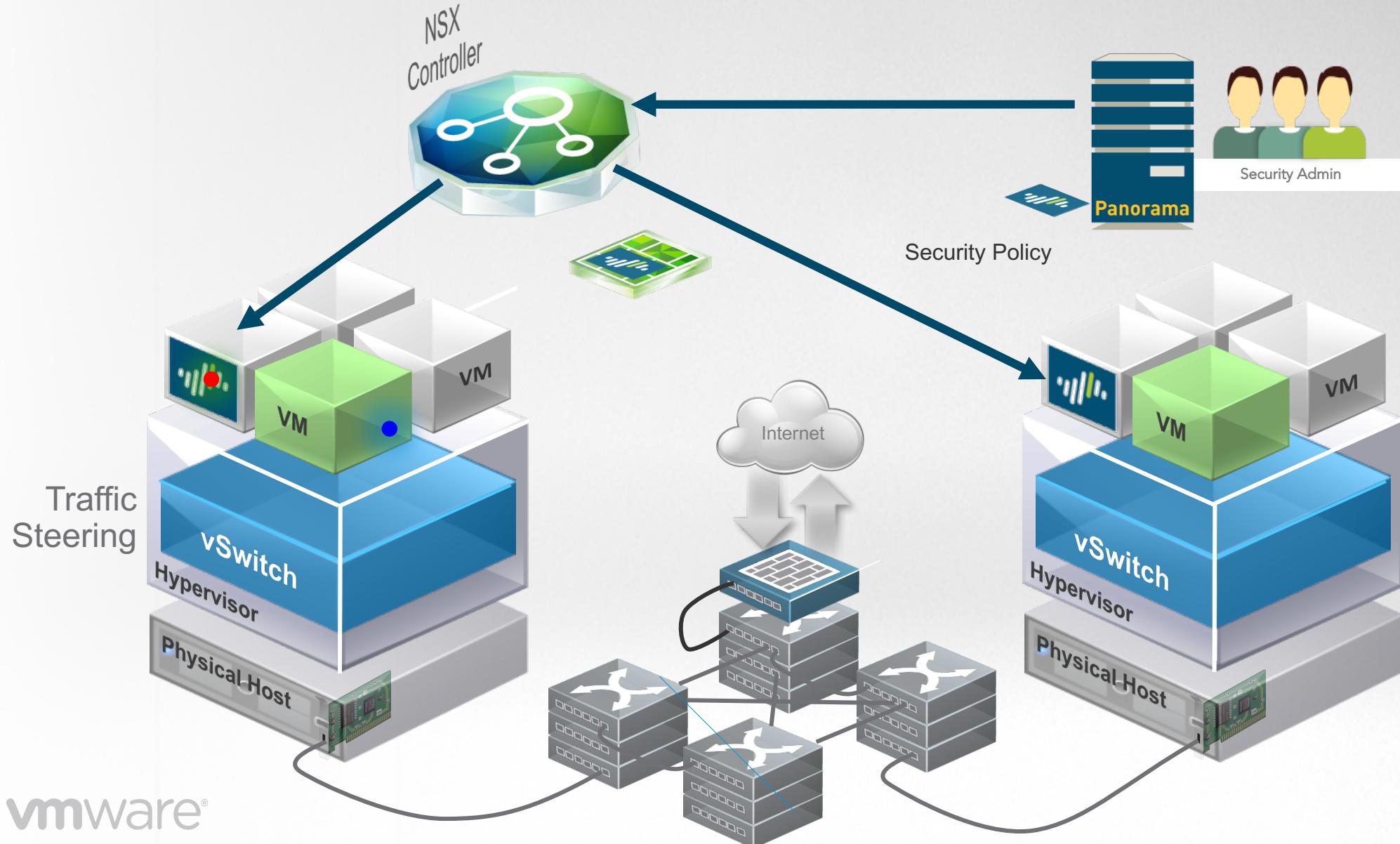
Lower cost - Fewer devices

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



NSX Partner Ecosystem





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

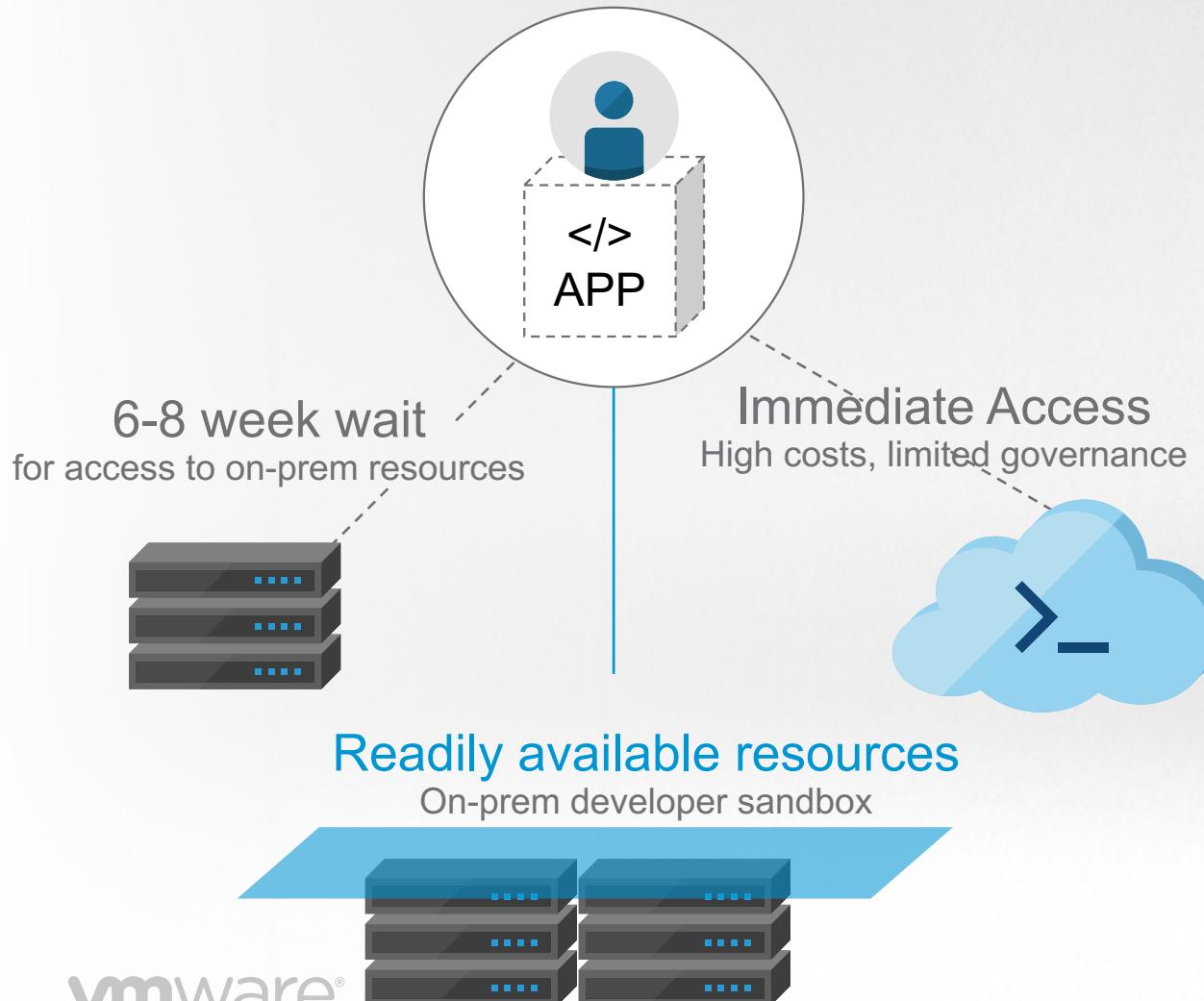
vRA or Openstack enabled network automation.

Configure Application Blueprints

Enable self-service catalog based on known application configurations

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

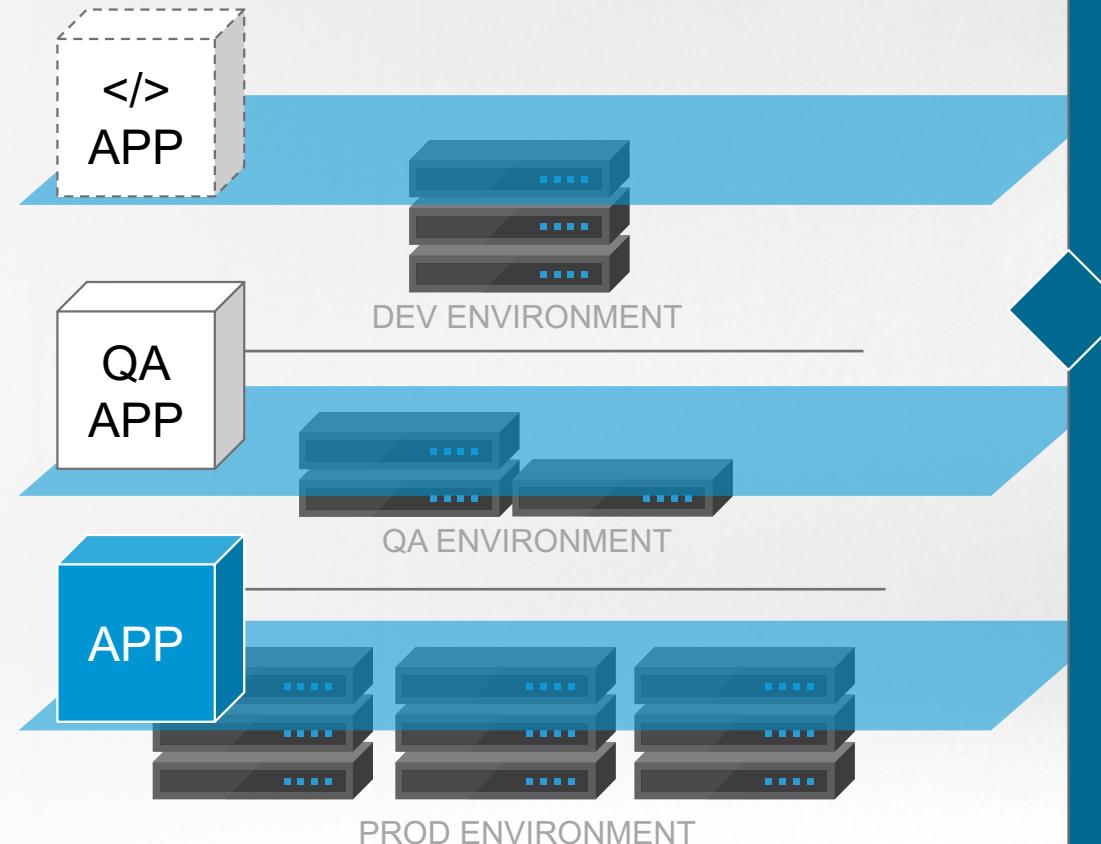
Automated provisioning of isolated application pods.
Initiation portal for requesting applications and services

Developer Sandboxes

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

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

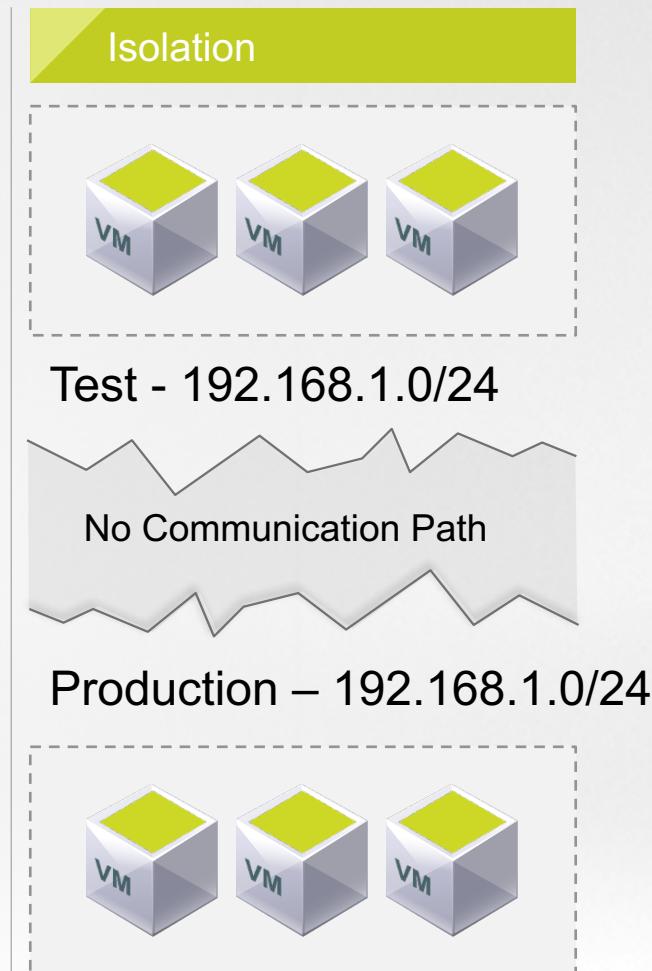
Identical Dev/Test/Prod

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

Snapshot Environments

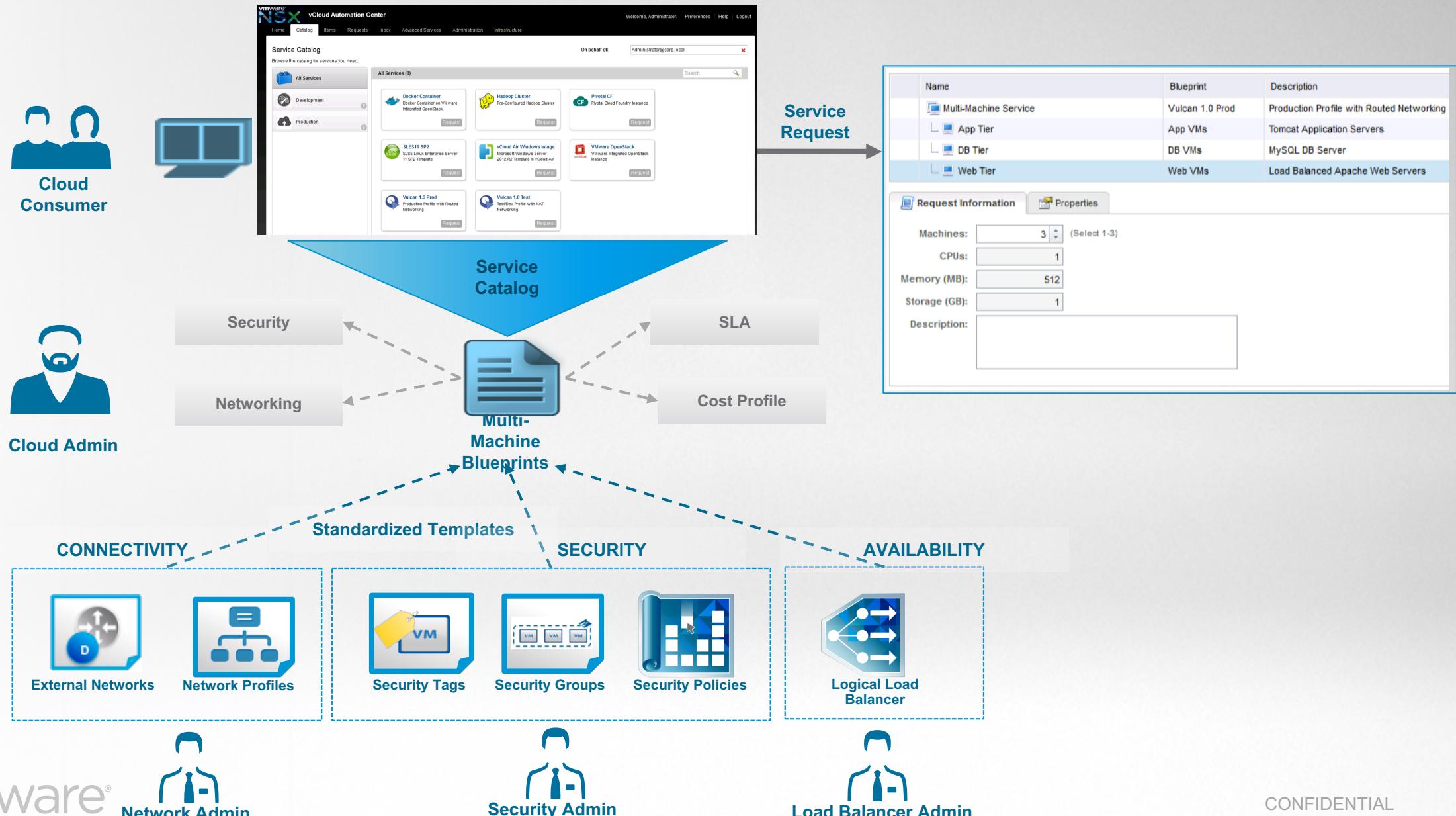
Enabling developers to roll back infrastructure configurations to a previous step in the lifecycle to debug applications

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



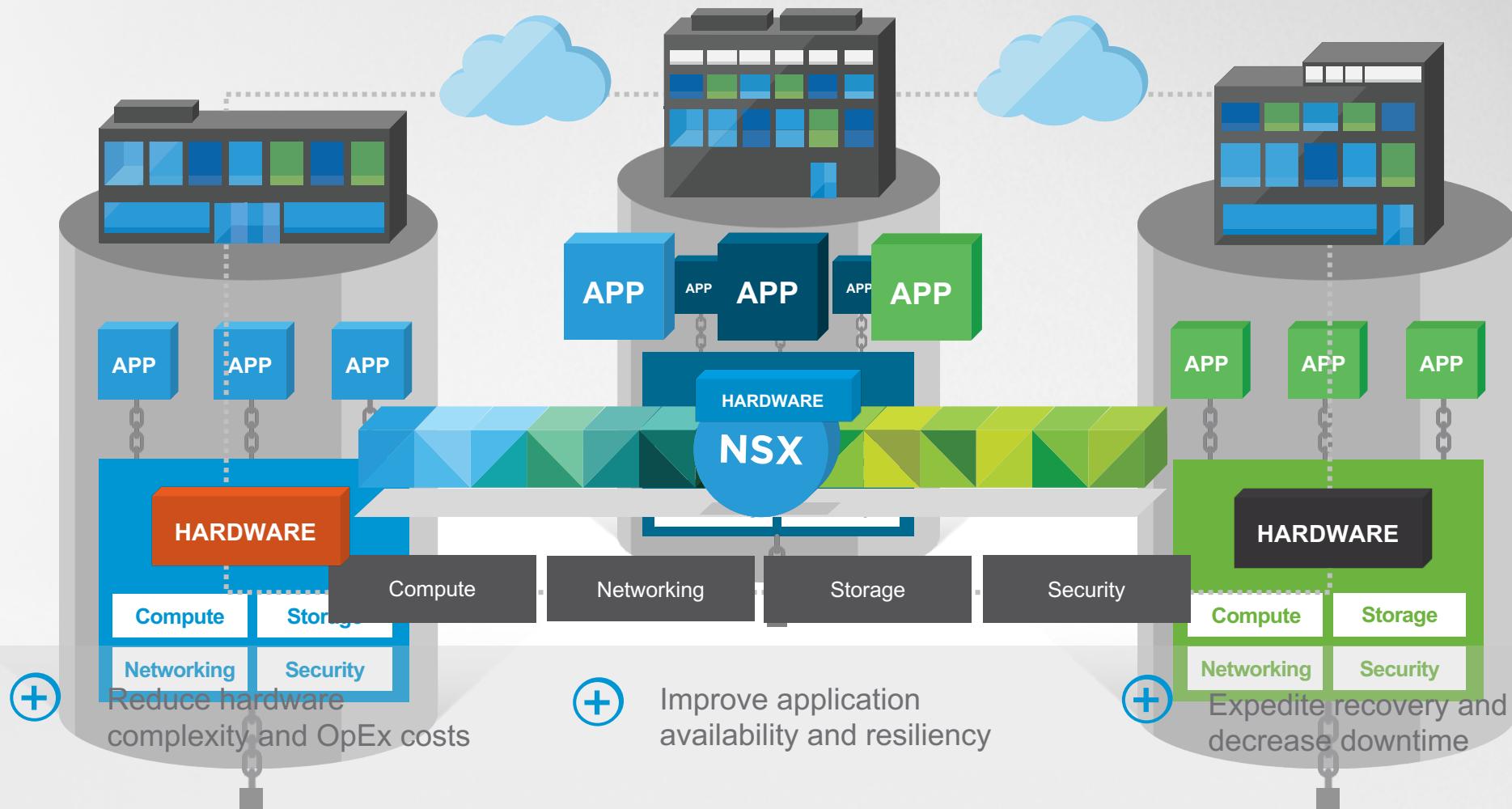


Application Continuity

Disaster Recovery

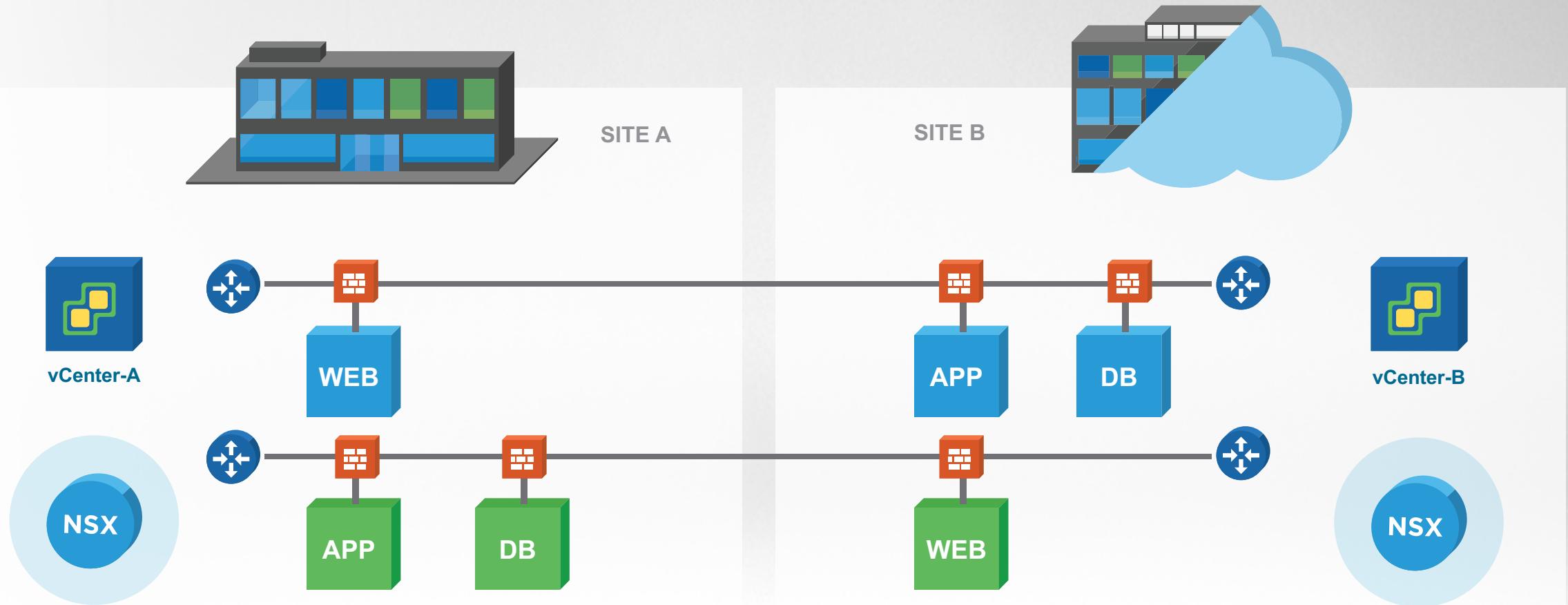


Enabling Data Centers Anywhere



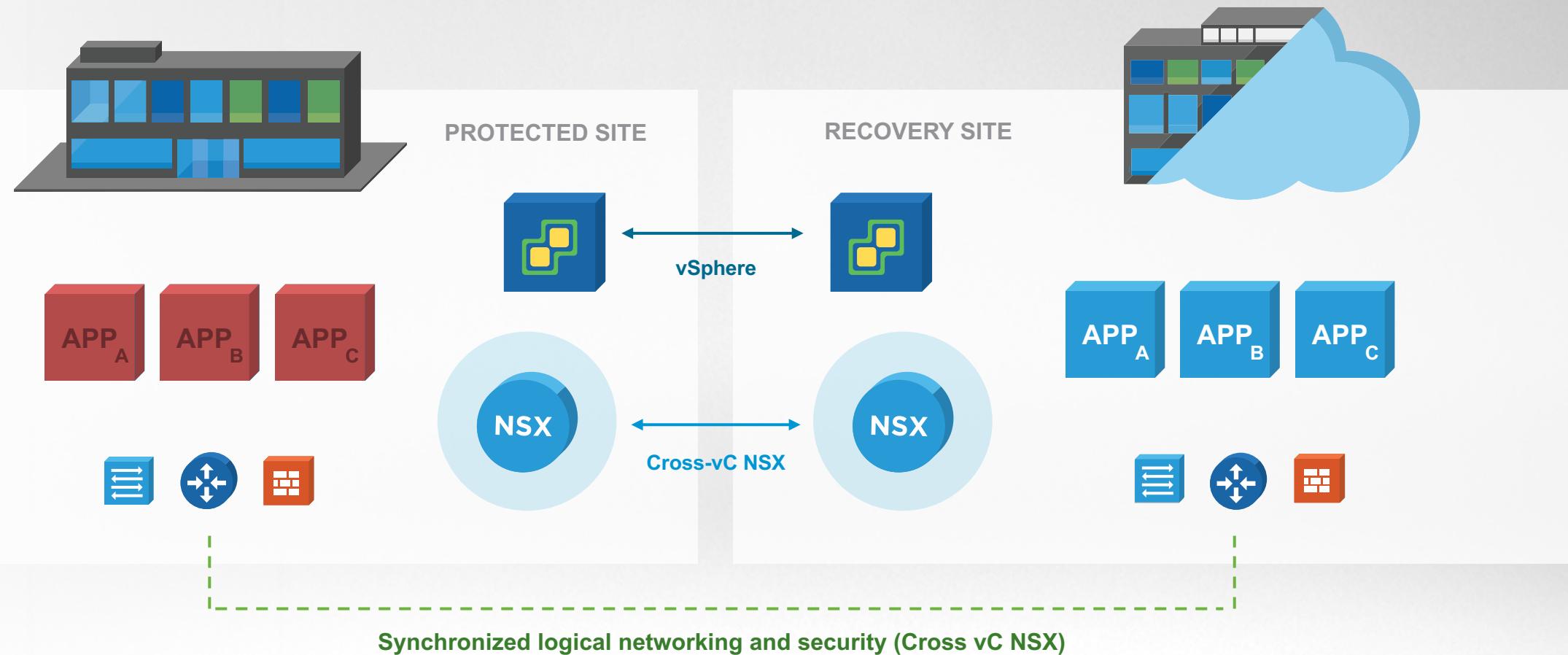
Application anywhere

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



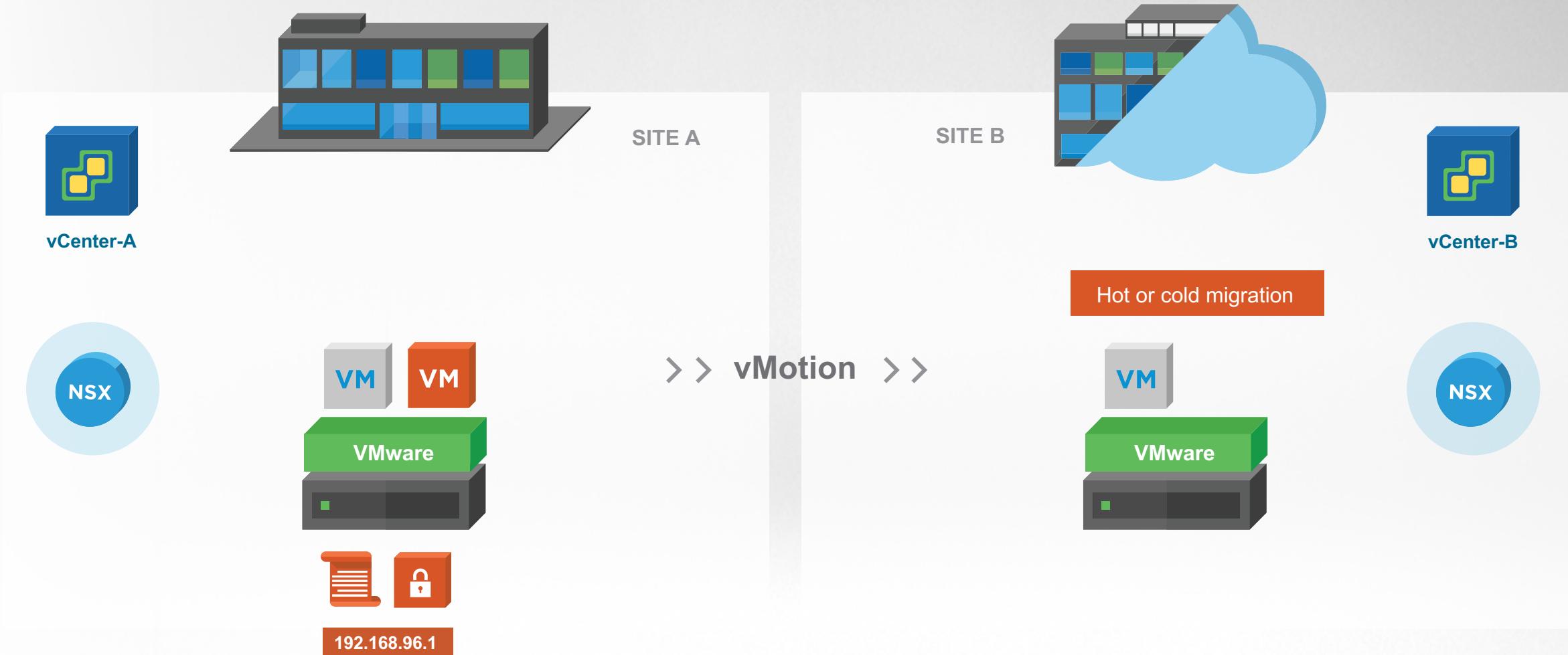
Disaster recovery

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

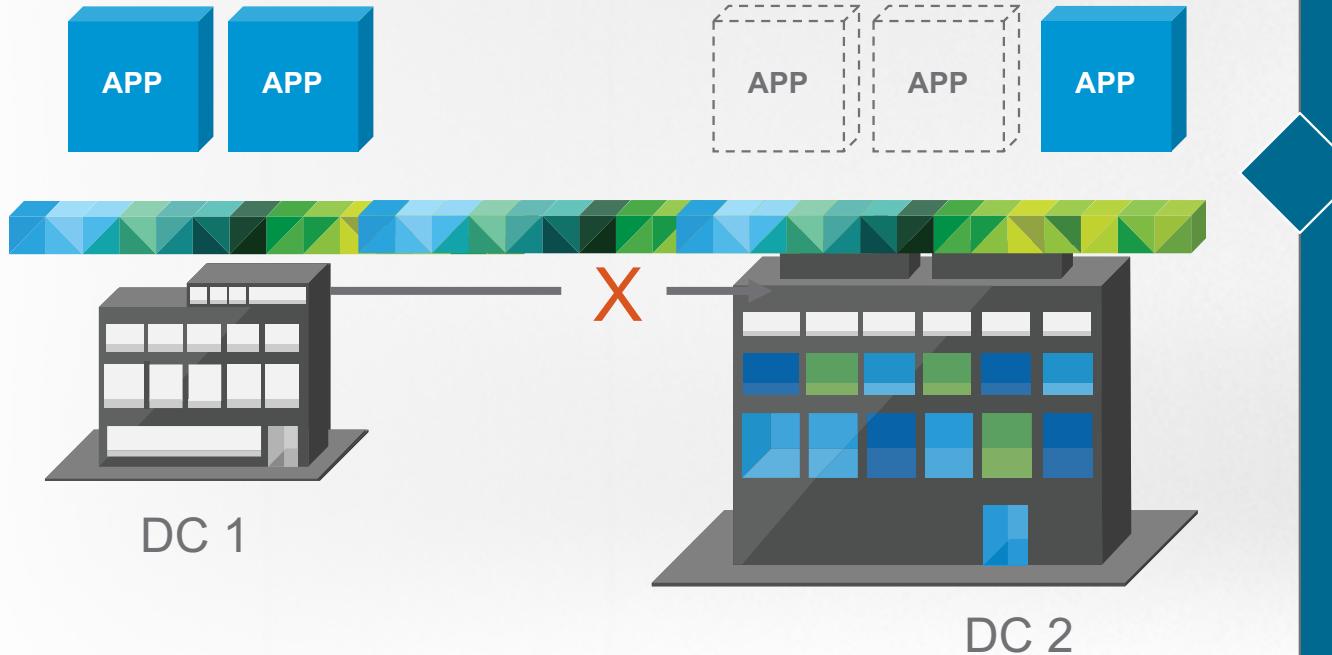


Workload mobility

Simplify how you move existing workloads across locations



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

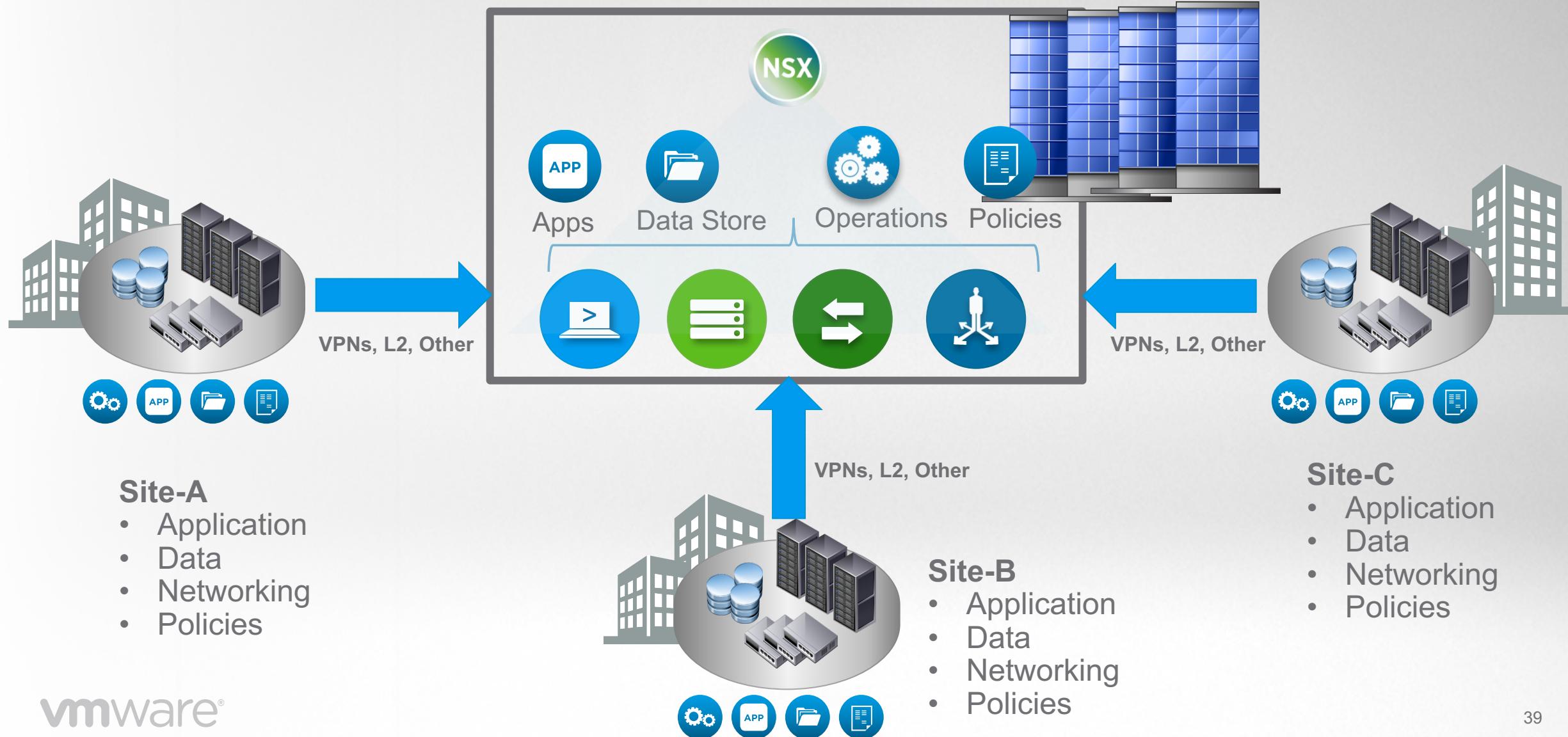
Non Disruptive Migration

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

DC Consolidation/Migration



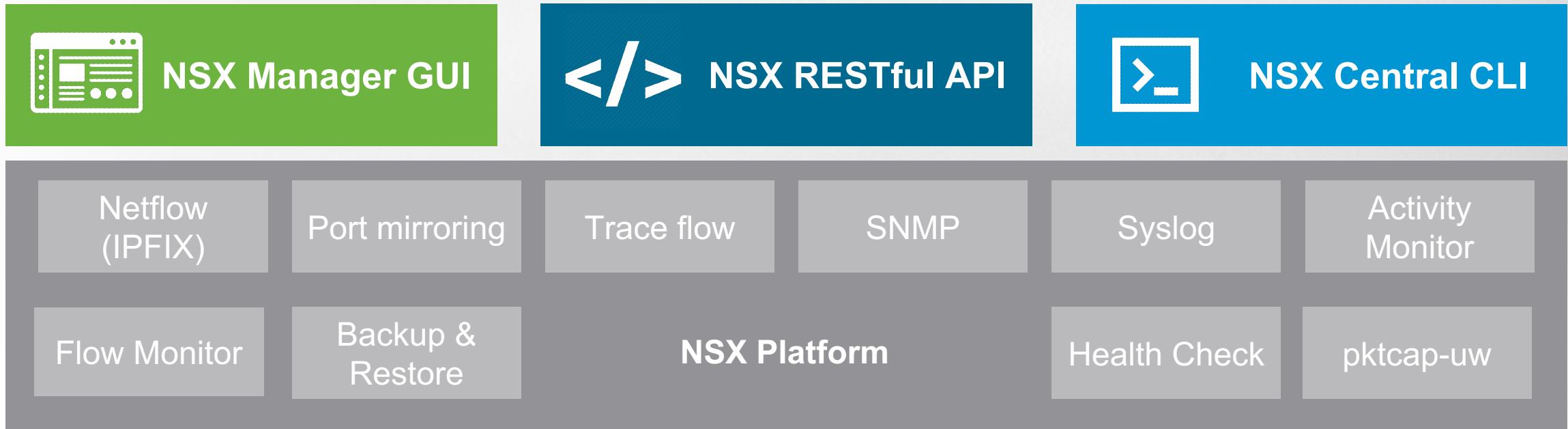


Operations

Managing & troubleshooting



NSX native operations capabilities



NSX Operation Tools – Traceflow

Traceflow

NSX Manager: 192.168.110.15 (Role: Primary)

Trace Parameters

Traffic Type: Unicast

Source: * web-01a - Network adapter 1 Change...
IP: 172.16.10.11, MAC: 00:50:56:ae:3e:3d

Destination: * db-01a - Network adapter 1 Change...
IP: 172.16.30.11, MAC: 00:50:56:ae:d4:2b

► Advanced Options

Trace

Trace Result: Traceflow delivered observation(s) reported

1 Delivered

Sequence	Observation Type	Host	Component Type	Component Name
0	Injected	esx-01a.corp.local	vNIC	vNIC
1	Received	esx-01a.corp.local	Firewall	Firewall
2	Forwarded	esx-01a.corp.local	Firewall	Firewall
3	Forwarded	esx-01a.corp.local	Logical Switch	Web-Tier-01
4	Received	esx-01a.corp.local	Logical Router	Local-Distributed-Router
5	Forwarded	esx-01a.corp.local	Logical Router	Local-Distributed-Router
6	Received	esx-01a.corp.local	Logical Switch	DB-Tier-01
7	Forwarded	esx-01a.corp.local	Physical	esx-01a.corp.local
8	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
8	Received	esx-02a.corp.local	Physical	esx-02a.corp.local
9	Received	esx-02a.corp.local	Firewall	Firewall
10	Forwarded	esx-02a.corp.local	Firewall	Firewall
11	Delivered	esx-02a.corp.local	vNIC	vNIC

NSX Operation Tools – Flow Monitoring

vmware vSphere Web Client Updated at 8:04 PM | root@localhost | Help ▾

Home ▶ Networking & Security ▶ Flow Monitoring

Monitor NSX Manager: 192.168.110.42 ▾ Time Interval: Last 15 minutes Change
Updated at 08:05 PM Auto refresh every minute

Flows Allowed: 91.55% Blocked By Rule: 8.45% Blocked By Spoofguard: 0.00%

Top Flows Top Destinations Top Sources

Service Protocol:port	Bytes	Packets	Sessions
Tomcat	4940302	9027	331
HTTPS	2252370	5964	206
MySQL	1485512	9140	648
HTTP	1363325	650	9
ARP	1794	39	39

Byte

Time

Legend:

- Tomcat (Orange circle)
- HTTPS (Green circle)
- MySQL (Blue diamond)
- HTTP (Yellow triangle)
- ARP (Grey square)

HTTP Sunday, August 18, 2013 7:50:33 PM 1363325

MySQL Sunday, August 18, 2013 7:50:33 PM 1485512

NSX Operation Tools – Live Flows

Flow Monitoring

Dashboard Details By Service **Live Flow** Configuration

NSX Manager: 192.168.110.42 ▾

Live Flow will be shown for the selected vNIC. Please select a vNIC and press start to see the live flows

vNIC:  web-sv-01a - Network adapter 1 [Browse](#) [Start](#) [Stop](#)

Refresh Rate: 5 Seconds ▾

■ New active flows ■ Flows with state change ■ Terminated 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°
Visibility & Analytics



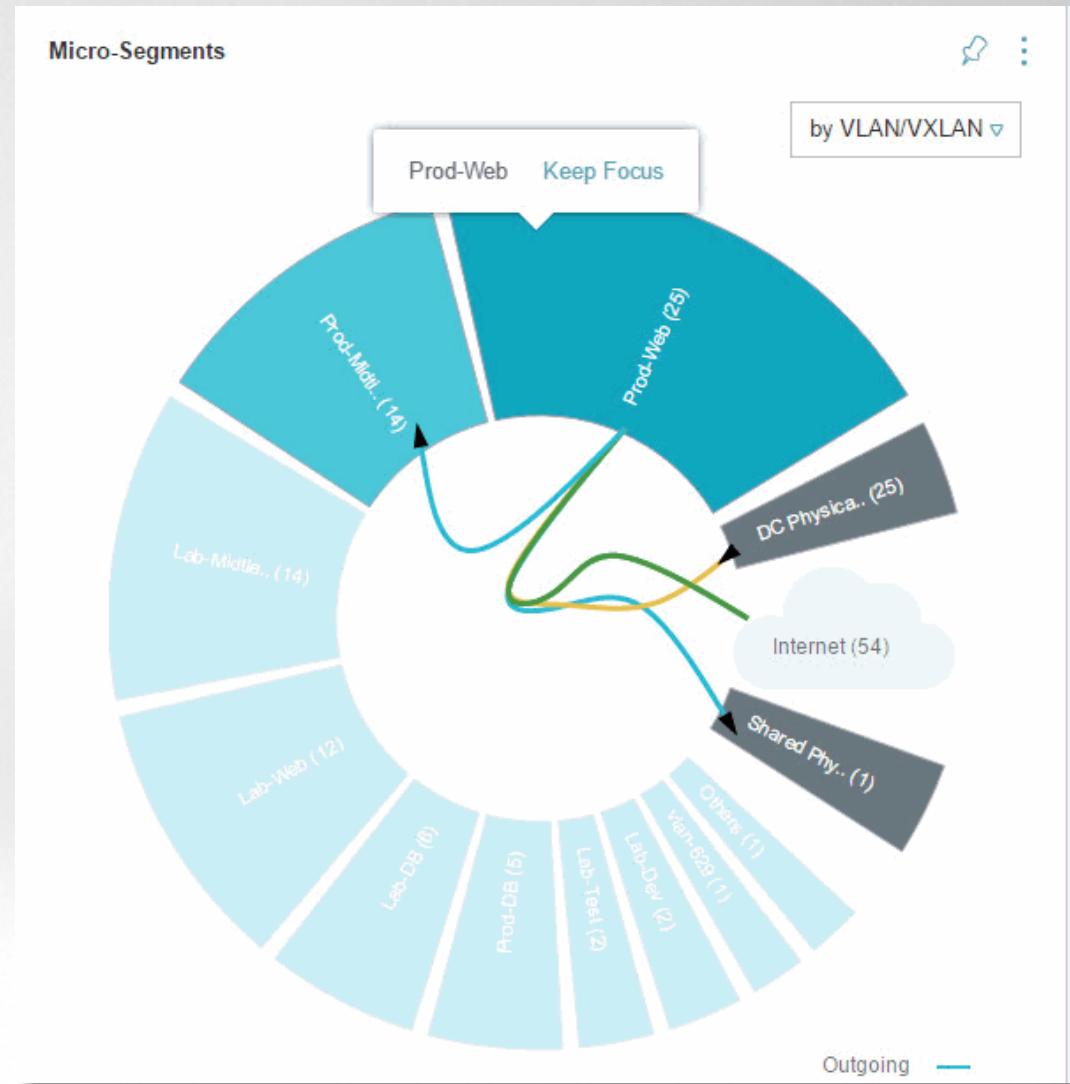
Ensure Best Practices,
Health and Availability of
NSX Deployment

Across Virtual, Physical and Cloud



Security Policy Automation – Micro-Segmentation

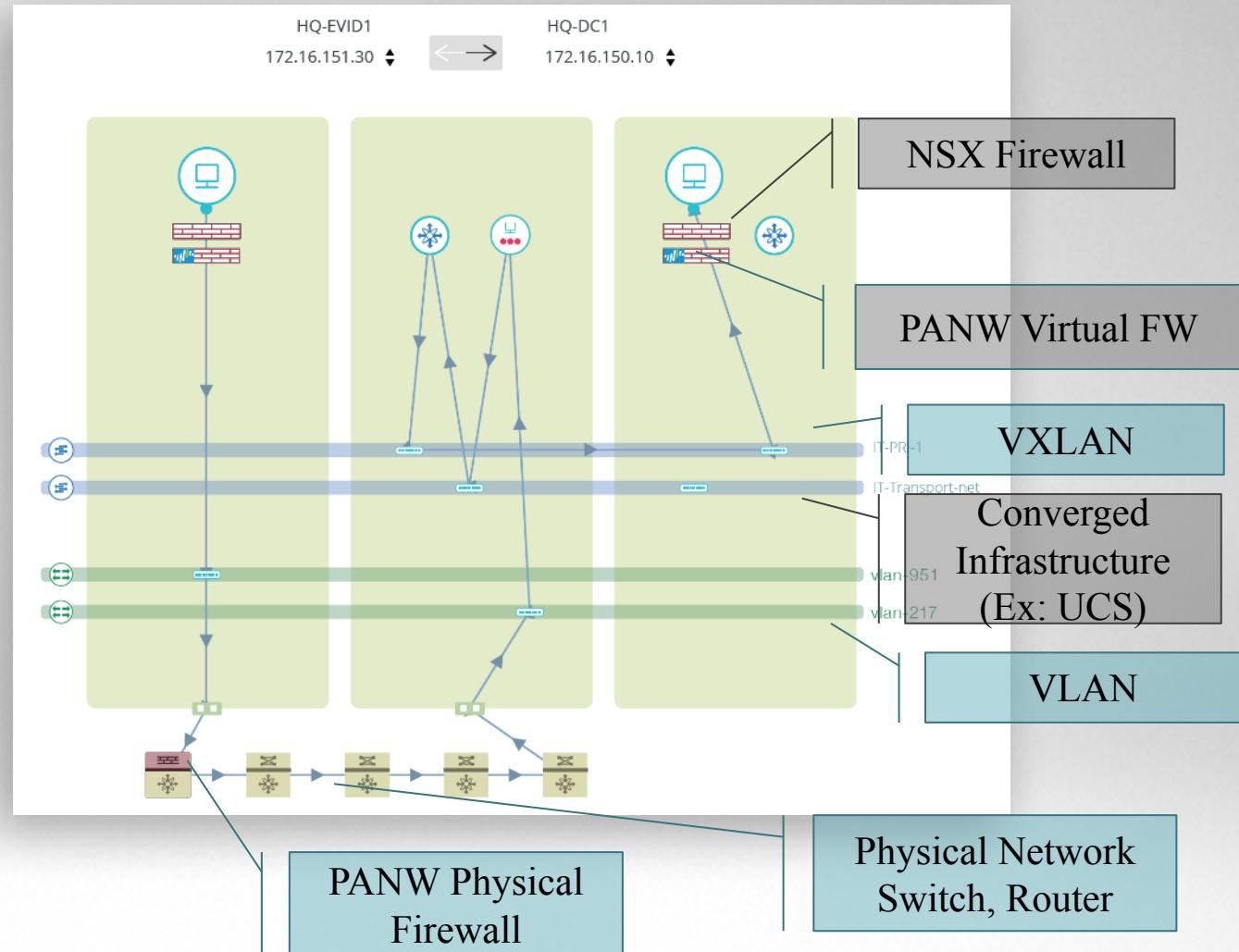
- Discover vCenter and NSX constructs (folders, clusters, vlans, security tags)
- Automated Security Groupings Based on vCenter and NSX Constructs, Workload Characteristics, Ports, Common Services
- Recommended Security Policies / Firewall Rules (Zero-Trust Model)
- See Network Traffic Per Host, Per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



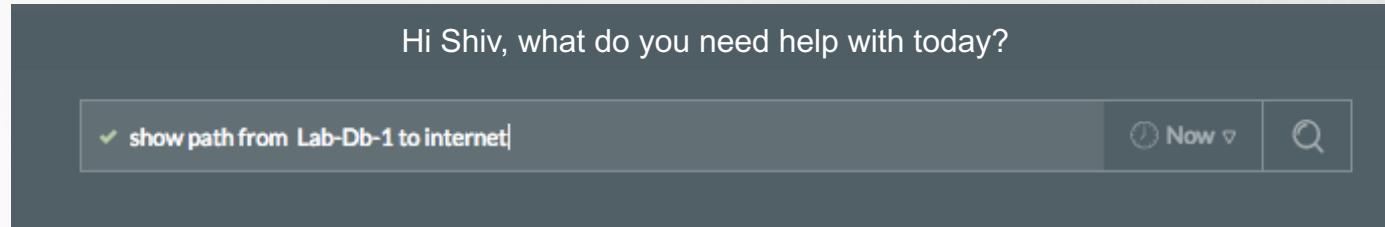
Data Paths Across Overlay And Underlay

Connectivity Graphs

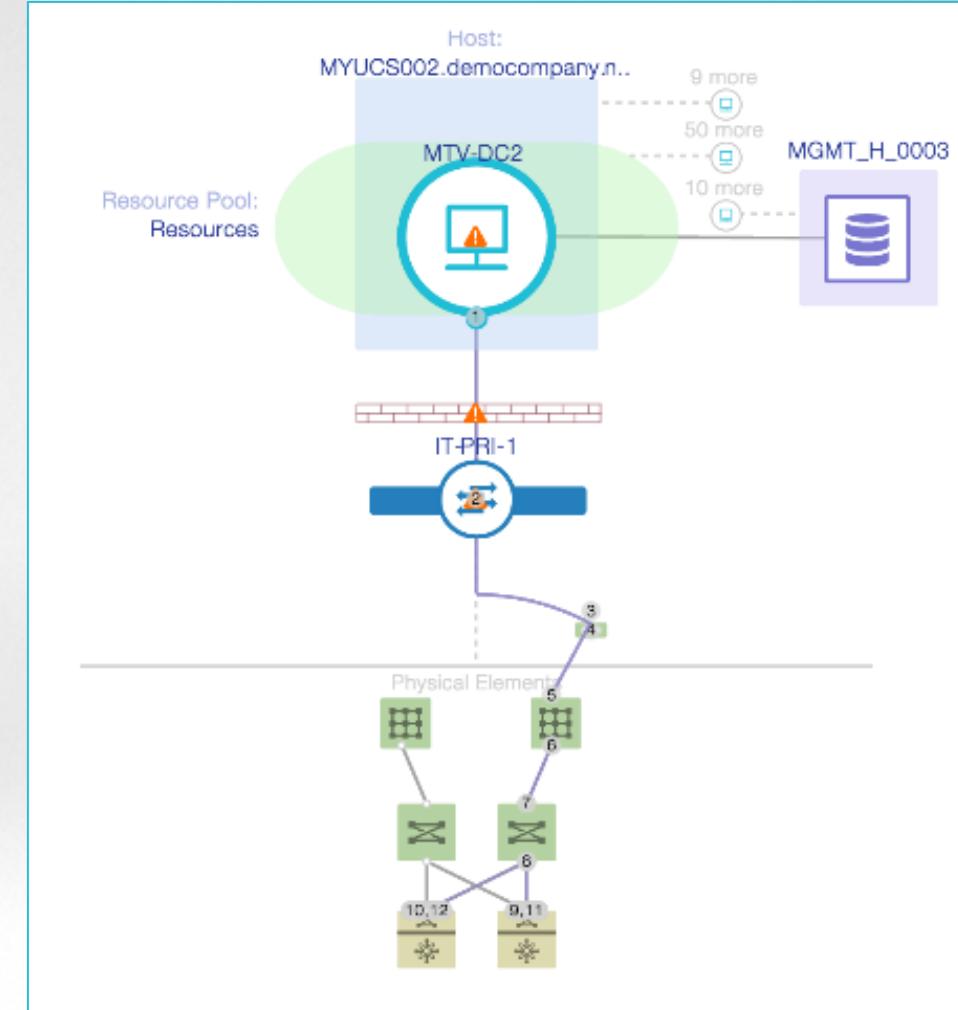
- VM to VM, VM to Physical, VM to Internet
- Hop-by-Hop Path across Overlay (LDRs, Edge Gateways) and Underlay (Physical VDCs & VRFs). See V-To-P Boundary
- Correlated Problems And Performance Metrics Across Virtual and Physical
- See Effective Firewall Rules and Security Policies across NSX and PANW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



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



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

Checklist Rules - Failed

Filters

Search Properties or Metrics

All

Event Type

All

Host network control plane connection failure (1)

Host network control plane mismatch (1)

Host network control plane out of sync (1)

Module network connection failure (1)

Module not loaded (1)

Search Values

NSX Edge in Critical Condition (1)

NSX Edge VM Heartbeat Failure (1)

VTEP Subnet Mismatch (1)

NSX Manager to Edge VM Communication Failure (1)

NSX Edge in Critical Condition (1)

VTEP Subnet Mismatch Cluster: Pod2-cave1 (with NSX Manager: 10.16.128.170) (1)

9 entities

Host network control plane mismatch
Multiple controllers detected for VXLAN: Test-VXLAN-8 (NSX Manager: 10.16.128.170)
40 days

Module network connection failure
Module: vsfwd on Host: ddc1-pod2esx044.dm демокомпания.net under NSX: 10.16.128.170 VC: vc01 на корпоративной
40 days

Module not loaded
Module: netcpa-worker on Host: ddc1-pod2esx035.dm демокомпания.net under NSX: 10.16.128.170 VC: vc01 на корпоративной
40 days

Host network control plane connection failure
The connection between Host: ddc1-pod2esx044.dm демокомпания.net under NSX: 10.16.128.170 VC: vc01 на корпоративной
40 days

Host network control plane out of sync
Host: ddc1-pod2esx035.dm демокомпания.net under NSX: 10.16.128.170 VC: vc01 на корпоративной
40 days

NSX Edge VM Heartbeat Failure
NSX Edge VM Heartbeat Failure for VMware
40 days

NSX Manager to Edge VM Communication Failure
NSX Manager to Edge VM Communication Failure
40 days

NSX Edge in Critical Condition
NSX Edge in Critical Condition for VMware
40 days

VTEP Subnet Mismatch
Cluster: Pod2-cave1 (with NSX Manager: 10.16.128.170)
40 days

Topology

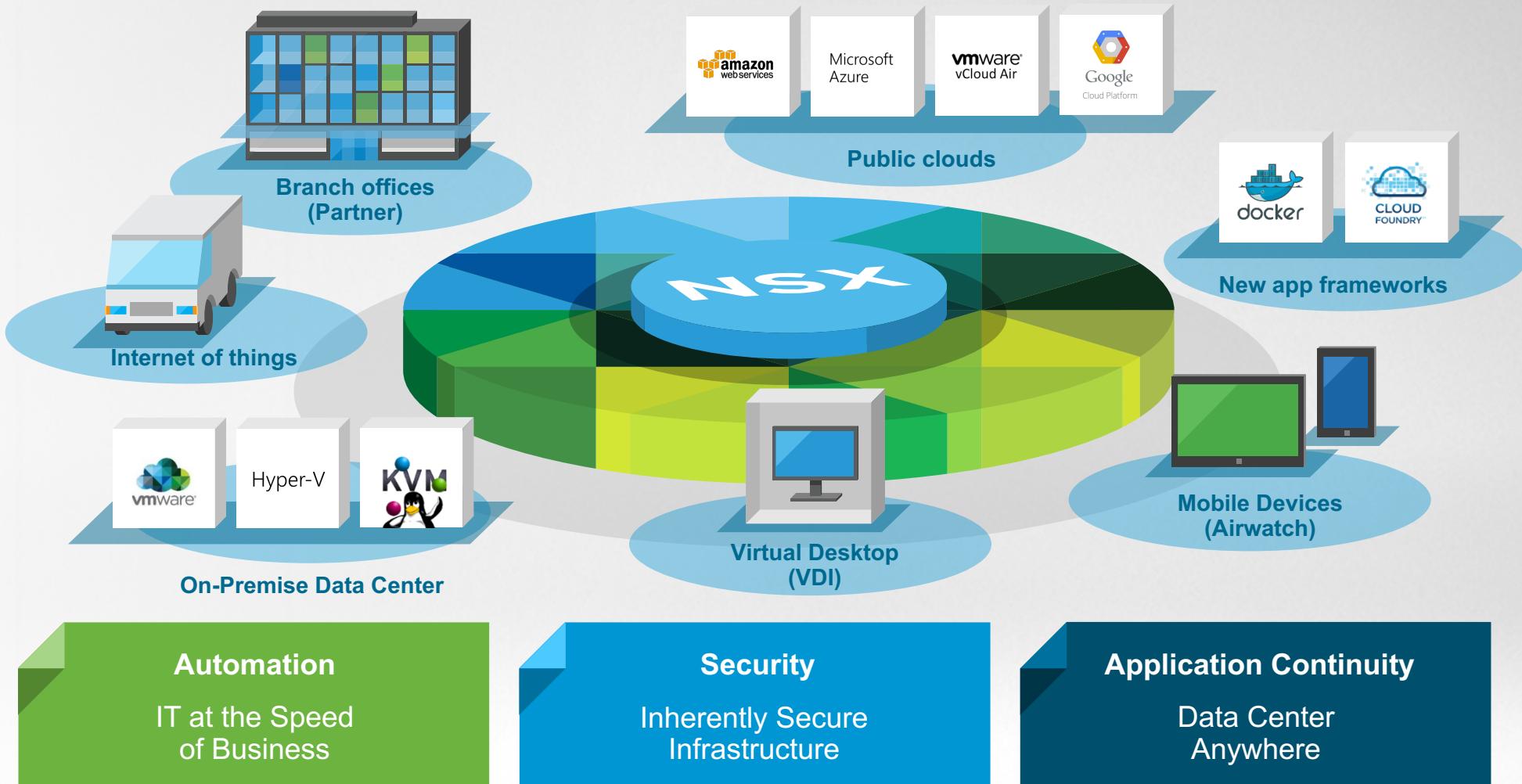
The diagram illustrates the NSX infrastructure topology. At the top left is a 'VCenter' icon. A dashed line connects it to an 'NSX Manager' icon. From the 'NSX Manager', three solid lines descend to three separate 'Edge' icons, each represented by a green square with a network symbol. A dashed line connects the 'NSX Manager' to a 'NSX Services' block on the right. The 'NSX Services' block contains a '1 Firewall' icon, '5 LDRs' icon, '46 VxLANS' icon, and '4 Edge VMs' icon. Below the 'Edge' icons, a dashed line connects them to a 'Clusters' block, which in turn connects to a 'Hosts' block. The 'Clusters' block contains '6 Clusters' and the 'Hosts' block contains '39 Hosts'. Each cluster and host icon has a red exclamation mark indicating a critical issue.



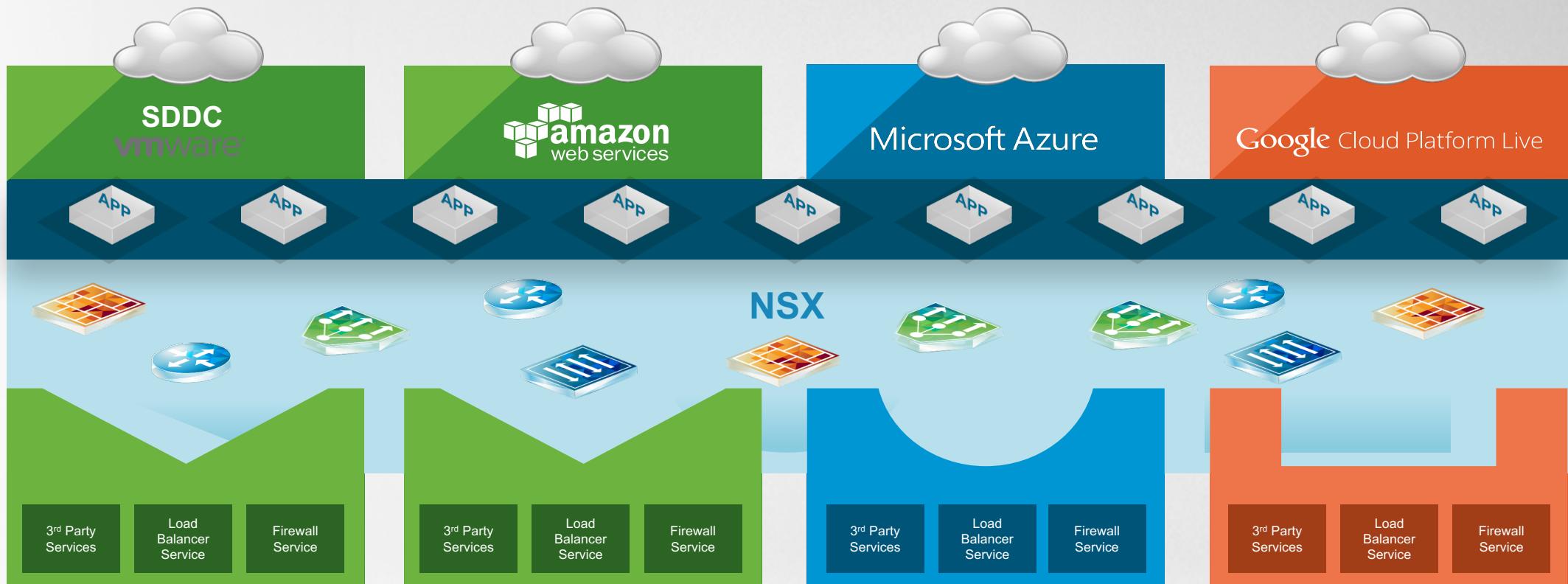
Next Generation

Clouds & Containers

NSX Vision: Driving NSX Everywhere



VMware Cross-Cloud Services



NSX with Containers & CNA

Container Management (CaaS)



Platform as a Service (PaaS)



Pivotal Cloud Foundry®



OPENSIFT
ENTERPRISE
by Red Hat®



IBM Bluemix

NSX Container Networking & Security

Private Cloud



Public Cloud



Google Cloud Platform



Windows Azure



Thank You!