STAR TREK BEYOND

Let your Business Live Long and Prosper

NSX Network Virtualization Platform

Jeff Nydegger

Sr. Systems Engineer
Networking and Security

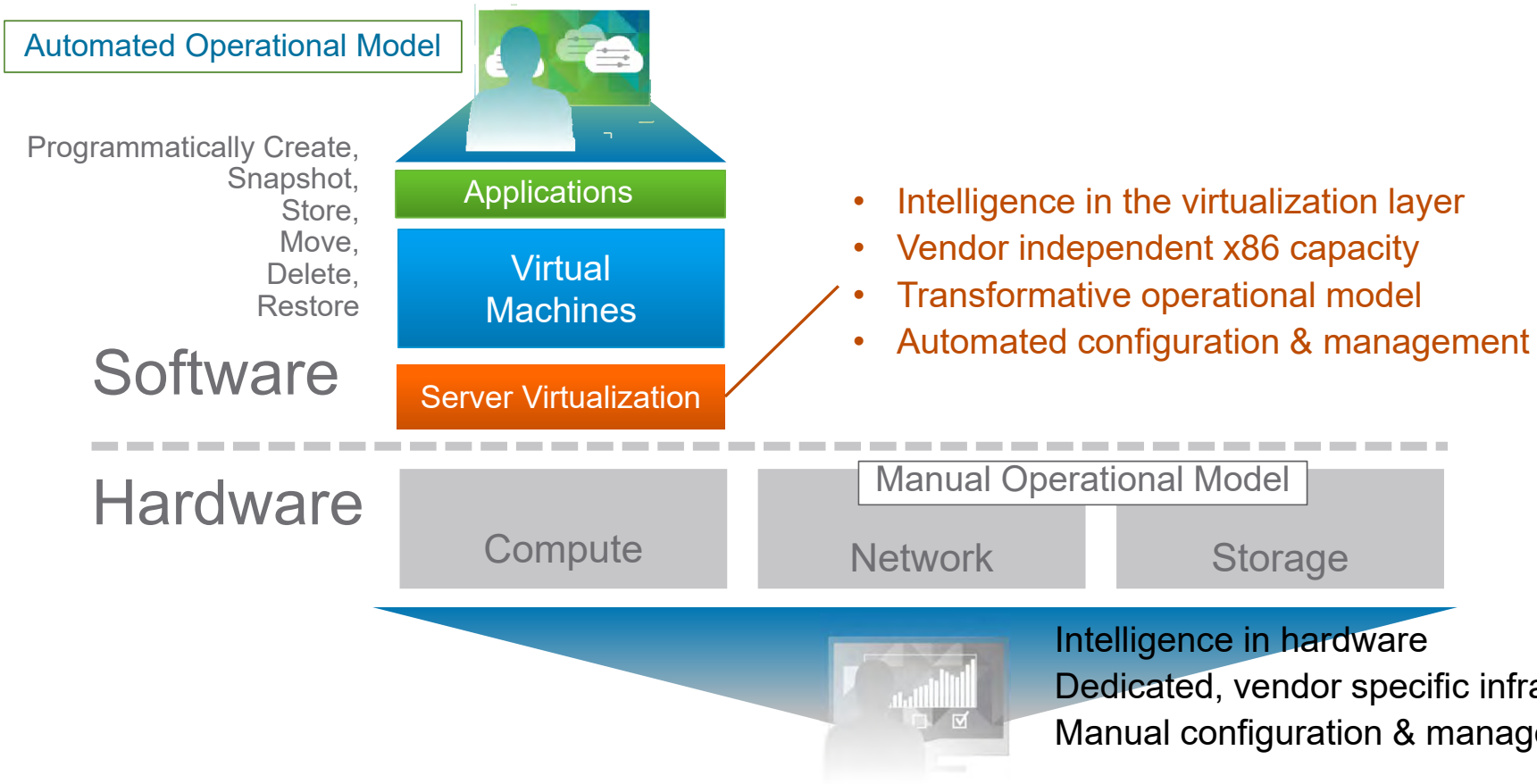
vmware

möbius PARTNERS

© 2016 VMware Inc. All rights reserved.

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

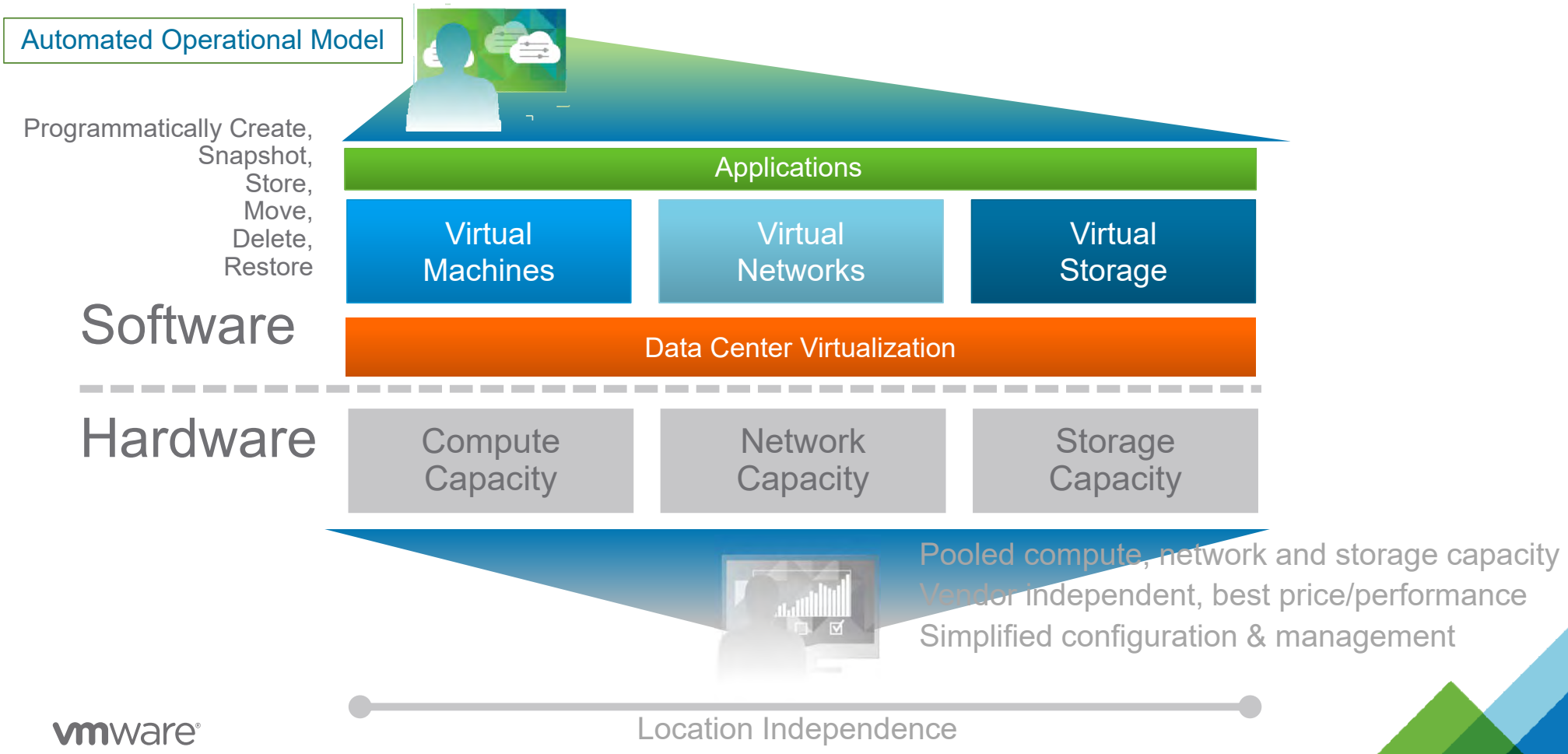
Taking what we have learned….



vmware

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

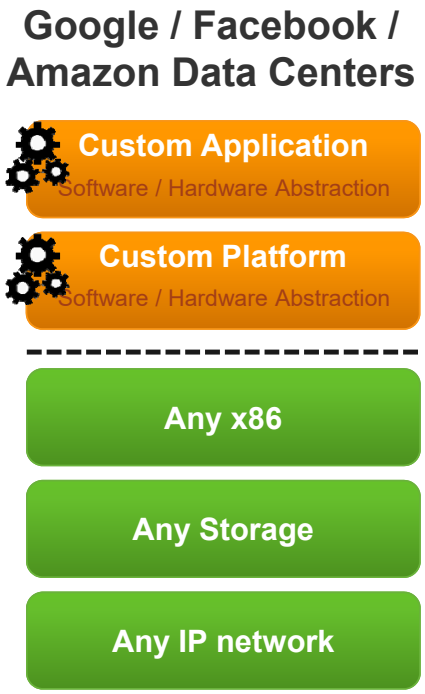
To deliver a Software Defined Data Center approach



vmware

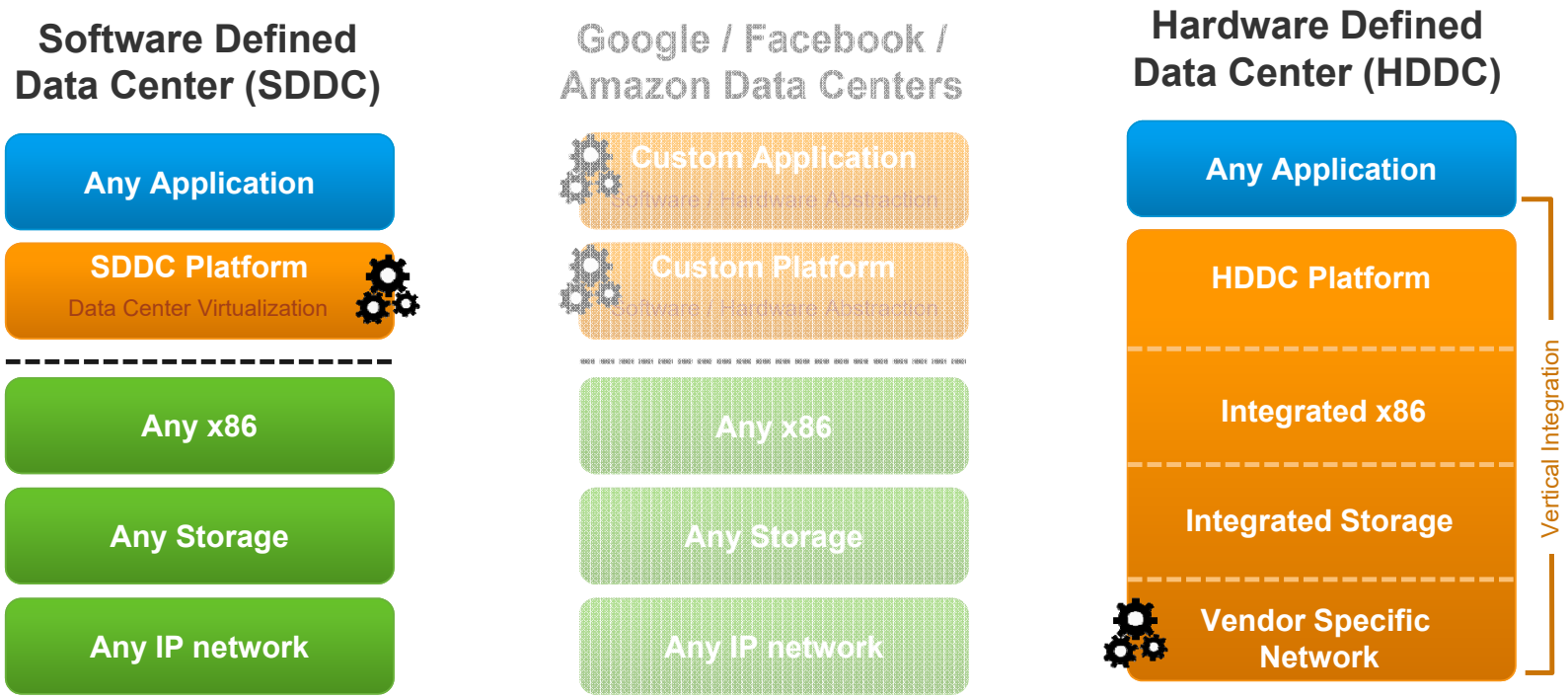
Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

The anatomy of the most agile & efficient data centers is SDDC



vmware

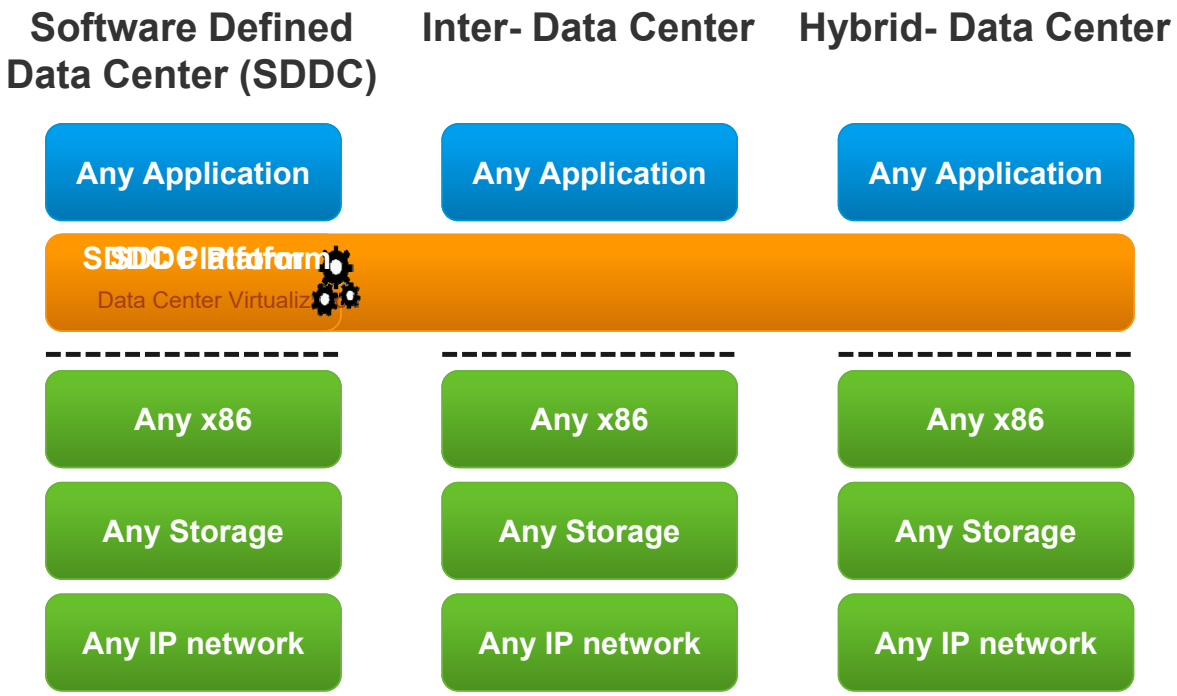
The Choice for “New IT” – SDDC or HDDC



vmware

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

“New IT” will be SDDC



Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

Benefits of a Software Defined Data Center

Automation

- IT Automating IT
- Developer Clouds
- Multi-tenant Infrastructure

Security

- Micro-Segmentation
- DMZ Anywhere
- Secure User Environments

Application Continuity

- Disaster Recovery
- Metro Pooling
- Hybrid Cloud Networking

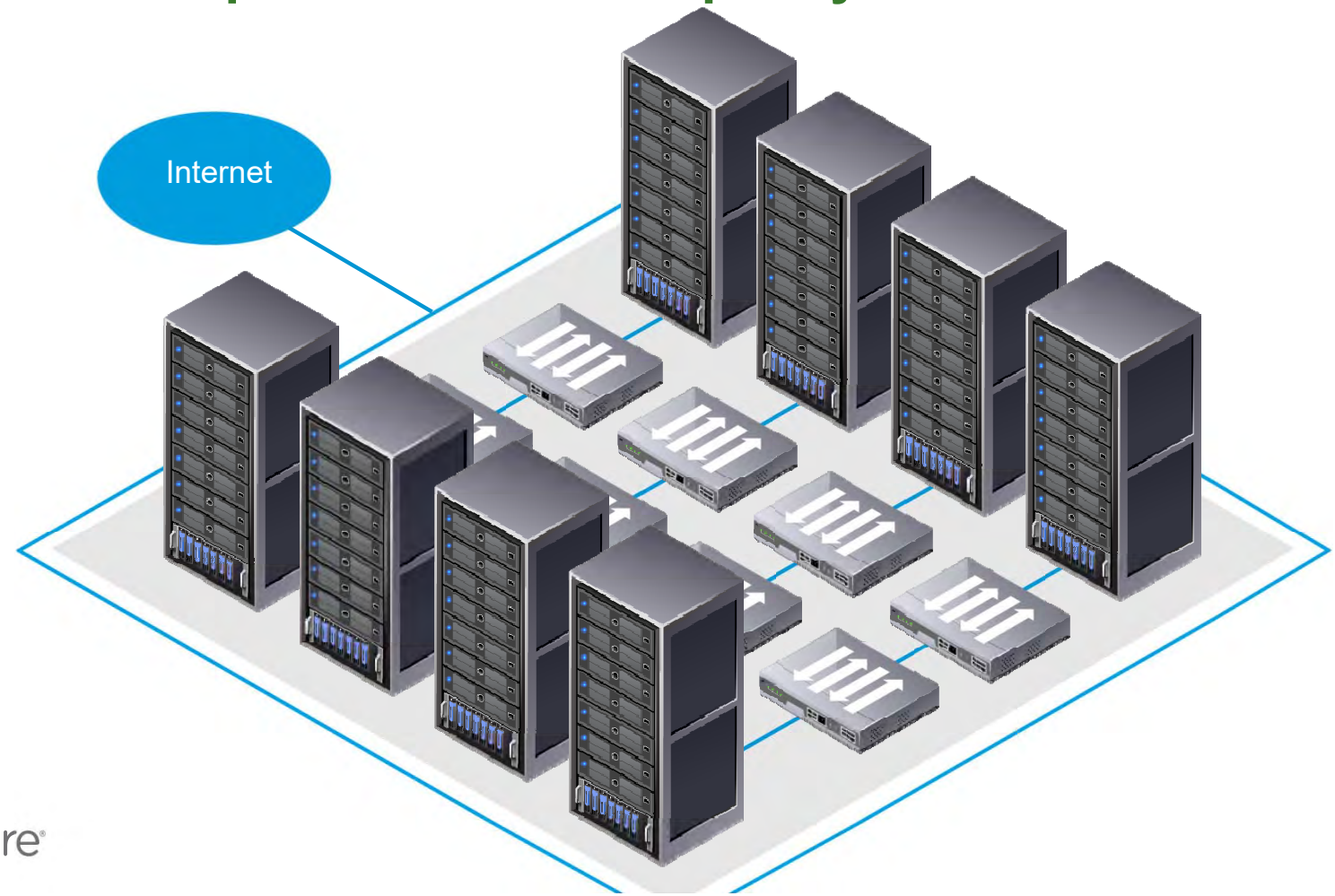
vmware

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

Who is doing this? Big, Small, All Verticals

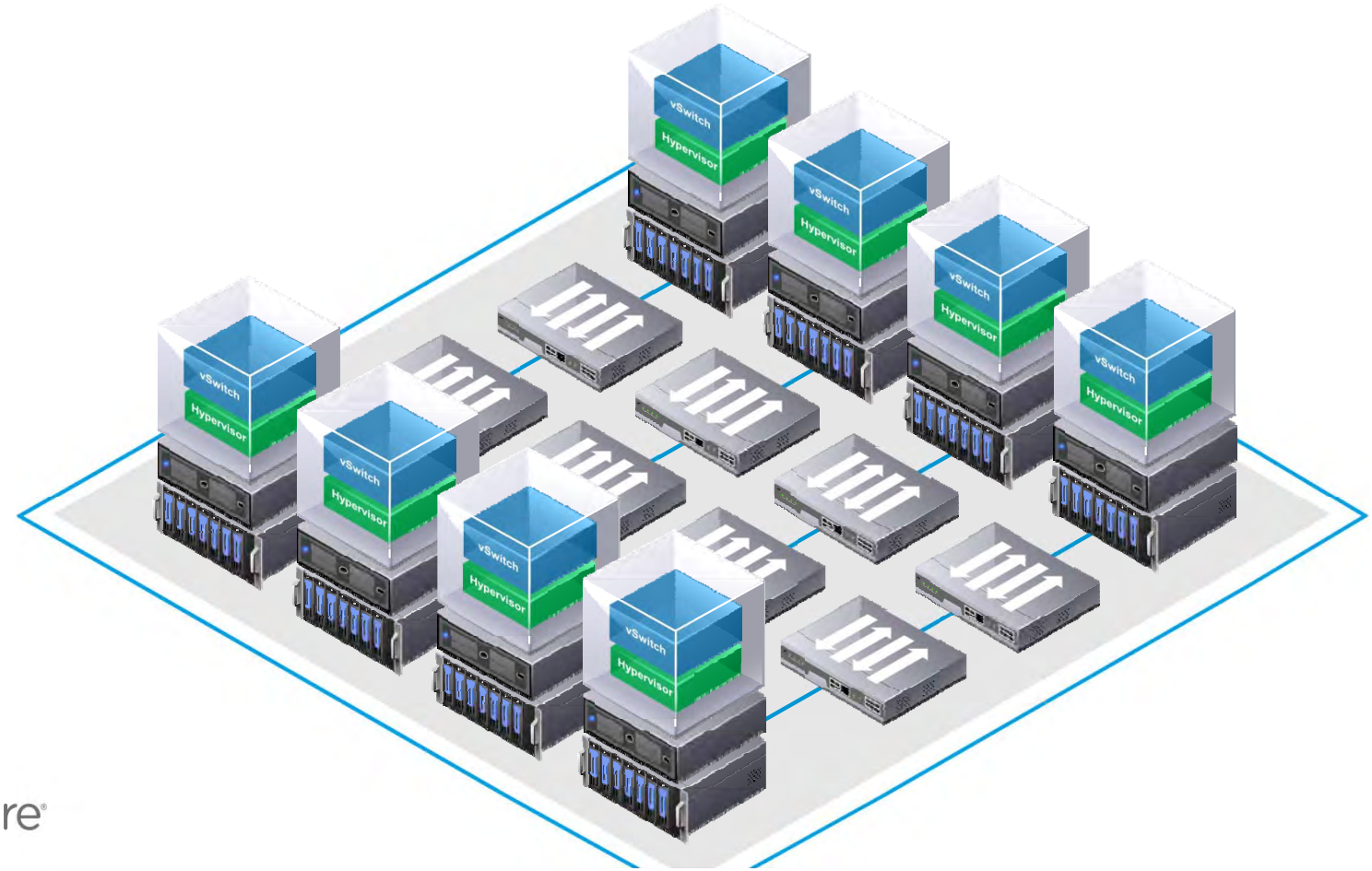
Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

A traditional data center starts with physical compute & network capacity



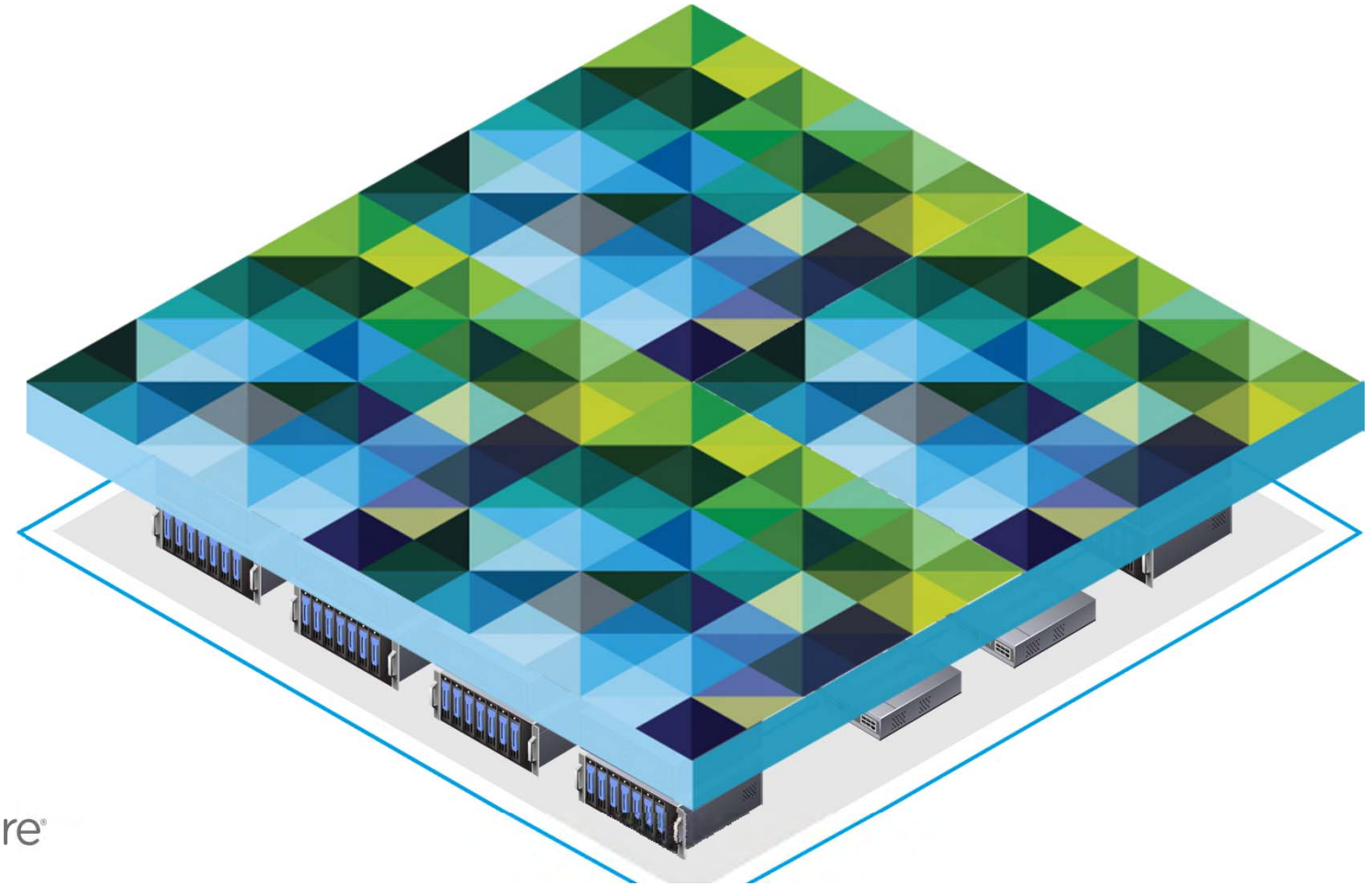
vmware

Then you virtualize your compute



vmware

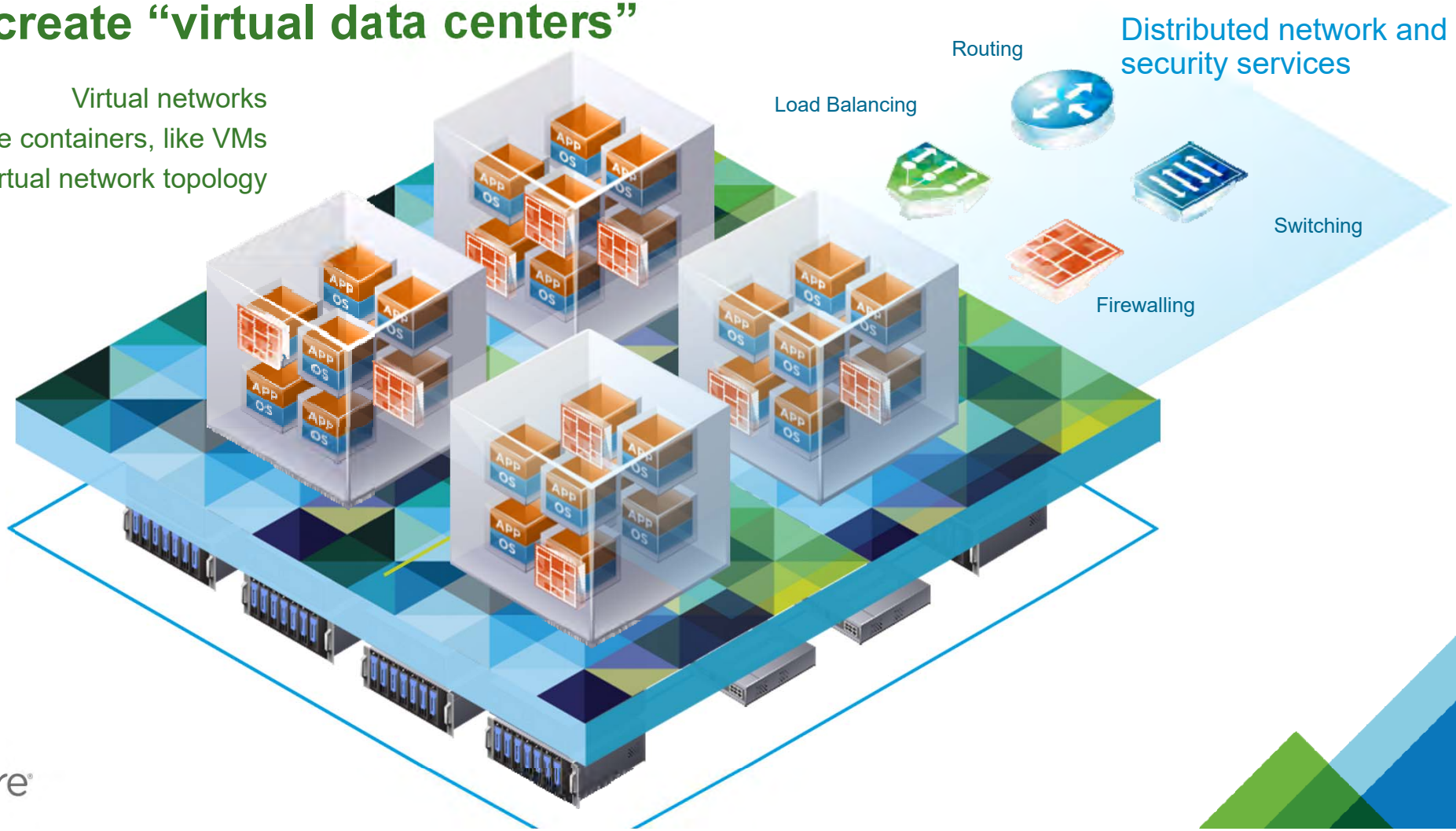
Add a “Network Hypervisor”



vmware

And create “virtual data centers”

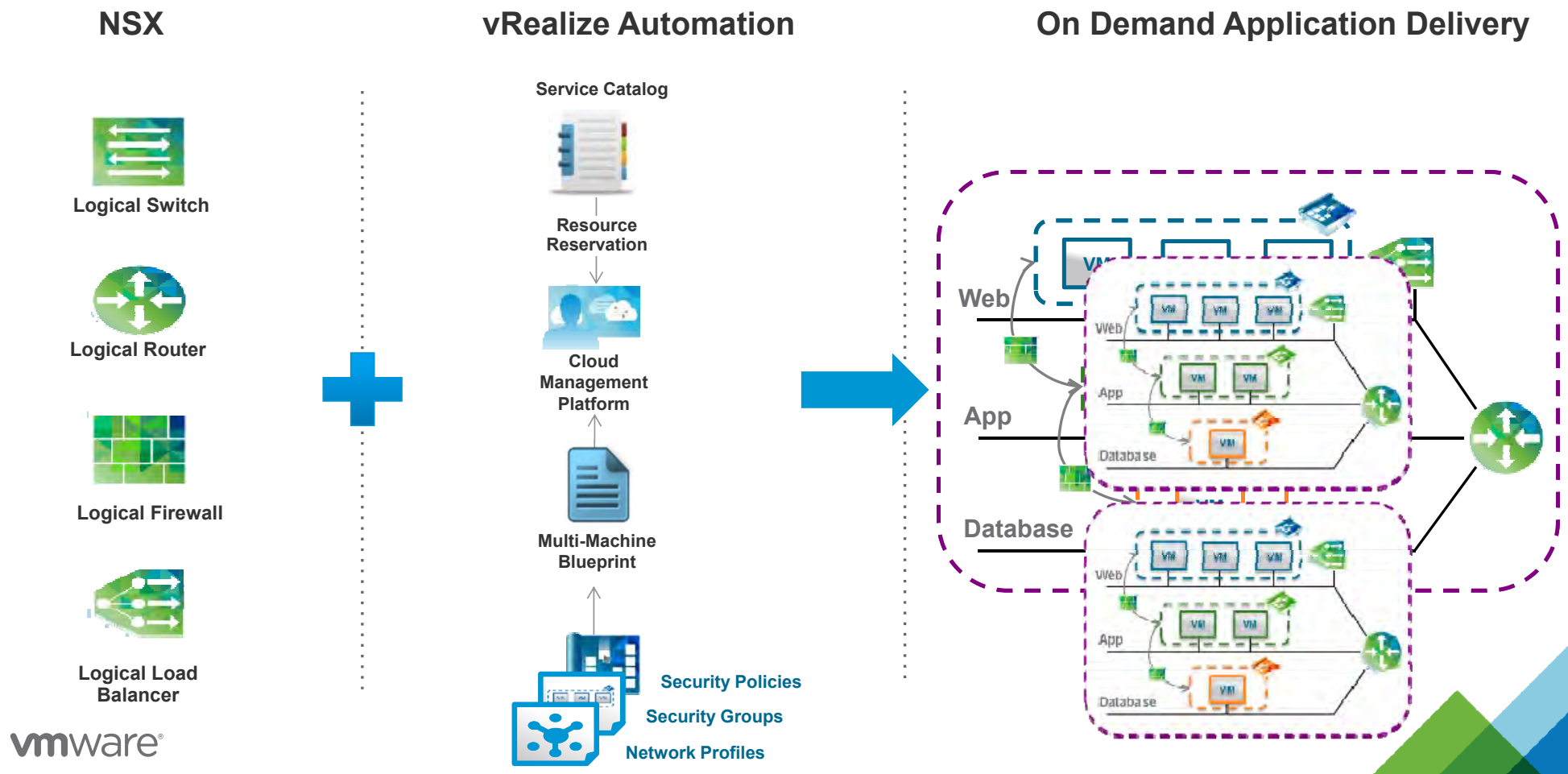
Virtual networks
Software containers, like VMs
Virtual network topology



vmware

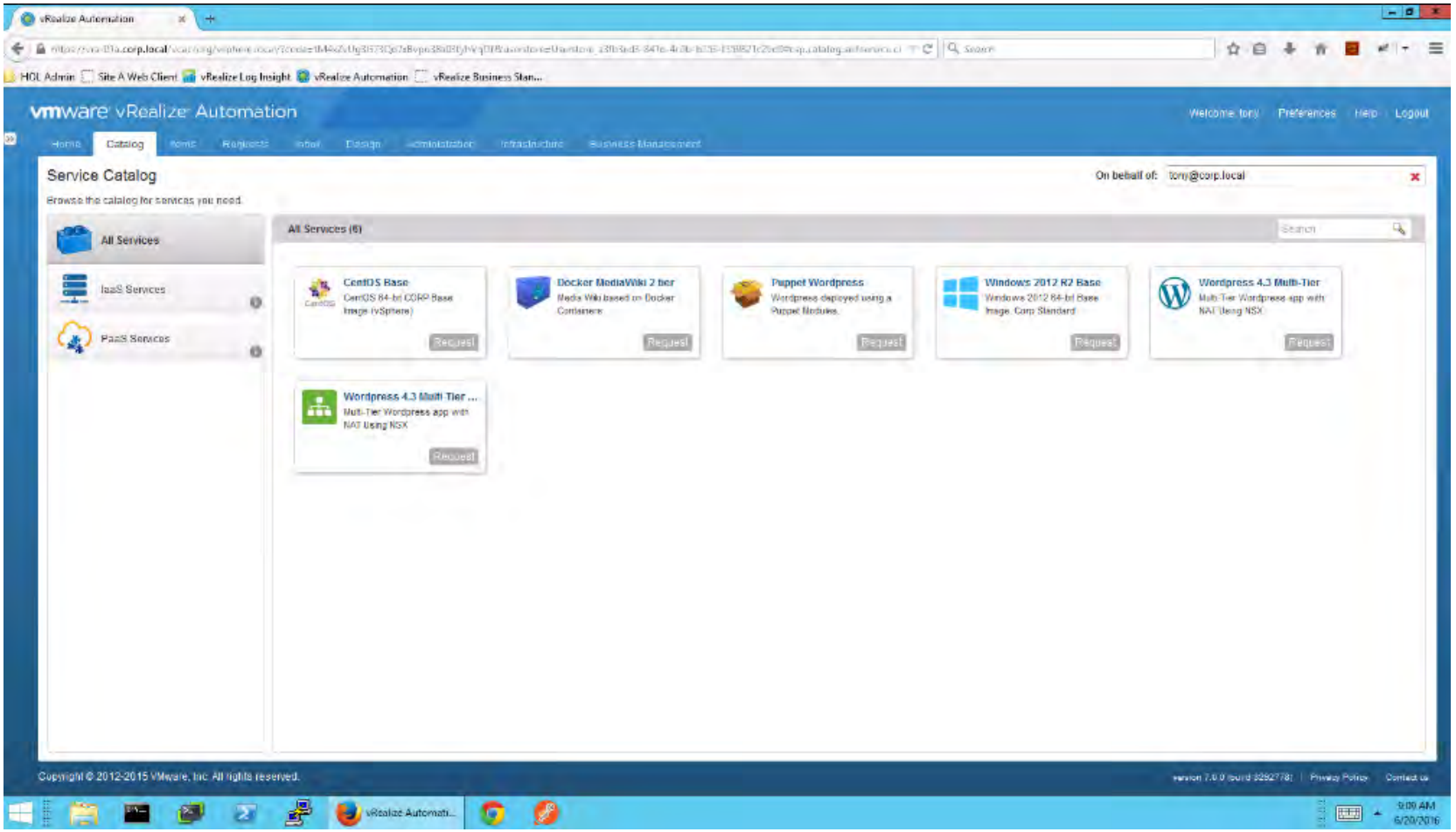
NSX with vRealize Automation

Dynamic Configuration and Deployment of NSX Logical Services



Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

vRealize Automation – Self Service Catalog

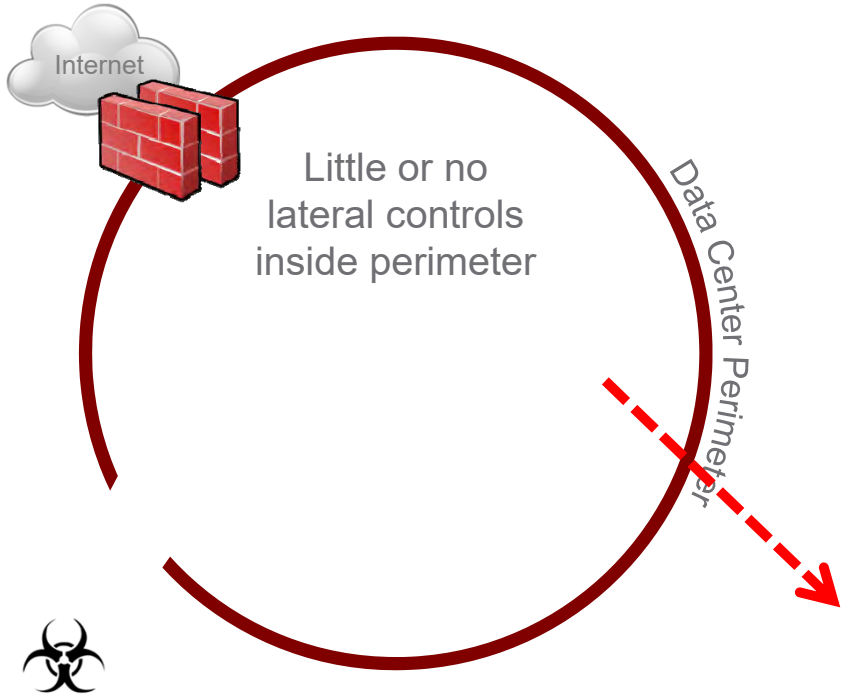


vmware

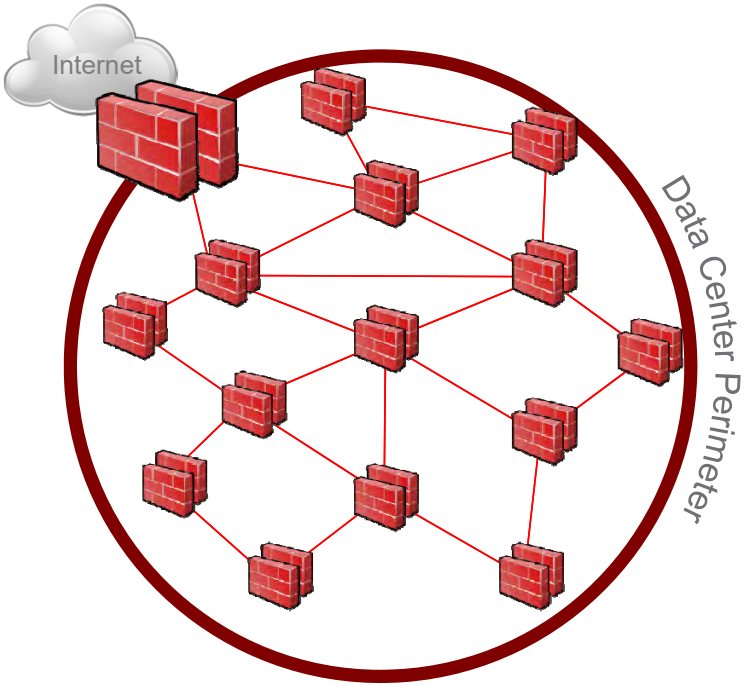
Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

Problem: Data Center Network Security

Perimeter-centric network security has proven insufficient, and micro-segmentation is operationally infeasible



Insufficient

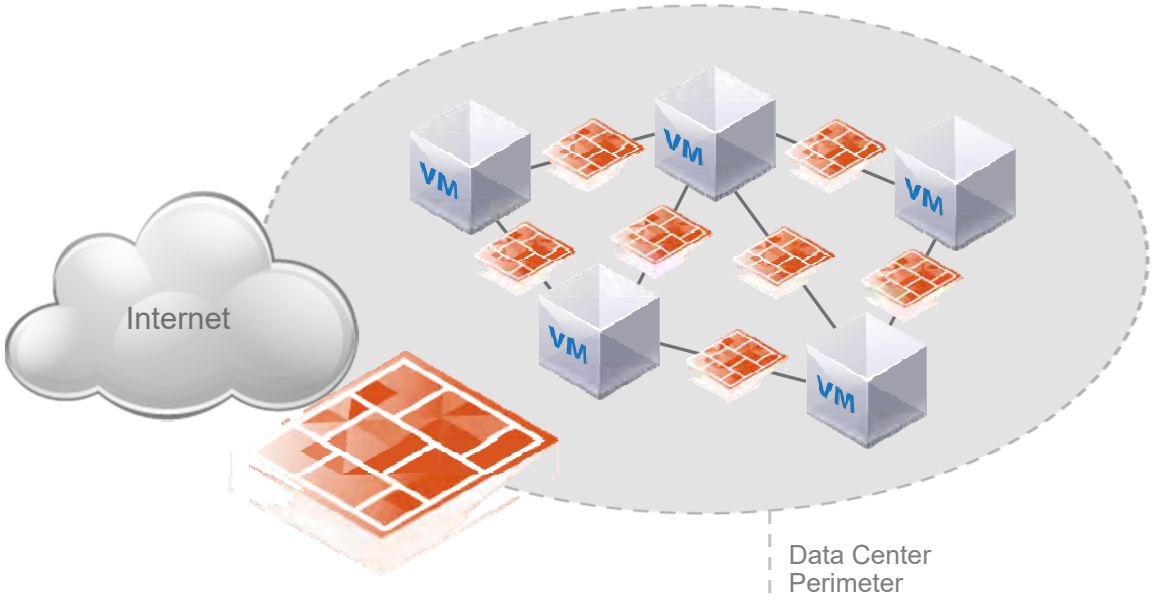


Operationally
Infeasible

vmware

Security is Needed Throughout the DC

Why can't we have individual firewalls for every VM?



With traditional technology, this is operationally infeasible.

Physical firewalls

High Throughput, but

Expensive and complex

Virtual firewalls

Distributed but

Slow and Policy Complexity in Co-Mingled Environment

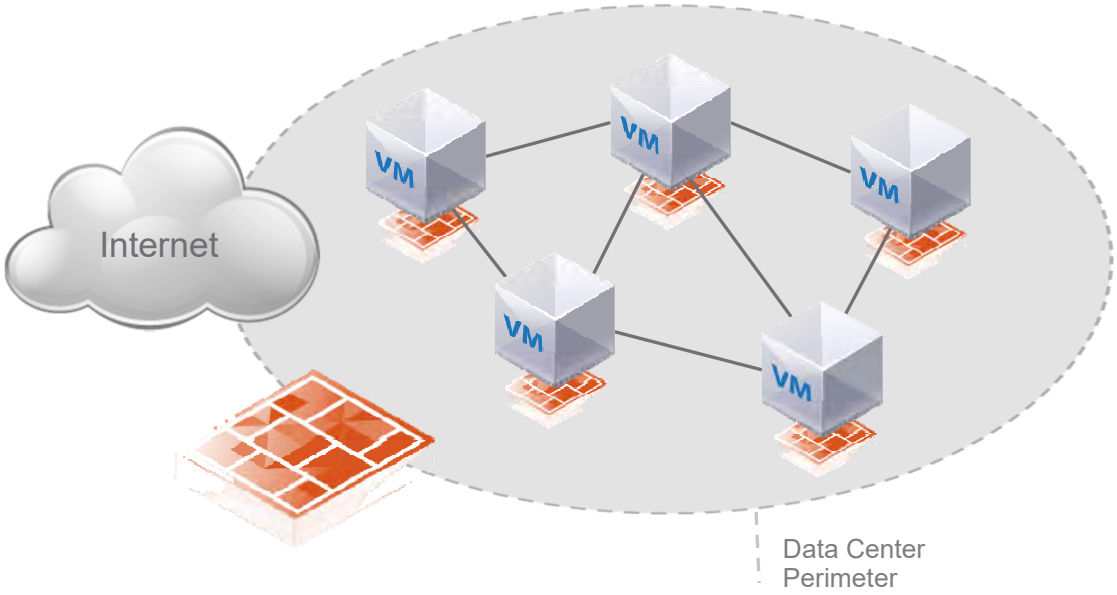
vmware

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

How about a Hypervisor based, Distributed Firewall?

Best of Both Worlds:

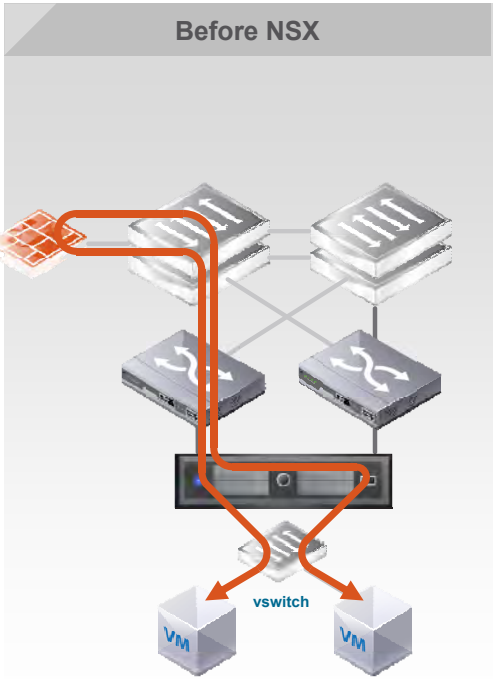
1. Policy Managed Centrally
2. Enforced in the Hypervisor Kernel, right at the virtual NIC



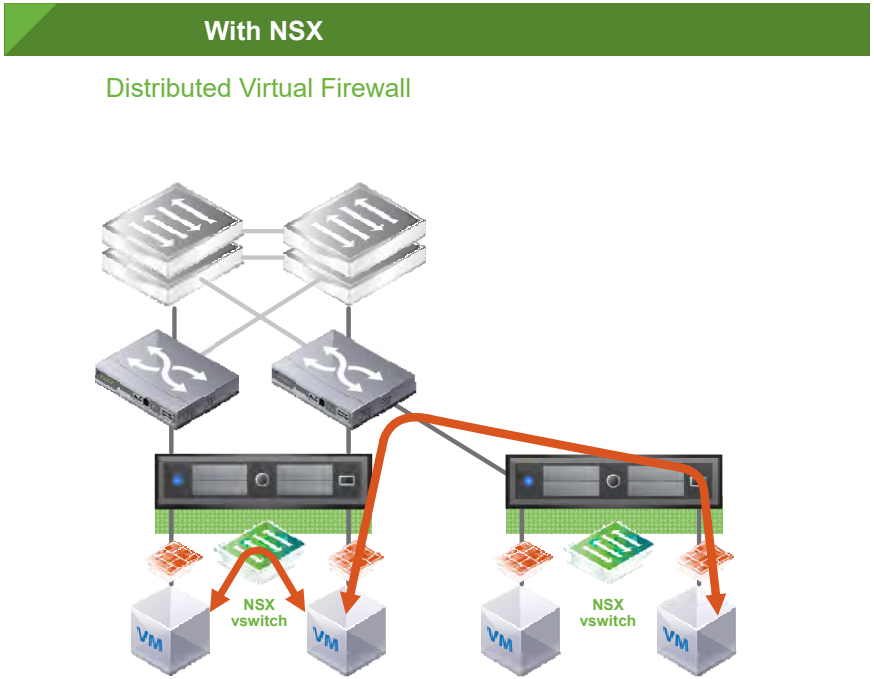
vmware

Distributed Services – Efficient, Scale-out

East-West Firewalling / Host to host



Hairpin



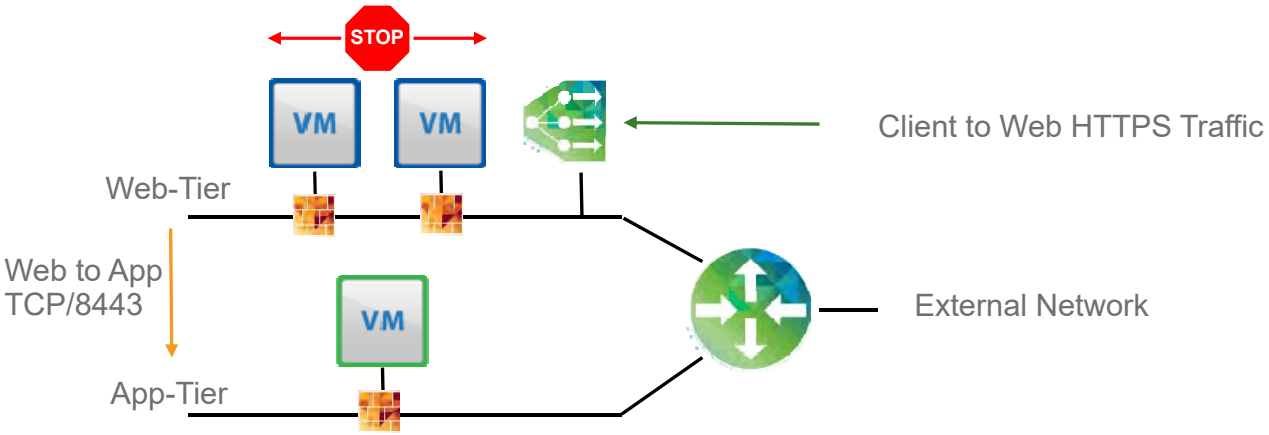
Direct VM-VM Path

Shortest Network Path

vmware

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

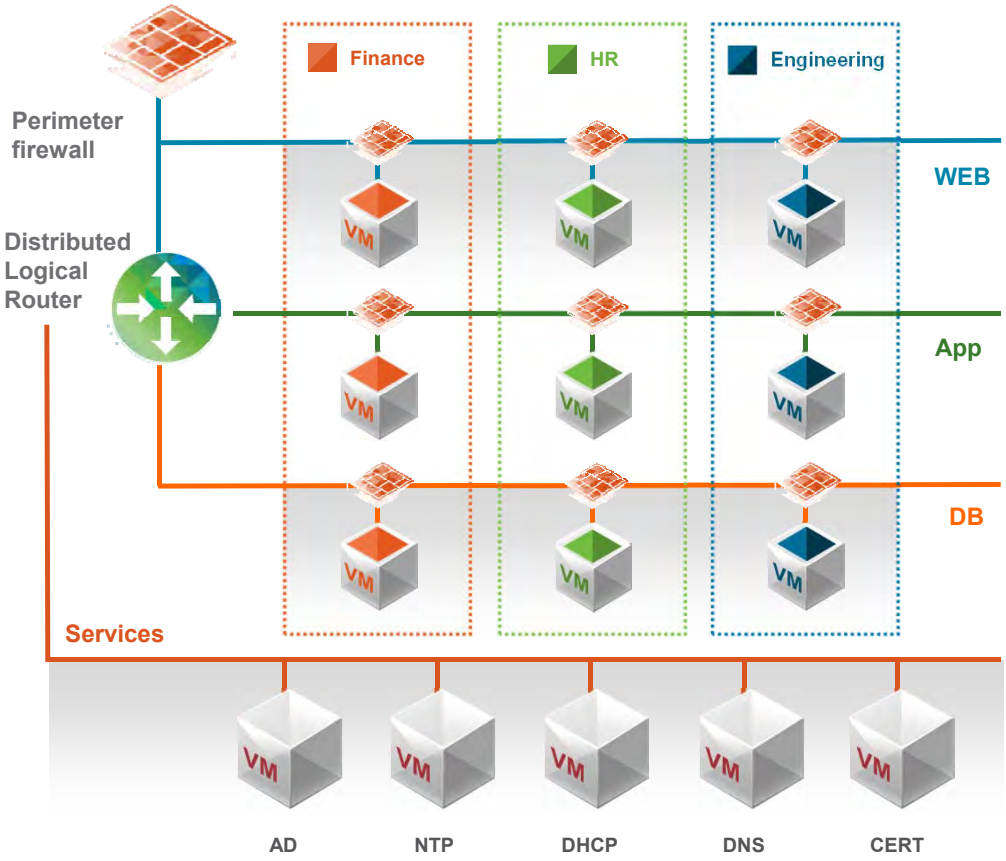
Example Building a Web DMZ



Source	Destination	Service	Policy
Web-VM1	Web-VM2		Block
Any	Web-Tier LS	HTTPS	Allow
Any	Web-Tier LS		Block
Web-Tier LS	App-Tier LS	TCP 8443	Allow
Any	App-Tier LS		Block

vmware

Micro-segmentation simplifies network security



- Each VM can now be its own perimeter
- Policies align with logical groups
- Intelligent security grouping
  - If the security tag:
    - Begins with the letters DB *~Tier*
    - Contains the letters HR *~Dep*
    - Ends with the letters SOC *~Type*

Example Security Tag: DB02-HR-SOC

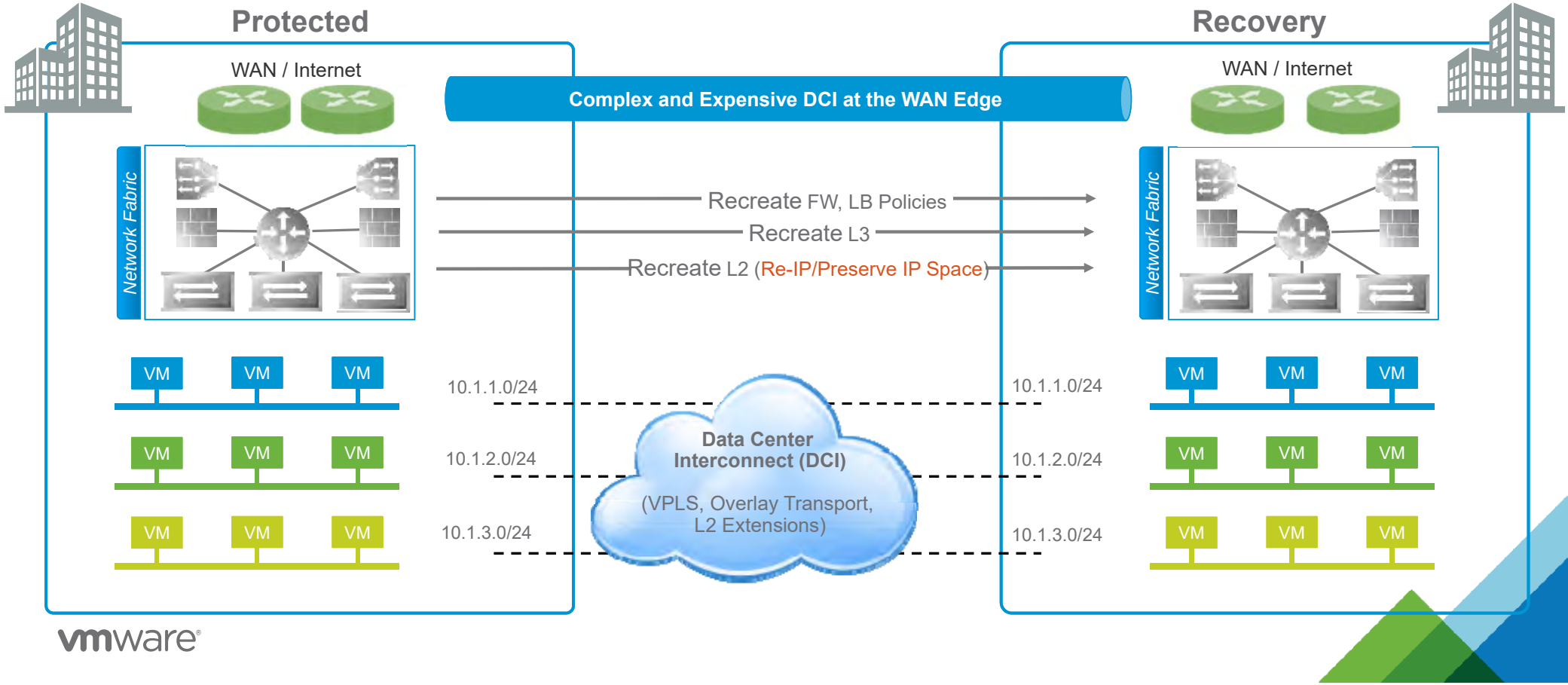
vmware

SDDC – A Platform for Industry Innovation

Questions? Please contact lizl@mobiuspartners.com or call 972.403.8045.

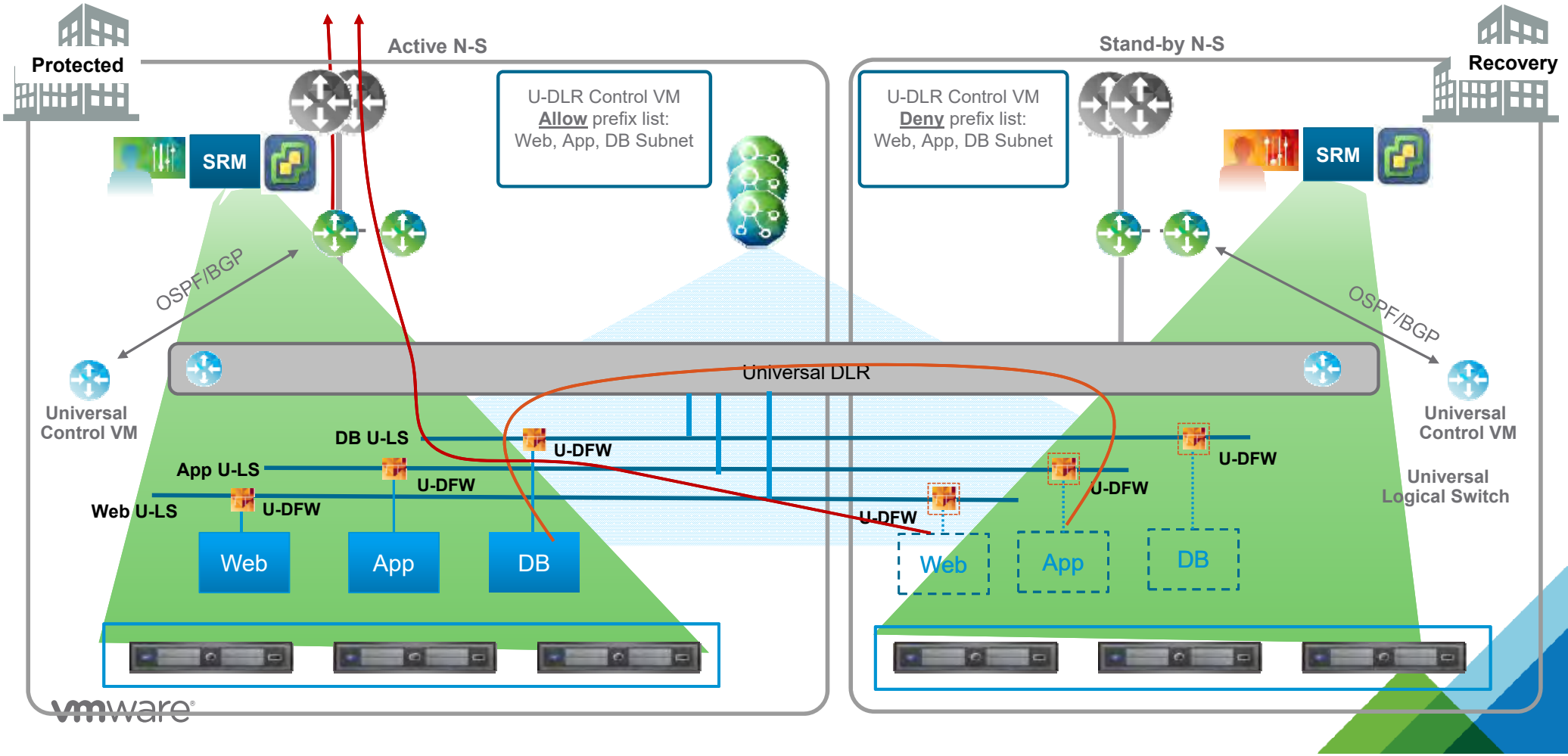
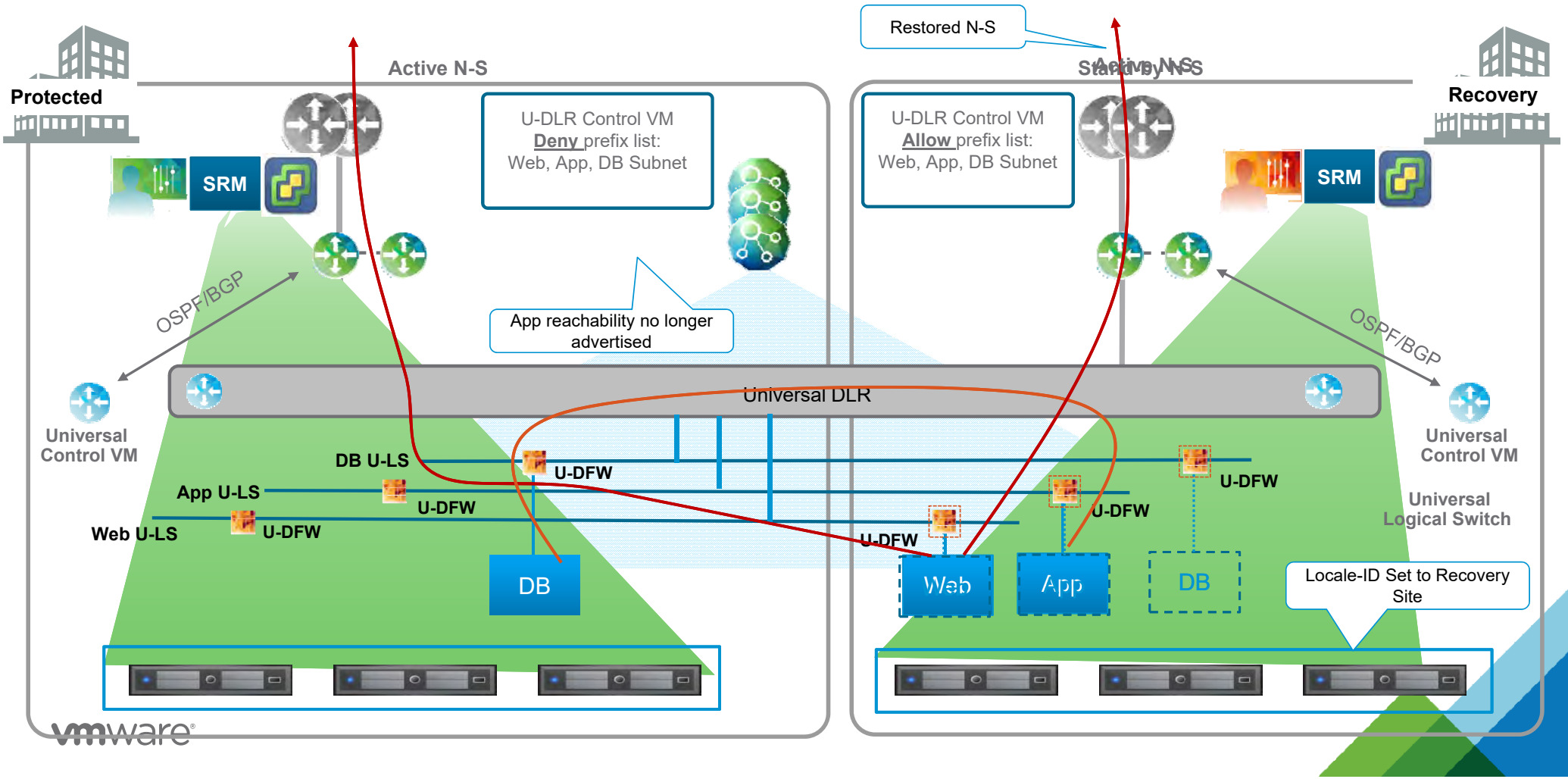
Traditional Disaster Recovery

Infrastructure Challenges: Site Connectivity



vmware

DR with NSX+SRM: Planned Migration/Partial Failure



DR with NSX+SRM: Complete Application Failure