



VMware Security ...and not only

Overview

Pavel Kovář

Senior Solution Engineer / VMware

5.5.2022

Security is Fundamentally Broken

Digital Risk Management

crisp CYBERSPRINT digital shadows_ DigitalStrikeout
EXPANSE LOOKINGGLASS NAMO-G-O-O FISHLABS
RISKIQ SafeGuard Cyber FIDELITY ZEROFOX

Mobile Security

appdome BETTER StackBerry blue cedar Fyde
Check Point cellrox COMMUNITAKE CyberodAPT
INMEDI0 KODOLPRN Lookout mobletron
CO pradeo KAVITA PSafe SaltDNA alert drive SOTI
Synaastac TeleSign antigerntext TRUSTLOOK
VULTO wafers wickr ZIMPERUM

Endpoint Security

AhnLab avast Avecto Avira Baidu
BINARY DEFENSE BLUEBOLT BUFFERZONE Carbon Black
Check Point COMODO CROWDSTRIKE CYBERARK
cybereason CYLANCE deepinstinct ENDGAME
ERICOM ESSENTIAL F-Secure FORNICS FORTINET
HYSOLATE Integro ivanti Kaspersky McAfee
Microsoft MORPHSEC NYOTRON OPSWAT panda
SentinelOne SAPHOS sparkognition symantec
Synaastac TETRIS WEBCOAT ZEN

Data Security

ANJUNA boffle boxcrypter CipherCloud CLOUDMASK
CryptoMove DATABLOCKER Fortanix NUCYBER VINTU
dearswift CODE42 FIDELITY McAfee
Synaastac BlueTalon druid openext SECOLINE

Block Chain

Chain guardtime DEE NuID remme
vchain ShoCard xage

Security Operations & Incident Response

BlackStellar CORRELOG CYCLANT DEVO
esbeam FORTINET HanSight HUNTRESS IBM RSA
IGLOO JASK logentries logpoint #LogRhythm
logio McAfee PAGER Palantir SANS SECURIX
solarwinds splunk sumologic TIBCO Trustwave
starlabs Cayla CYBERM Day One DASTRACE AWAKE
CROWDSTRIKE COMAND
DEMISTO DELIA FIREYE mistnet observe.it
Microsoft Minsight radar RAPID
servicenow SENSIFY SET
SWILANE thycor THETARAY
ThreatConnect UPLEVEL VERINT VECTRA SECURIX

Threat Intelligence

4i@ Blueiv ANOMALI 100M00LAGE NUCLEON
Blueviant Centripetal CISO Recorded Future EXINTELLIGENCE RISKIQ
digital shadows_ DOMAINTOOLS SenseCy Shogun SURFWATCH
Oleclotick F-SIGHT GROUP SpyCloud ThreatConnect
FLASHPOINT HanSight Minus ThreatMetrix THREATQUANTUM
INTELLAT INSIGHTS KELA ThreatGRID TRUSTAR WEBCOAT

Cloud Security

anchore aqua deepfence FIREWALL GUARDICORE TRUST
NaiVector POLYVERSE portable threat stack ARMOUR AVANAN
Quayis StackRox Sysdig ThreatMetrix Microsoft netscope
Twistlock AWS natively AWS SUMO Lockwork SHIELDX
SPACETEC cavin Check Point bltglass CyberCloud CISO FORNET
Cloud Custody CLOUDWAY CYBERARK

Risk and Compliance

AXONIOUS Balabit cavin CLOUDSERVER
cyber GRX DELVE FIREHORN KENNA
infosec NOPSEC OPAG Outpost24
panasas MEVALINT REUSEAL riskrecon
skybox Tenable UpGuard VENAFT
Zeguro BITSIGHT CORAX FICO RiskLens
SecurityScorecard FORTINOS Cobalt CROWDSTRIKE
CYBERRAT CYCLOPS CVMULATE JETIN
MAZEBOLT PCOYS PICUS
RAPID ESafesearch VERODIN
algosec ESOLIFE Lodgpath MetricStream
netwrix Onspring RESOLVER RSA
Barracuda CyberVista SAGLOBAL
IRONSCALE proofpoint RANGEFORCE

WAF and Application Security

Acan Acan Acan Acan
Barracuda CloudSec check ergon THREATX
Barracuda FORTINET
Imperva NETSPI Onapside TEMPLARIT
netwrix ONESIDE THYR VSPACK STACKPATH
Quayis CRACLE wallarm VULNUS
portafit PURISSEC lockness 360WORKS
RAPID RAVEN RAVEN RAVEN
Rapid7 Radware Rapid7
Santitas AWAKE BRODATA
DASTRACE Extremepoint
PERCH Piber SSR

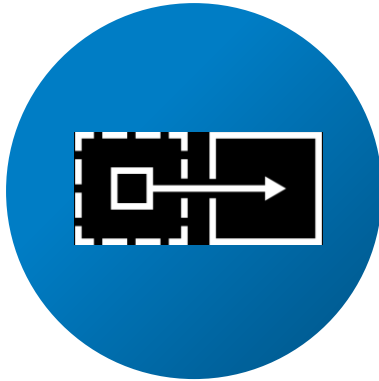
Identity & Access Management

Accepto Auth0 Caveron BehaviorSec BIOCATCH Collign
CORE DEO EXO-STAFF FUDU Google
Impactor INTEKID NOK pingpp PLOIN SASPASS
transit SECUREPUSH SILVERFIN tascant ThredMaltix
TransUnion TRUSONA UNBAND UNEN VKEY VIRSA
Cantrity IBM idaptive Microsoft okta RSA HPR
onelogin ORACLE THALES BeyondTrust PAGER
CYBERARK HITACHI ManageEngine ONE IDENTITY
Remediate SECURELINK THYR Axiomatics Duxify
helpsystems SafePoint simelo CAMEL Experts
logradius Tulco vchain verato VERIFF IDMS

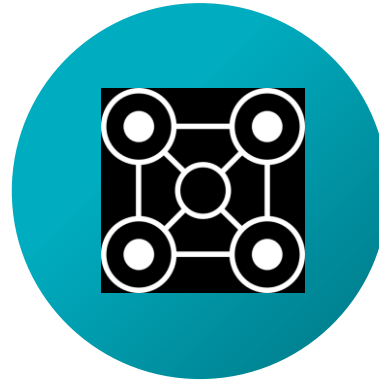
Network & Infrastructure Security

Barracuda BLUEHEXAGON BLUVECTOR CISCO SCORSA
FIREYE FORTINET HUMAN HYSOLATE JOSSecurity JUNE
minicast OPSWAT paloalto RESEC SATELLITE SONICWALL SAPHOS
Symantec BLUE ARUBA BLUEWAVE AXONIOUS Cyber-Quad
Barracuda EDR GIGABYTE MANAGED SYSTEMS VULNUS
Trustwave Zenoss GIGABYTE VULNUS
Check Point Imperva neustar HUMAN VULNUS CRACLE Corelight
netwrix STACKPATH BLUECAT neustar ThreatGRID Quad9 MidMode
Lodgpath Infoblox algosec CARO CLOUDVIEW FIREHORN lastline
endian Fortinet GIGABYTE HUMAN OPAG SANS McAfee
secucloud SONICWALL STOREHOUSE HUMAN FIDELITY ACALYPS
Algo Counter Craft VULNUS CyberThreat SANS VERINT
CyberArk TRAPX APENIO BRYSHORE BELDEN CIPHERNET NISSE
CYBERM FIRMATA Indegy SANS CARV NETSCOUT
CyberX DRAGOS ALPES RHEBA CORE
CloudShark ulinacco OREYCORTEX

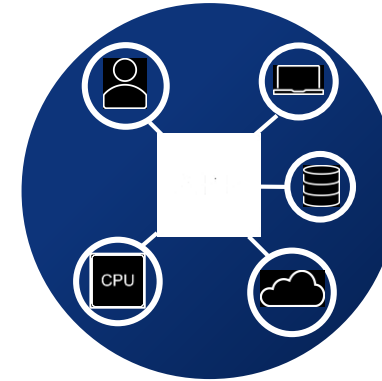
Security Must be Transformed



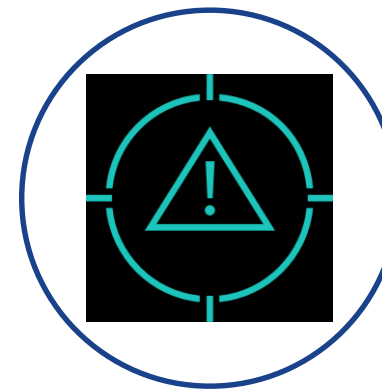
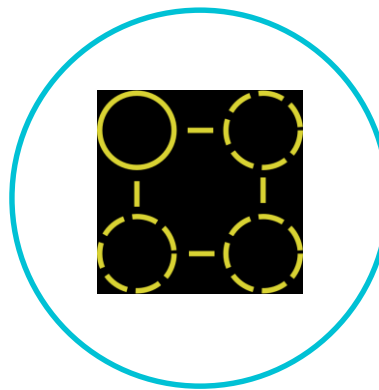
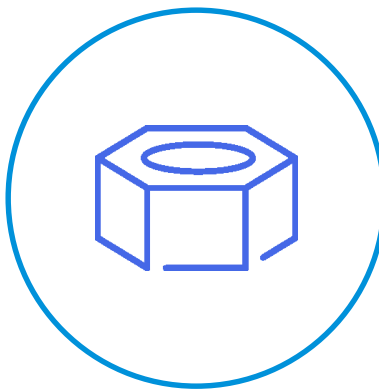
Built-in
Bolted-on



Unified
Siloed

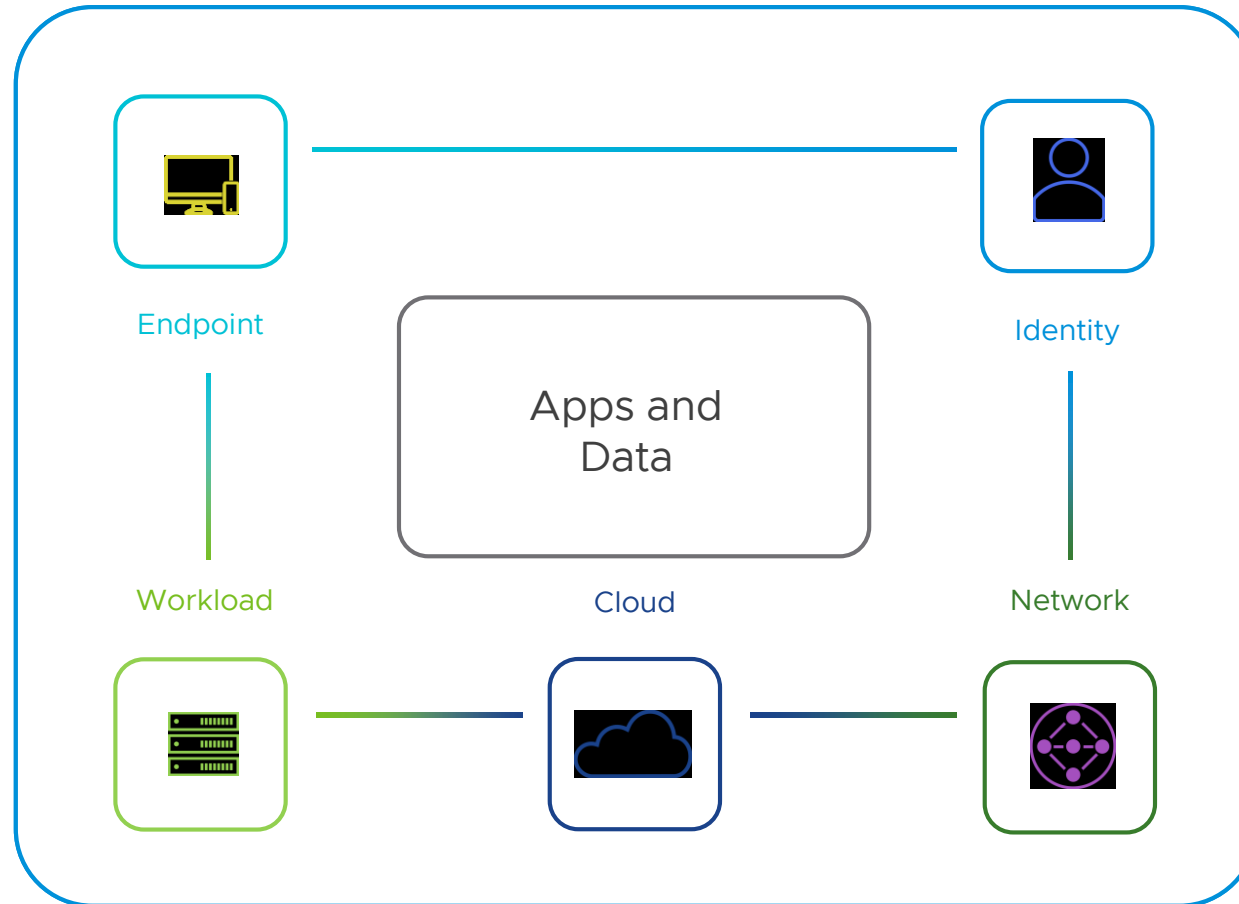


Context-centric
Threat-centric



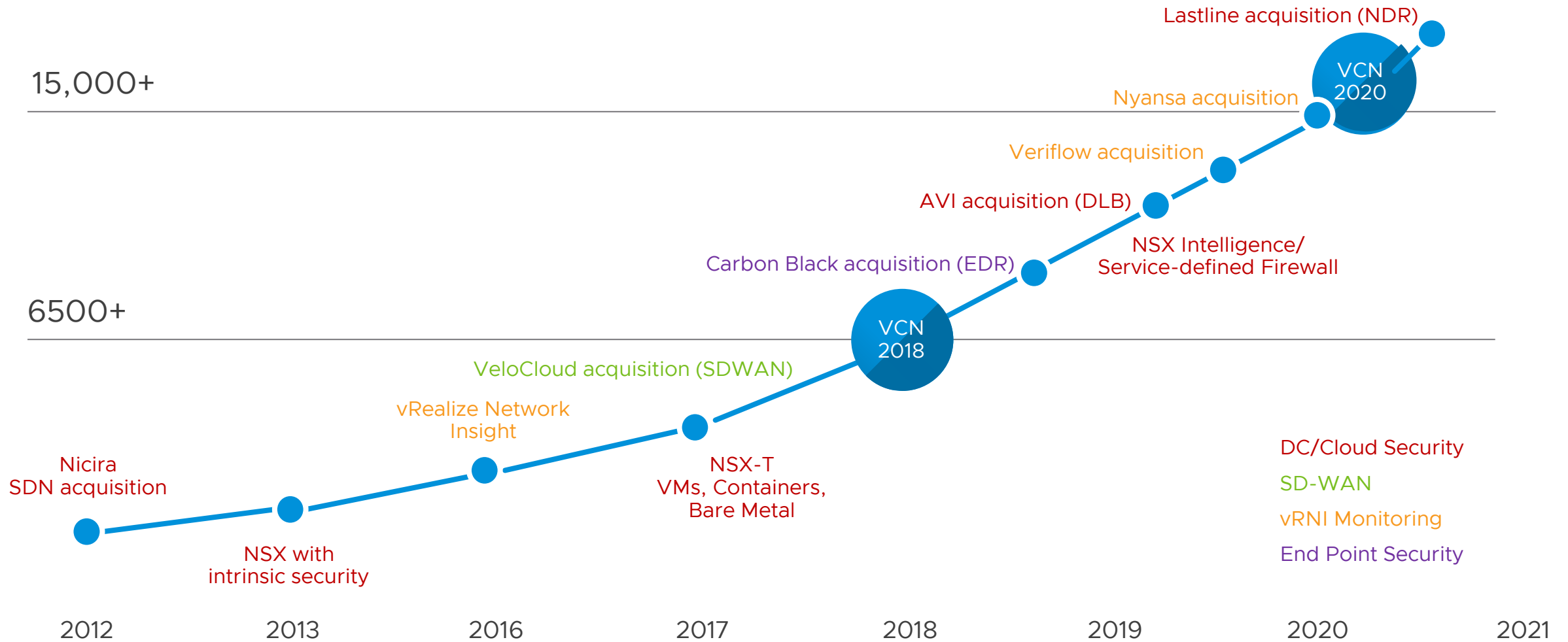
VMware Security Vision

Control Points across the Infrastructure and Endpoints

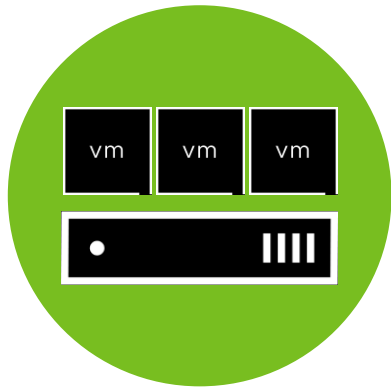


VMware Security Journey

far beyond standard



VMware Security Solutions



Endpoint / Workload
Security



Network Security



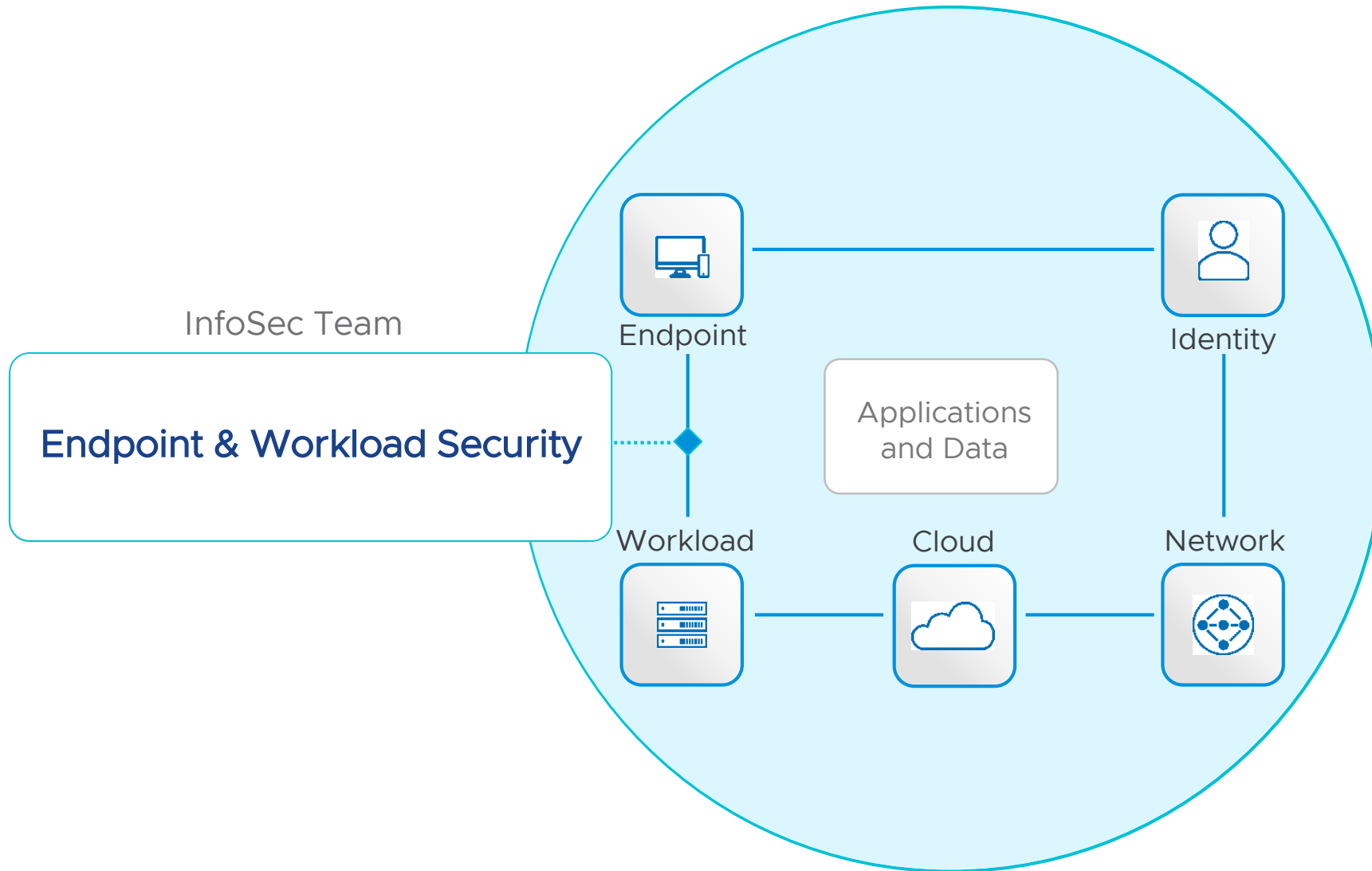
Workspace
Security



Cloud Security

VMware Security Solutions

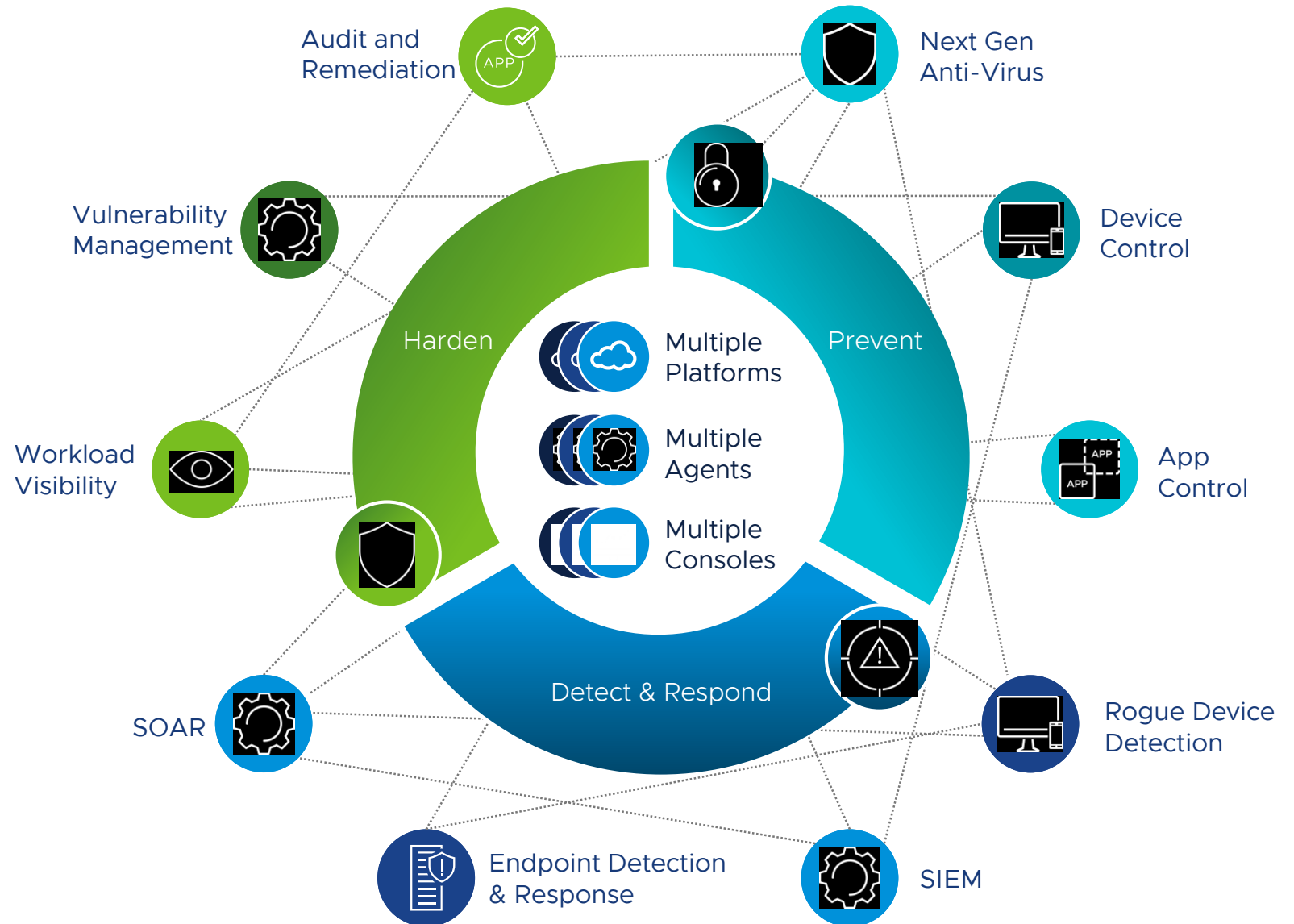
Intrinsic Security



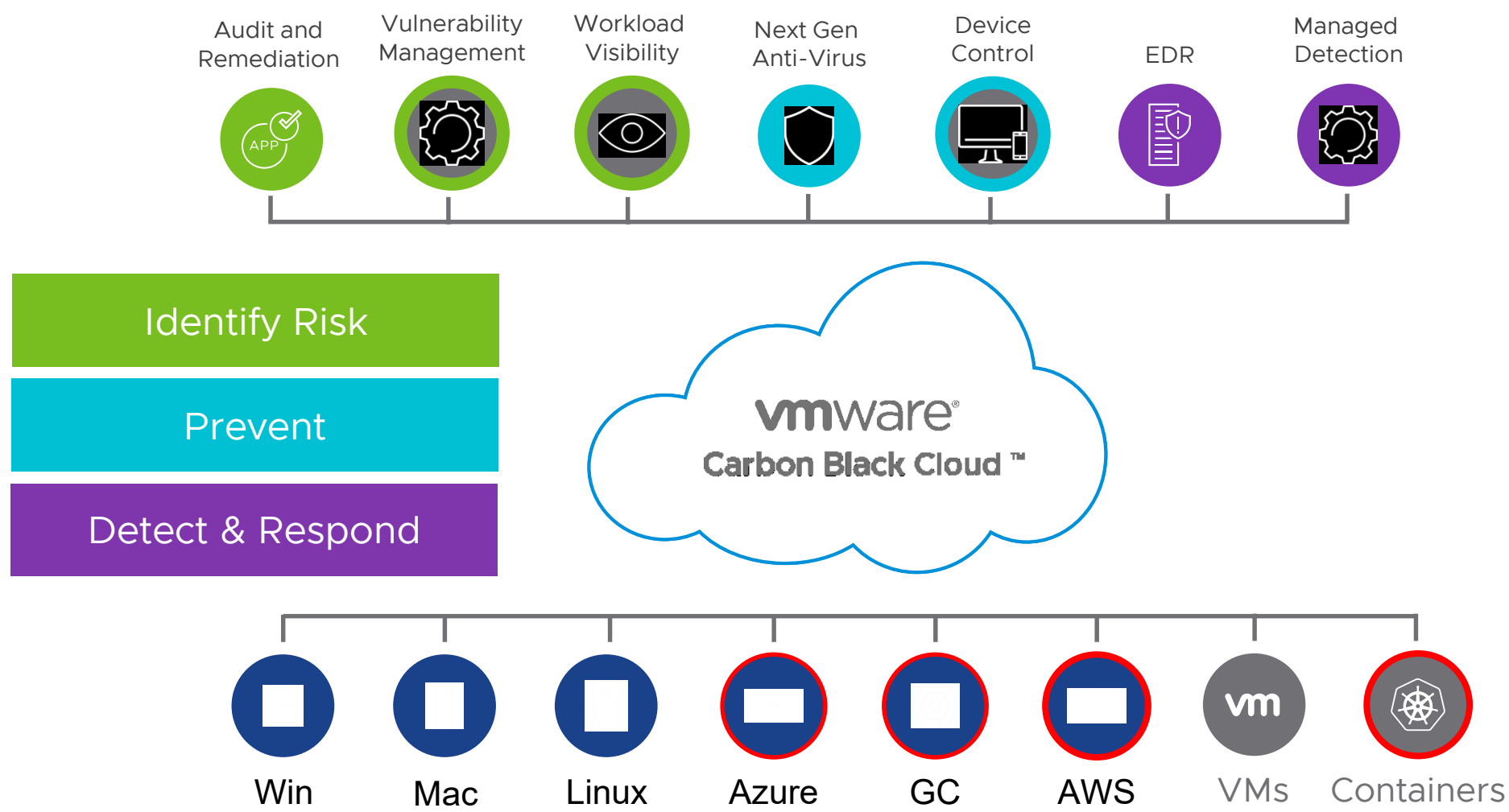
Securing Endpoints & Workload

Challenges

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

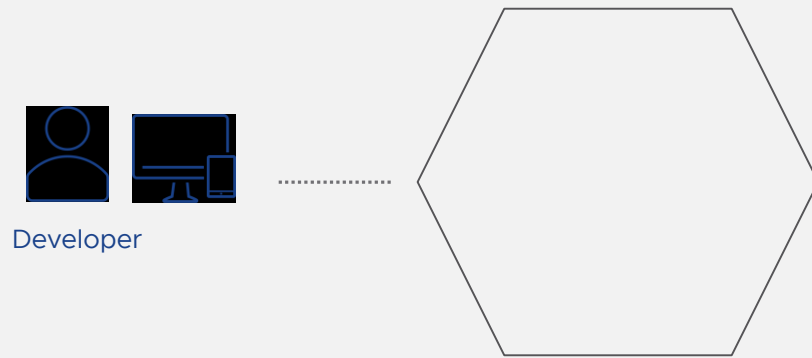


VMware Carbon Black Cloud



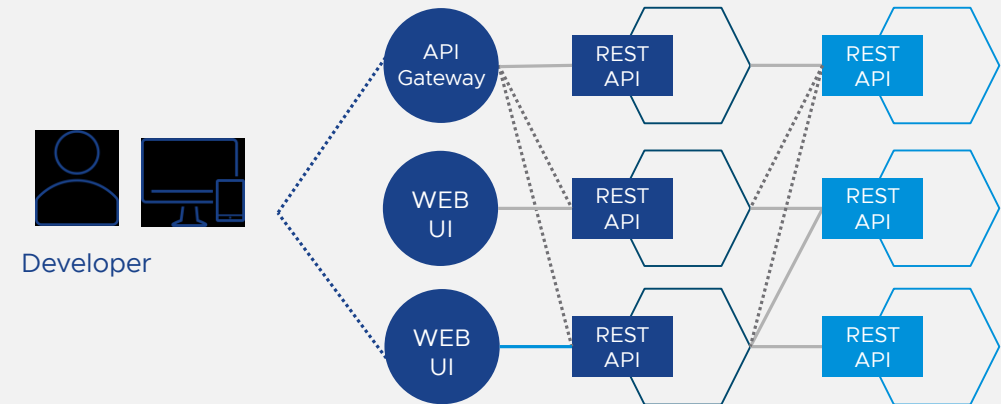
The Definition of an Application Has Changed

An application used
to be built as a monolith



Single, large code base

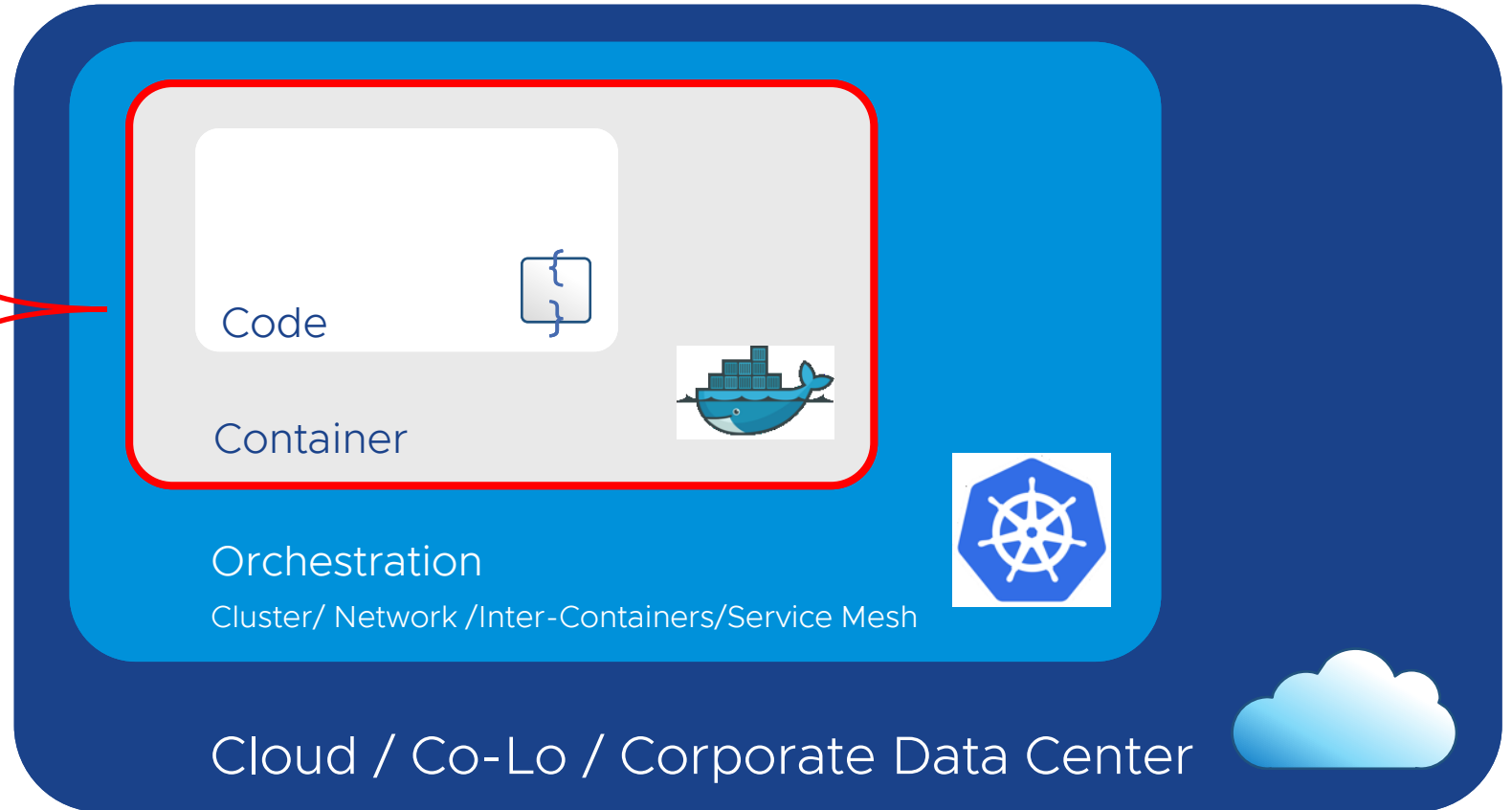
Modern apps are built with
microservices and APIs



Small, modular code base

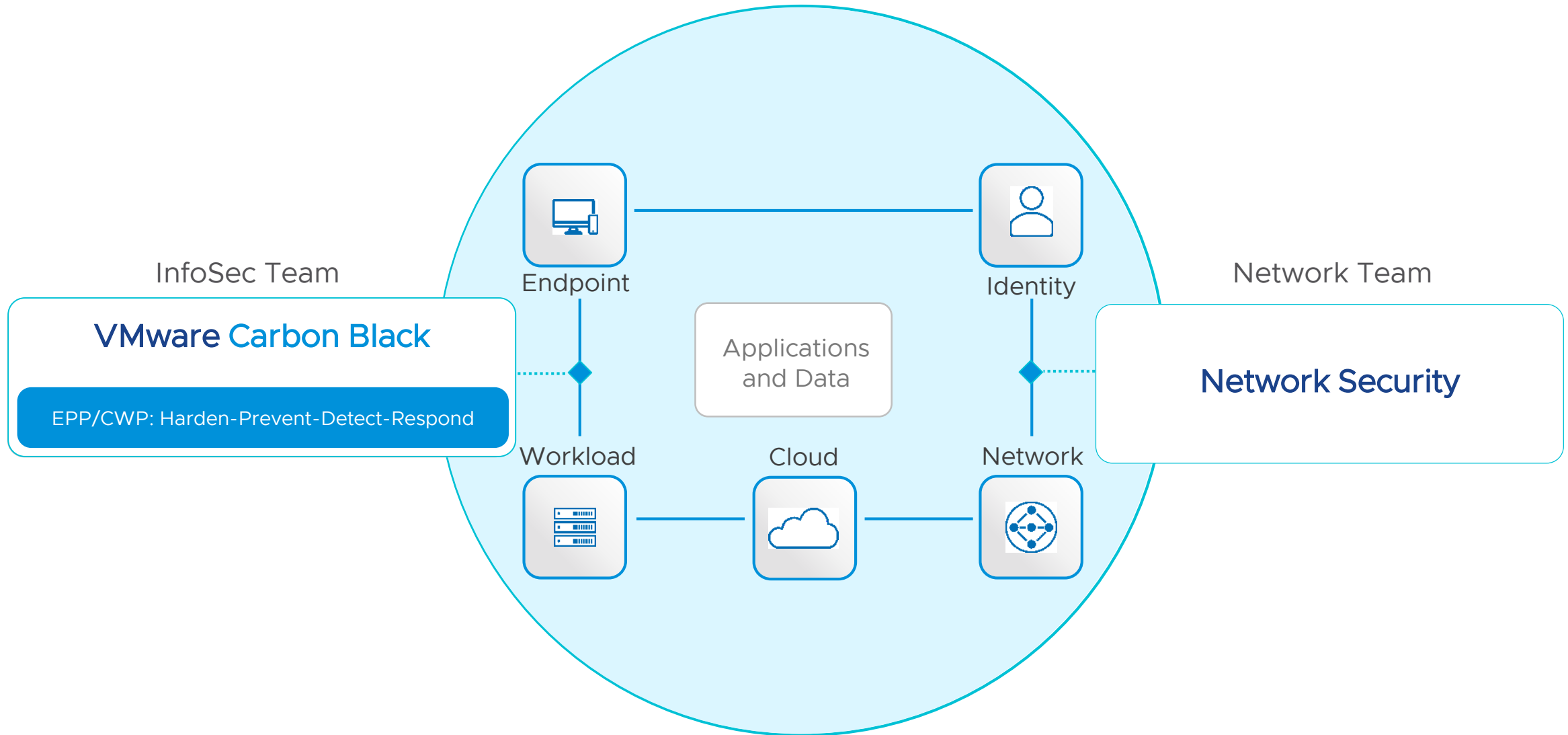
5 Common Container Security Risks

- 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

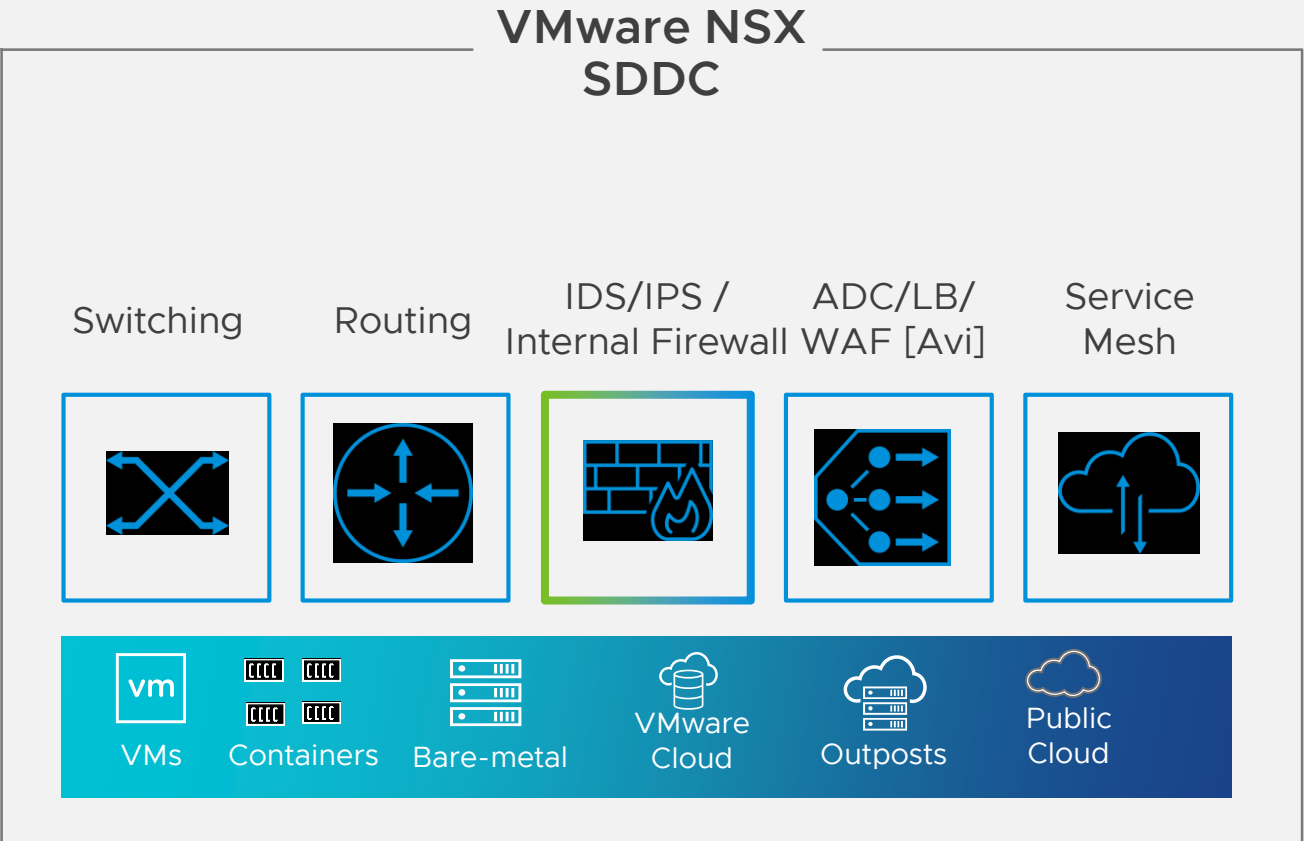


Network Security

VMware NSX

NSX Full DC Networking and Security

VMware



SWITCH 1

SWITCH 2

SWITCH 6

SWITCH 5

SWITCH 4

SWITCH 3

ANALYTICS

IDS/IPS

FIREWALL

LOAD BALANCER/WAF

VIPRION



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

ANALYTICS

IDS/IPS

FIREWALL

LOAD BALANCER/WAF

SWITCH 1

SWITCH 2

SWITCH 6

SWITCH 5

SWITCH 4

SWITCH 3

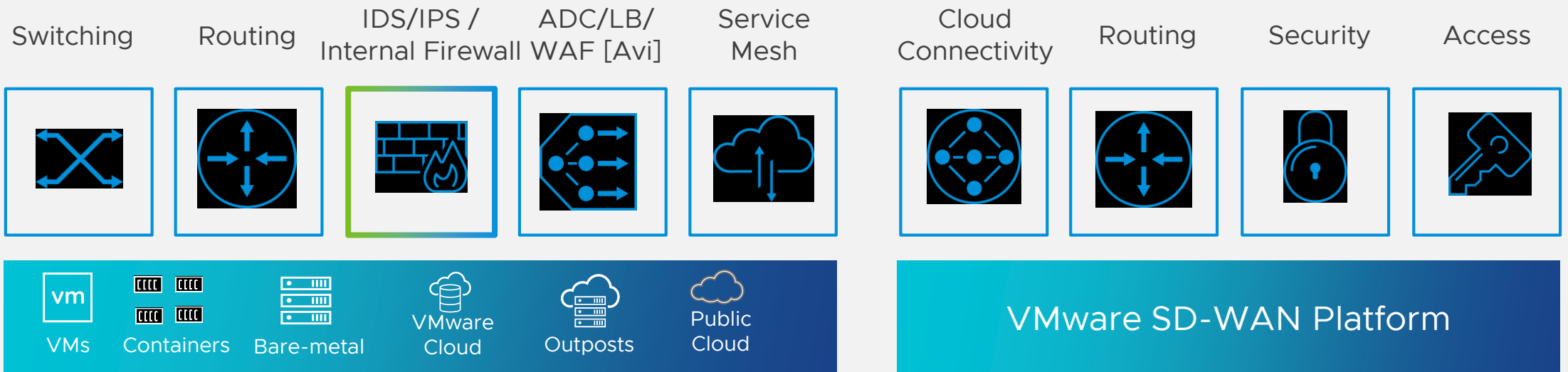
SWITCH 2

NSX

VMware NSX

Network virtualization and Security

VMware NSX - SDDC



Key Use Cases

Network Segmentation

Create Zones in software with no network changes

Quickly segment using existing constructs

Secure VDI

Stop lateral movement of attackers by blocking vulnerabilities

Stop malware from spreading in VDI environments

Compliance

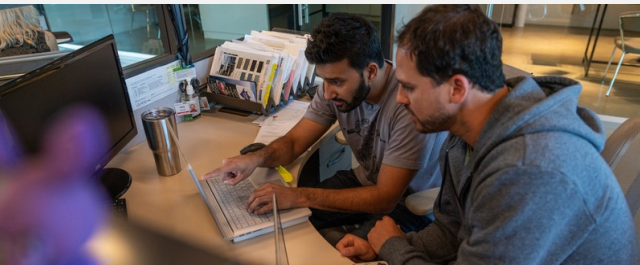
Easily achieve compliance for PCI-DSS, HIPAA, SOX

Eliminate blind-spots

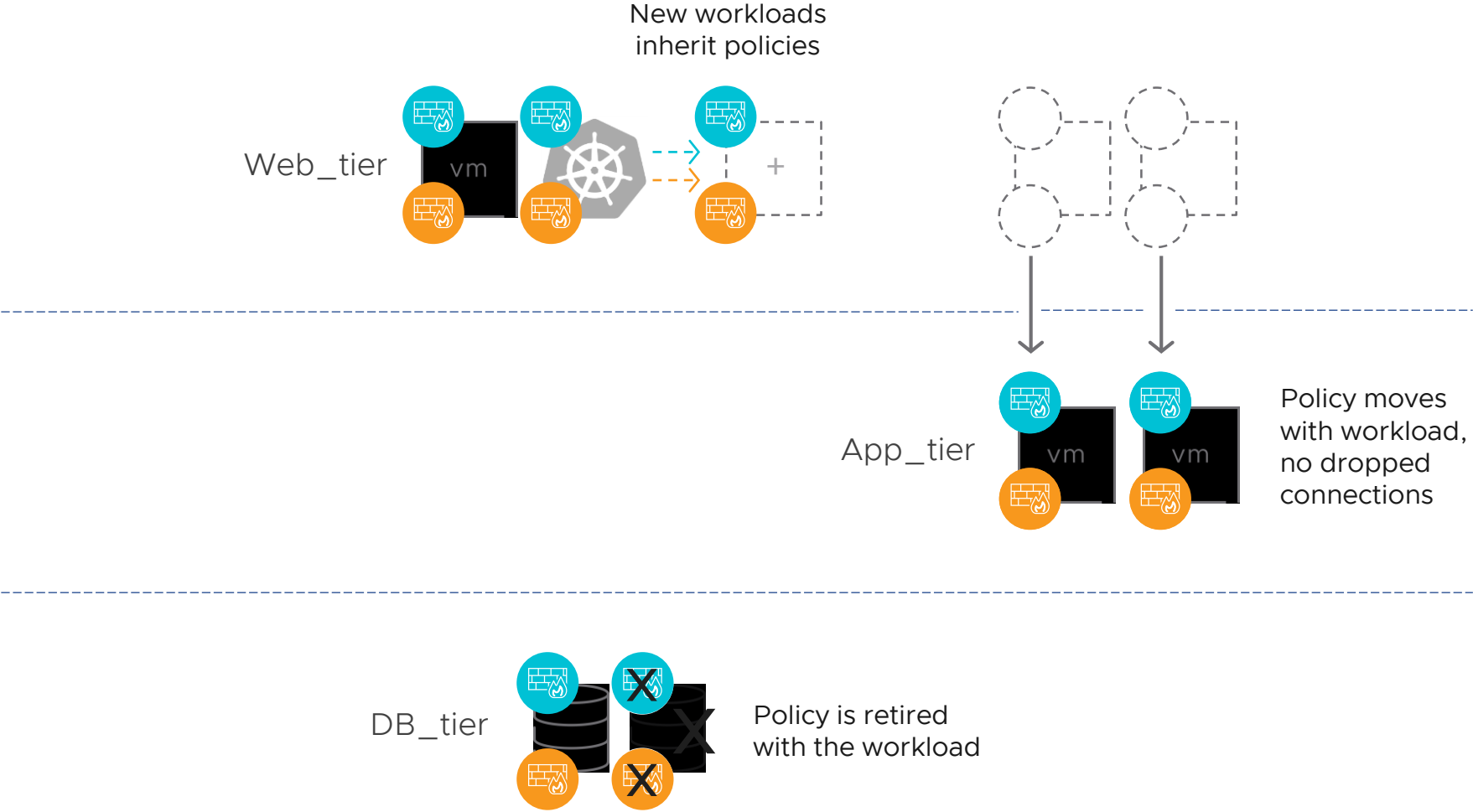
Appliance Consolidation

Replace discrete centralized appliances

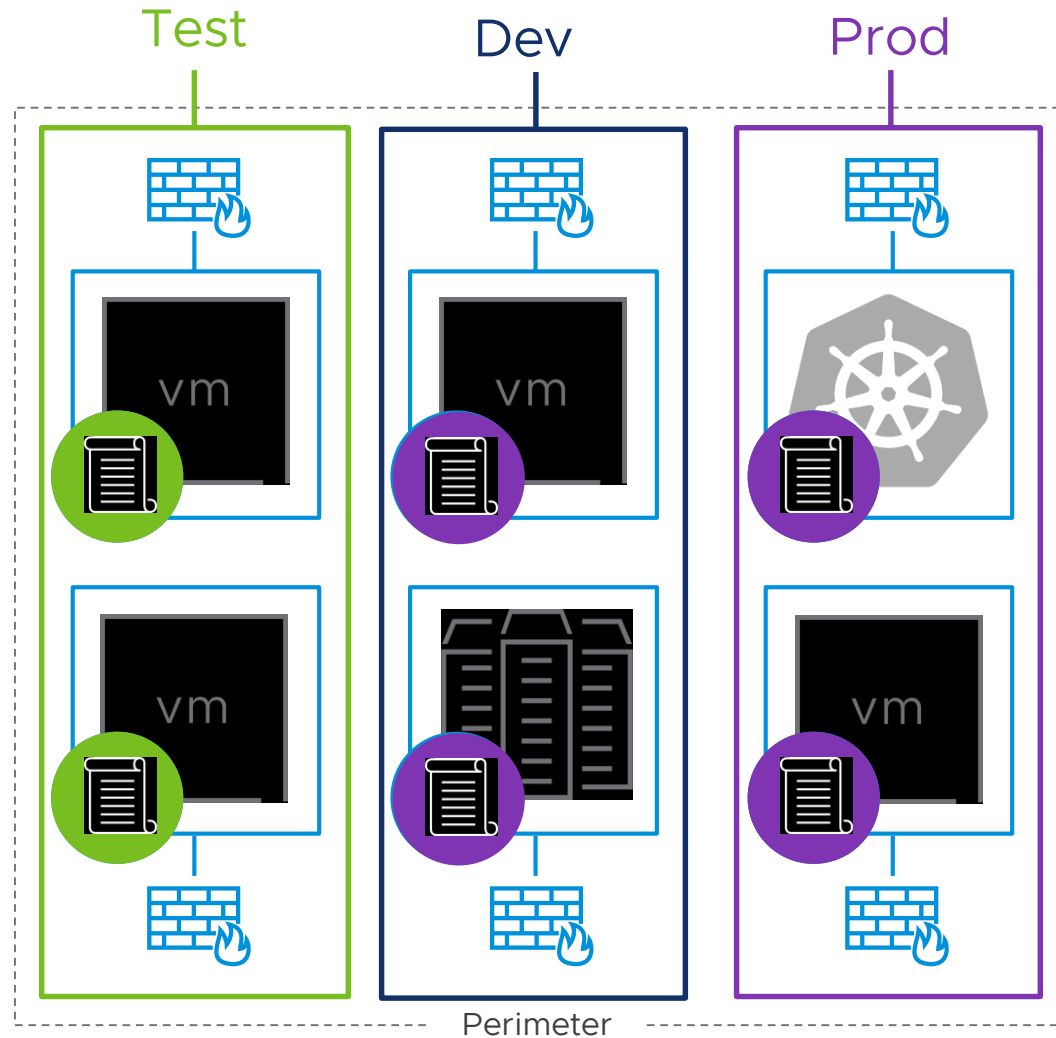
Use native distributed IDS/IPS capabilities in NSX—simply “turn it on”



NSX Service-defined Firewall: Massively Simplifies Operations



Network Segmentation



Use existing objects

Test/Dev/Prod

Network/Tags

Quickly achieve compliance

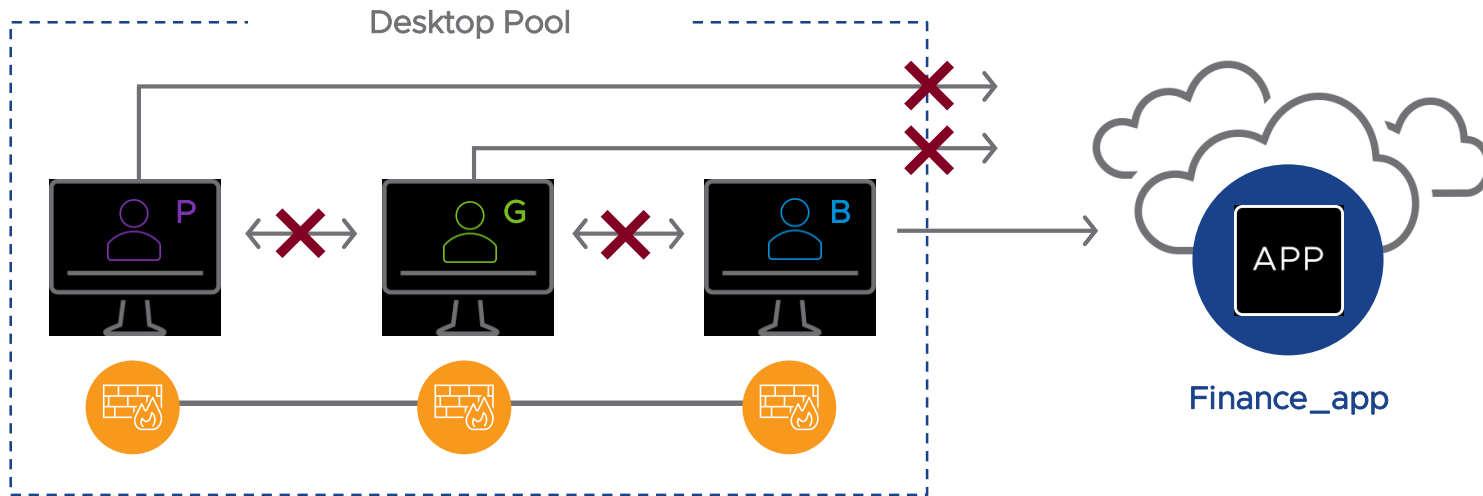
Quickly deploy independent of scale

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

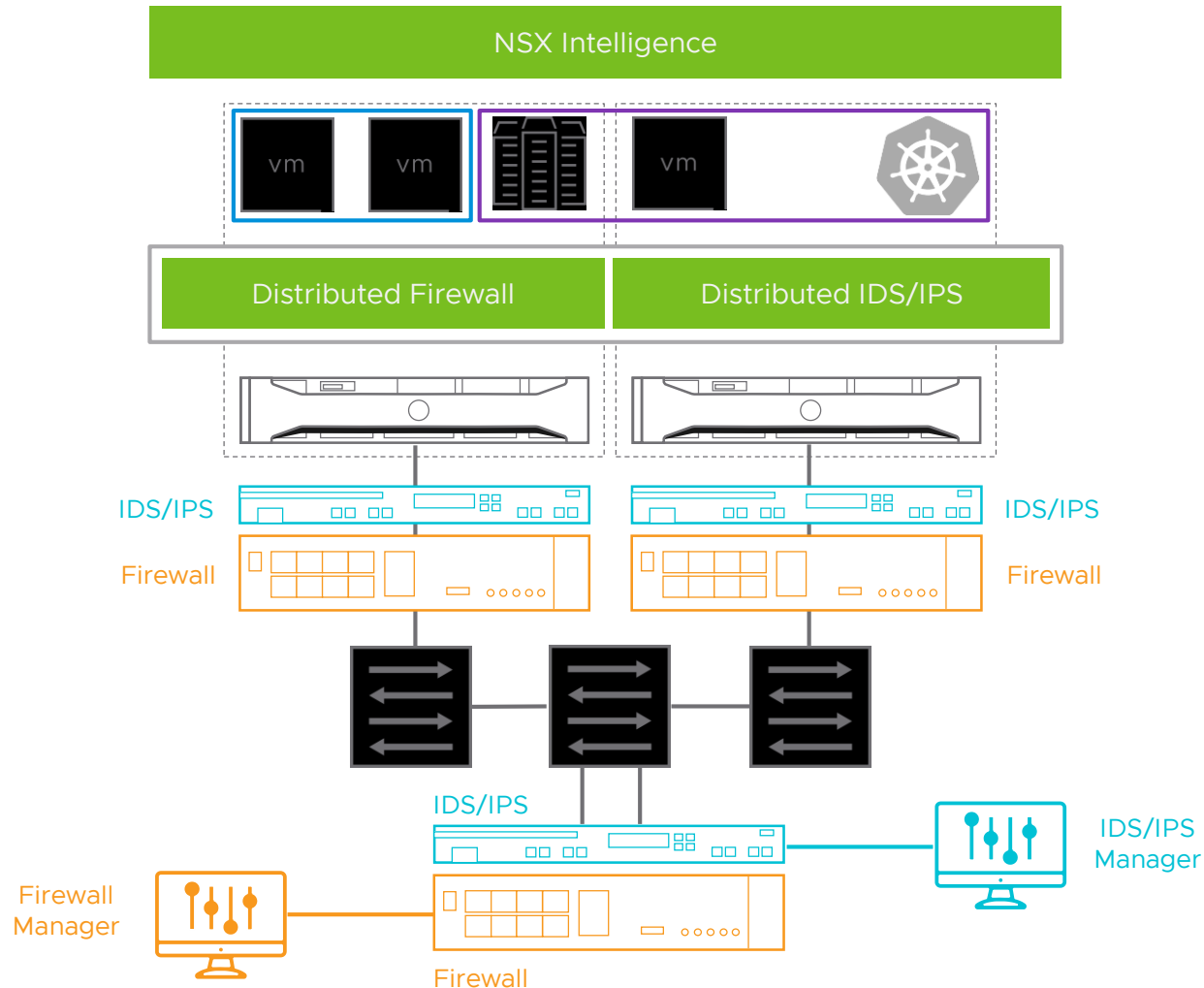
Identity based policy

Use existing 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 closer to the workload

Save time and money

Power and cooling

Operational simplicity

60% Reduction in traditional firewalls

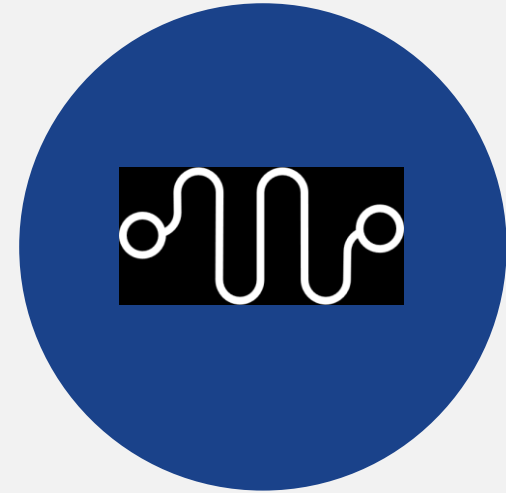
Radically Change the Equation: Cost, Complexity, Capacity



Simplified Network
Architecture

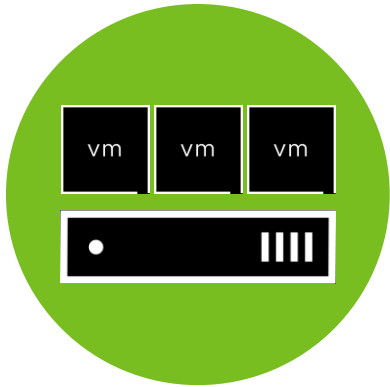


Operational
Simplicity



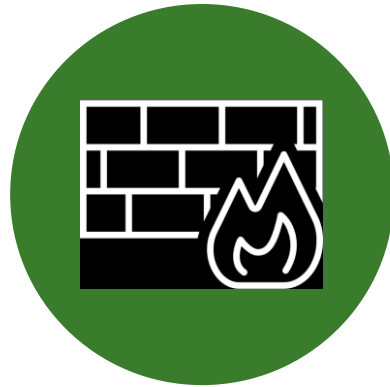
Distributed
Performance

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

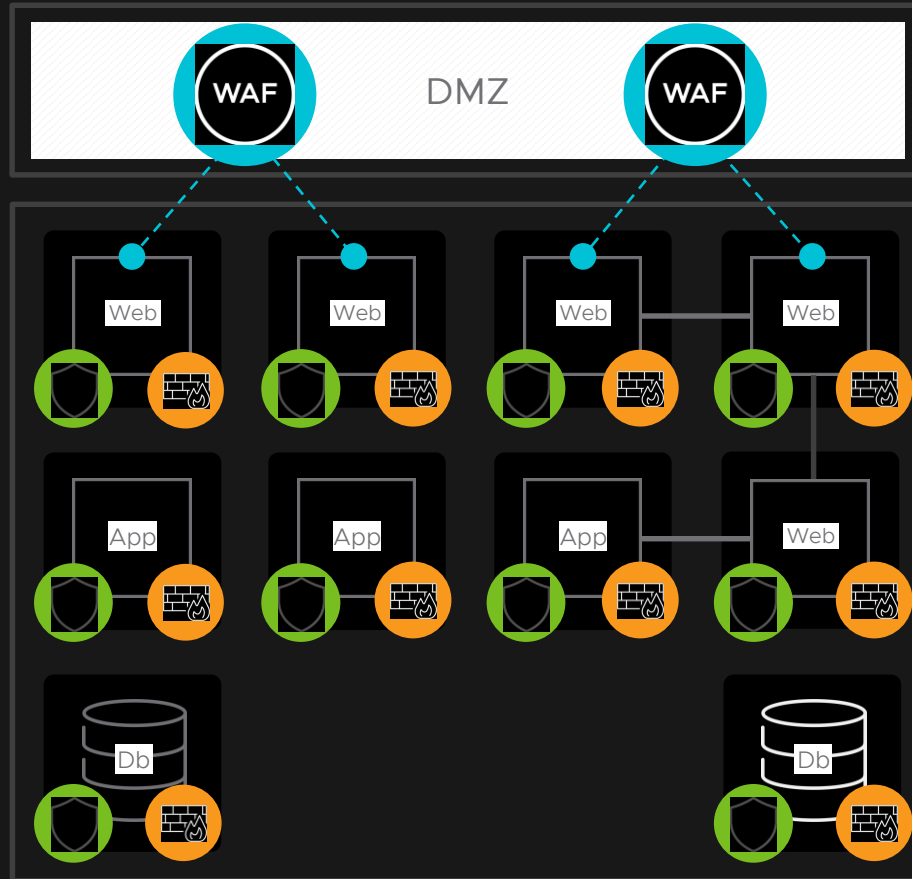
Modern management and EDR capabilities for a Zero Trust approach to endpoint security while providing an exceptional user experience



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