Building the Network of the Future with the Virtual Cloud Network

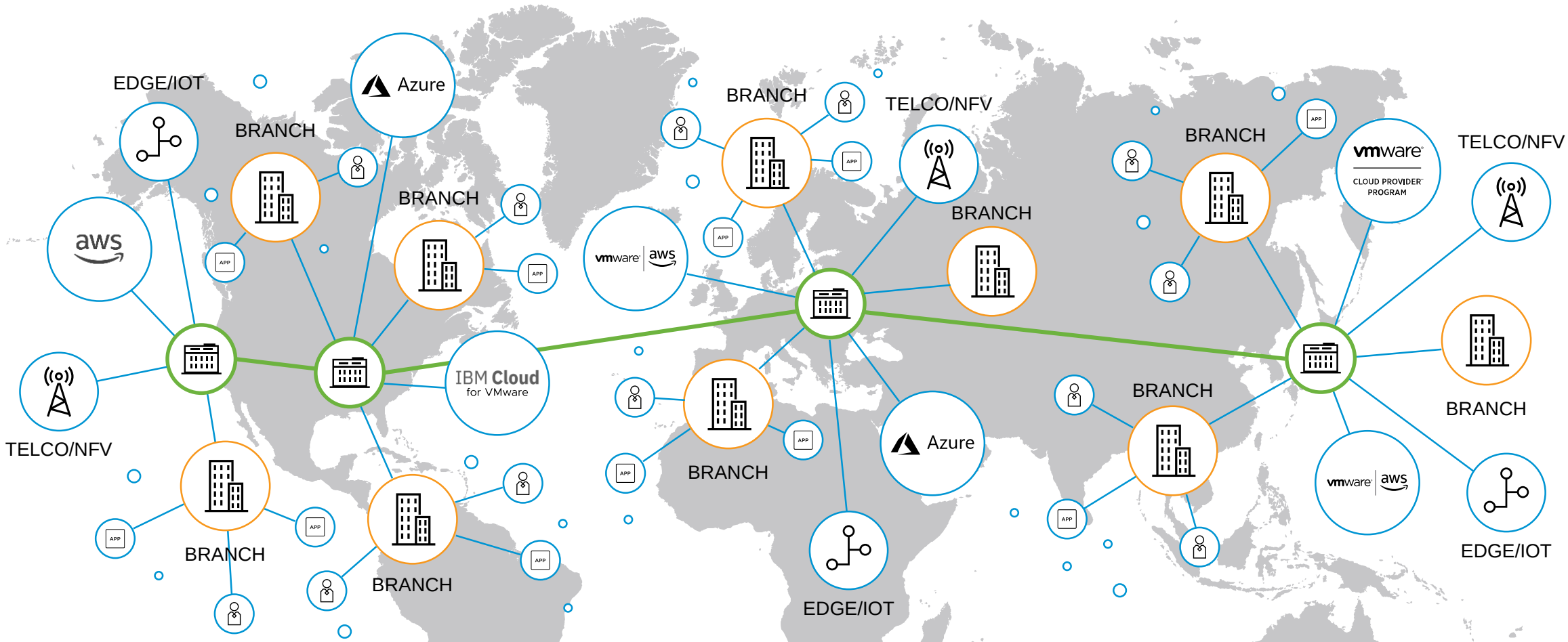
“Why build something in hardware, that can be built in software?”

Anders Krus

Sr. Systems Engineer

Network and Security Business Unit

vmware®



The Virtual Cloud Network

Delivered by VMware NSX

vmware

VMware NSX Portfolio

NETWORKING AND SECURITY MANAGEMENT AND AUTOMATION

Cloud-Based Management | Workflow Automation | Blueprints / Templates | Insights / Discovery | Visibility

Network Insight
Network discovery and insights

vRealize Automation
End-to-end workload automation

NETWORK AND SECURITY VIRTUALIZATION

Security | Integration | Extensibility | Automation | Elasticity

NSX Data Center
Networking and security for data center workloads

NSX Cloud
Networking and security for Cloud workloads

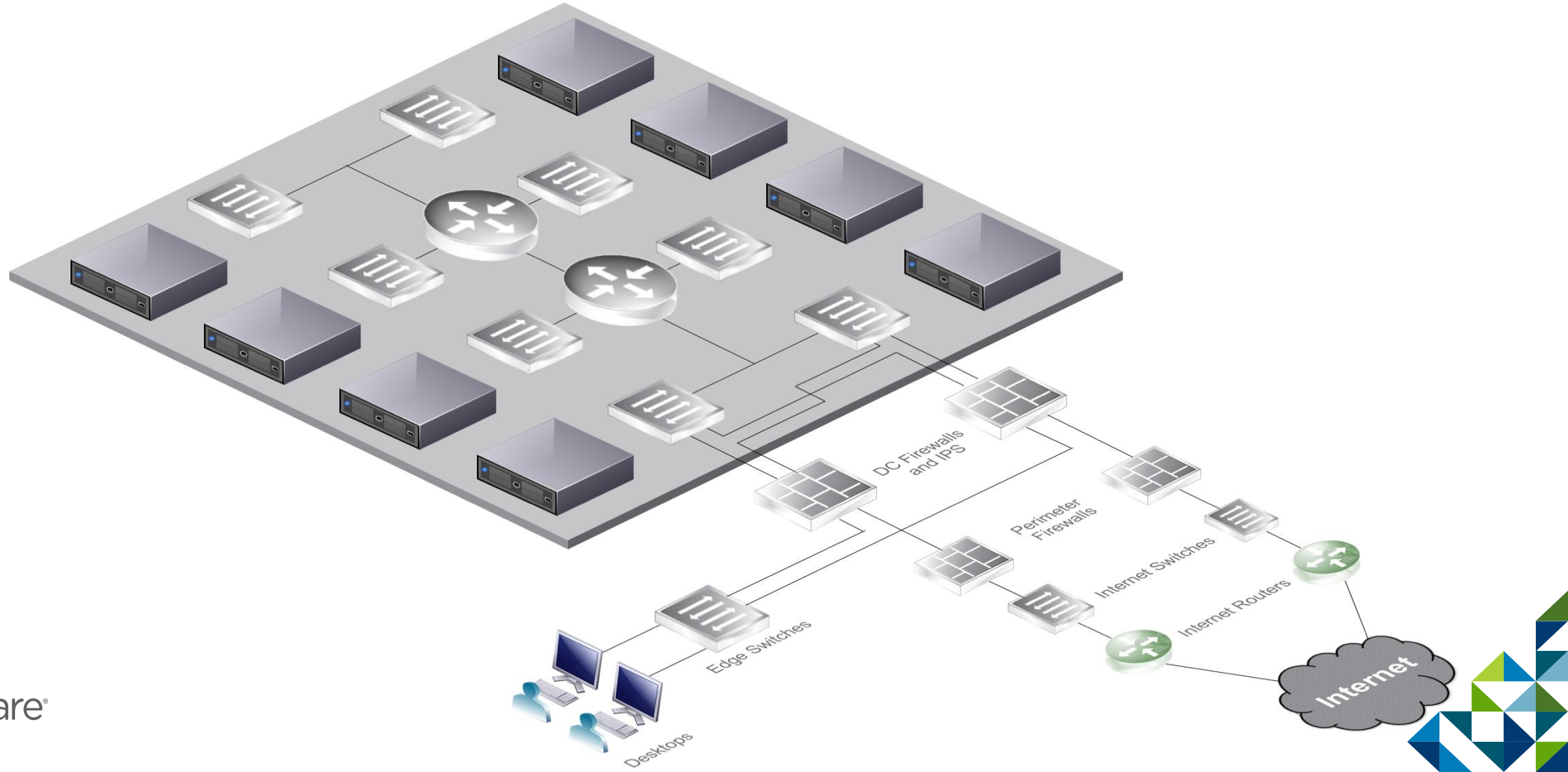
AppDefense
Modern application security

NSX SD-WAN by VeloCloud
WAN connectivity services

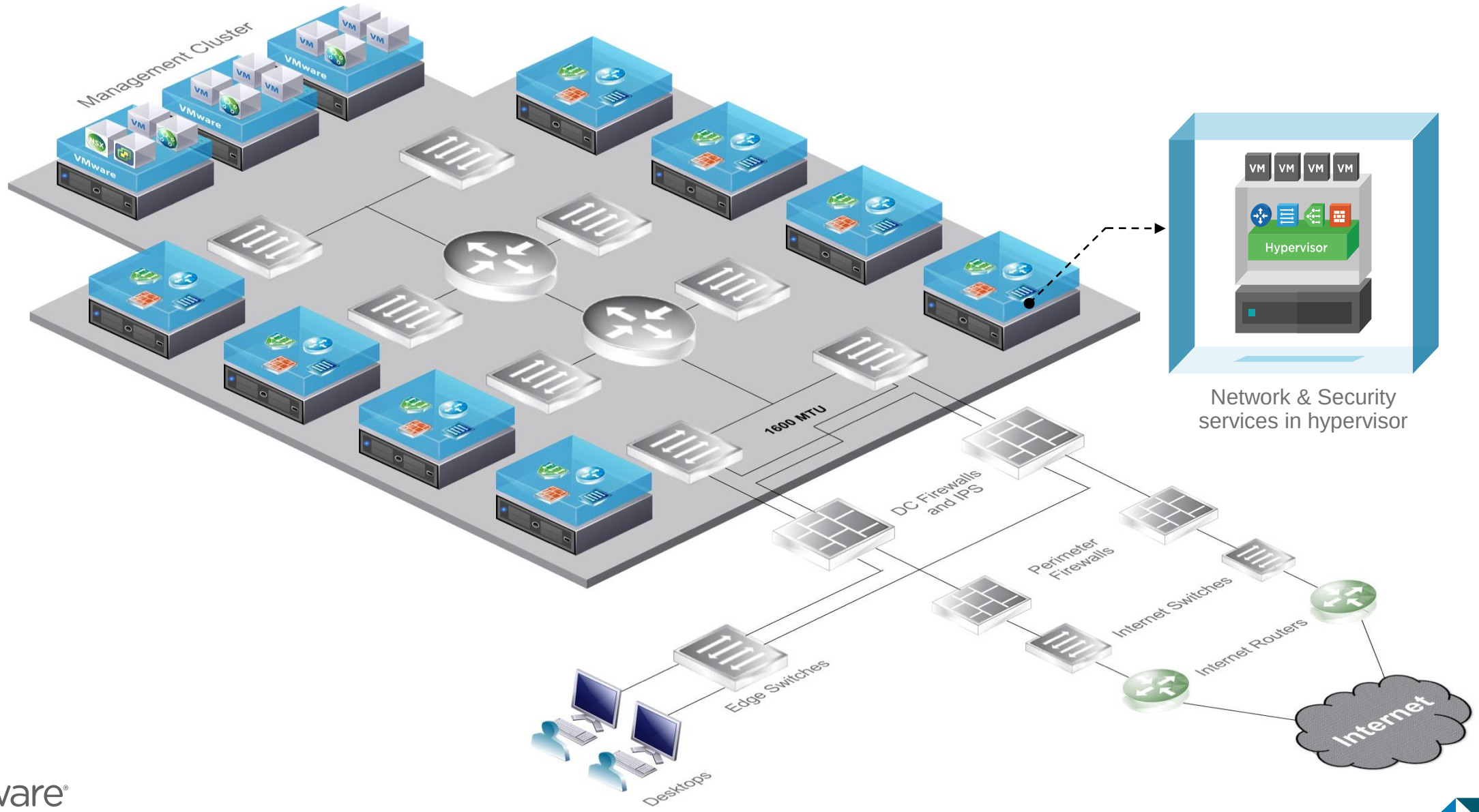
NSX Hybrid Connect
Data center and cloud workload migration

vmware

Traditional datacenter – NW & Sec comes from physical devices

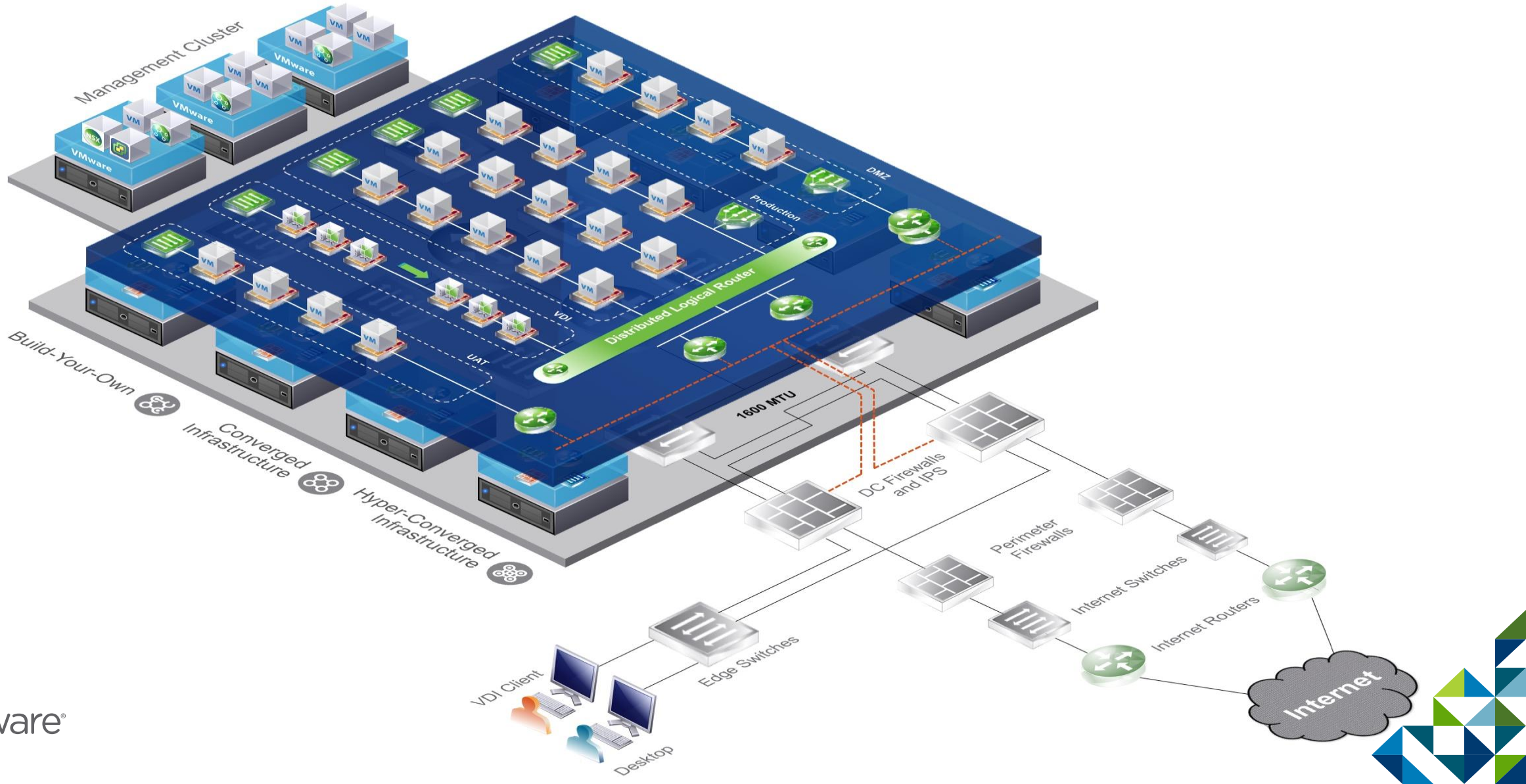


NSX adds NW & Sec to the Hypervisors



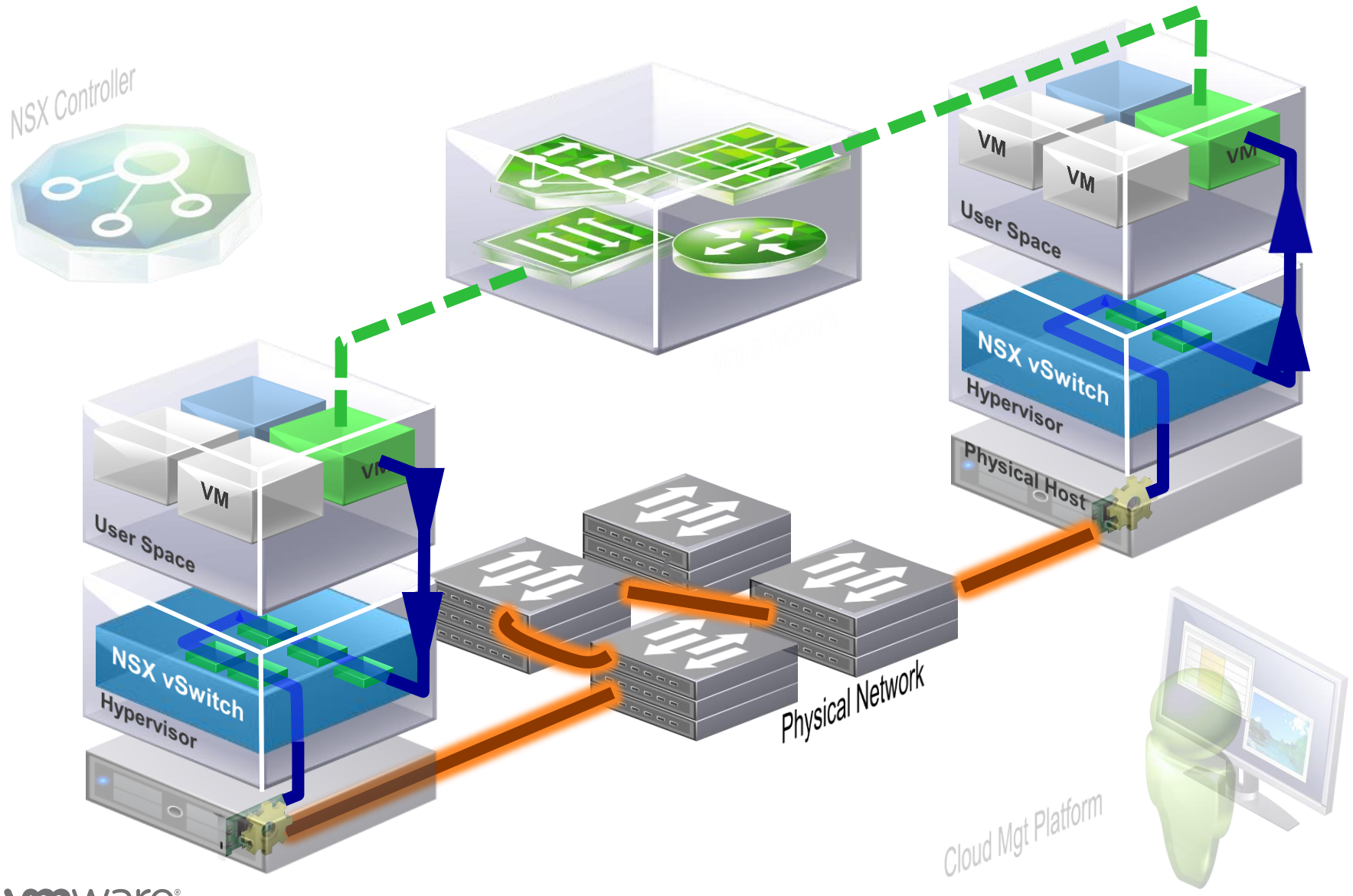
vmware

With NSX SDN – any topology can be built and be consumed anywhere



vmware

SDN by Overlay including Security - all in the hypervisor



SDDC:
- Compute
- Storage
- NW/Sec

NSX Use-cases:
- Automation
- Application Continuity
- Security

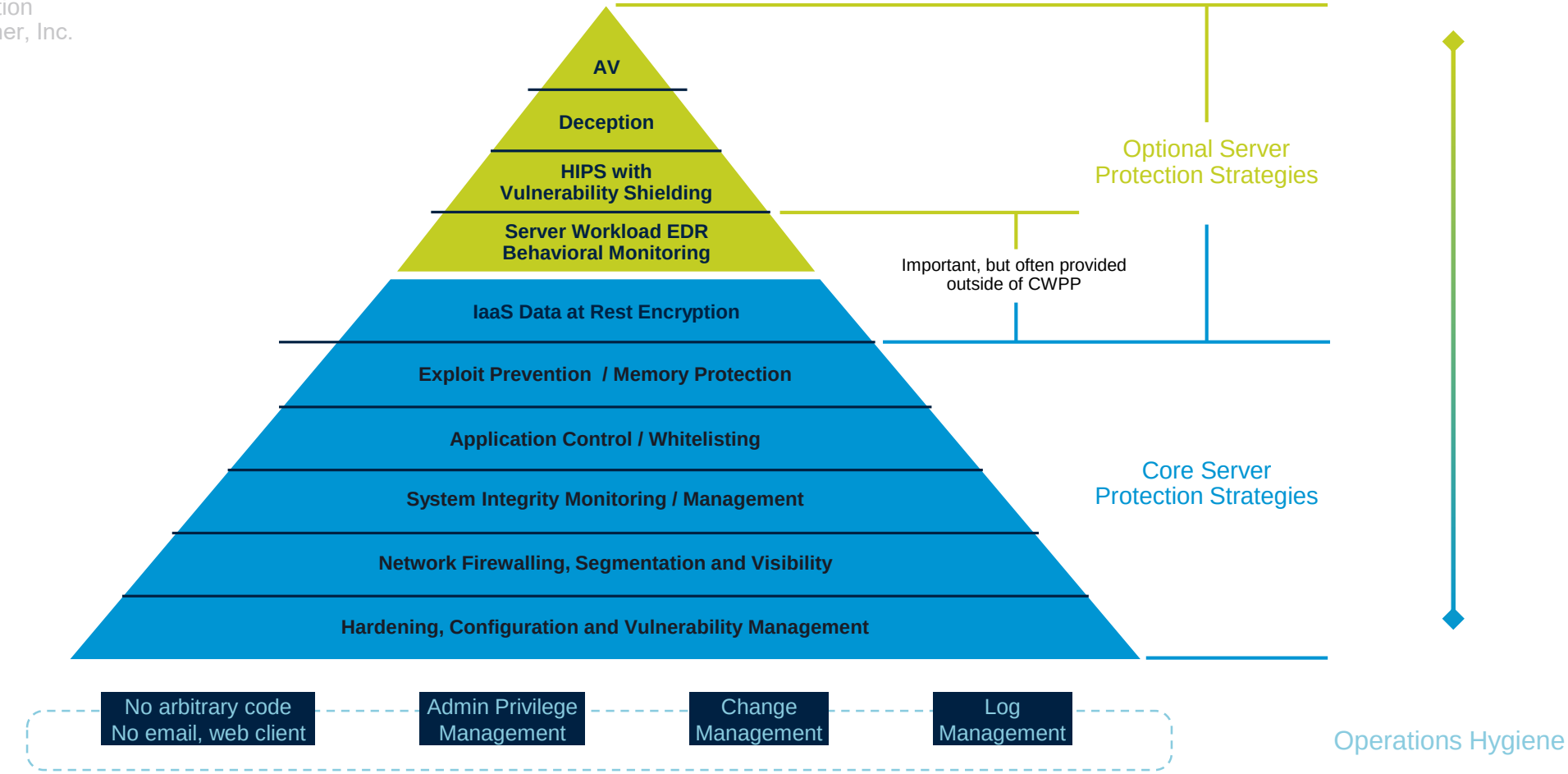
NSX Components:
- Switching
- Routing
- Load Balancing
- Firewalling

vmware

Focus on Core Protection Strategies

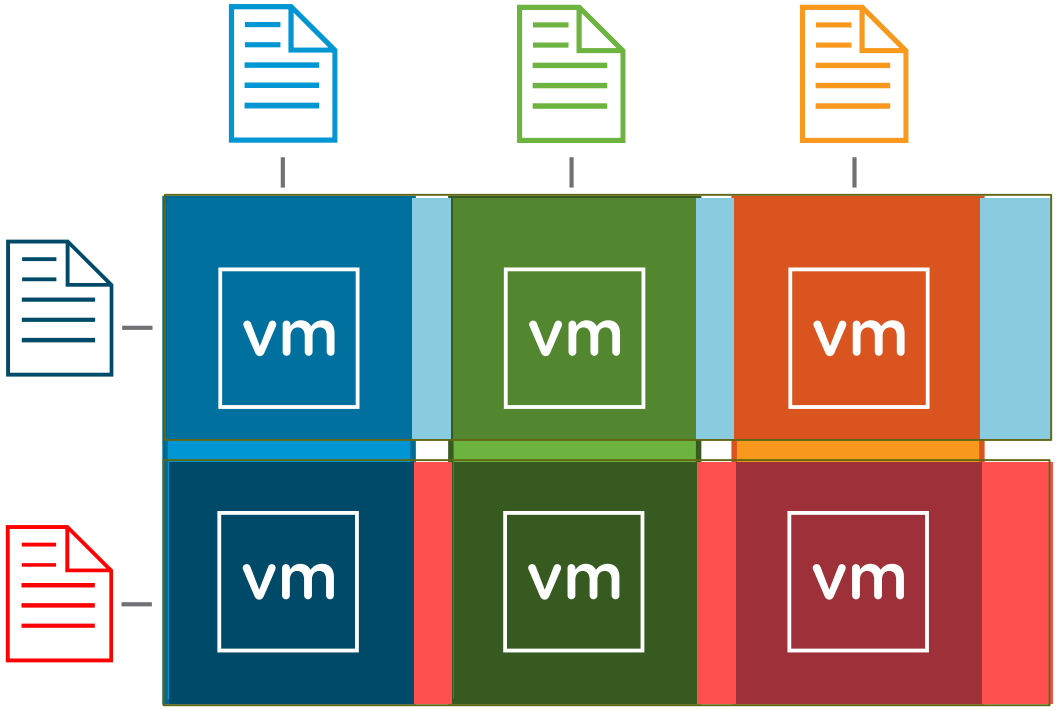
Gartner Market Guide for Cloud Workload Protection Framework

Figure 1. Cloud Workload Protection Controls Hierarchy, © 2018 Gartner, Inc.



Intelligent Grouping

Deep visibility and context of the virtual environment allows for alignment of policy based on workload attributes.

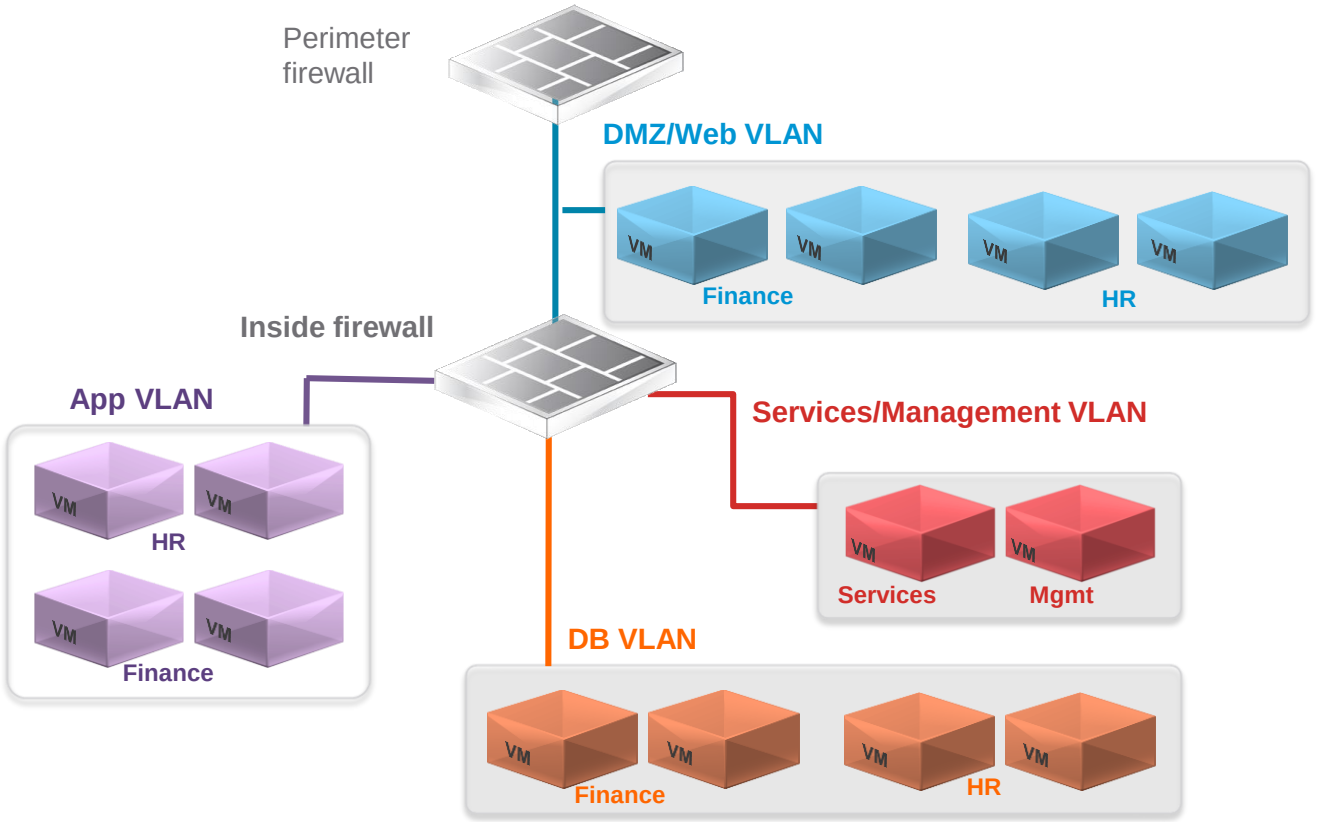


Groupings based on inherent workload attributes, such as:

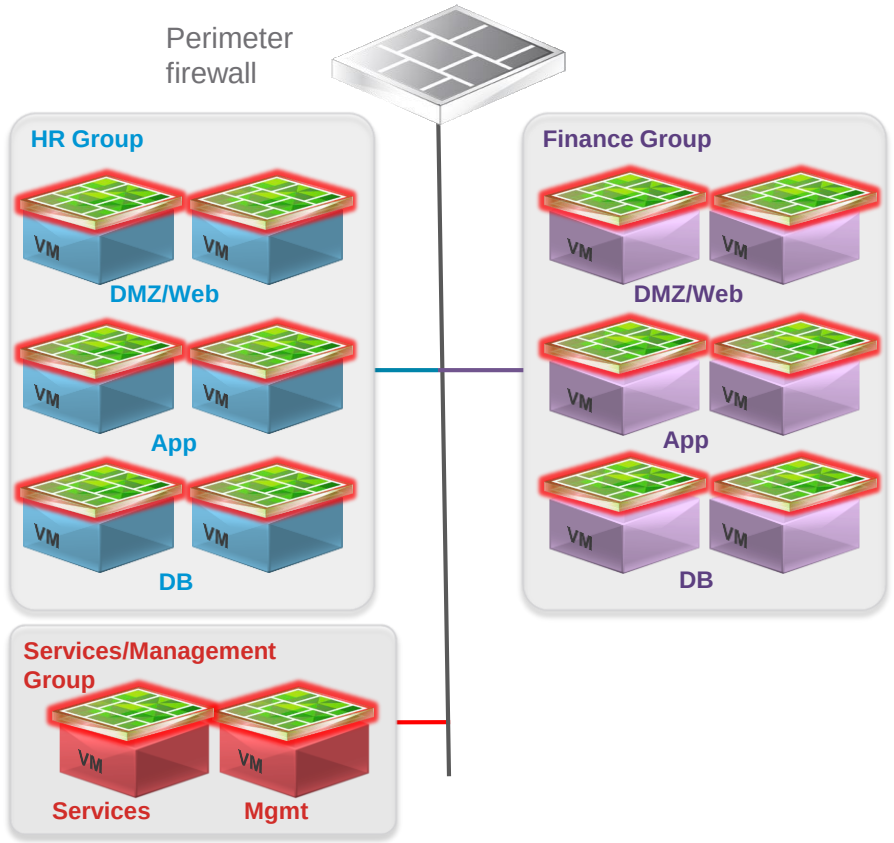
- Operating System
- Machine Name
- Services
- Application Tier
- Regulatory Requirements
- Security Tags

Achieving segmentation with NSX

Traditional Data Center without NSX:
IP segmentation is your "security tool"



NSX Micro-segmentation:
No obvious need for IP segmentation

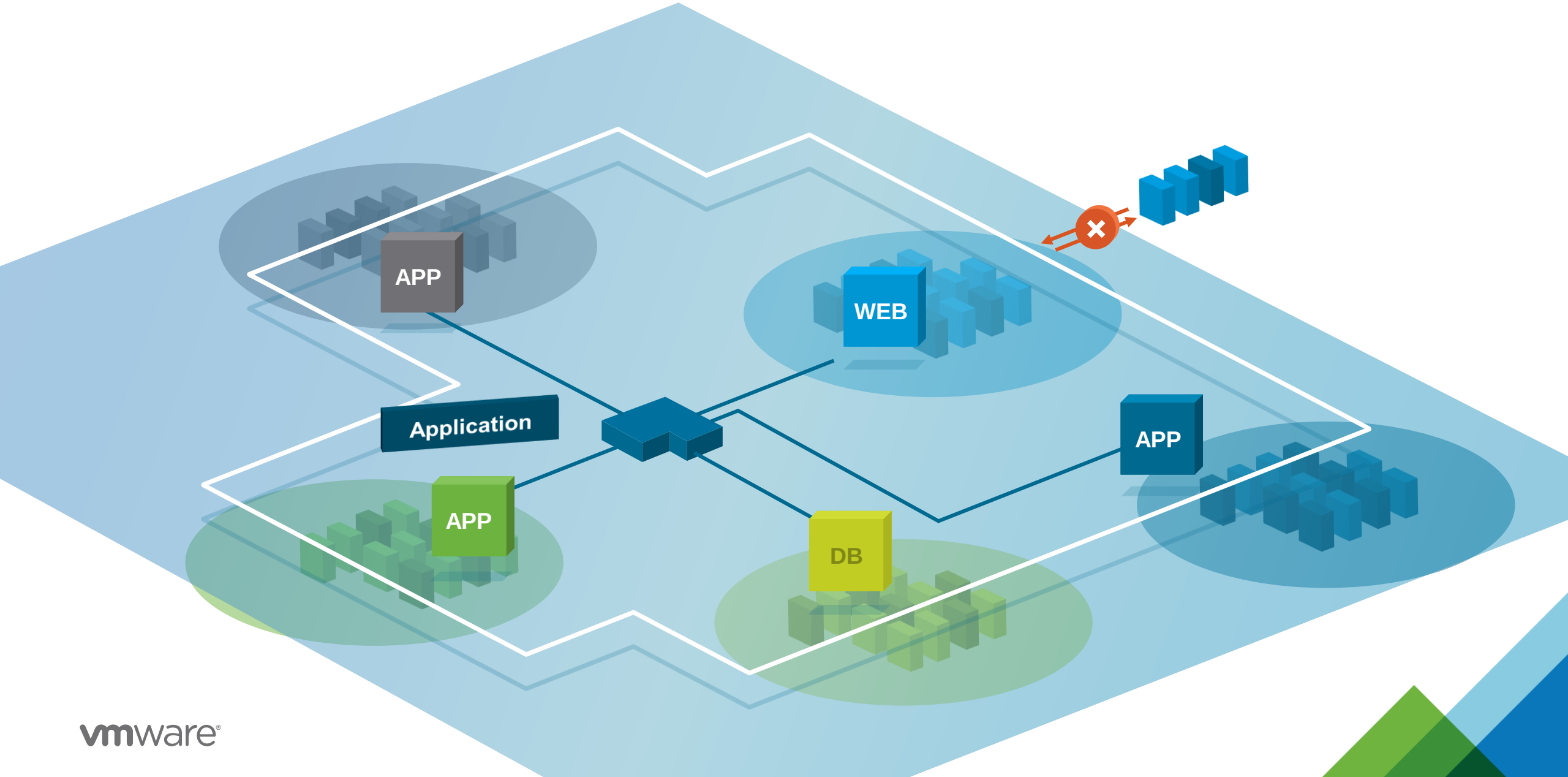


NSX segmentation simplifies network security

Firewall is -always- present

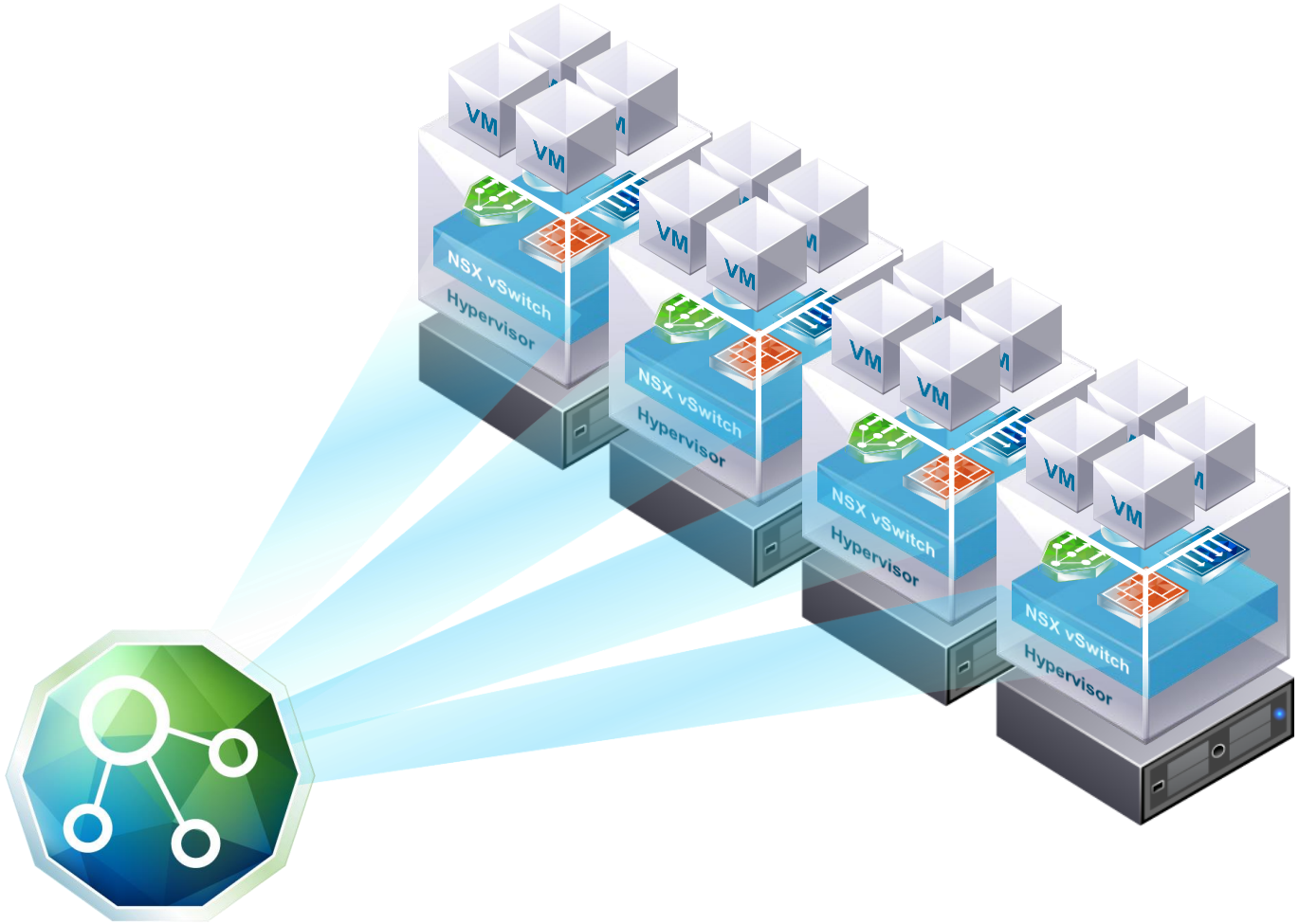
vmware

Microsegmentation – security is its own “Layer”



vmware

Take this approach to your entire environment



Reduce attack surface for every application/VM

Security Policy aligned to the application/project lifecycle

Each Hypervisor acts as a firewall providing line rate performance

Thank you!

“Why build something in hardware, that can be built in software?”

Anders Krus

Sr. Systems Engineer

Network and Security Business Unit

vmware®