VMware Security ...and not only

Overview

Pavel Kovář
Senior Solution Engineer / VMware

5.5.2022

Security is Fundamentally Broken

Digital Risk Management

Mobile Security

Endpoint Security

Data Security

Block Chain

Security Operations & Incident Response

Threat Intelligence

Cloud Security

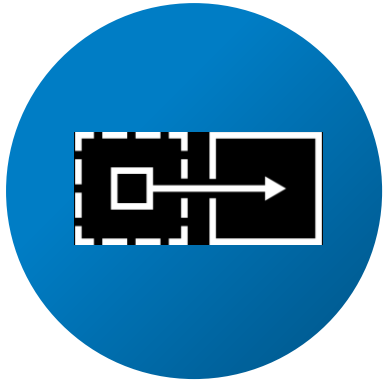
Risk and Compliance

WAF and Application Security

Identity & Access Management

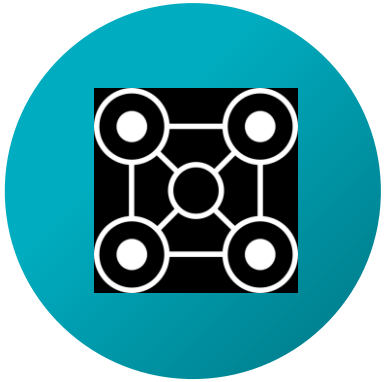
Network & Infrastructure Security

Security Must be Transformed



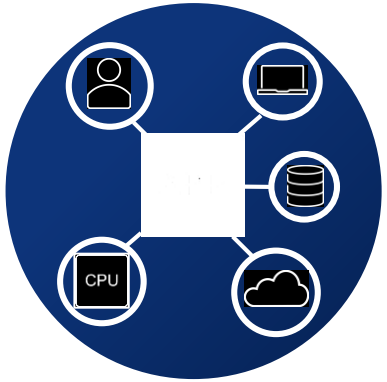
Built-in

Bolted-on



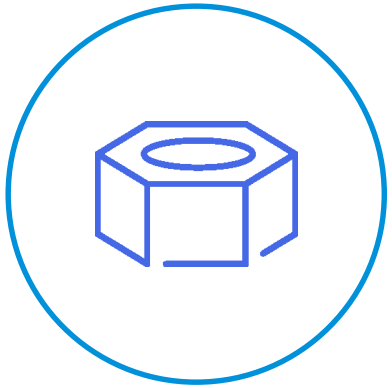
Unified

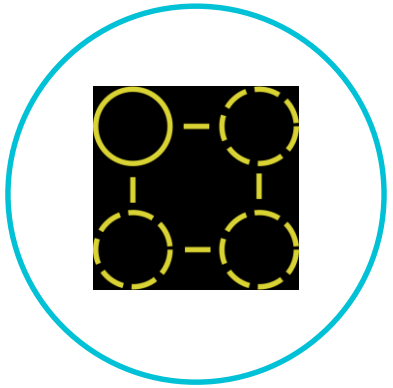
Siloed



Context-centric

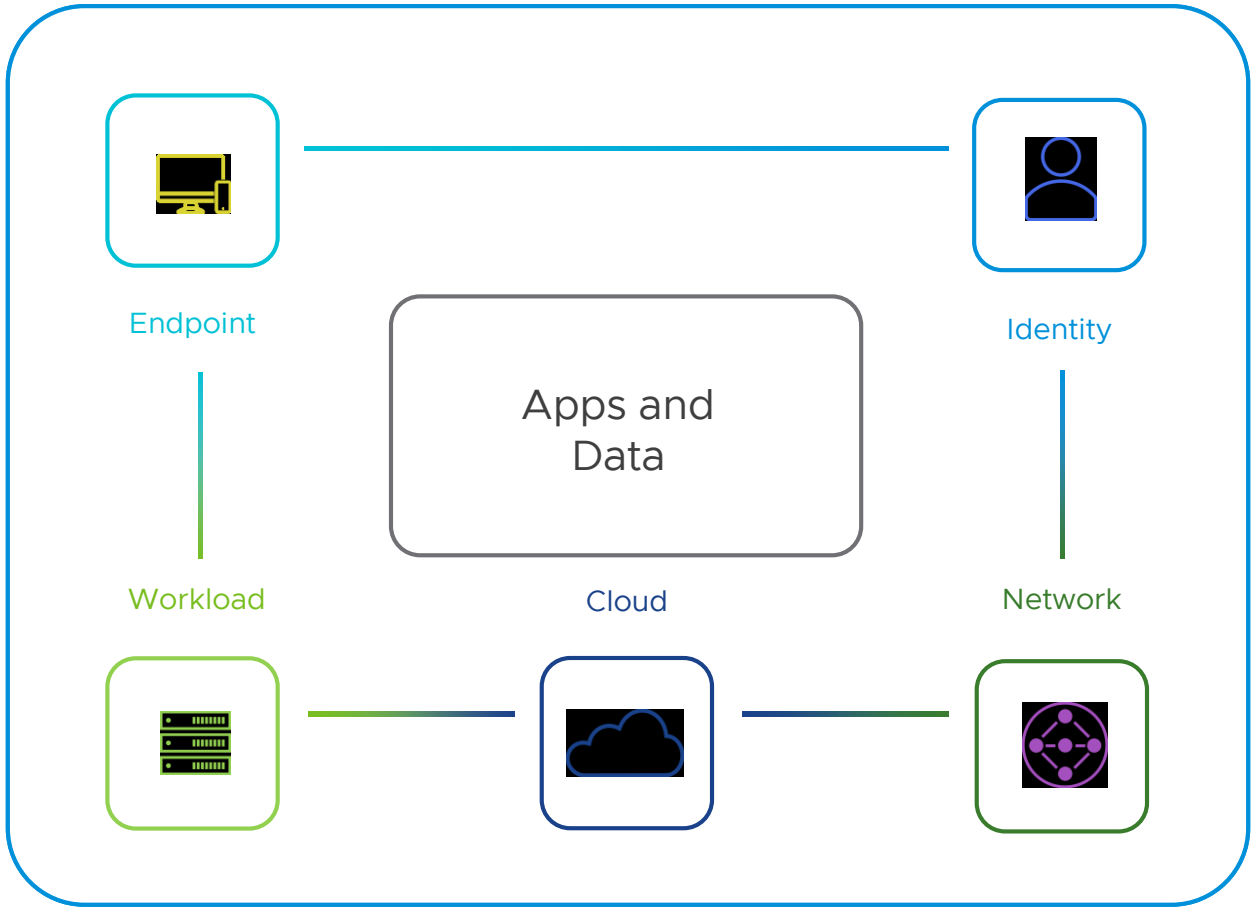
Threat-centric





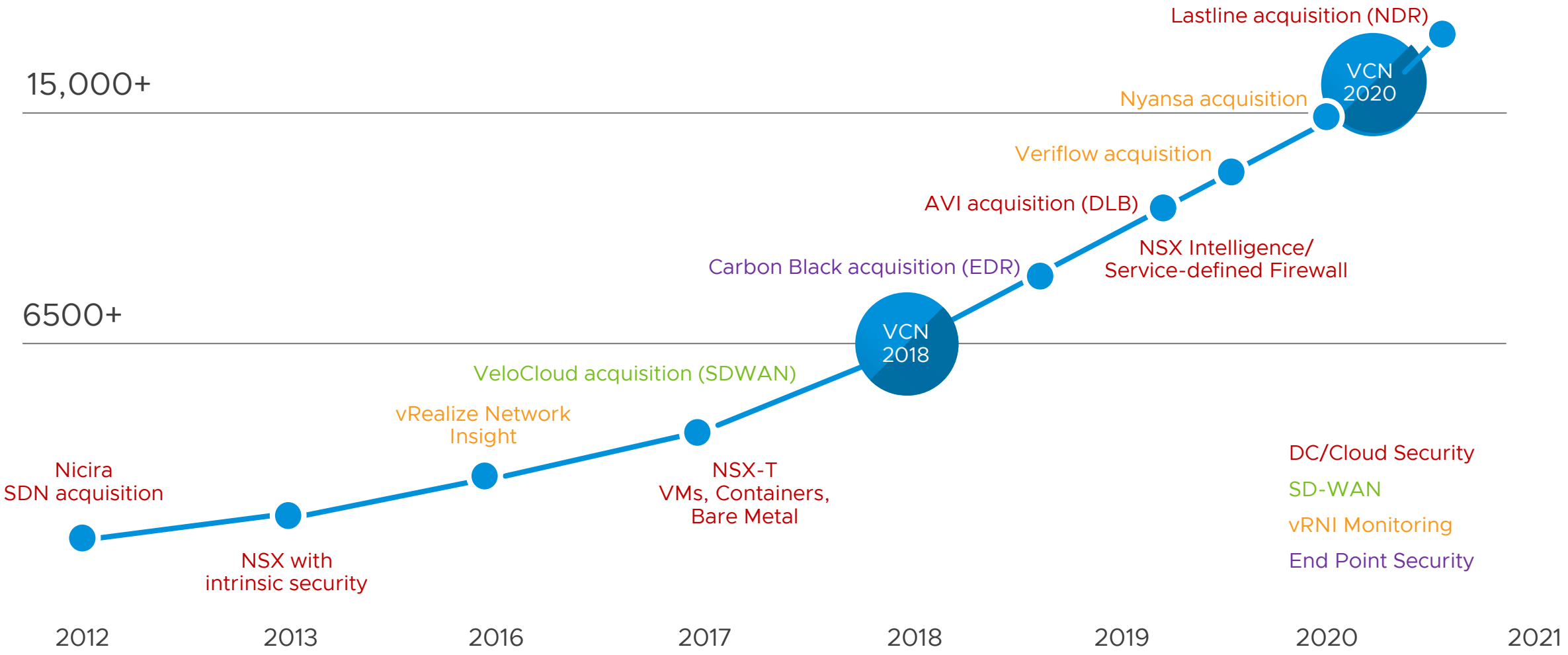
VMware Security Vision

Control Points across the Infrastructure and Endpoints

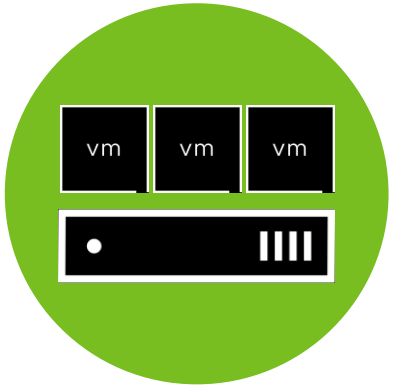


VMware Security Journey

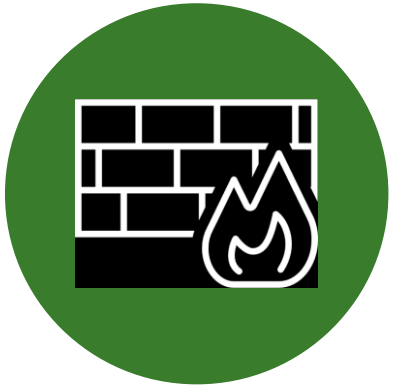
far beyond standard



VMware Security Solutions



Endpoint / Workload Security



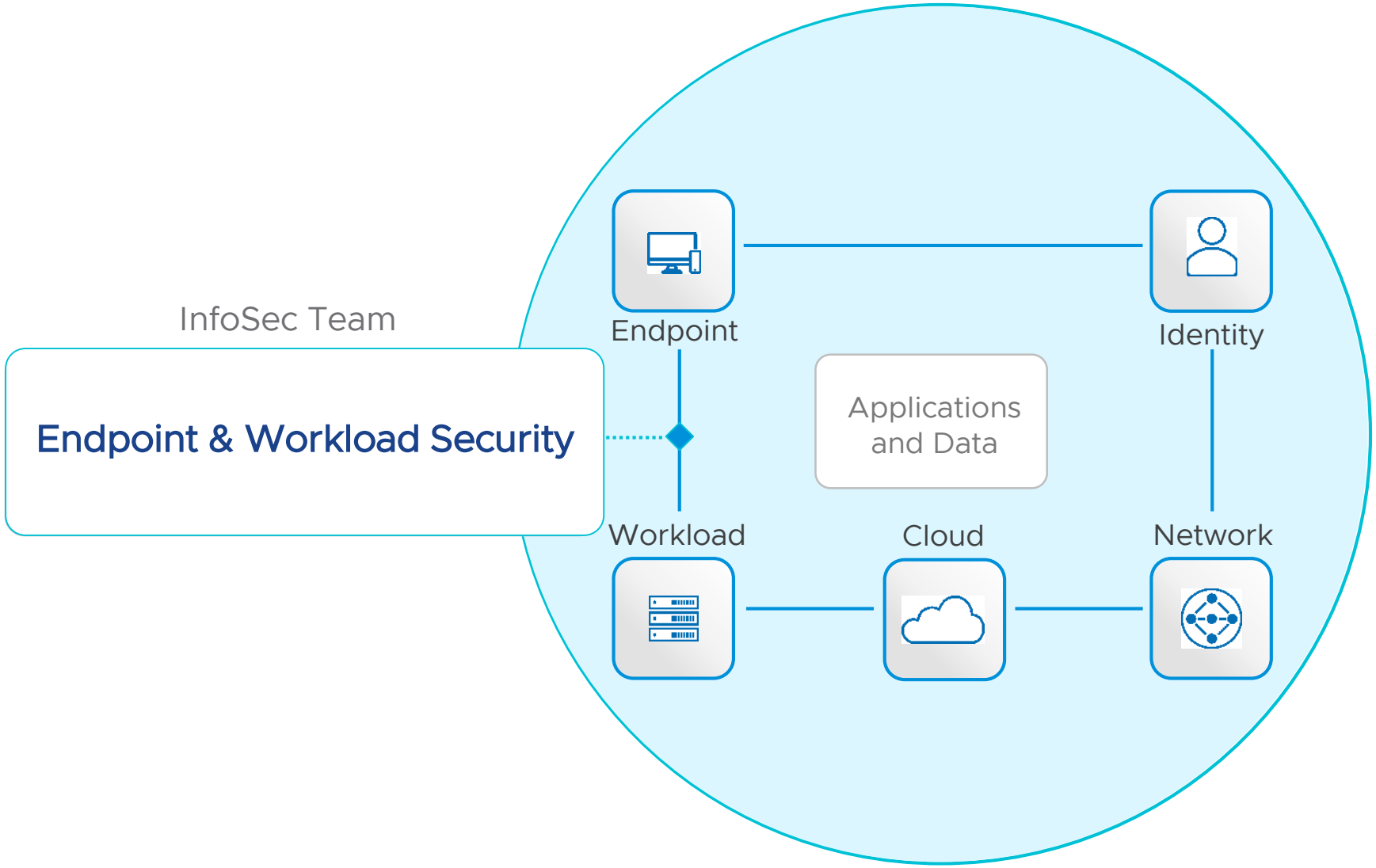
Network Security

Workspace Security

Cloud Security

VMware Security Solutions

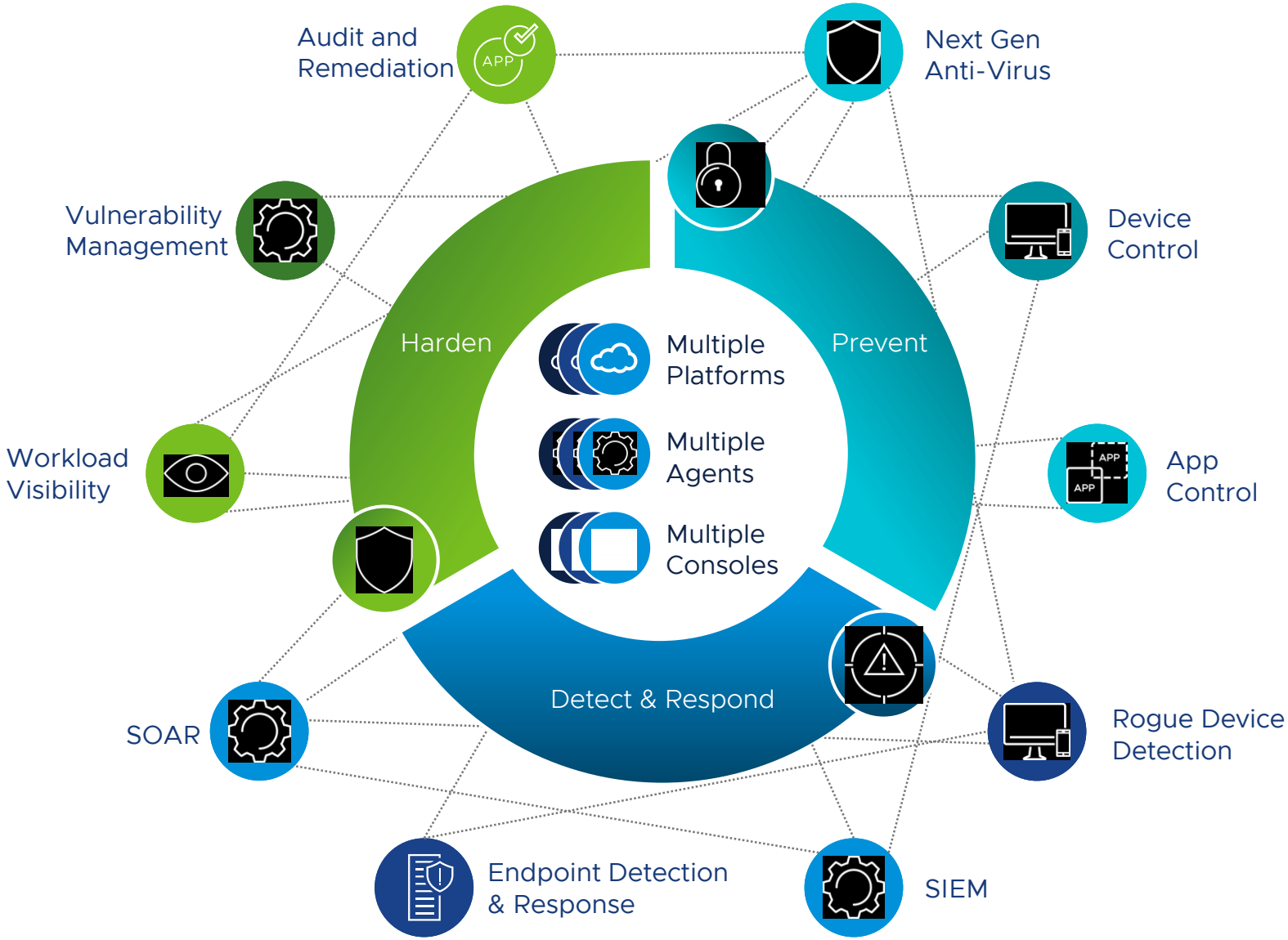
Intrinsic Security



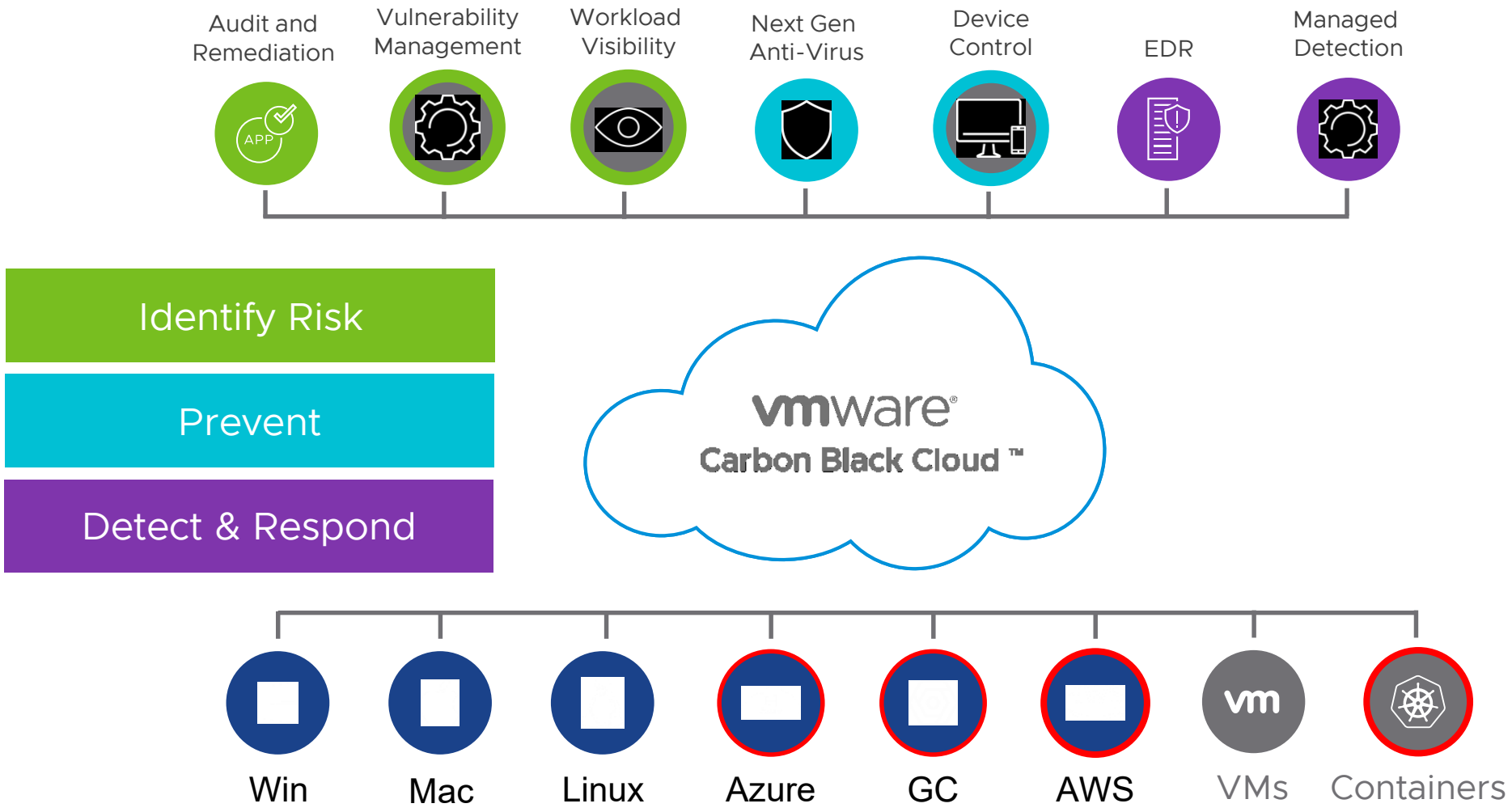
Securing Endpoints & Workload

Challenges

- Information Siloes
- Different Languages
- Different Processes
- Different Truths
- No Context

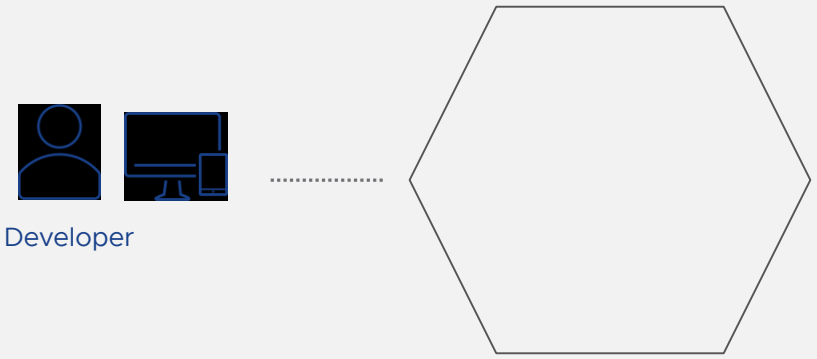


VMware Carbon Black Cloud



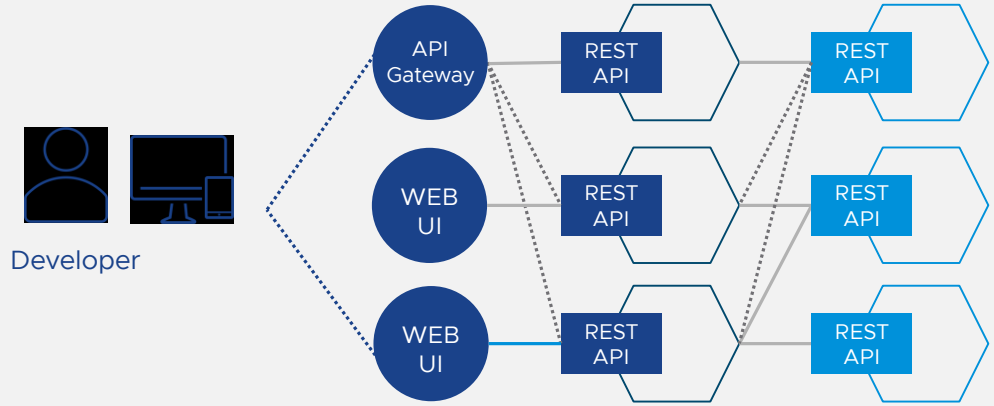
The Definition of an Application Has Changed

An application used
to be built as a monolith



Single, large code base

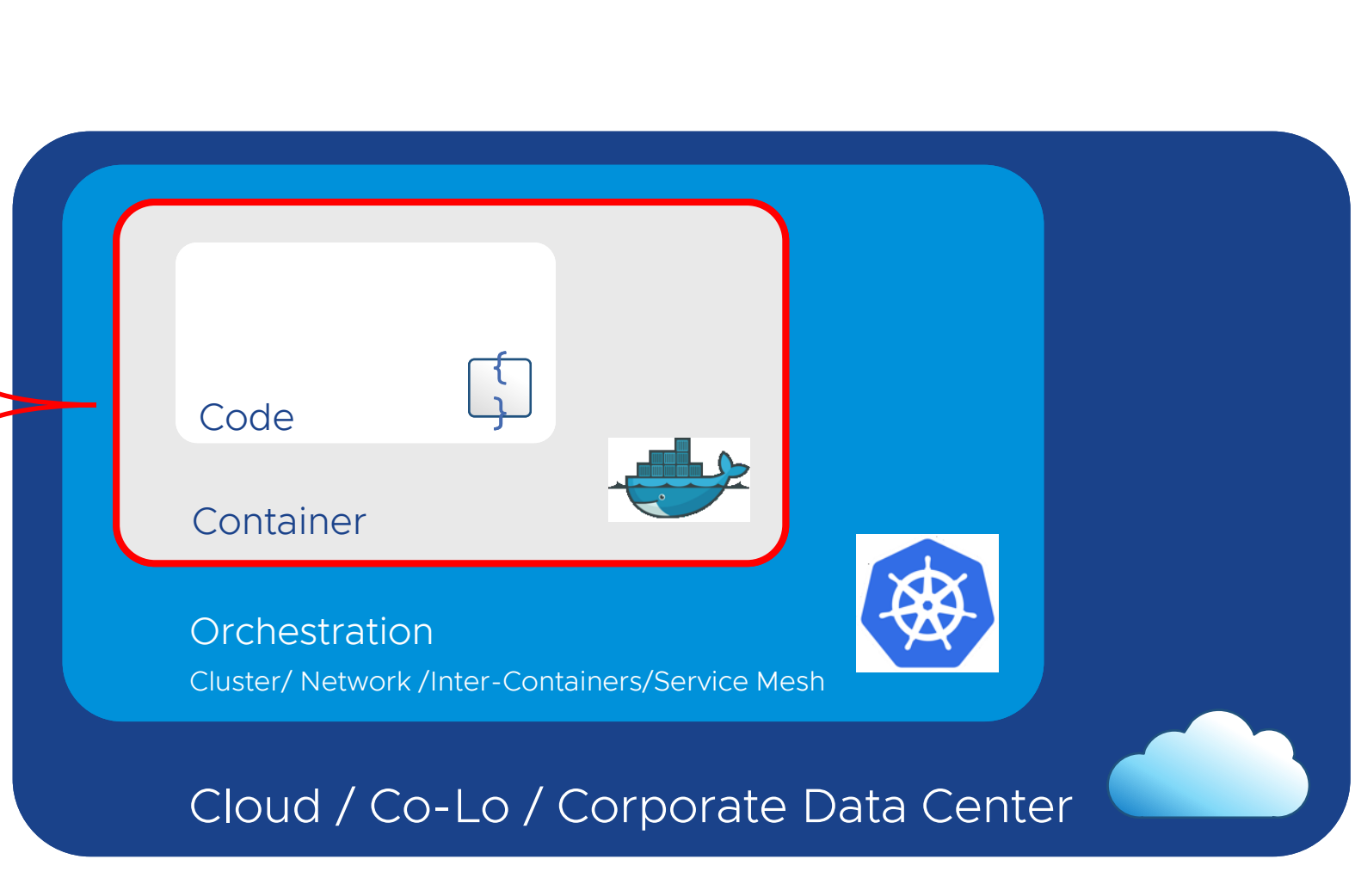
Modern apps are built with
microservices and APIs



Small, modular code base

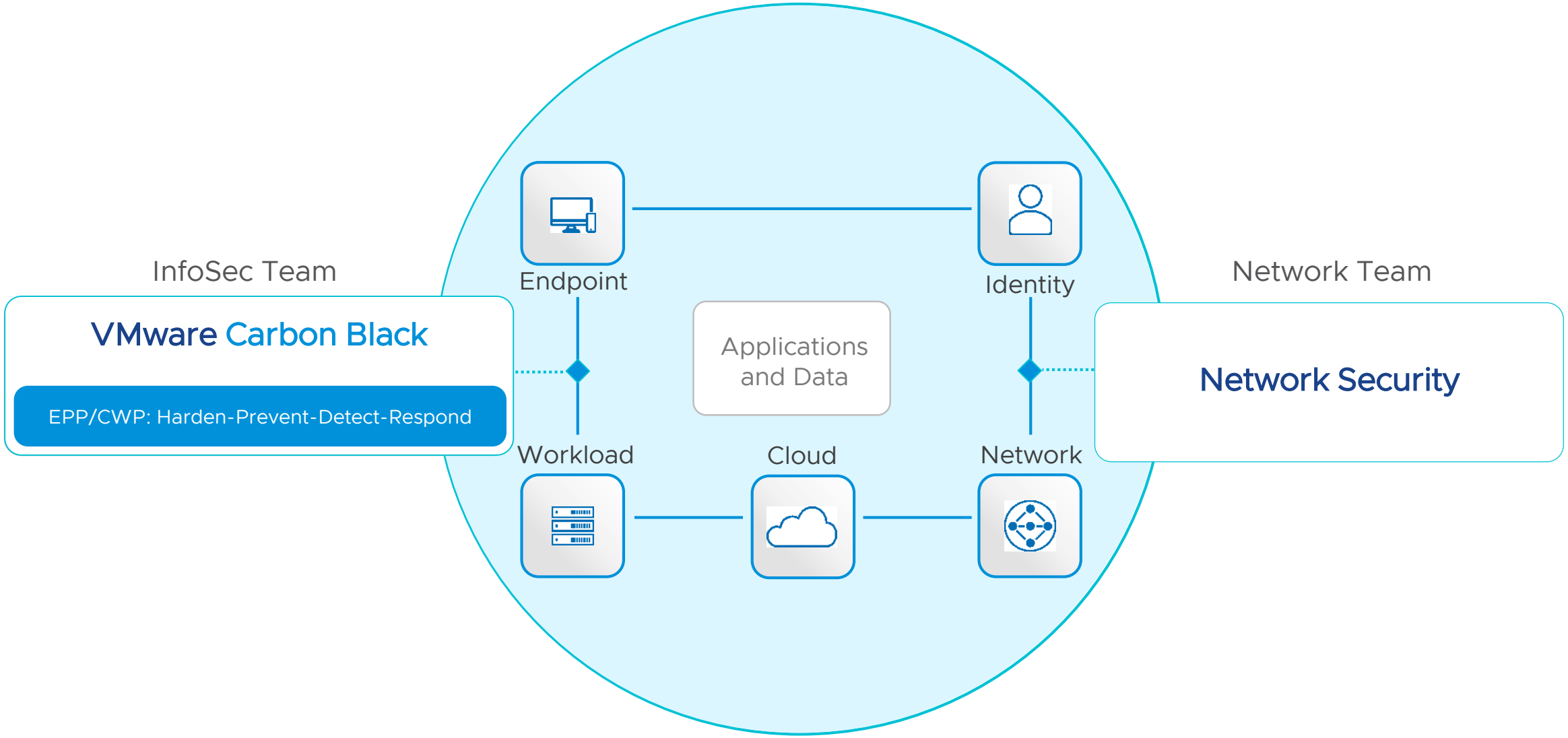
5 Common Container Security Risks

1. Using **unsecured images**
2. Containers running with the **privileged flag**
3. **Unrestricted comms** between containers
4. Containers running rogue or **malicious processes**
5. Containers **not properly isolated** from the host



VMware Security Solution

Intrinsic Security

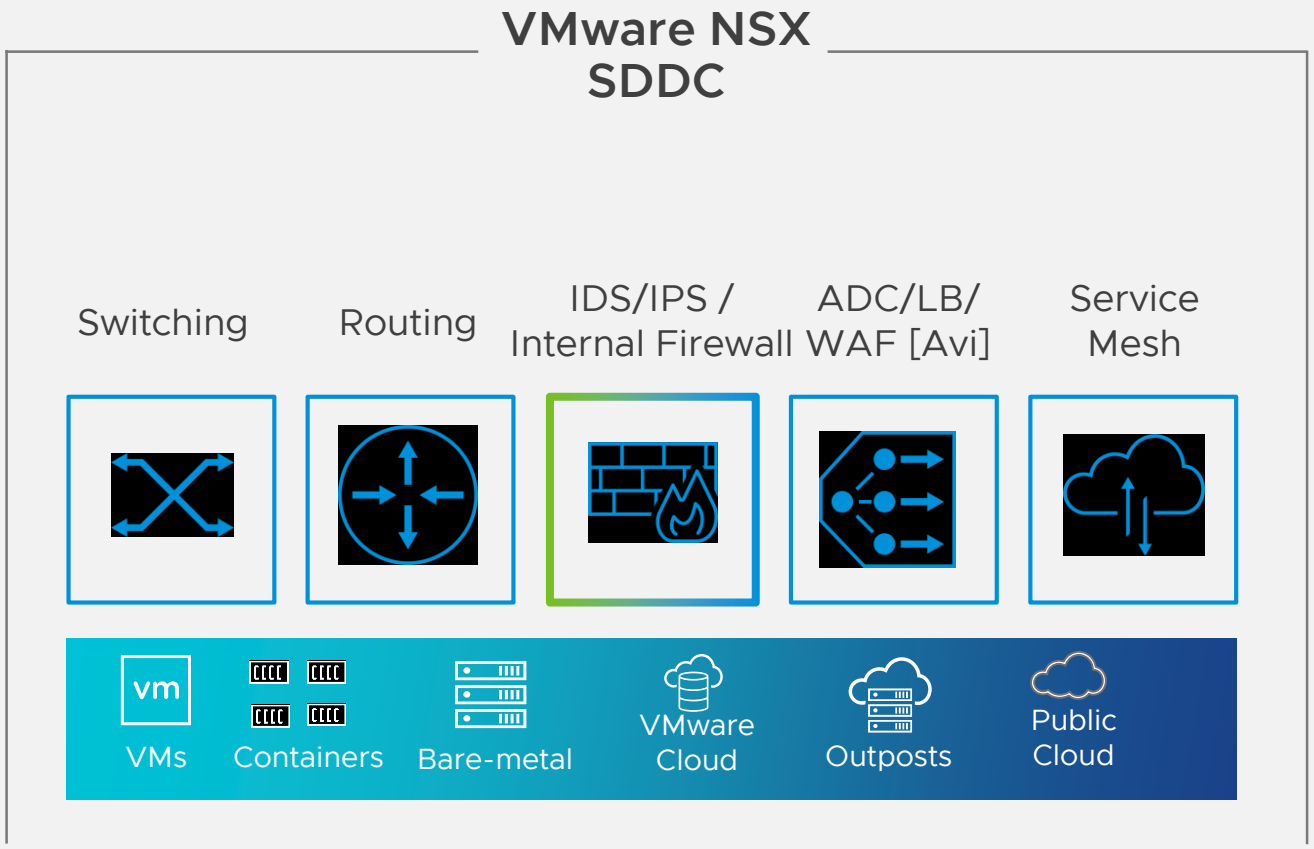


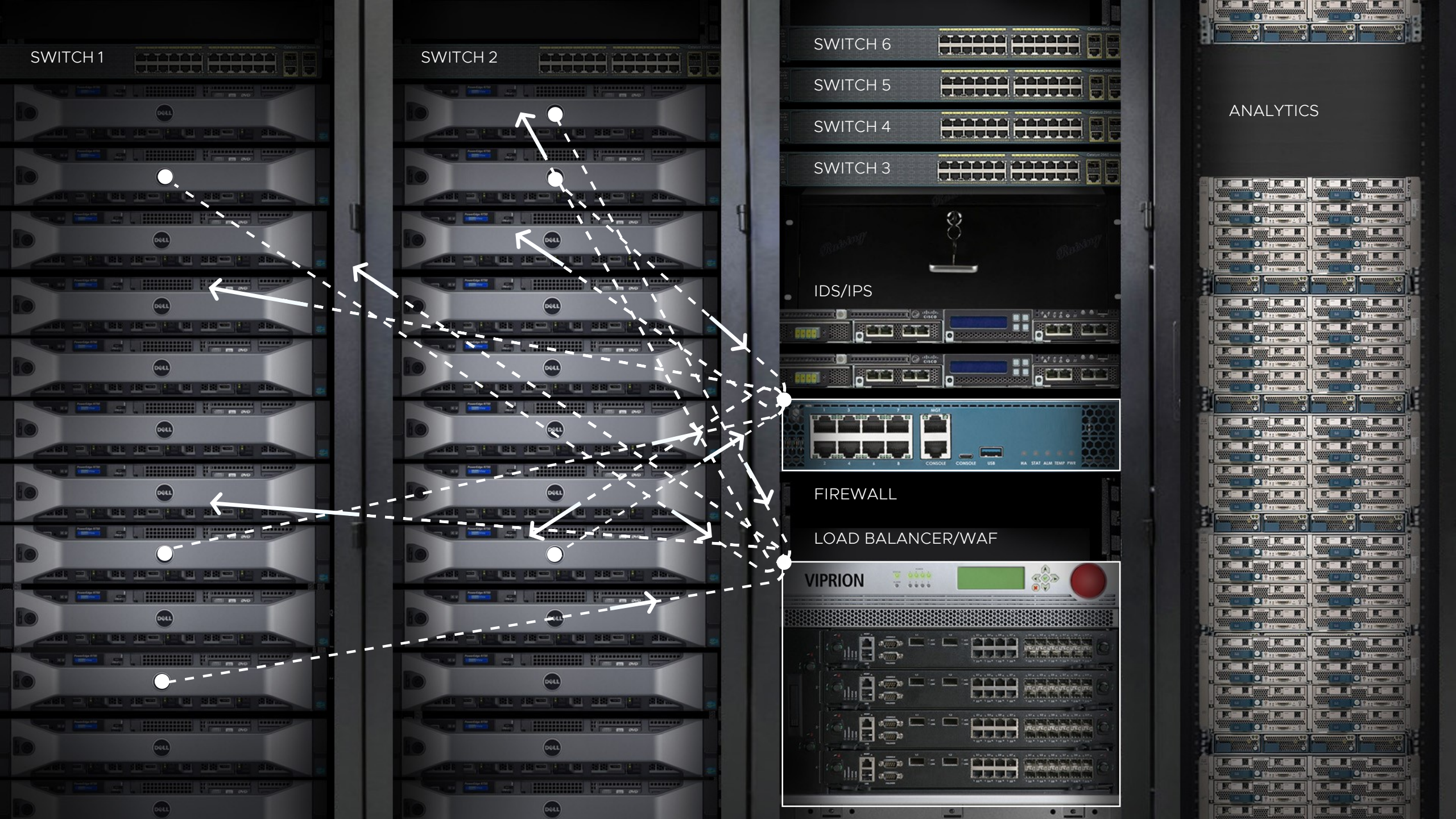
Network Security

VMware NSX

NSX Full DC Networking and Security

VMware




SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
VIPRION
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS

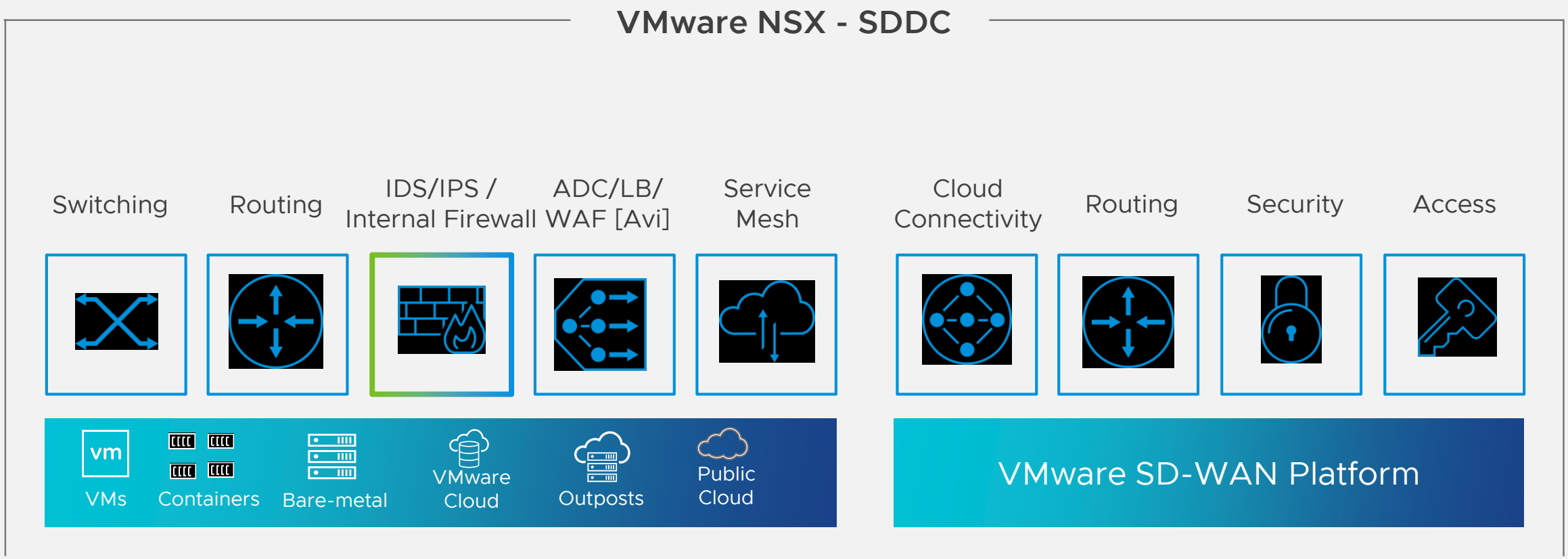

SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
IDS/IPS
FIREWALL
LOAD BALANCER/WAF
ANALYTICS


SWITCH 1
SWITCH 2
SWITCH 6
SWITCH 5
SWITCH 4
SWITCH 3
SWITCH 2
NSX

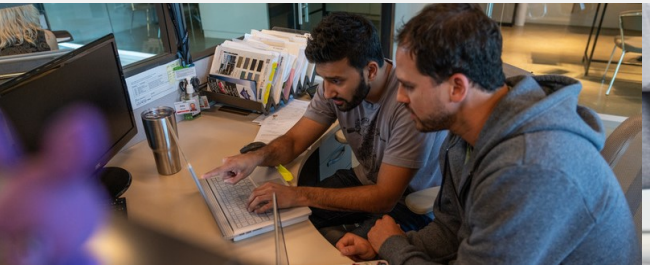
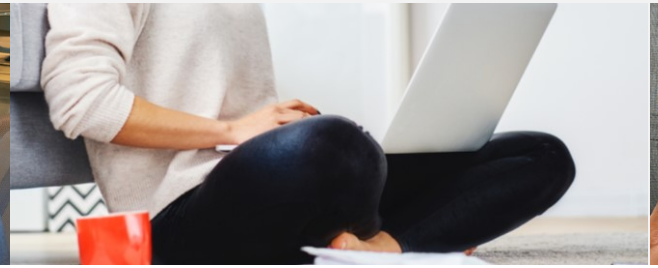
VMware NSX

Network virtualization and Security

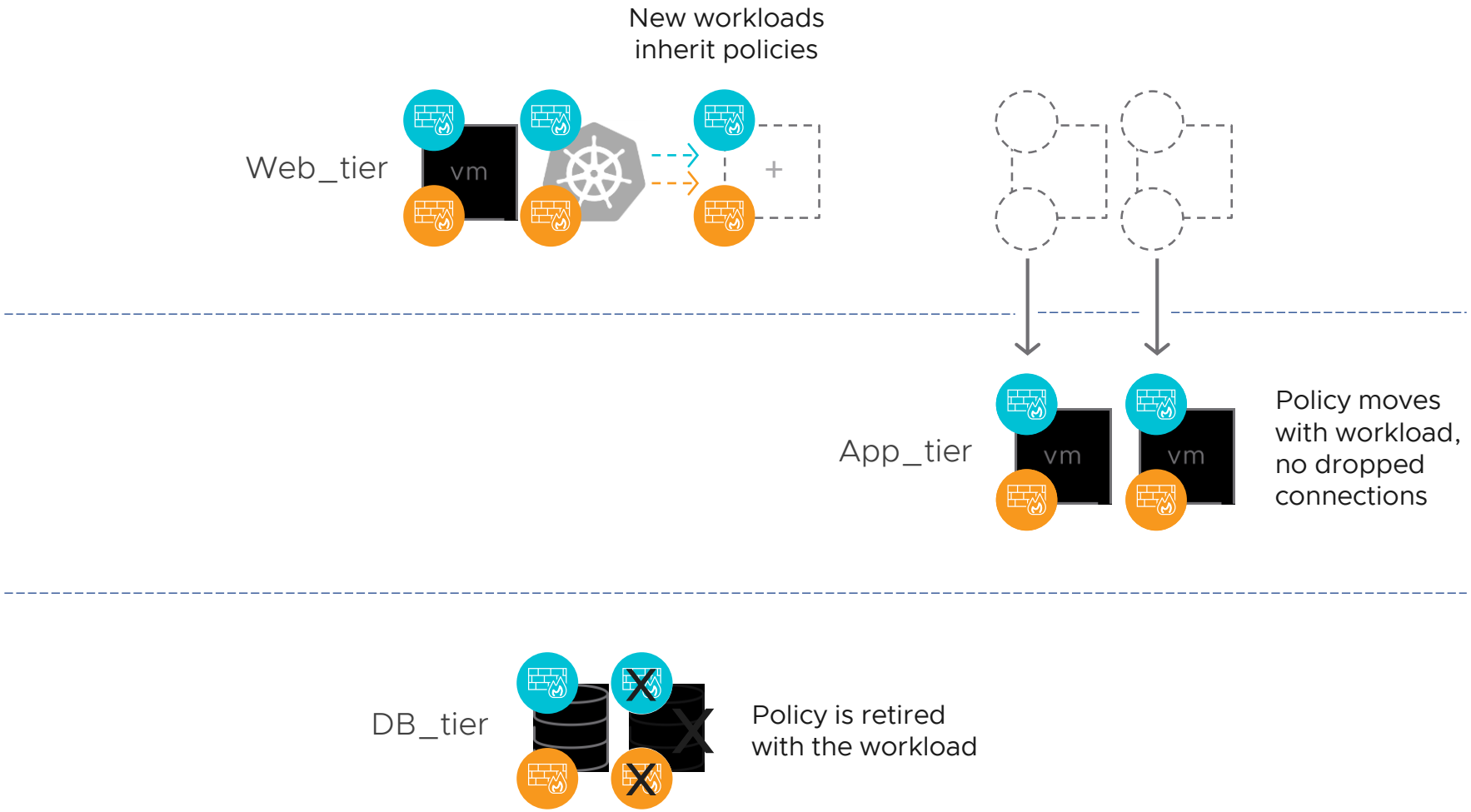


Key Use Cases

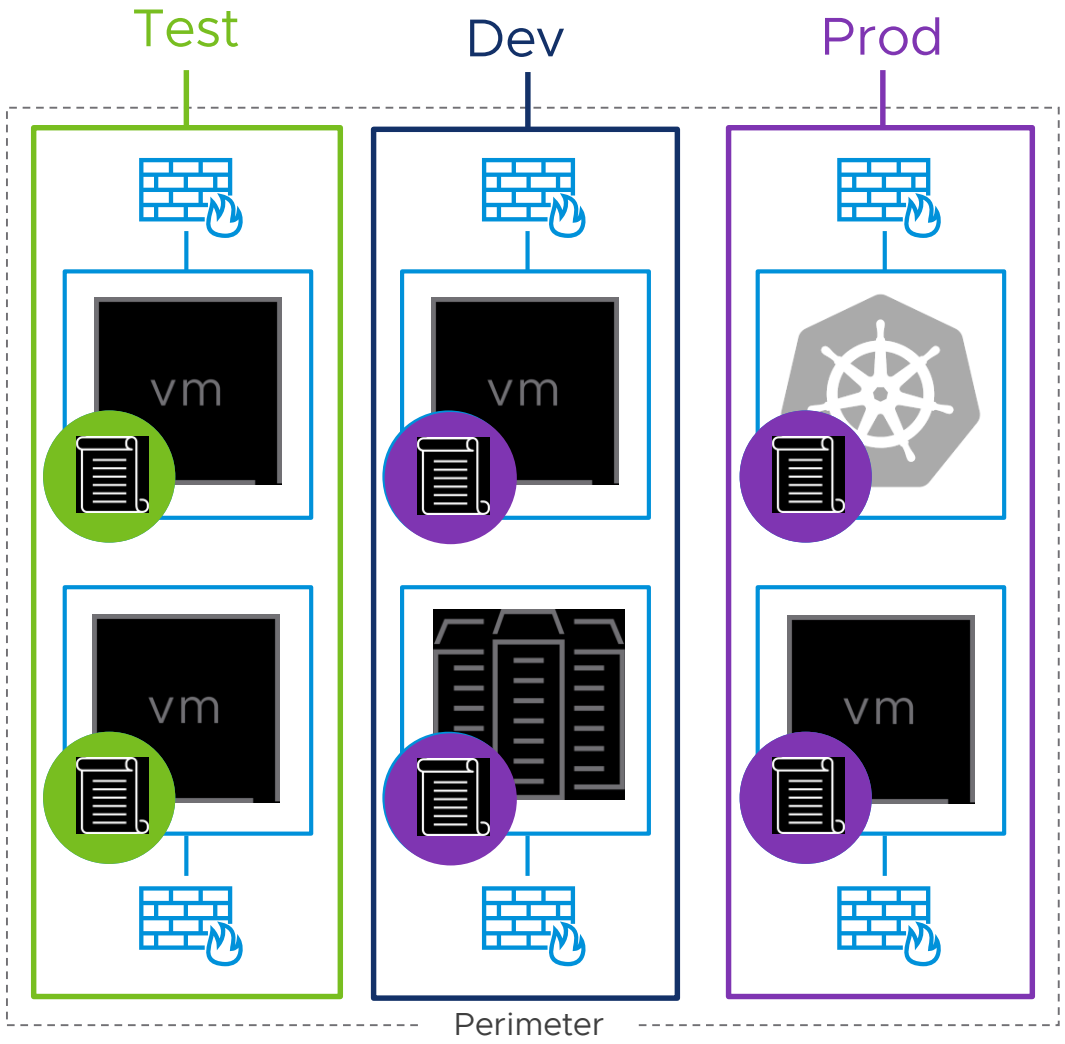
Network Segmentation	Secure VDI	Compliance	Appliance Consolidation
Create Zones in software with no network changes Quickly segment using existing constructs	Stop lateral movement of attackers by blocking vulnerabilities Stop malware from spreading in VDI environments	Easily achieve compliance for PCI-DSS, HIPAA, SOX Eliminate blind-spots	Replace discrete centralized appliances Use native distributed IDS/IPS capabilities in NSX—simply “turn it on”

NSX Service-defined Firewall: Massively Simplifies Operations



Network Segmentation



Use existing objects

- Test/Dev/Prod
- Network/Tags

Quickly achieve compliance

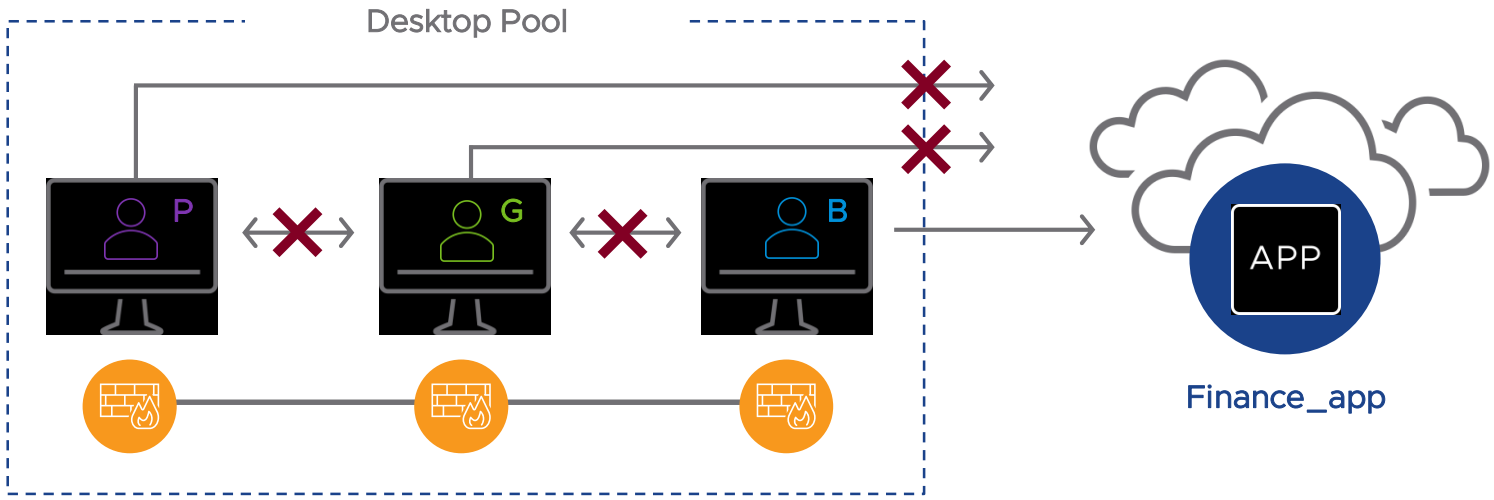
Quickly deploy independent of scale

Immediate application level visibility

No network changes

~85% of data center traffic is East-West

Identity Based Firewall - Secure VDI



SIMPLE RULES

User B in Desktop Pool can access Finance_app

Users in Desktop Pool cannot talk to each other

Deny communication between VDI instances

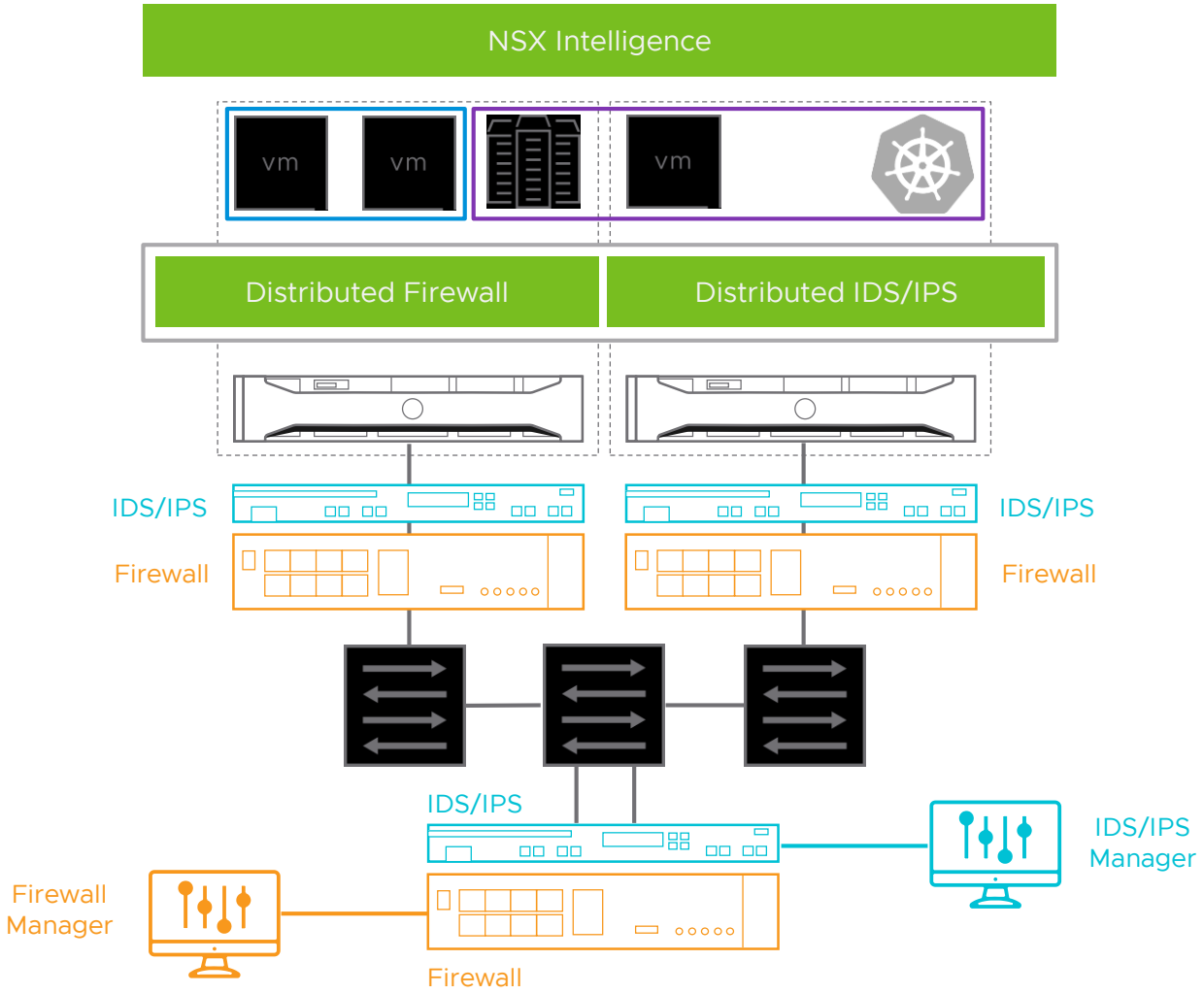
- Stop lateral malware movement
- Identity based policy

Use exiting user groups

Supported for both VDI and RDSH

Works with BOTH Citrix and Horizon

Internal Appliance Consolidation



Replace physical appliances

Unified management for Firewall and IDS/IPS

Move enforcement clos to the workload

Save time and money

Power and cooling

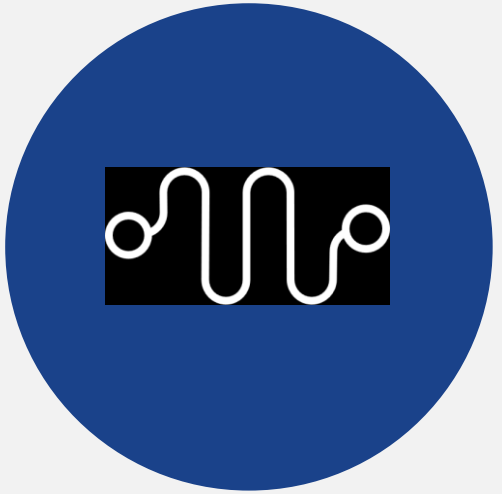
Operational simplicity

60% Reduction in traditional firewalls

Radically Change the Equation: Cost, Complexity, Capacity

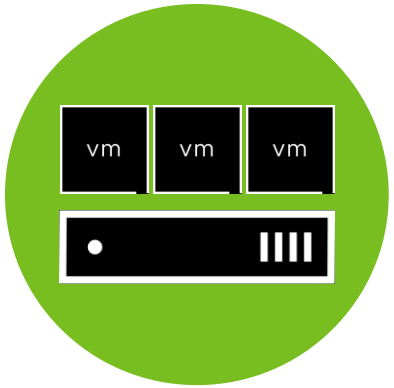
Simplified Network Architecture

Operational Simplicity



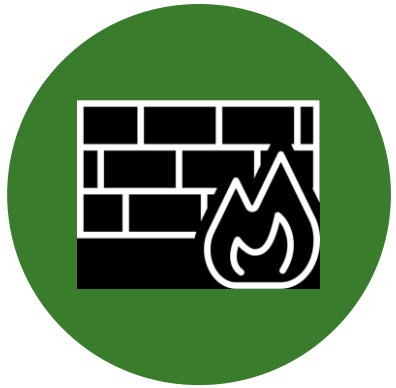
Distributed Performance

VMware Security Solutions



Endpoint / Workload Security

Advanced capabilities for endpoints and workloads: EDR, NGAV, visibility to identify risk and hardening based on behavior and intent



Network Security

Software-defined security services: firewall, IDPS, and WAF; fully distributed for E/W traffic in data centers, clouds, and the edge

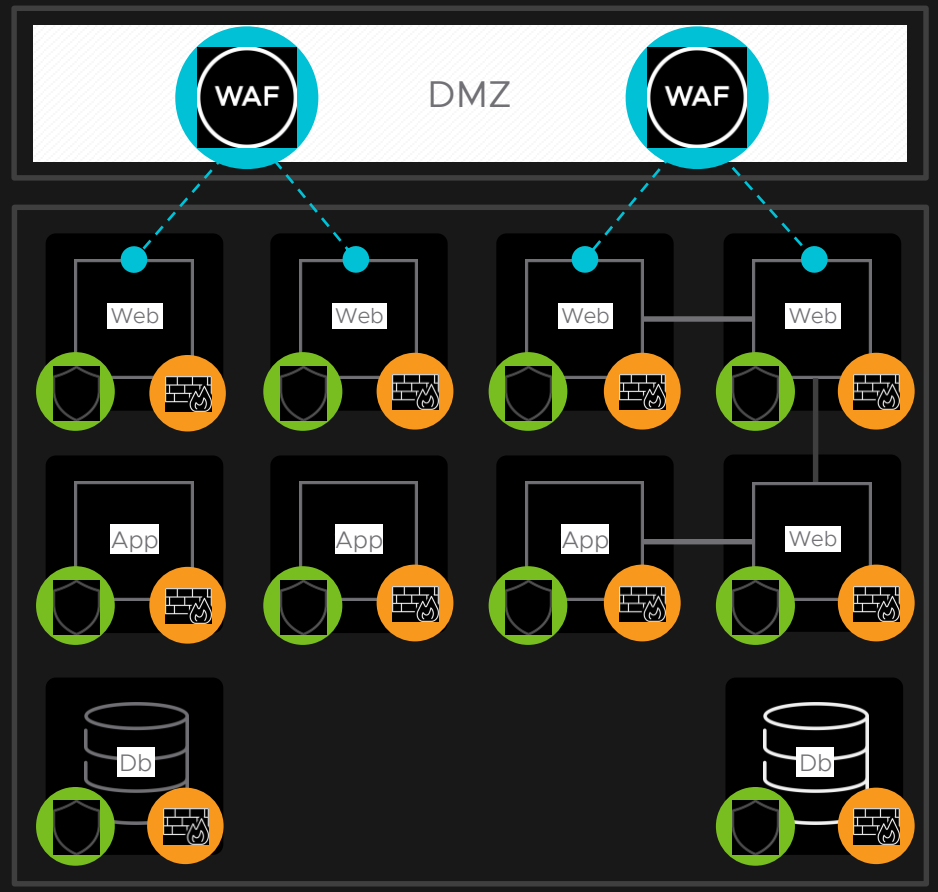
Workspace Security

Modern management and EDR capabilities for a Zero Trust approach to endpoint security while providing an exceptional user experience

Cloud Security

Ability to detect security misconfigurations, monitor compliance and scale best practices to teams using public cloud infrastructure providers

VMware - Best In Class DC Security



VMware NSX Advanced
Load Balancer/WAF

VMware Carbon Black
Workload Protection

VMware NSX
Distributed Firewall

Thank You