Securing VCF

With VMware vDefend

Introducing VMware Cloud Foundation

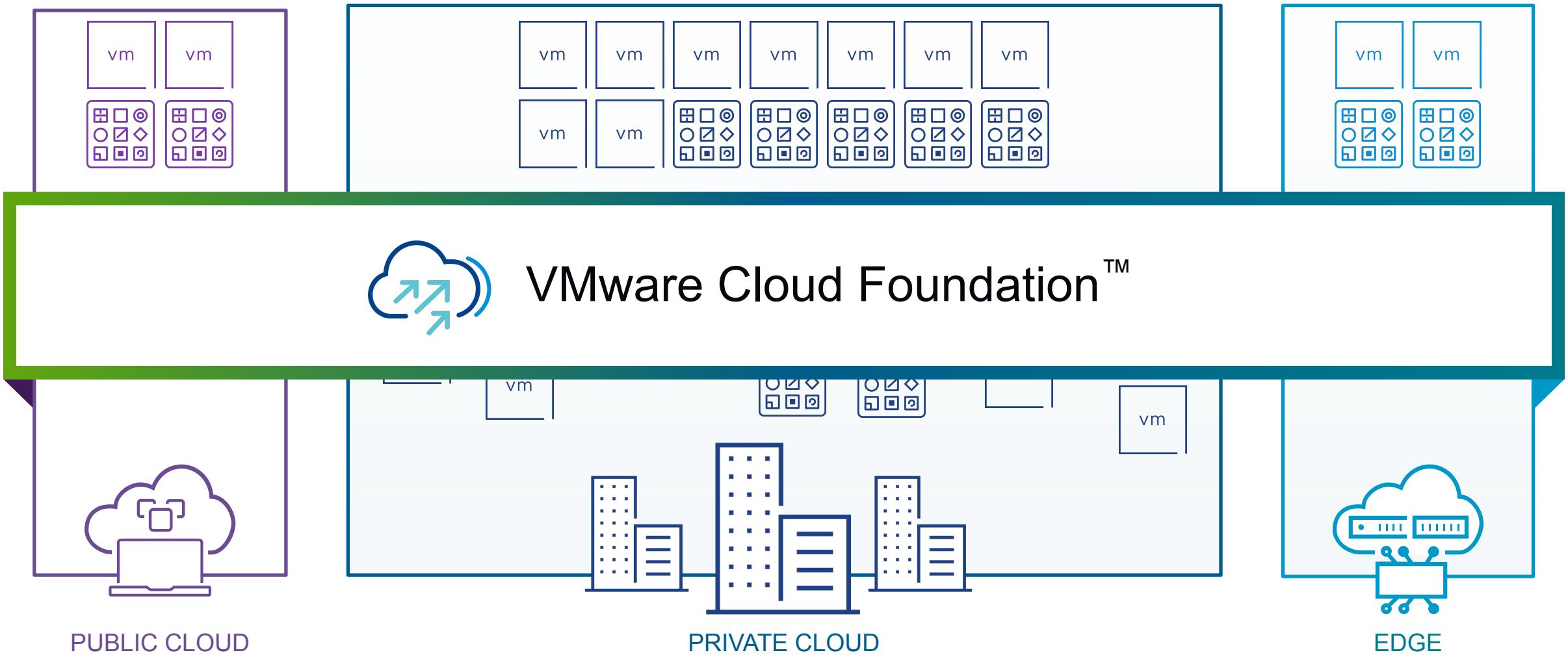
vmware by Broadcom

VCF Architecture

Definitions Reference

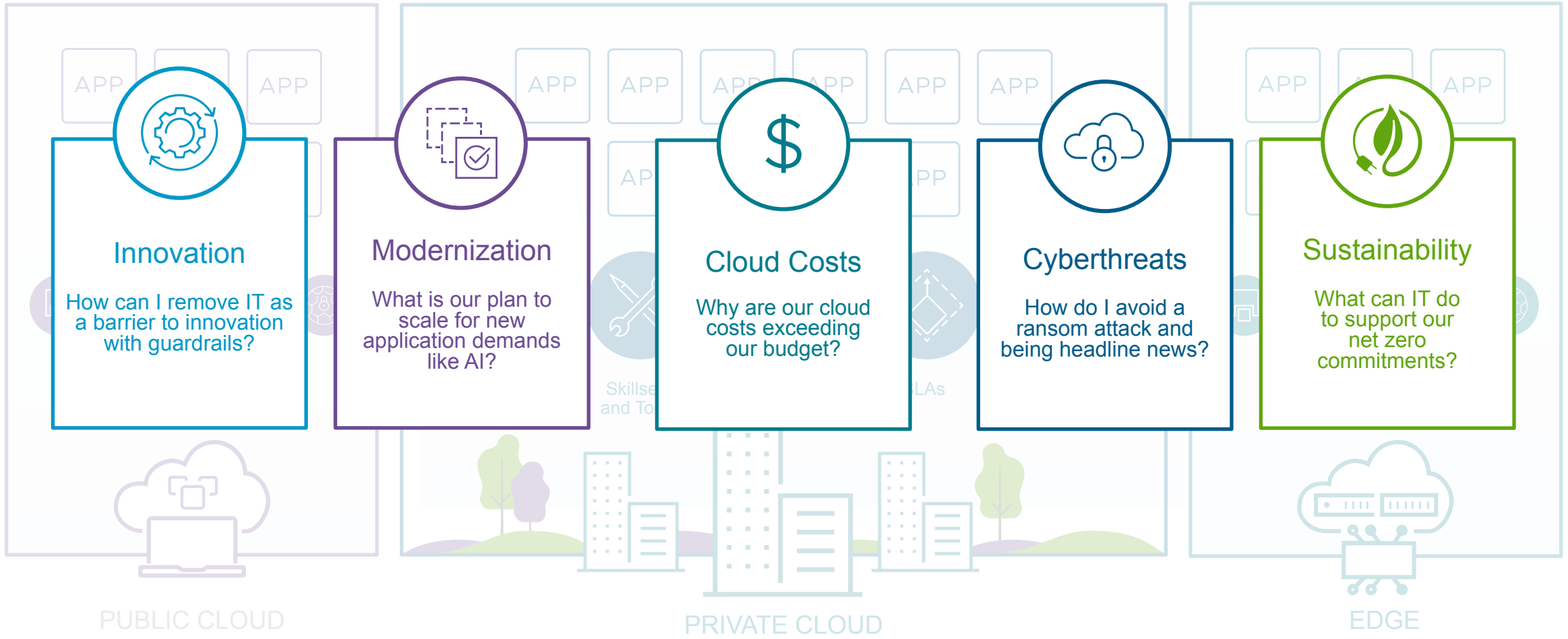
Availability Zone (AZ)	In VMware Cloud Foundation, an Availability Zone is defined by each group of hosts that make up a Stretched Cluster inside of a Workload Domain and usually when multiple Stretched Clusters exist, the groups from each share a common set of Infrastructure or Environmental Components that define the boundaries of a Fault/Failure Domain (e.g., Rack, ToR Switch Pair, Power Feed, HVAC Zone, etc.).
Consolidated SDDC	A Consolidated Domain/SDDC is a specific VCF Design option that focuses on reducing the footprint and overhead required to run a VCF Environment. Instead of Workload Domains and dedicated HW to separate different types of workloads from each other, it relies on Resource Pools.
Edge Services	Edge Services refers to the Networking and Security Services that run inside of VCF at the boundary between the Software Defined Network that is part of the VCF Architecture and the Physical Network in the Data Center. These Services include Routing, Firewall, NAT, VPN and other centralized built-in functions for the SDDC and the workloads running inside it. If these services are centralized, they will run on an NSX Edge Node.
Fault/Failure Domain	A Fault or Failure Domain is defined by a common set of Infrastructure or Environmental Components that define the boundaries (sometimes referred to as blast radius) where a single or multiple failure events when they occur will affect the availability of the workload relying on those components (e.g., Rack, ToR Switch Pair, Power Feed, HVAC Zone, etc.). The definition of the domain may vary based on the deployment and the level of impact from a failure they are willing to incur.
NSX Federation	Federation refers to the ability to connect the Networking and Security Services inside of one or more SDDC Instances together to present a consistent set of Security and Networking capabilities across workloads inside of those instances. It is enabled by implementing a one or more NSX Global Manager(s) between the NSX Domains inside the VCF instances.
Life Cycle/LCM Activities	VCF consists of a fixed set of Software with specific versions (BOM) combined with an engineered configuration. SDDC Manager is used to modify the software versions and their configuration. SDDC Manager is also able to perform many CRUD operations on the Infrastructure making up the SDDC as well. These operations are collectively referred to as Life Cycle Management Activities
Region	A Region is a common term used to define a geographic area that is outside of a "Metro" distance (5 ms RTT) which contains one or more VCF Instances.
Standard SDDC	A Standard SDDC is a specific VCF Design option that focuses on Scalability, Resiliency, and Separation of Duties as opposed to reducing footprint. It relies on Workload Domains and dedicated HW to separate different types of workloads from each other and always uses a dedicated Management Workload Domain.
Stretched Cluster	A Stretched Cluster is when more than one group of hosts in a vSphere Cluster that configured with vSAN Storage contains a full copy of the data stored and witnesses required to present a healthy copy of the vSAN data store. If there are only two groups of hosts that meet this requirement, a special node called a vSAN Witness is required.
VCF Instance	A VCF Instance refers to the entire SDDC stack of software and the HW it is deployed on required to present a Software Defined Data Center. The instance is bounded by a single SDDC Manager and may be deployed in a single location or across multiple locations if the locations meet the requirements of VCF
Workload Domain (WLD)	A Workload Domain (WLD) is a defined set of physical infrastructure that is dedicated to a single vCenter and VCF Instance. This set of infrastructure is maintained at the same versions and utilizes the same configuration. The consumption of a WLD is implementation specific however it commonly represents a unit of tenancy or use case. An example of a WLD that is based on use case is the Management WLD in a Standard SDDC implementation.

Delivering On Your Goals, Everywhere



“Complexity is the Enemy of Execution”

- Inconsistent operations stifle innovation, throttle productivity, and increase cost



VMware Cloud Foundation Components

SDDC MGR

Consistent Operations and Automation

vSphere

Built on Virtualized Infrastructure

vSAN

Hyper-Converged

NSX

Integrated Networking and Security *

TKG

Conformant Kubernetes

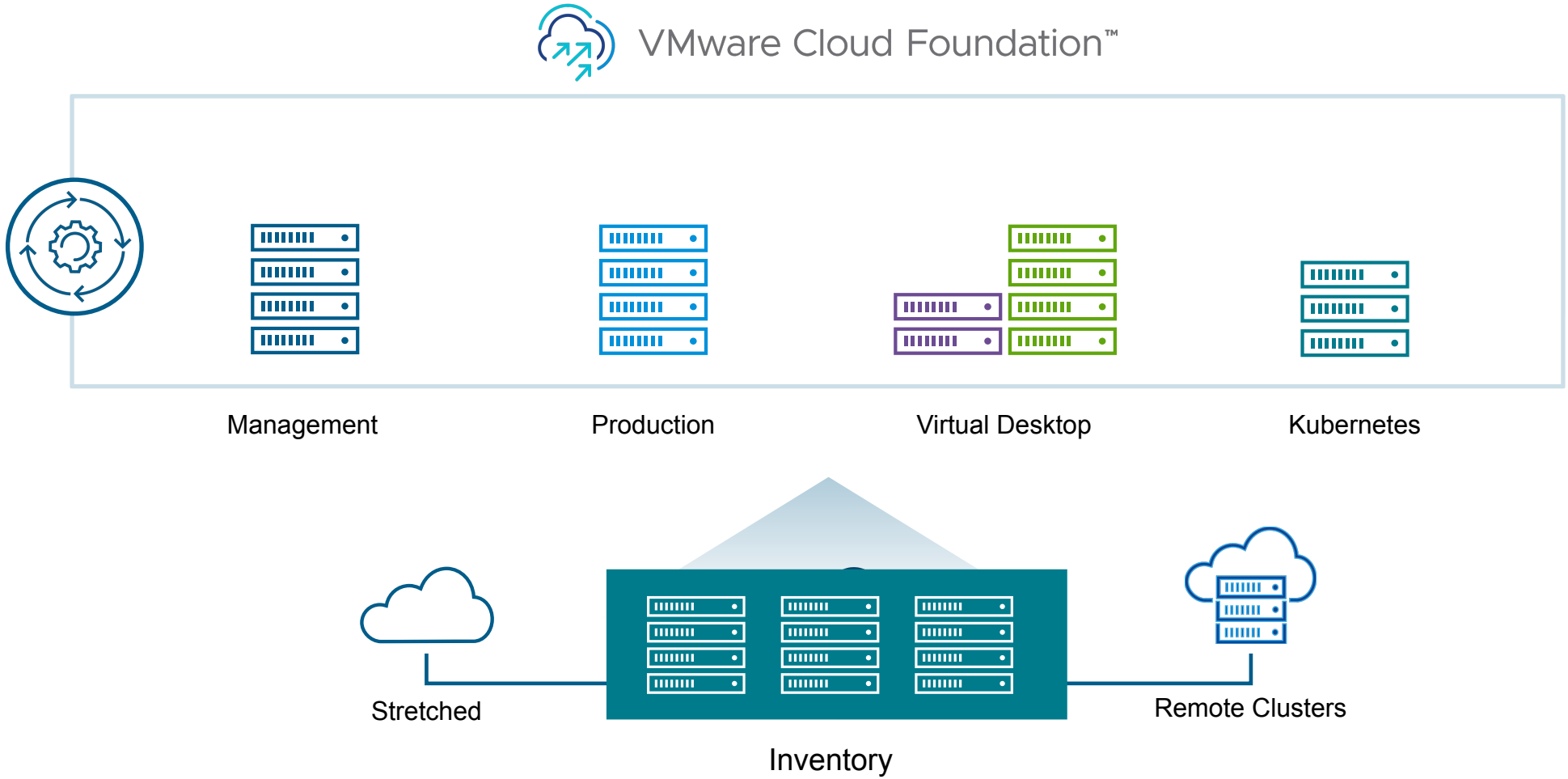
Aria

Cloud Management

Run any kind of workload from basic to AI-accelerated applications on VMs or containers

Workload Domains

Deliver a Scalable Private Cloud



VCF

Security Offerings

Ideal For:

- Securing Infrastructure
- Tenant Environment separation
- Application Zoning
- App Microsegmentation

VMware Firewall

- Distributed Firewall
- Gateway Firewall
- Security Intelligence
- Container Security

VMware Firewall with ATP

- Distributed and Gateway IDS/IPS
- Malware Prevention
- NTA, NDR
- Distributed Firewall
- Gateway Firewall
- Security Intelligence
- Container Security

Ideal For:

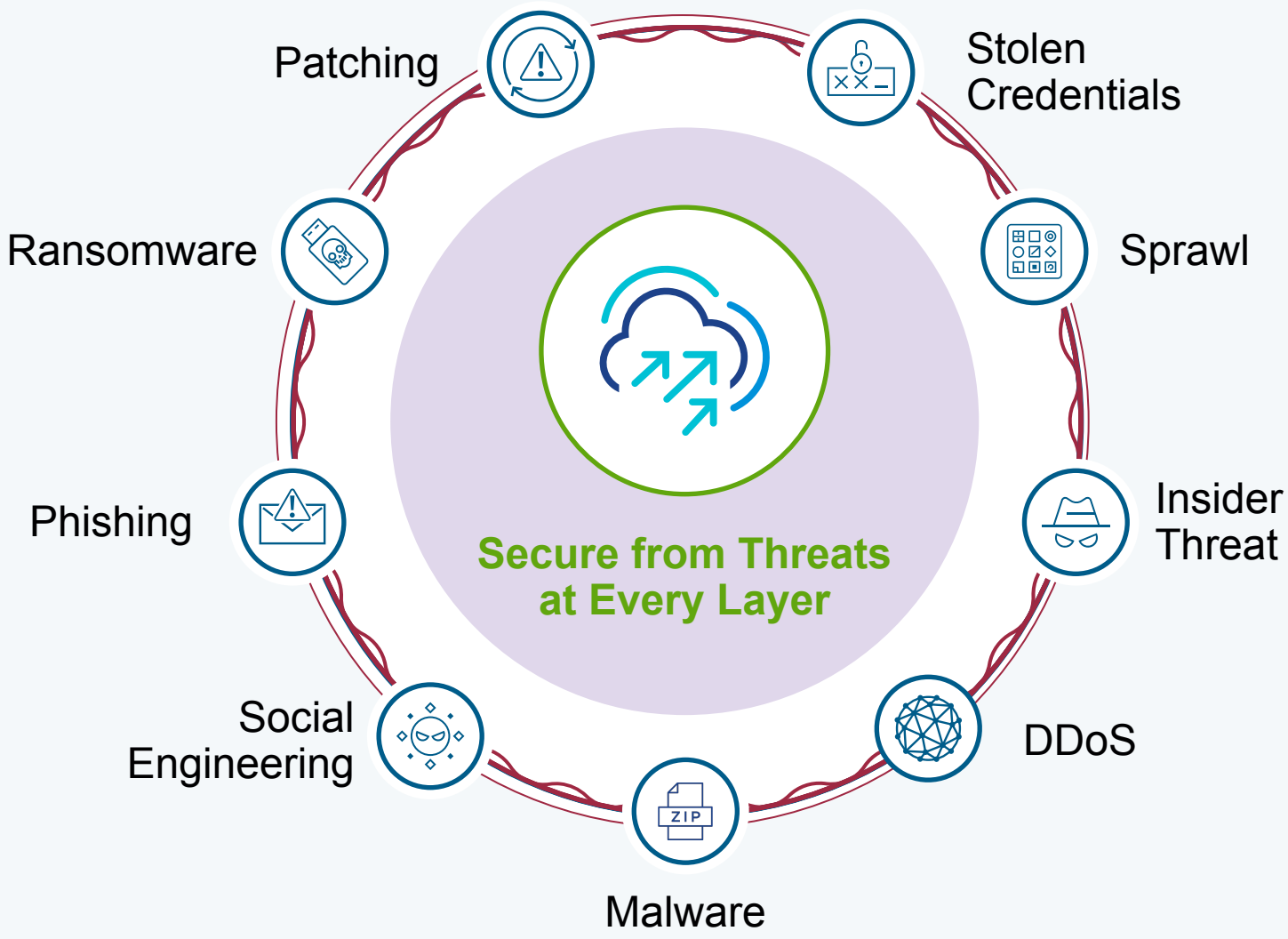
- IDS/IPS
- Malware and Ransomware Protection
- Breaches and Compliance
- Threat Monitoring

VMware Cloud Foundation (VCF)

MANAGING RISK & CYBERSECURITY*

Secure, systematic approach to attacks

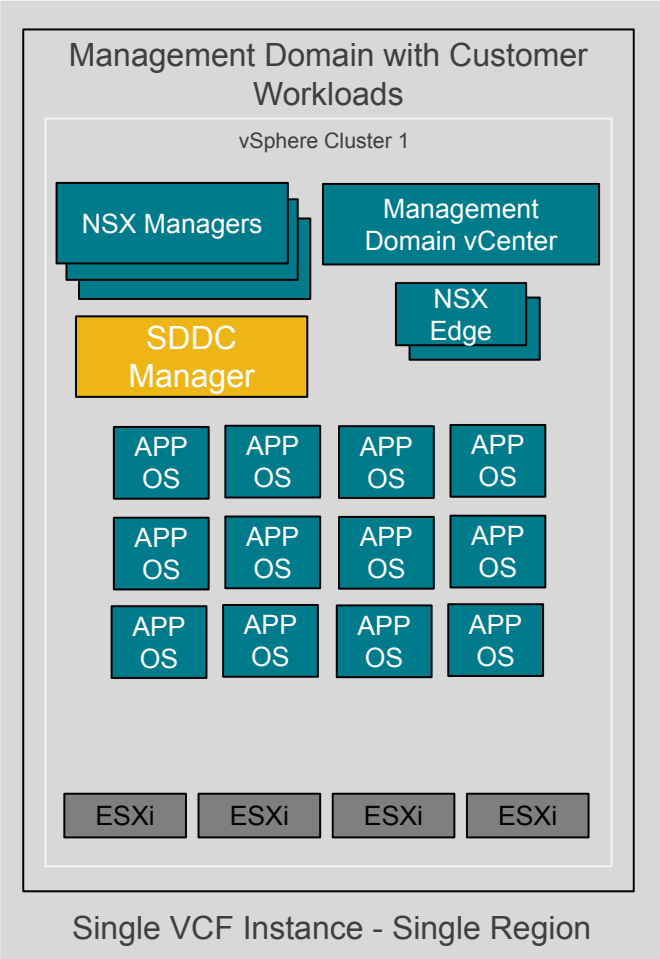
- Implement zero-trust defense for app and data security
- Proactively inspect and monitor for threats
- Establish a rapid recovery plan for potential attacks



*Available with VMware Firewall + ATP

VCF Architectures

Single Site Deployment (Consolidated Architecture)



Management is a self contained NSX Domain with NSX Managers

Collapsed Management VMs and customer workload VMs are co-located, single pool of resources

Single change window, single version of the BOM

Typically use cases:

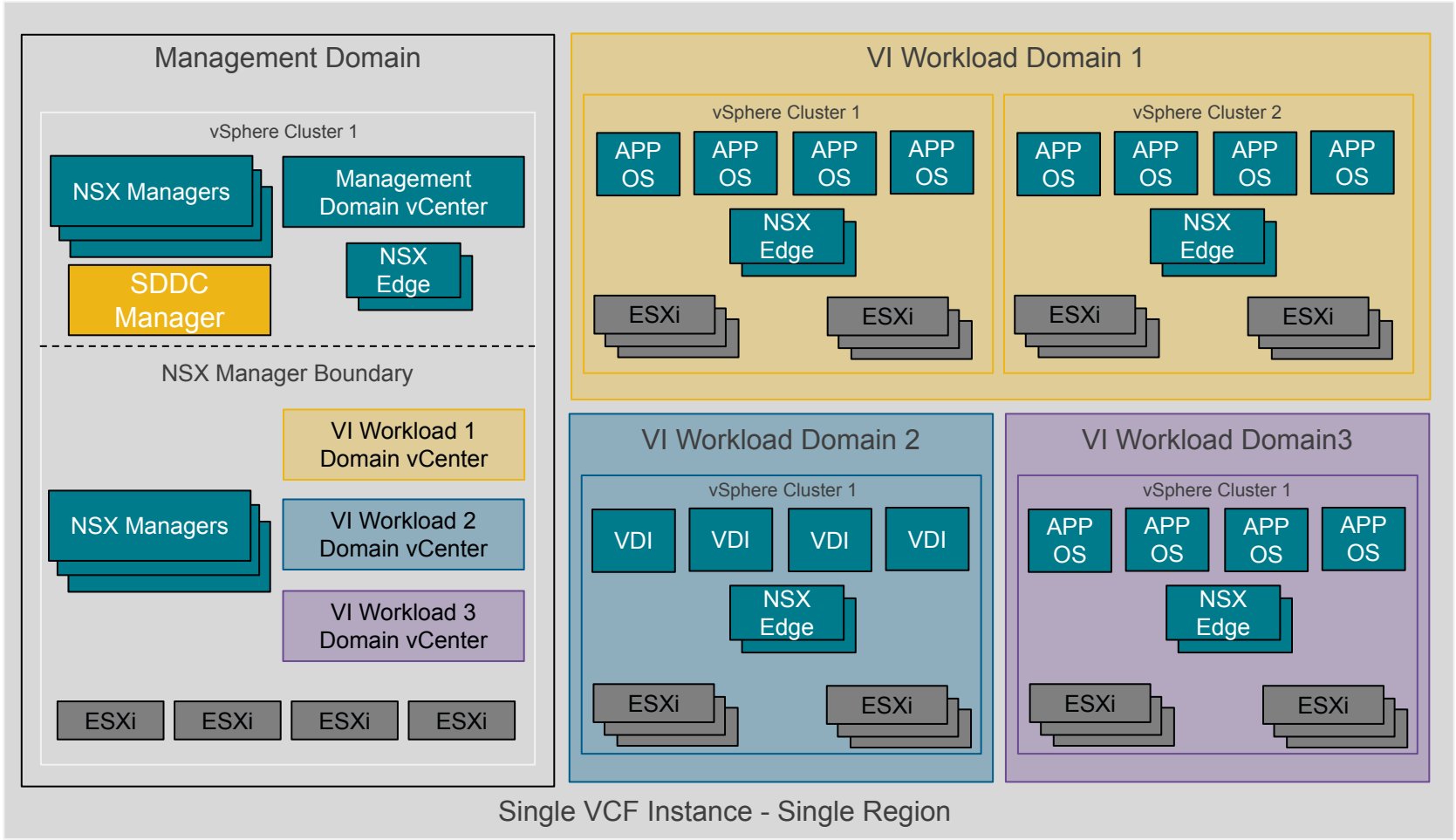
- Small-scale environment
- Lab/Proof-of-concept testing

Scale from 3 up to 100 ESXi hosts

Scale out Cluster (more nodes = more availability for vSAN), Multi AZ and Multi VCF Instances with NSX Federation is supported

VCF Architectures

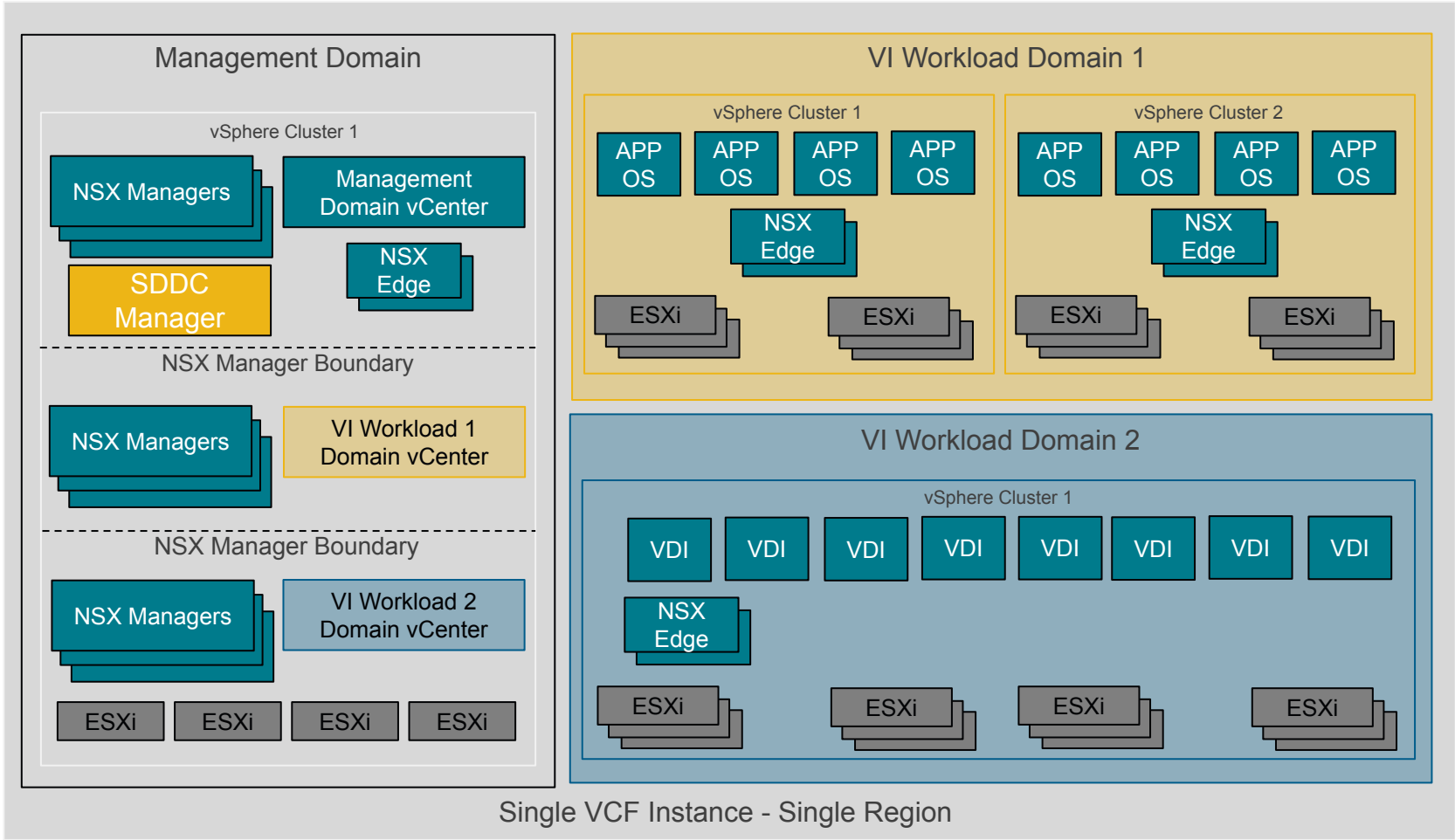
Single Site Deployment (Standard Architecture)



- Management is a self contained NSX Domain with NSX Managers
- Management Domain is dedicated to running infrastructure management workloads
- Production compute workloads run in a VI WLD and are managed by separate vCenter servers
- Single NSX Domain for consistent security and networking across multiple VI WLDs
- Extendable to Multi AZ or Multi VCF Instances using NSX Federation
- Single NSX Domain = Single change window
- Scale from 100 up to 1000 ESXi hosts

VCF Architectures

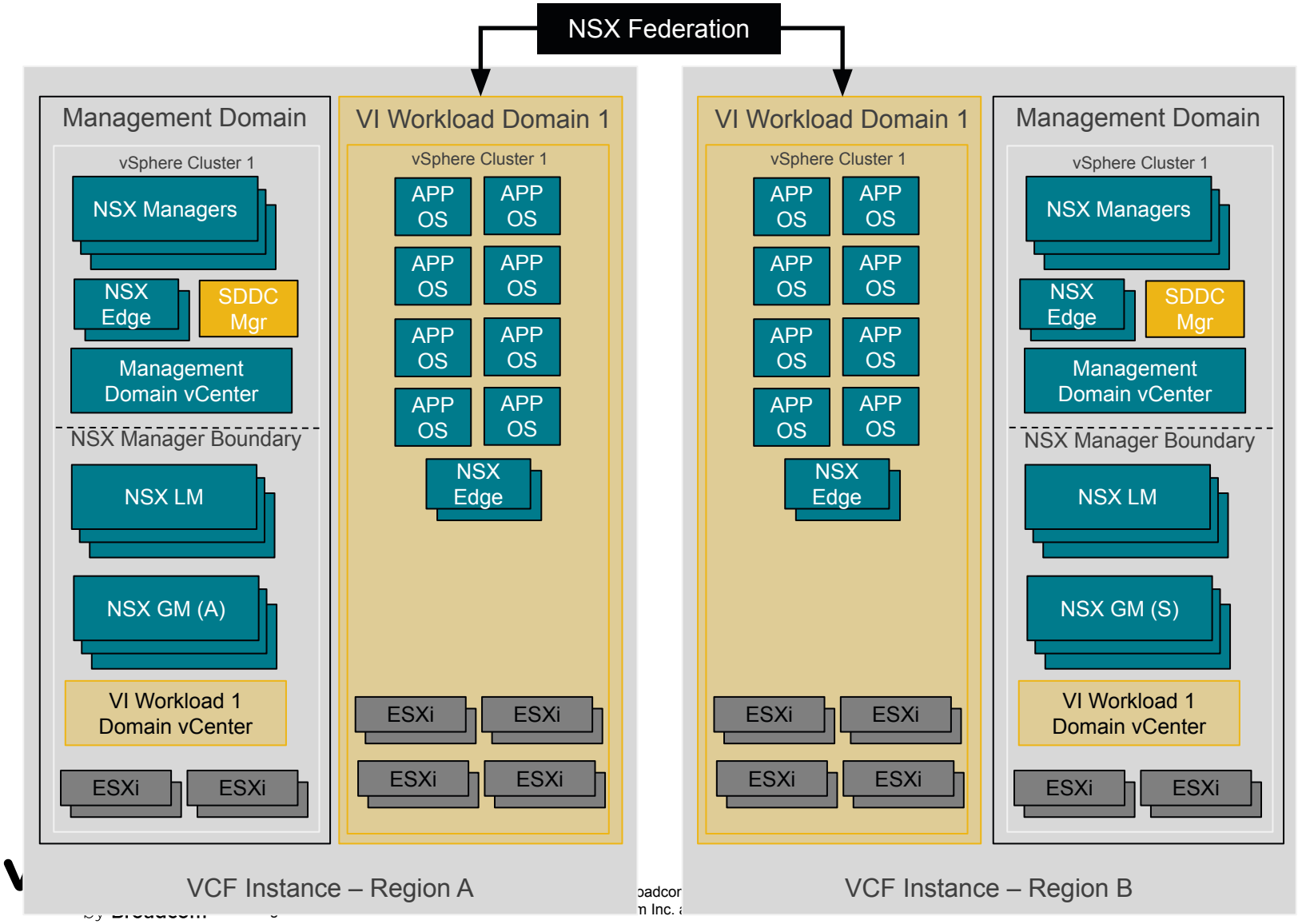
Single Site Deployment (Standard Architecture)



- Management is a self contained NSX Domain with NSX Managers
- Management Domain is dedicated to running infrastructure management workloads
- Production compute workloads run in a VI WLD and are managed by separate vCenter servers
- Single VCF Instance with multiple independent VI WLD/NSX Domains
- Extendable to Multi AZ or Multi VCF Instances using NSX Federation
- Multiple NSX Domains = Multiple groups with isolated change windows
- Scale from 100 up to 1000 ESXi

VCF Architectures

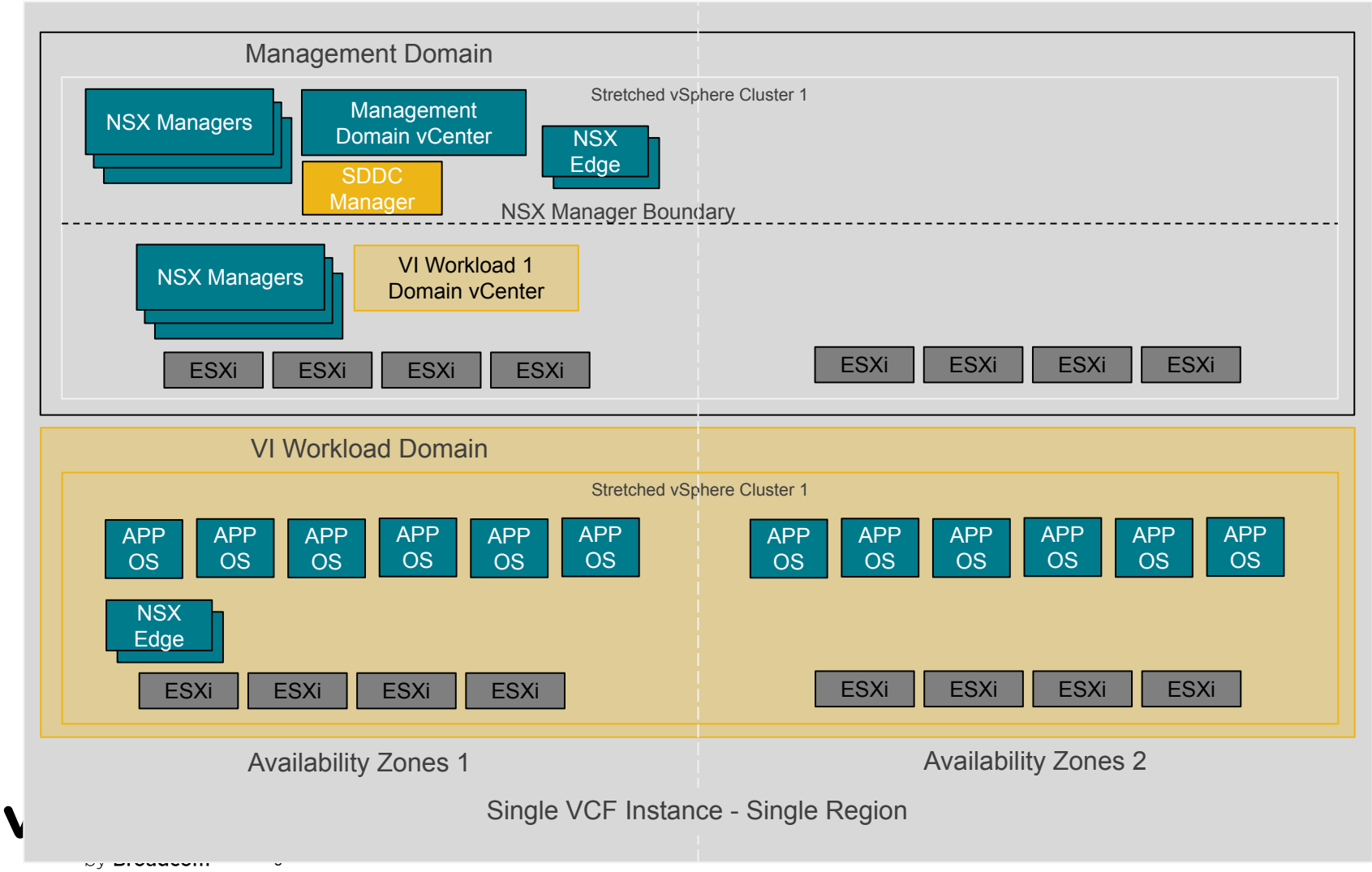
Multi VCF Instance Deployment using NSX Federation



- Multiple VCF Instances connected via NSX Federation for consistent security policy, global networking, and disaster recovery
- NSX Federation extend compute pooling across NSX Domains
- NSX Federation between VI WLD or/and between Management Domains from different VCF instances
- Manual NSX Federation deployment process following VMware Validated Solutions (VVS) guidance
- Note: Multi VCF Instances using NSX Federation is enabled per NSX Domains, not for the whole VCF

VCF Architectures

Multi Availability Zone (AZ) Deployment using stretched Clusters



A vSphere Cluster with vSAN Storage that spans multiple Availability Zones (AZ) where each Availability Zone constitutes a Failure Domain.

The stretched cluster retains vSphere HA and DRS functionality allowing for a fully automatic recovery from an Availability Zone failure

vSAN witness node is required

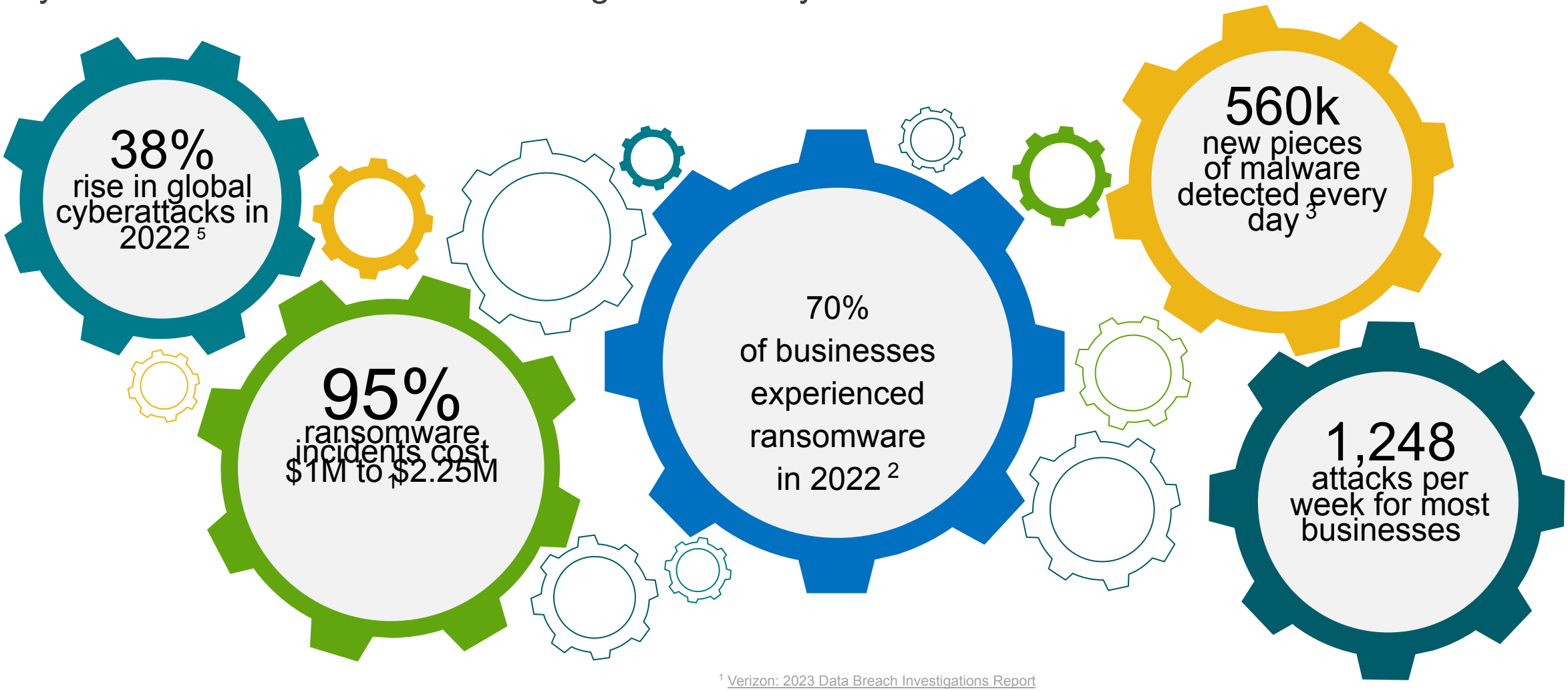
Management Domain cluster must be stretched prior to stretching any VI WLD vSAN clusters

Stretch other vSAN clusters as needed for availability

Today’s Security Realities

Today's Security Realities

Cyber attackers and threat actors target data everywhere – all the time



[1] Verizon: 2023 Data Breach Investigations Report
[2] www.statista.com/statistics/204457/businesses-ransomware-attack-rate/
[3] https://dataprot.net/statistics/malware-statistics/
[4] https://pages.checkpoint.com/forrester-wave-for-enterprise-email-security-2023.html
[5] https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks

Today's Security Realities

Operational Inefficiencies and Unmitigated Risks

Today's Security Realities

Lack of Segmentation and Automation - Freedom of Lateral Movement

44%

of breaches perform some form of lateral movement [1]

Most island hoping is

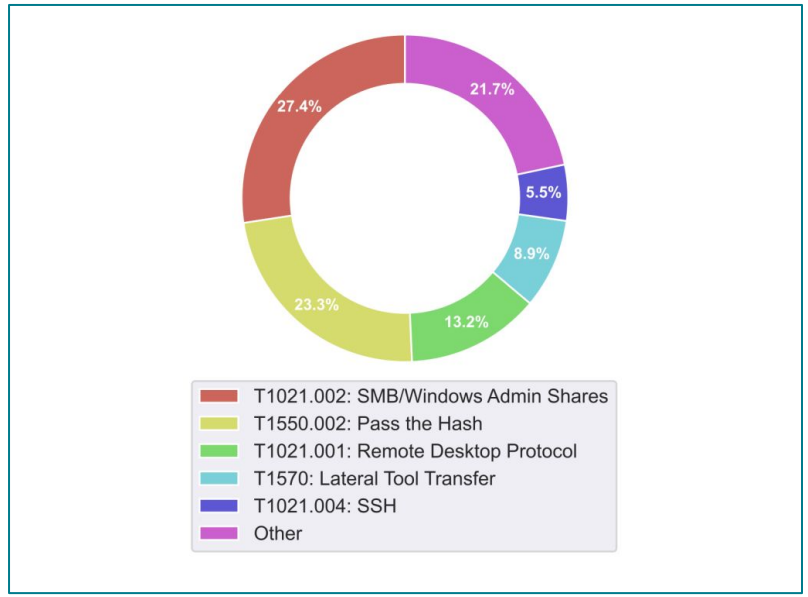
2-3 Hops

and very rarely 4, making for swift closing and laser focused propagation attempts [2]

64%

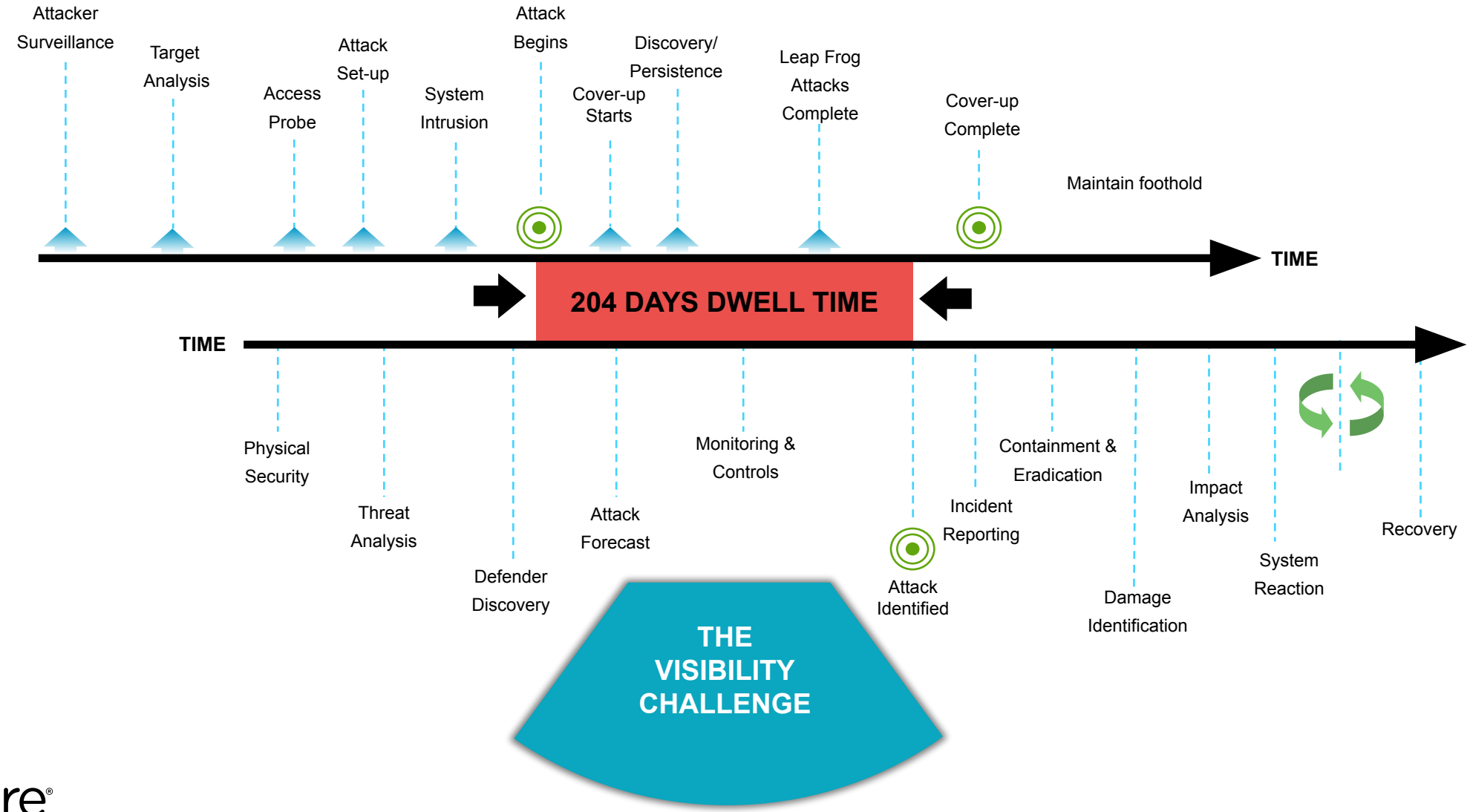
use of the Samba service, Pass the Hash and the Remote Desktop Protocol

"The Remote Desktop Protocol and SSH connections are probably two of the easiest techniques to perform lateral movement. These intrusion events are particularly difficult to identify as they easily get lost among the events associated with legitimate administrative activity. "



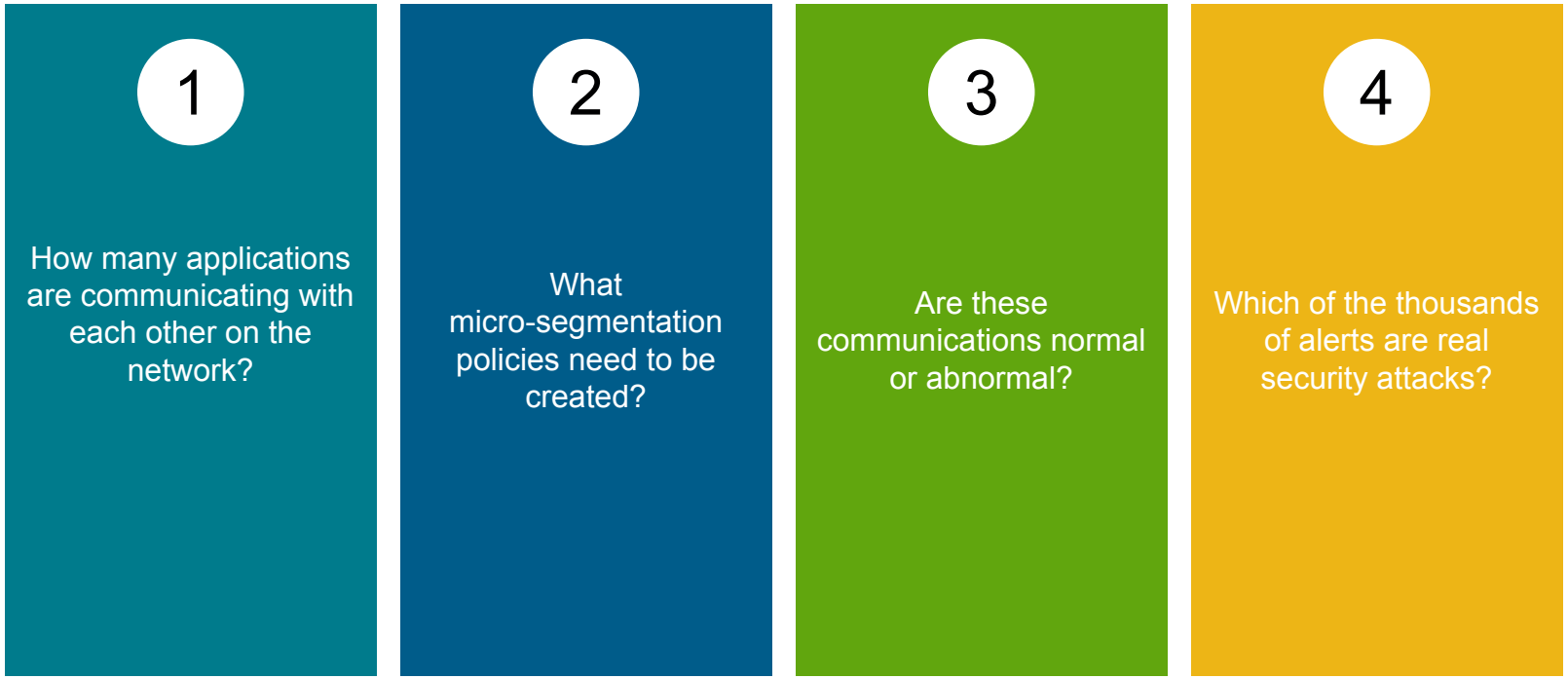
Today's Security Realities

Lack of Visibility - Lengthy Dwell Times



Today's Security Realities

Lack of Visibility - You cannot protect what you cannot see



Data Center Network hosts thousands of application components

It is a black box for most Network Security teams

Today's Security Realities

Lack of Patching Urgency – Exposed Attack Surface

"60% of breach victims said they were breached due to an unpatched known vulnerability where the patch was not applied"

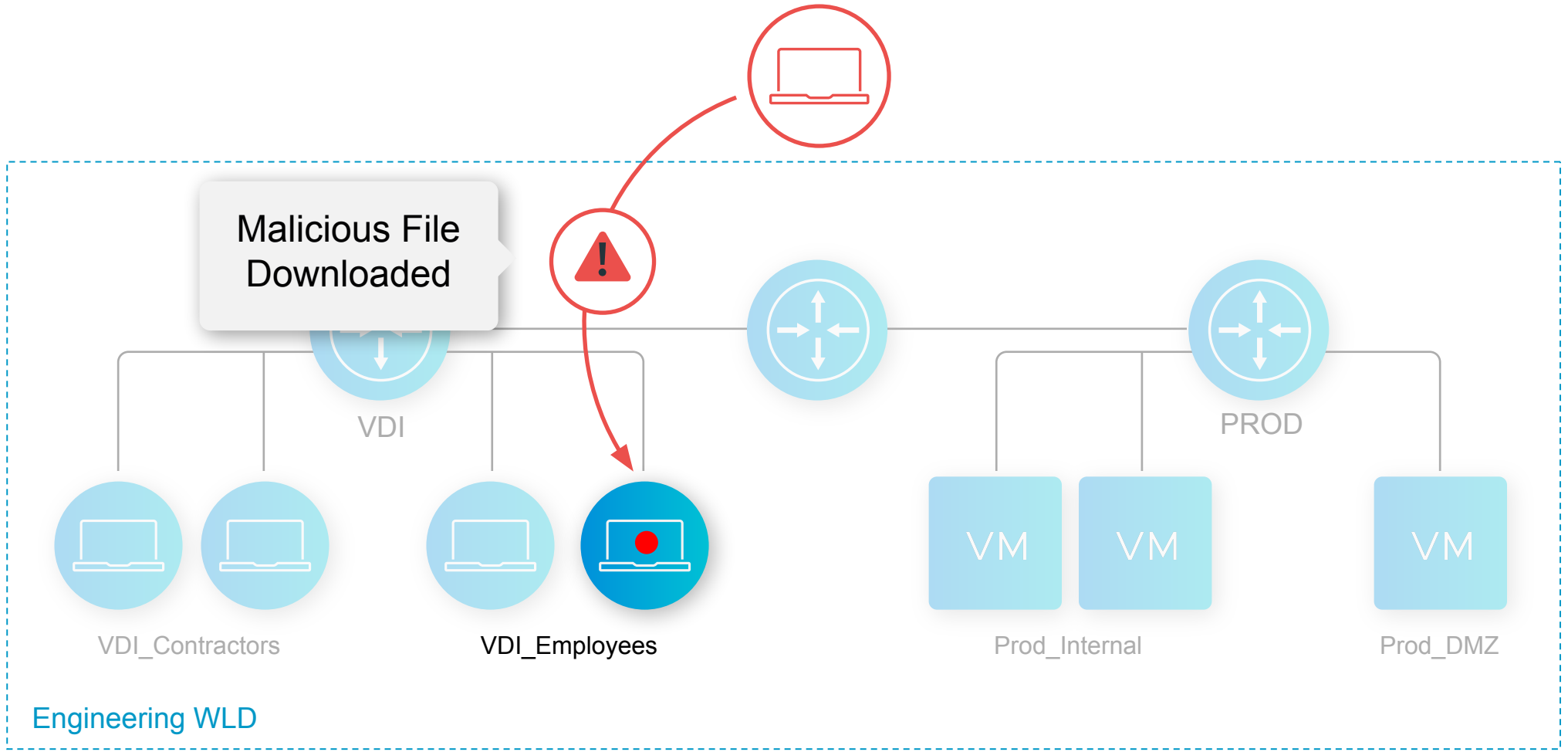
Ponemon Institute

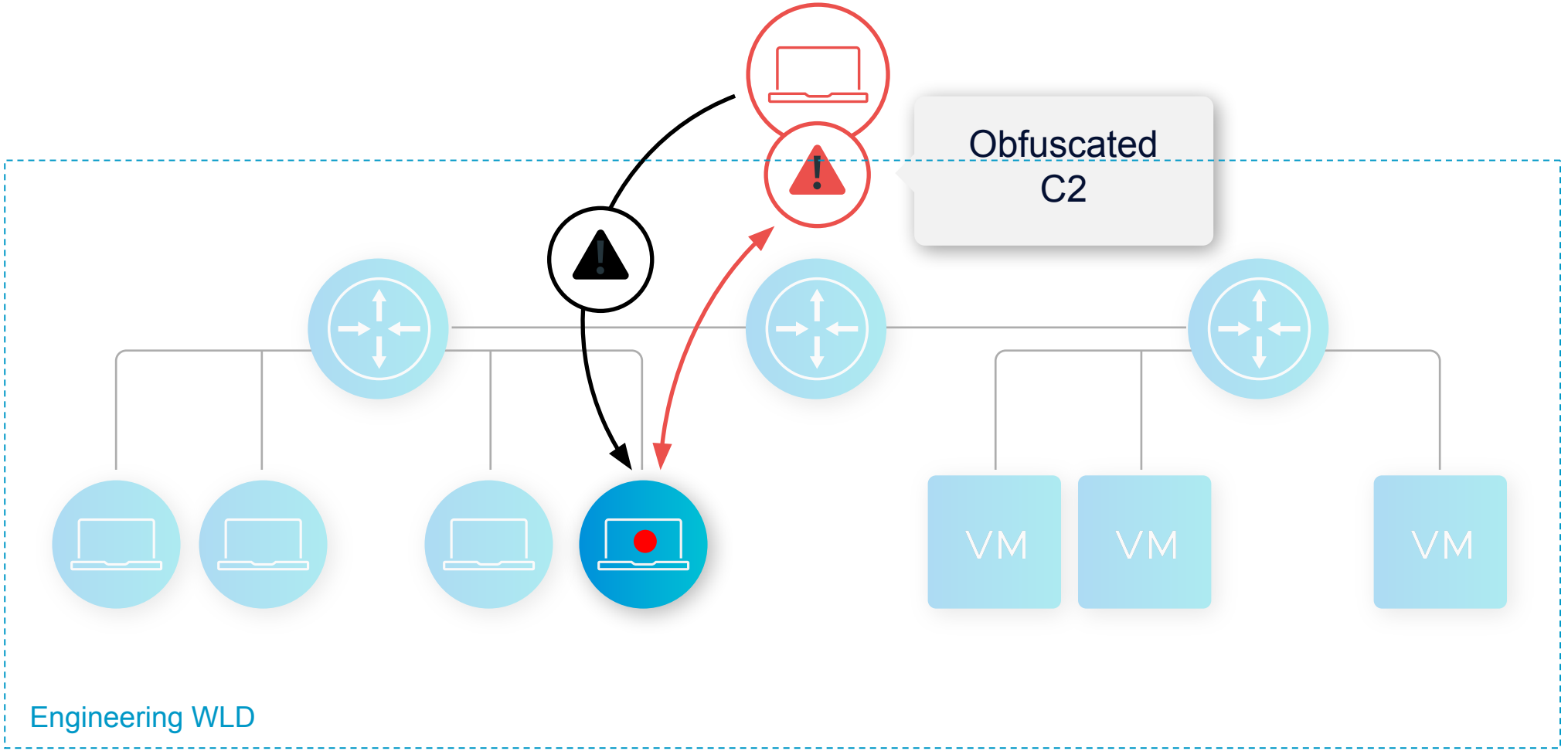
Today's Security Realities

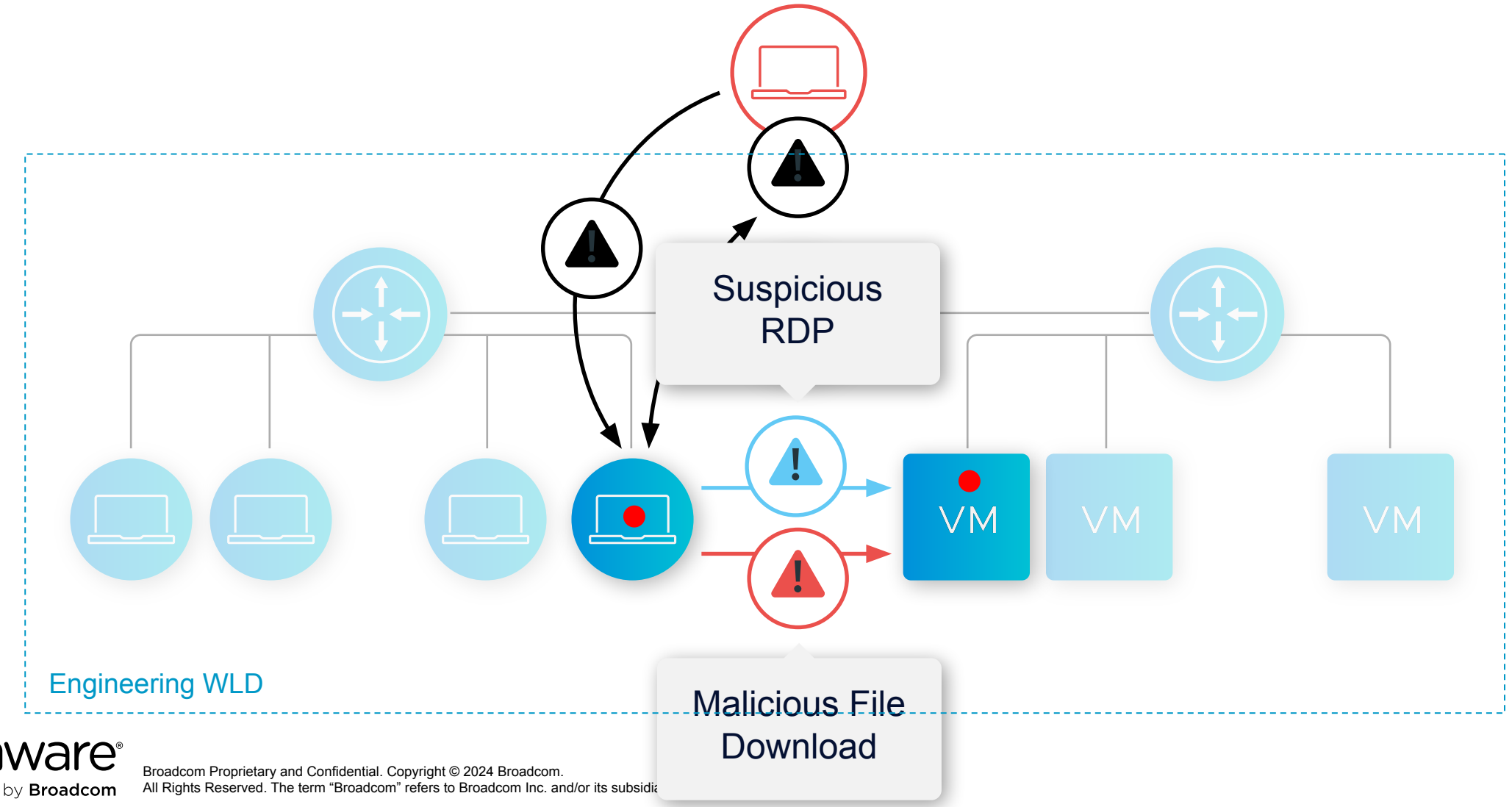
Lack of Context - Misaligned Priorities and Delayed Triage

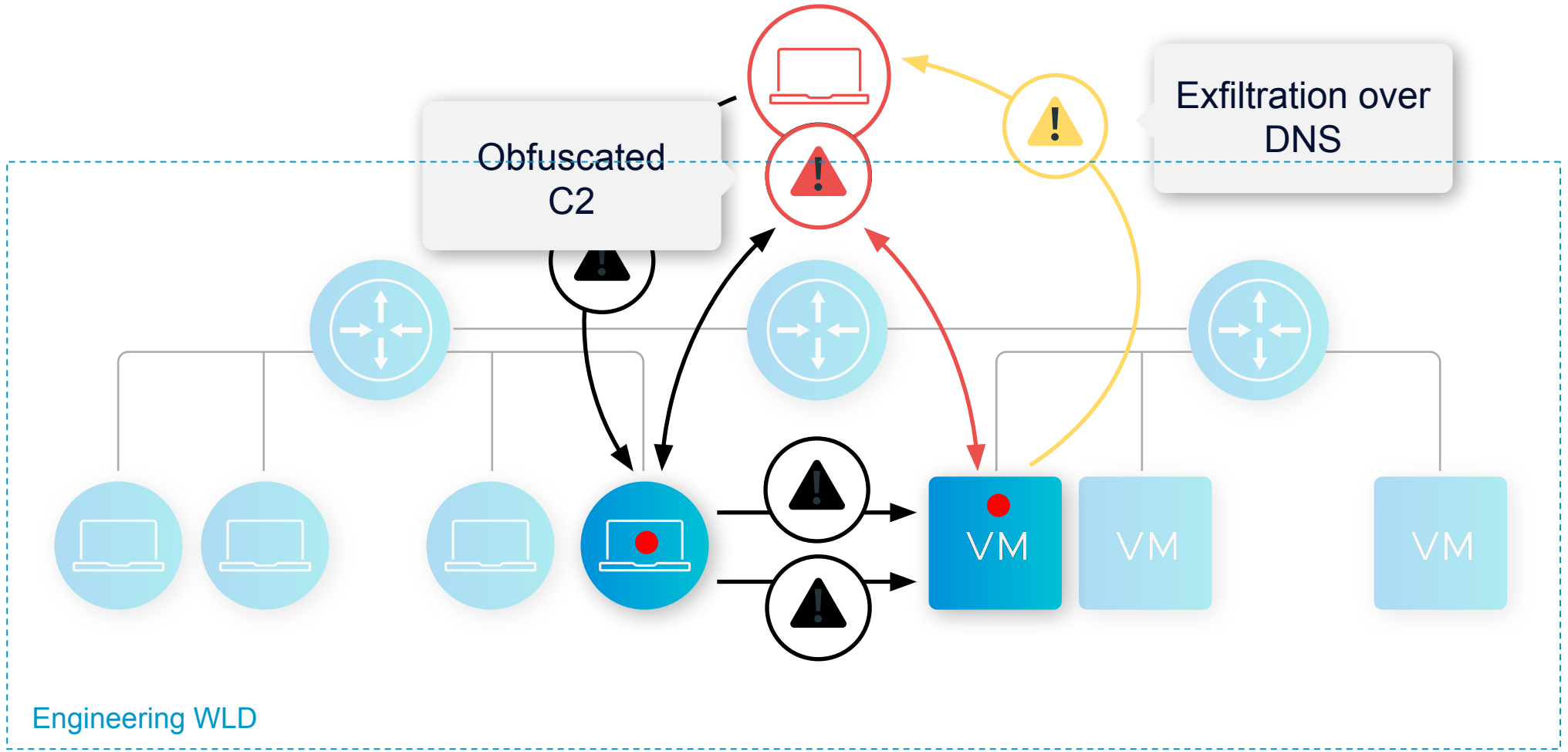
"Outdated security technology and processes and too many alerts or false negatives with detection software are listed among the top obstacles"

Scale Venture Partners 2020 Cybersecurity Perspectives



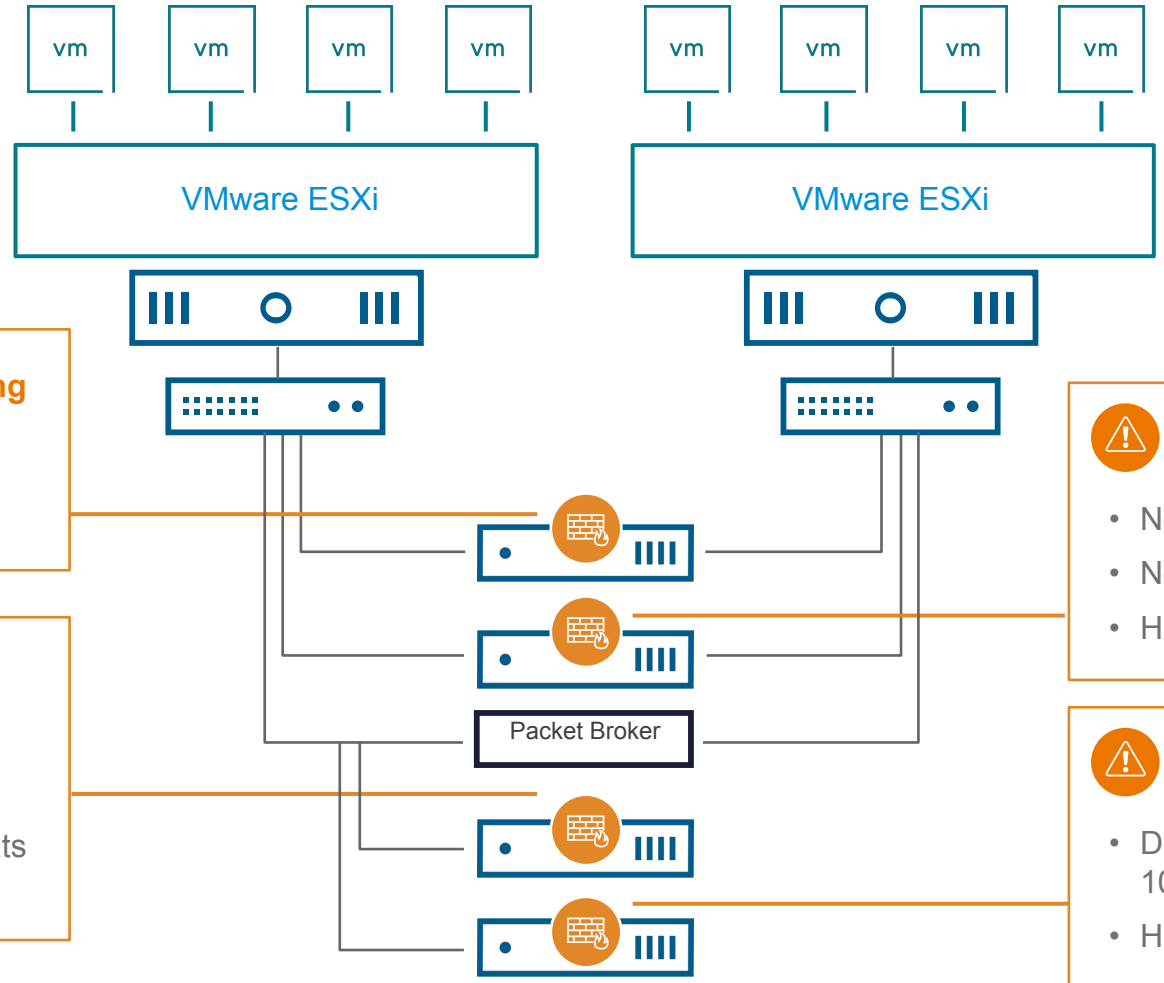






Today's Security Realities

Legacy Security



Network-Based Firewalling

- Manual and labor-intensive
- IP/Subnet based

Network Sandbox

- Detection technology easily bypassed by evasive malware
- Fails to detect advanced threats

IDS/IPS

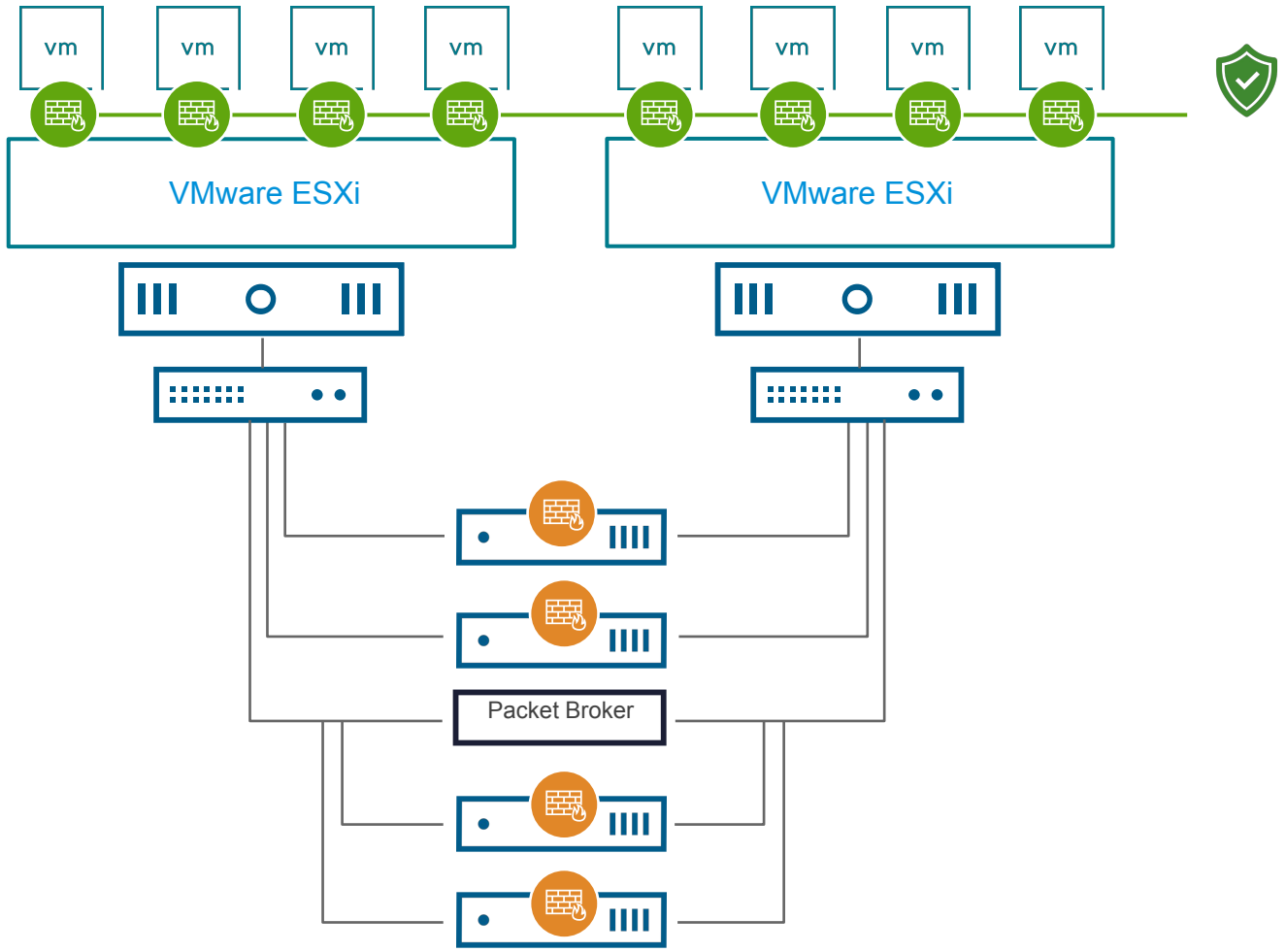
- No Environmental Context
- No East/West Visibility
- High false positive rate

Network Traffic Analysis

- Difficult and costly to hairpin 100% of traffic
- High false positive rates

Securing VCF with VMware Firewall

VMware Firewall - Hypervisor Based Advanced Threat Protection



No Network Changes

Hypervisor Observability

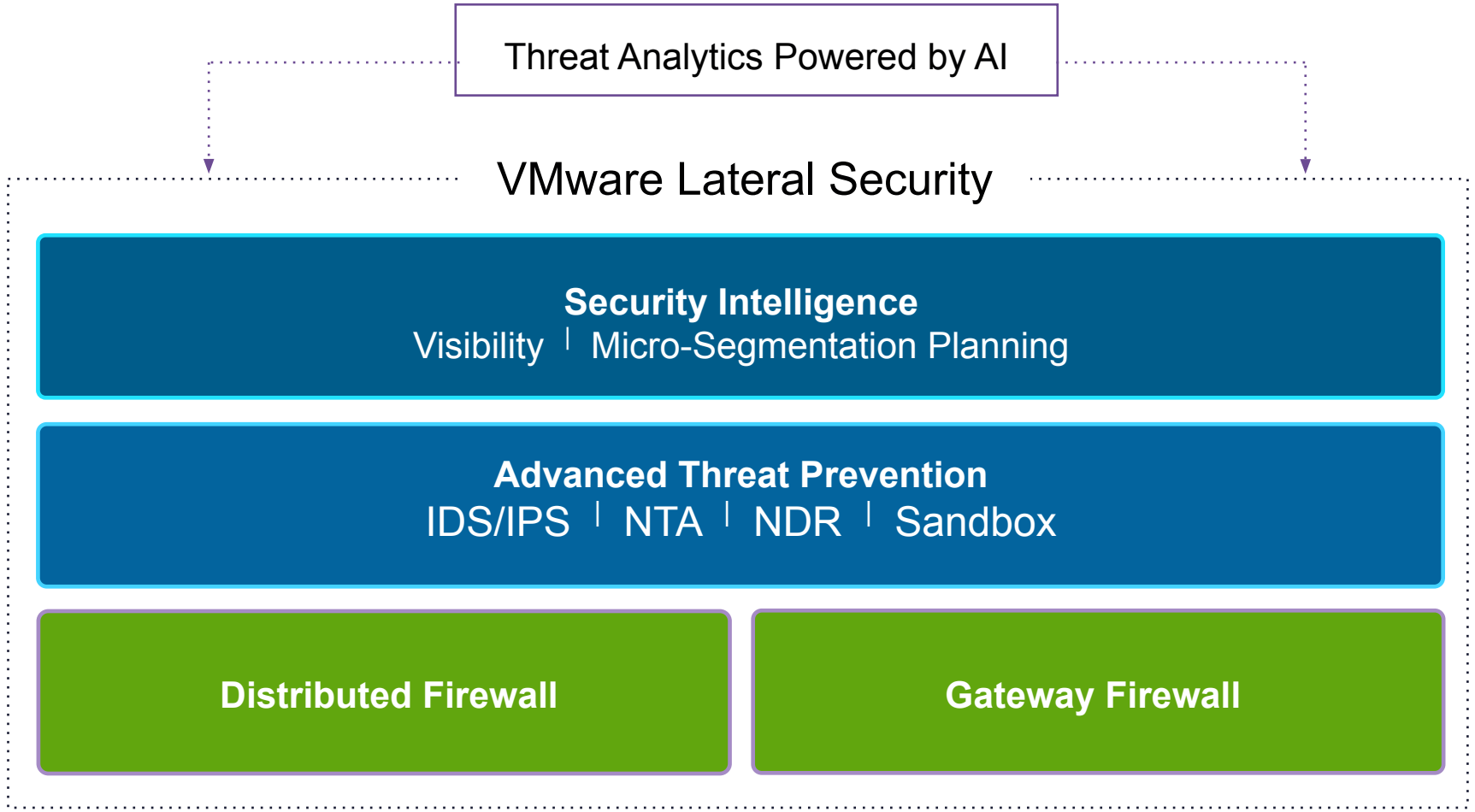
Segmentation/ Microsegmentation

NSX Network Detection & Response

- Tapless NTA (E-W Visibility)
- NSX Sandbox (Guest Introspection)
- NSX Distributed IDS/IPS
- Network Event Correlation

Securing VCF with VMware Firewall

Comprehensive VMware Lateral Security Defense



App Discovery
Security Analytics
Rule Recommendations

Zero-day Exploits
Known Vulnerabilities
Anomaly Detection

Micro Segmentation
Segment Zones

Securing VCF with VMware Firewall

Lateral Security Use cases

Zero Trust

SECURE INFRASTRUCTURE

DFW

Protect critical infrastructure services

Eg., allow sshv2 only, no telnet

SECURE VIRTUAL ZONES

DFW, GFW

Create zones in software with

No changes to underlying infra

SECURE APPS

DFW, Security Intelligence

Secure critical applications

Eg., EPIC, SWIFT, Horizon VDI

Ransomware Protection

VIRTUAL PATCHING

IDPS

Protect from known vulnerabilities

Reduce risk while you schedule maintenance

MALWARE PREVENTION

Sandbox, IDPS, DFW

Protect against known and zero-day ransomware

Prevent lateral movement associated with ransomware

THREAT INVESTIGATION

Sandbox, IDPS, NTA NDR

Detect advanced Threats

Correlate Threats, Scope impact, prioritize respond

Security Solutions

Secure VCF

DFW, ATP

Secure management and infra

Secure workload domains

SECURE RANSOMWARE RECOVERY

DFW, ATP, VCDR

Recover to a known clean state

Monitor recovery points before restoration

COMPLIANCE

DFW, GFW and IDS/IPS

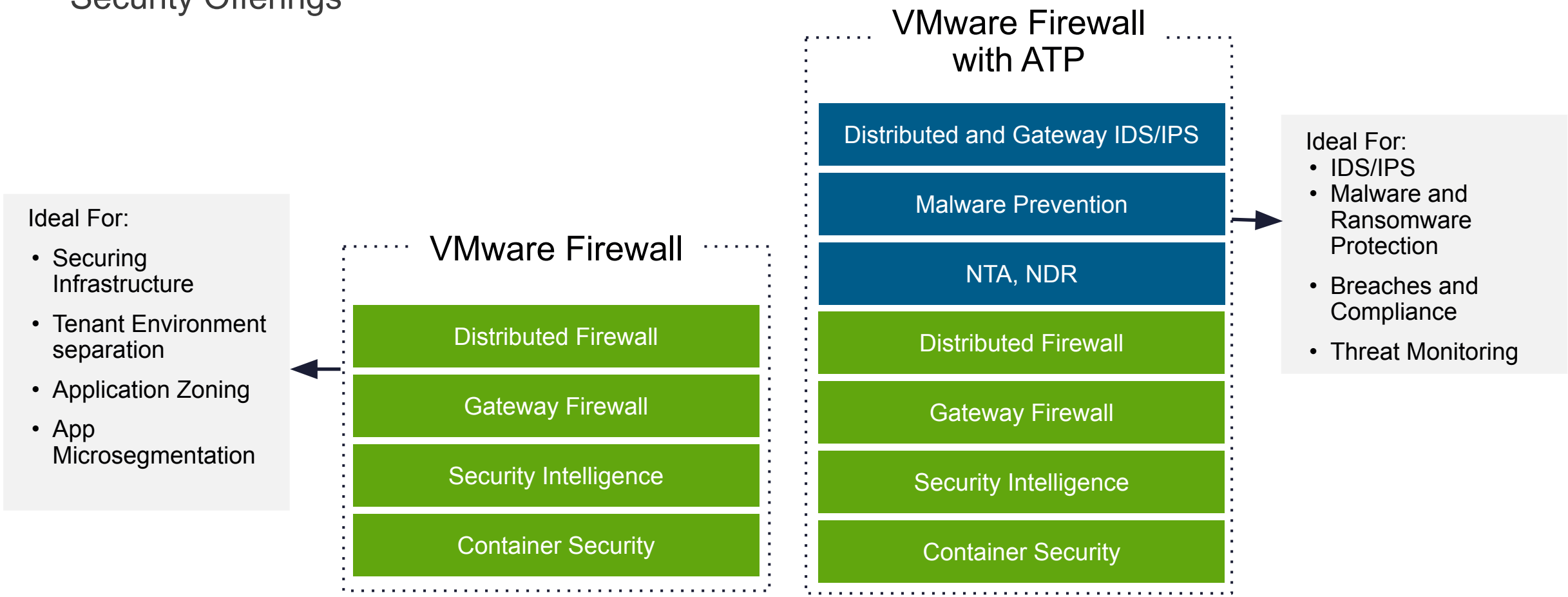
Assist to create compliance zones

Meet Audit goals. PCI, HIPAA requires IDS/IPS

vmware by Broadcom

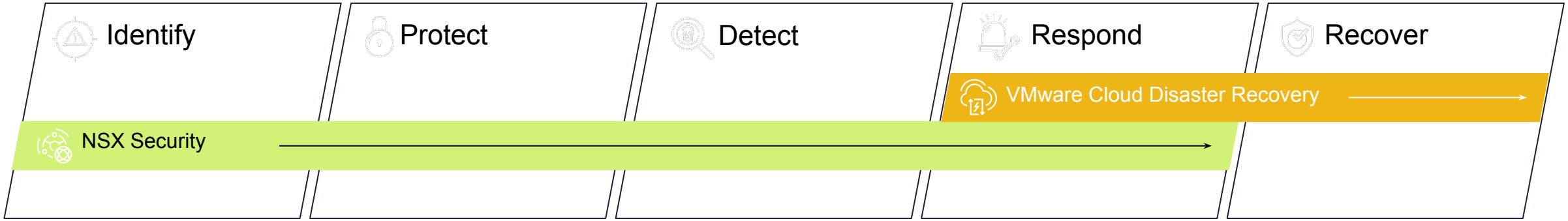
Securing VCF with VMware Firewall

Security Offerings



Securing VCF with VMware Firewall

Mapping to NIST Cyber Security Framework



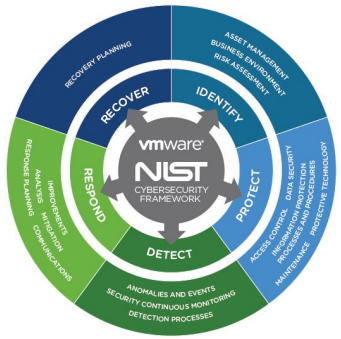
- Baseline Network Environment
- High Value Assets Tagging
- Flow Visualization
- DR Plan Config, Test, Check
- Application Dependency Mapping

- Network Segmentation
- IDS/IPS/Deep Packet Inspection
- Attack Surface Reduction
- Micro-segmentation
- Malware Prevention

- Signature-based & behavior-based detection (Network)
- Signal Correlation Across Detectors
- Sandbox/Malware Detection
- Network Anomaly Detection

- Network Quarantine
- Network Resets
- Allow/Deny
- Failover to Isolated Recovery Environment
- Identify restore point candidates

- Validation of recovery points
- File and folder-level recovery
- Delta-based Failback
- Review, Audit & Remediate



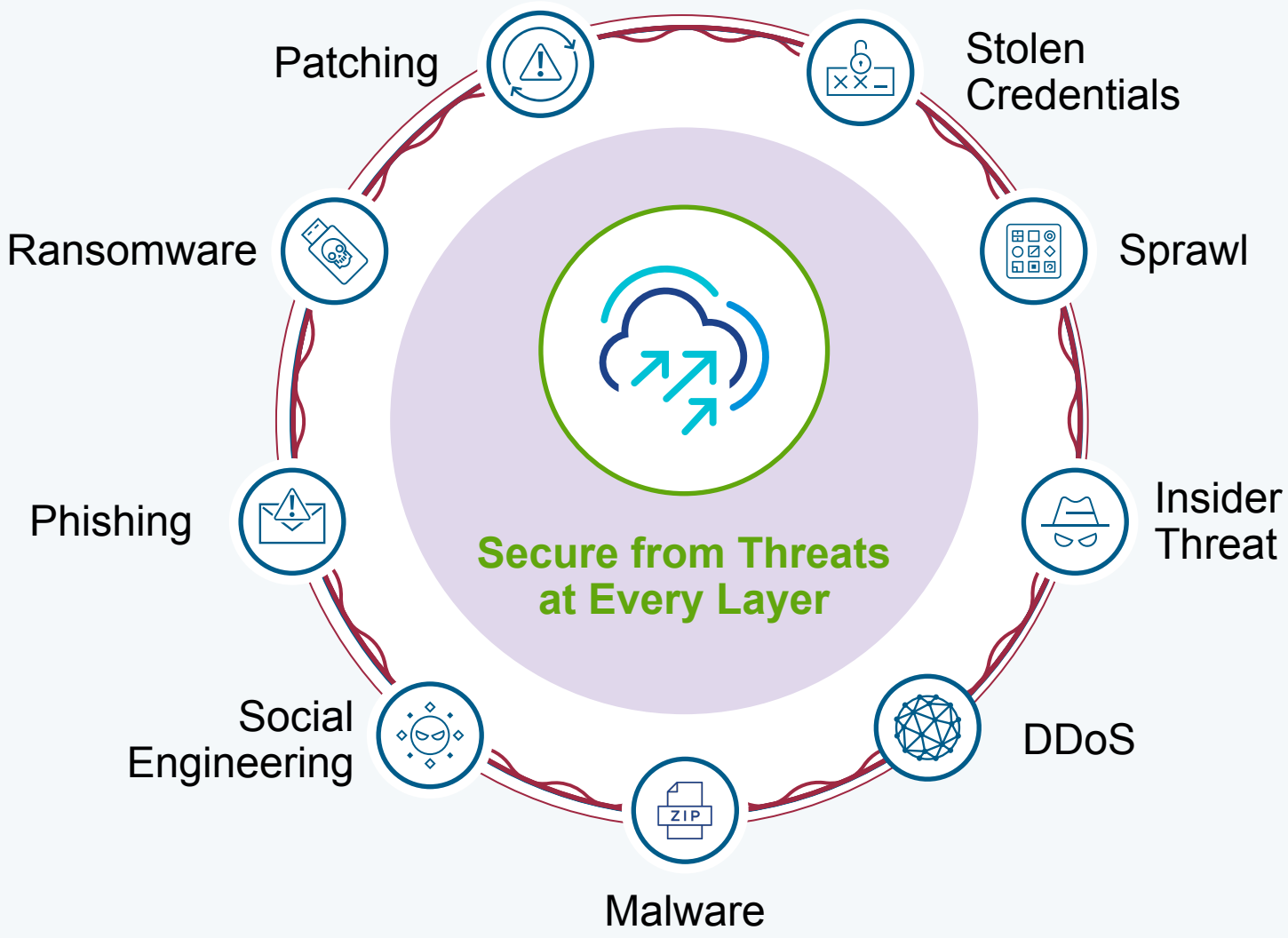
VMware Firewall/ATP

VMware Cloud DR

MANAGING RISK & CYBERSECURITY*

Secure, systematic approach to attacks

- Implement zero-trust defense for app and data security
- Proactively inspect and monitor for threats
- Establish a rapid recovery plan for potential attacks

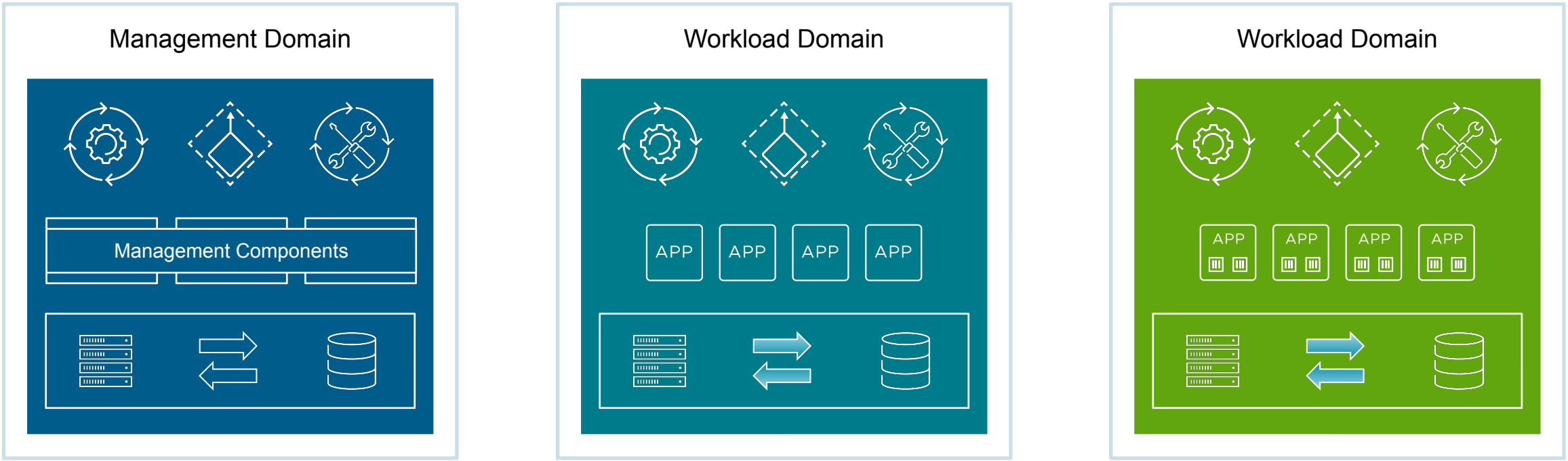


*Available with VMware Firewall + ATP

Securing VCF Workload Domains

Management and Workload Domains

Delivering a Scalable Private Cloud Platform



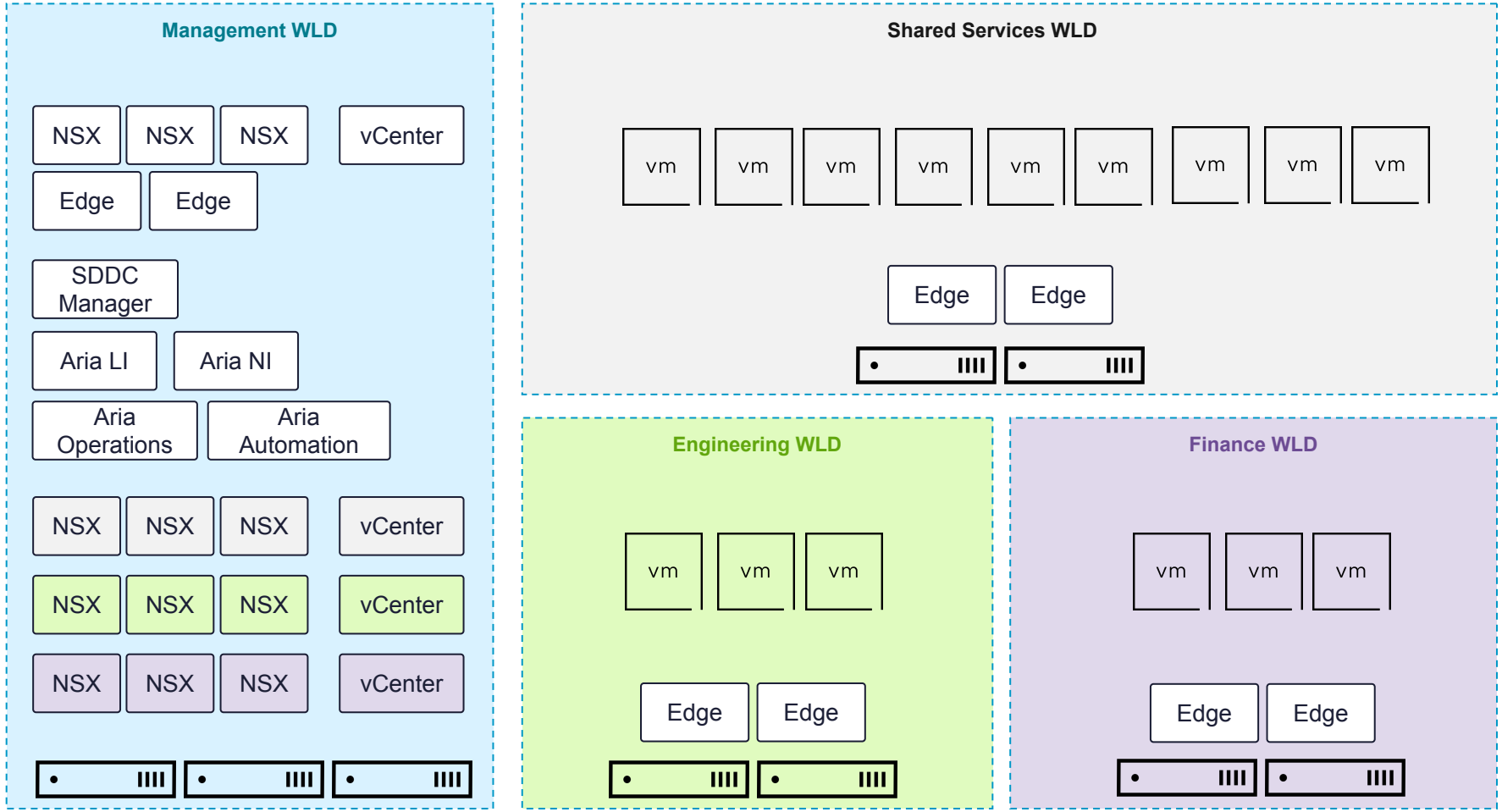
Securing VCF with VMware Firewall

VCF Workload Domains at a Glance

Management Domain has dedicated NSX Managers and Edge cluster

Multiple VI Workload Domains can be added, using new or exising NSX Managers

VI Workload Domain NSX Managers and vCenters are located in the Management Worload Domain



Securing VCF with VMware Firewall

VI and MGMT WLDs

Securing VI WLD

Secure Apps with Security Intelligence and DFW

Ransomware Protection & Threat Investigation with NSX ATP

Secure Virtual WLD zones using the GFW/DFW

Securing MGMT WLD

Secure Infrastructure using the Distributed Firewall

Compliance

Securing Virtual Infrastructure Workload Domains

Highlighted Use Cases

Secure Zones

Gateway or Distributed Firewall

Between WLDs or within a WLD

Create network-based or network-agnostic zones/environments (i.e. dev/test/prod/compliance)

Isolated zones or provide controlled zone access

Secure Apps

DFW and Security Intelligence

Minimize the blast radius/attack surface

Zero-Trust model for Network Security

Align security policy lifecycle with application lifecycle

Ransomware Protection & Threat Investigation

Advanced Threat Prevention

Prevent exploits and extend patching cycles with Virtual Patching

Detect & Prevent evasive malware

Prioritize and correlate threats into actionable campaigns

Security across Sites with NSX Federation

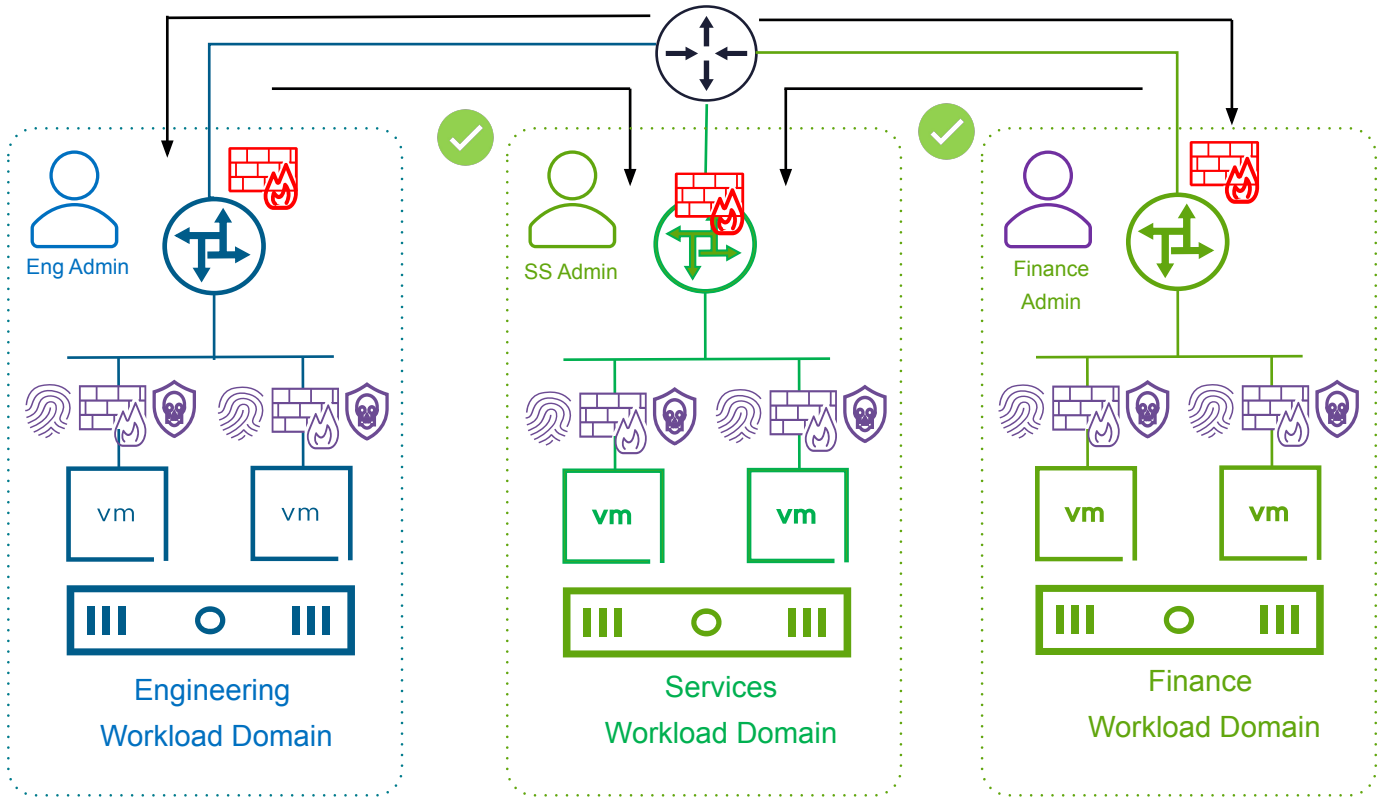
Secure VI WLD Zones

Zoning Between WLDs using the Gateway Firewall

GFW can be used to implement zoning between WLDs

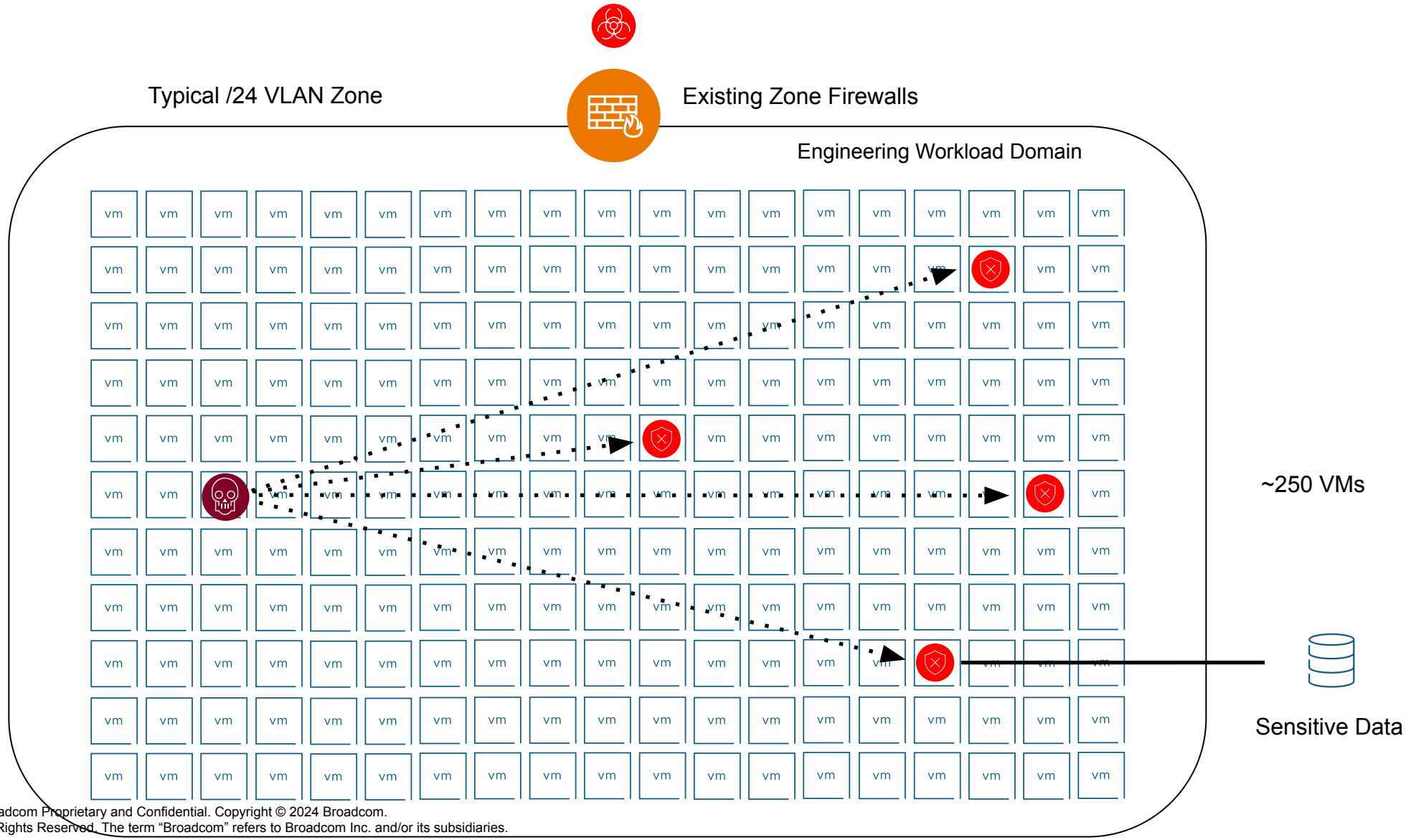
Restrictive inbound GFW rules

intra-WLD security with full NSX stack (DFW, DIDPS, MP, …)



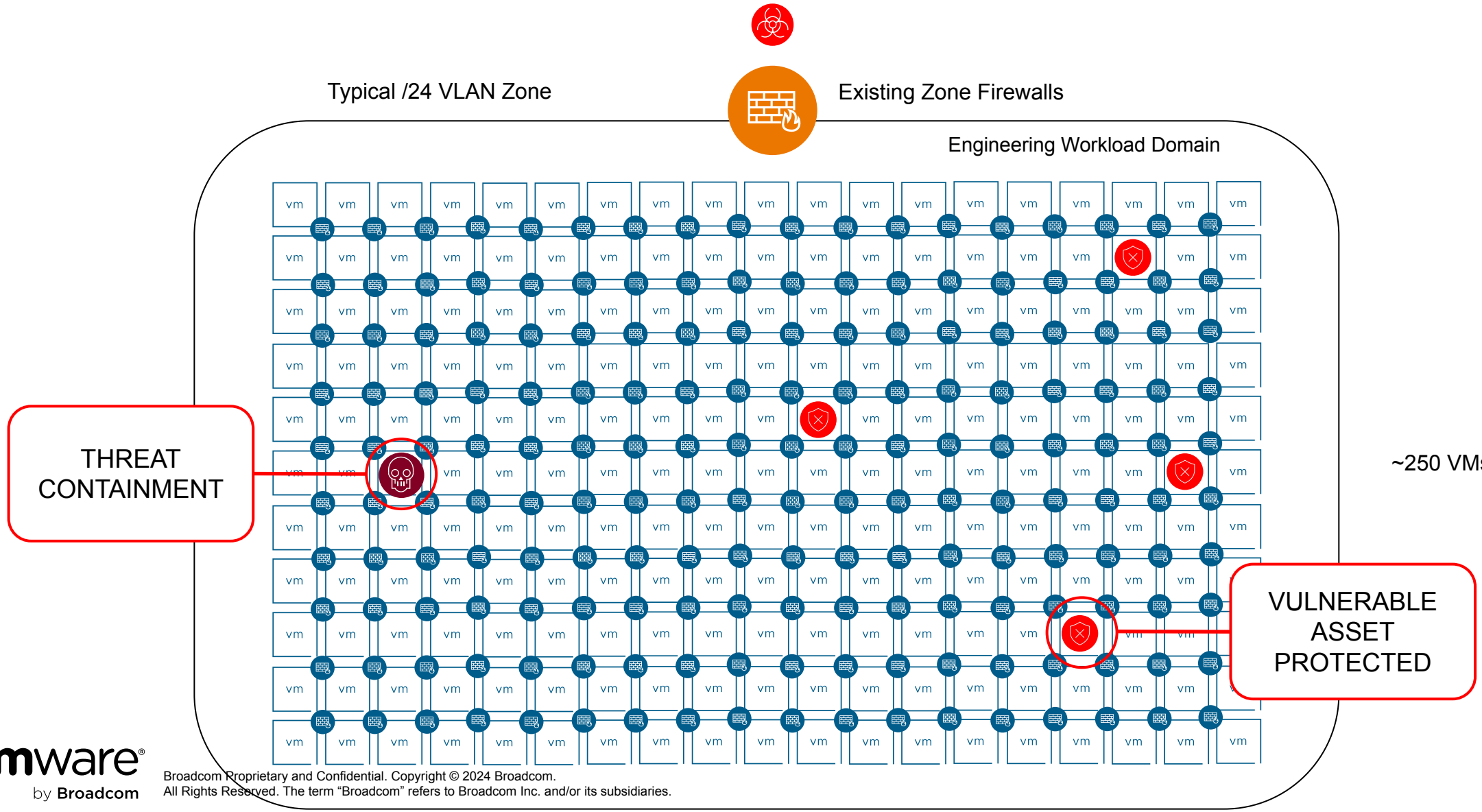
Security within a VI WLD

My WLDs are isolated, but what about…Security WITHIN the WLD ?



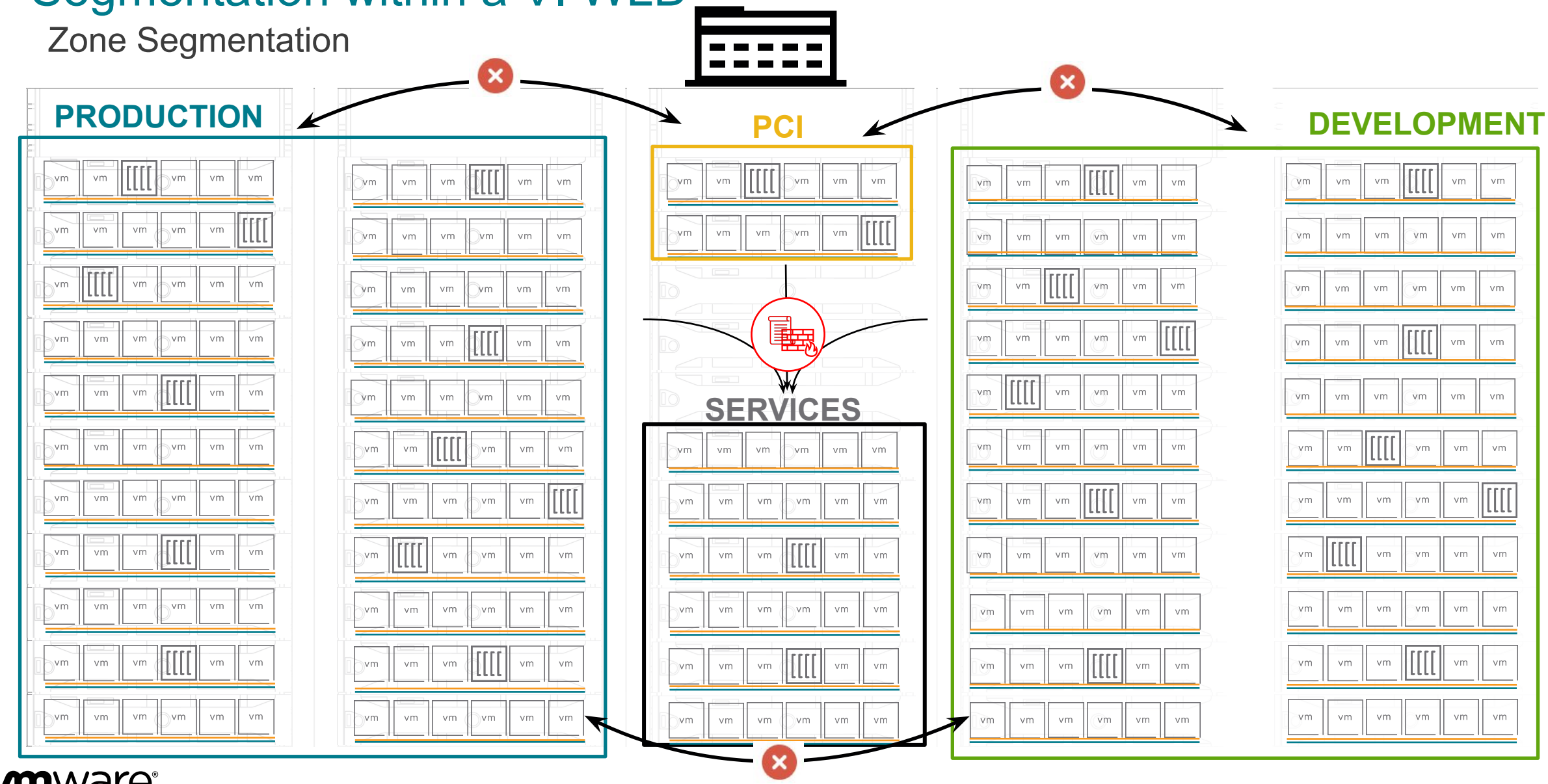
Segmentation within a VI WLD

My WLDs are isolated, but what about…Security WITHIN the WLD ?



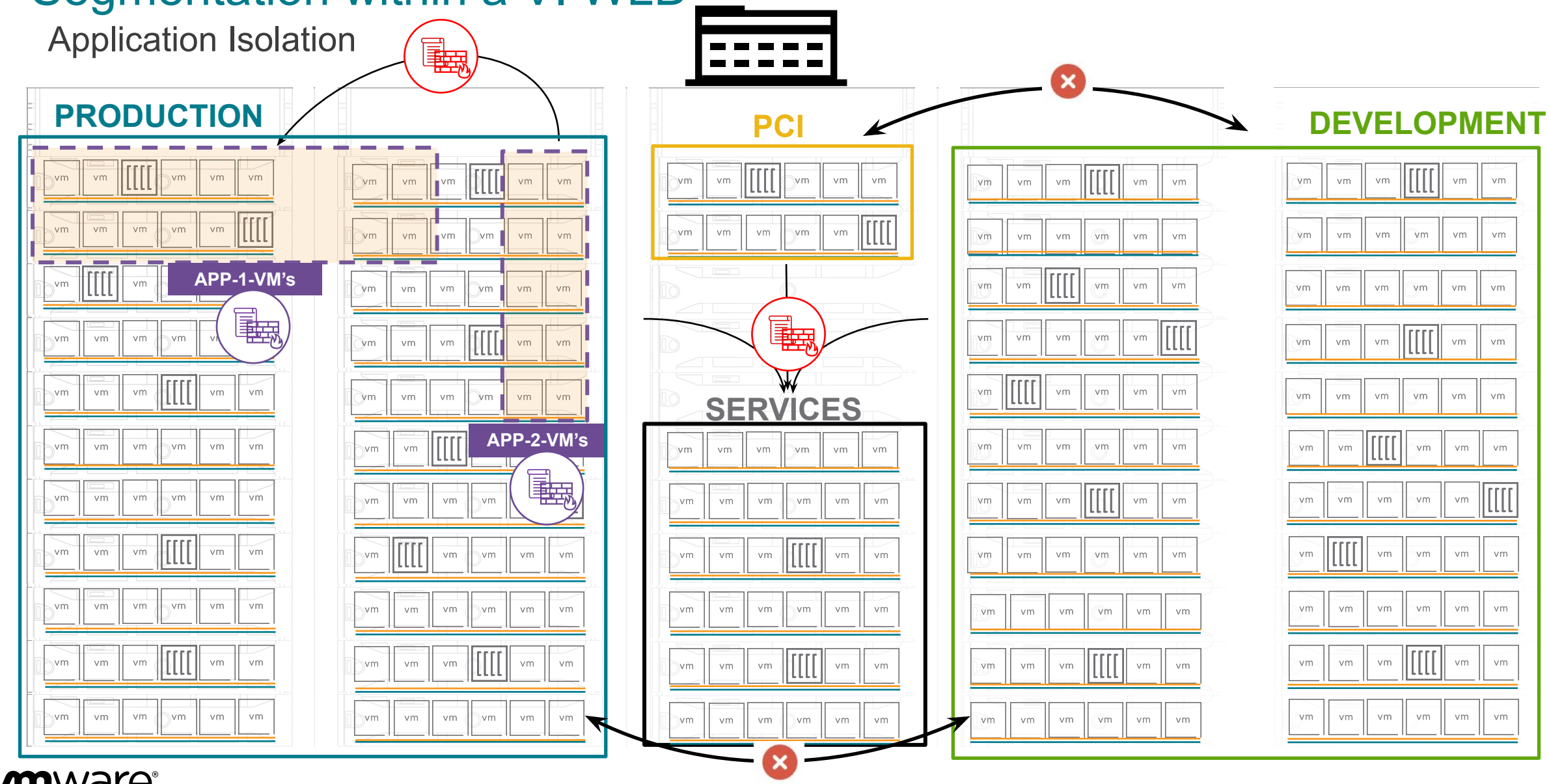
Segmentation within a VI WLD

Zone Segmentation



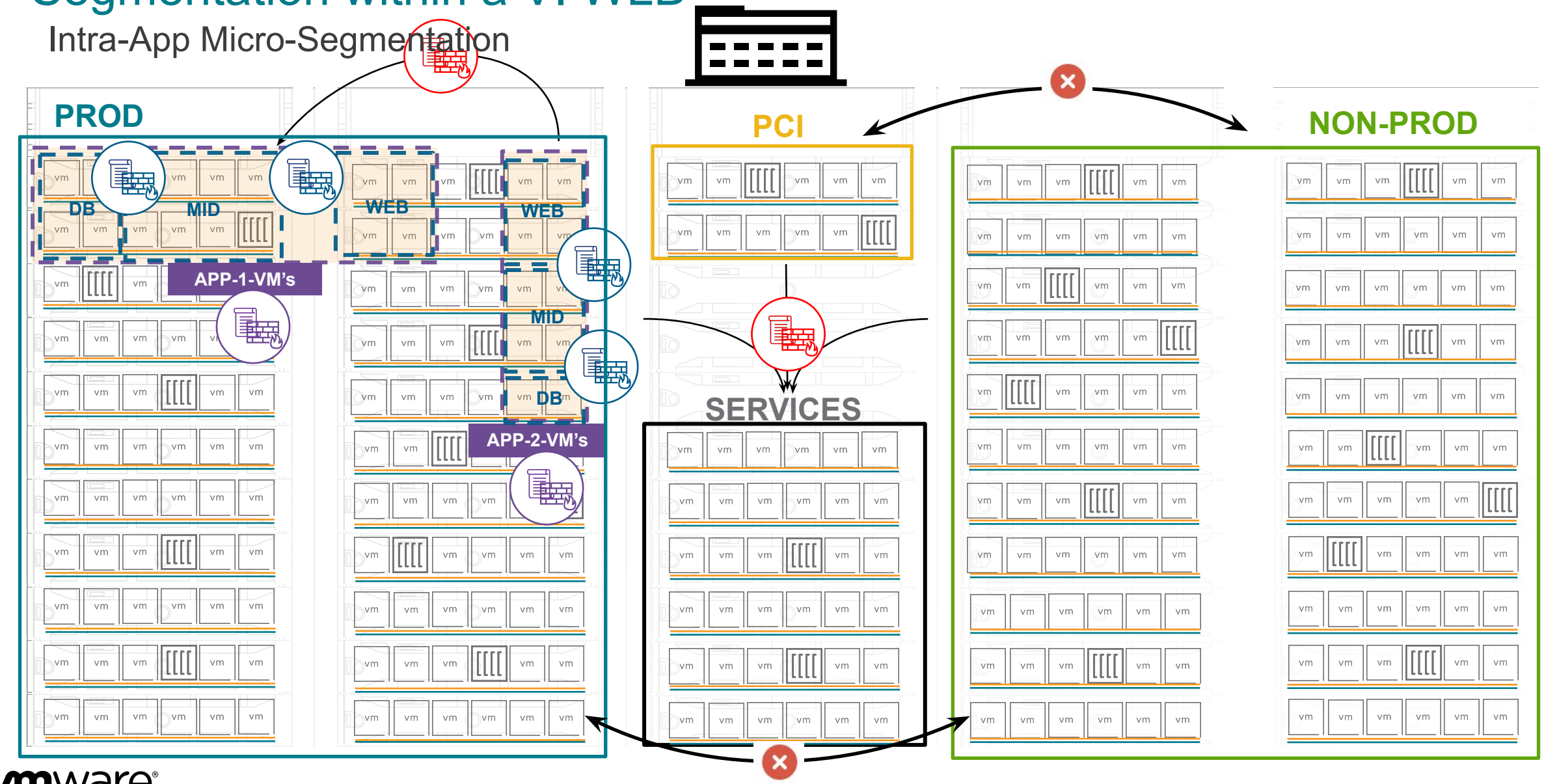
Segmentation within a VI WLD

Application Isolation



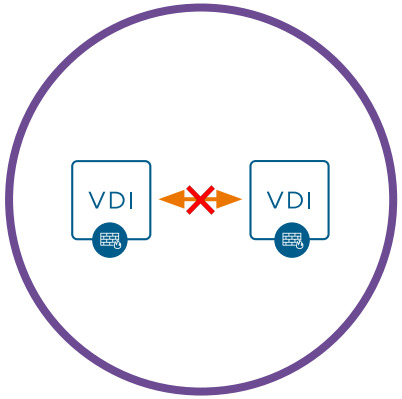
Segmentation within a VI WLD

Intra-App Micro-Segmentation



Segmentation within a VI WLD

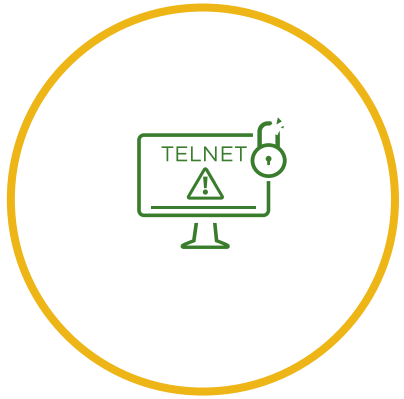
Quick Win Segmentation Use-Cases



VDI/EUC
Published
App
Security

Lock/Monitor
East/West
RDP

Obsolete
Operating
Systems

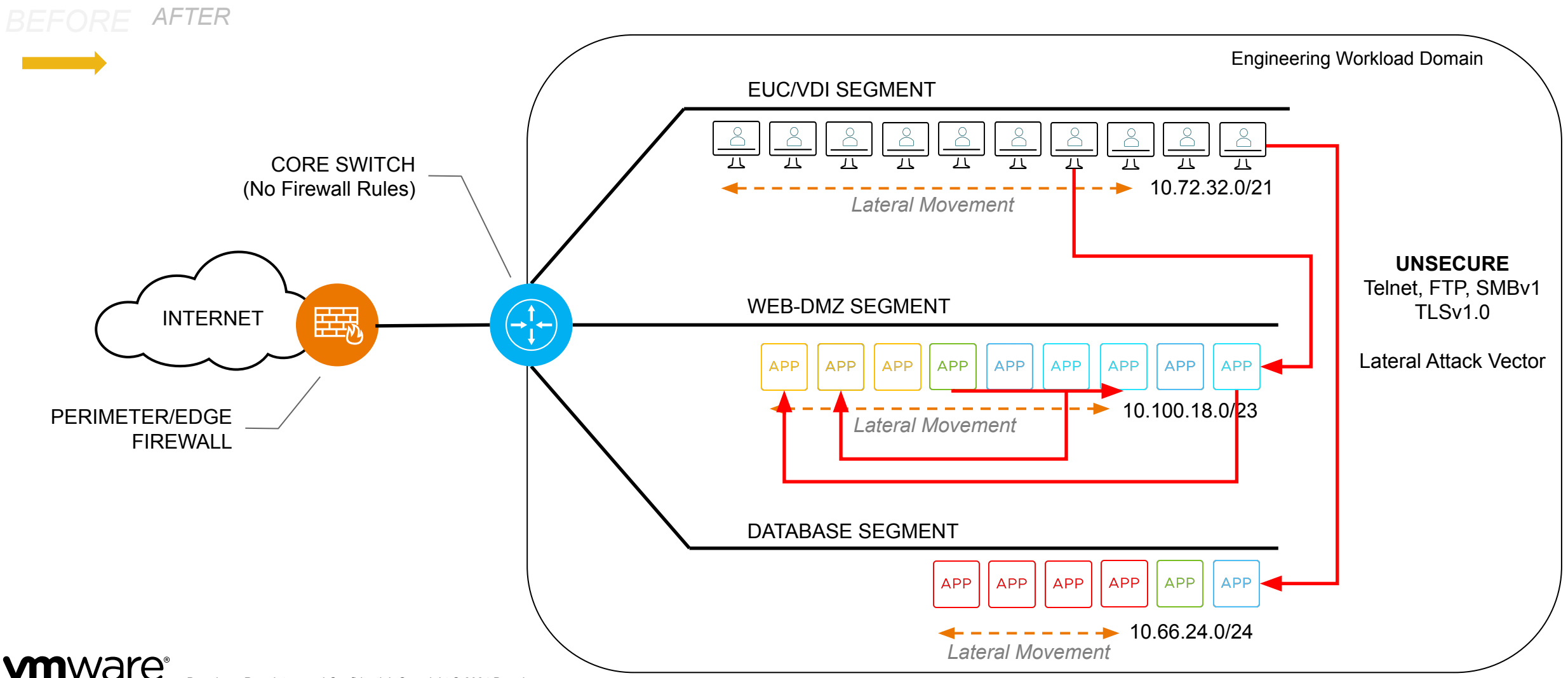


Block
Unsecure
Protocols
(Compliance)

VDI/RDSH
Identity
Firewall

Segmentation within a VI WLD

Unsecure Protocols



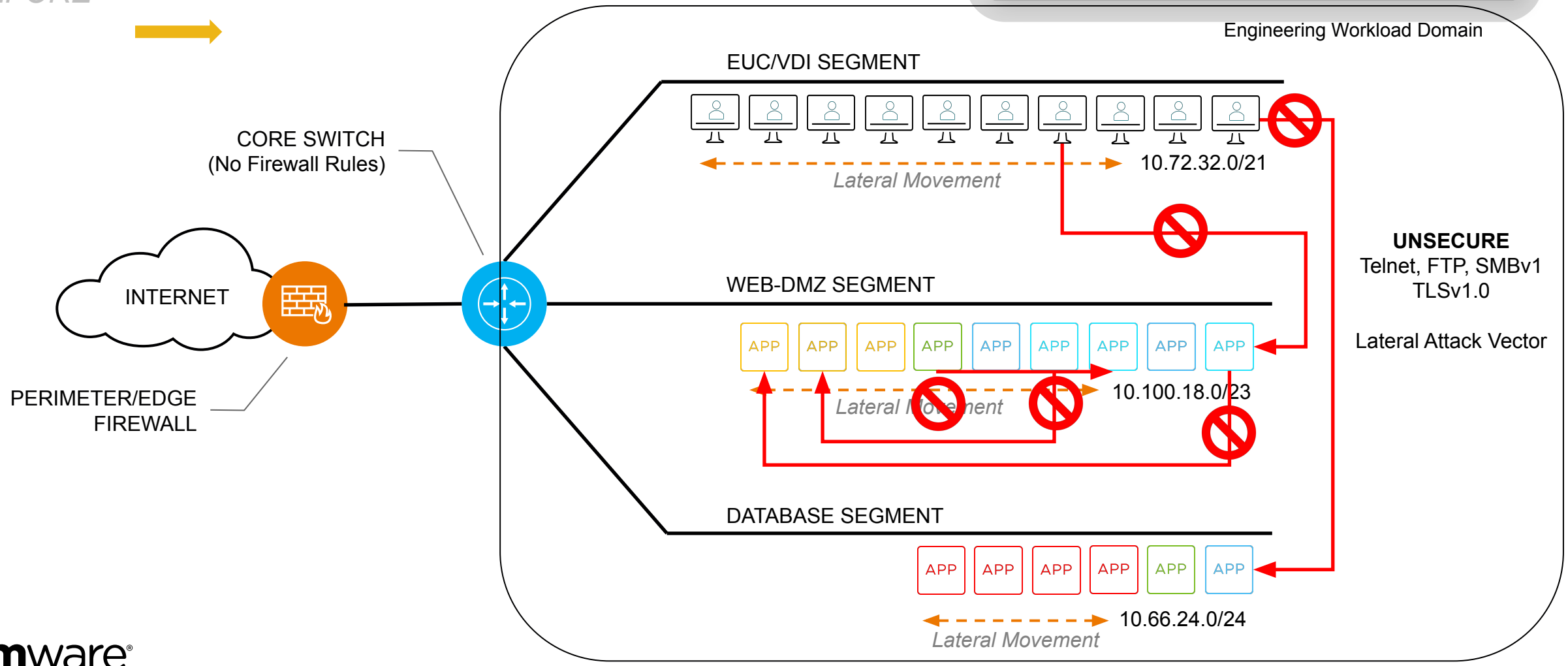
Segmentation within a VI WLD

Unsecure Protocols

4 SIMPLE RULES

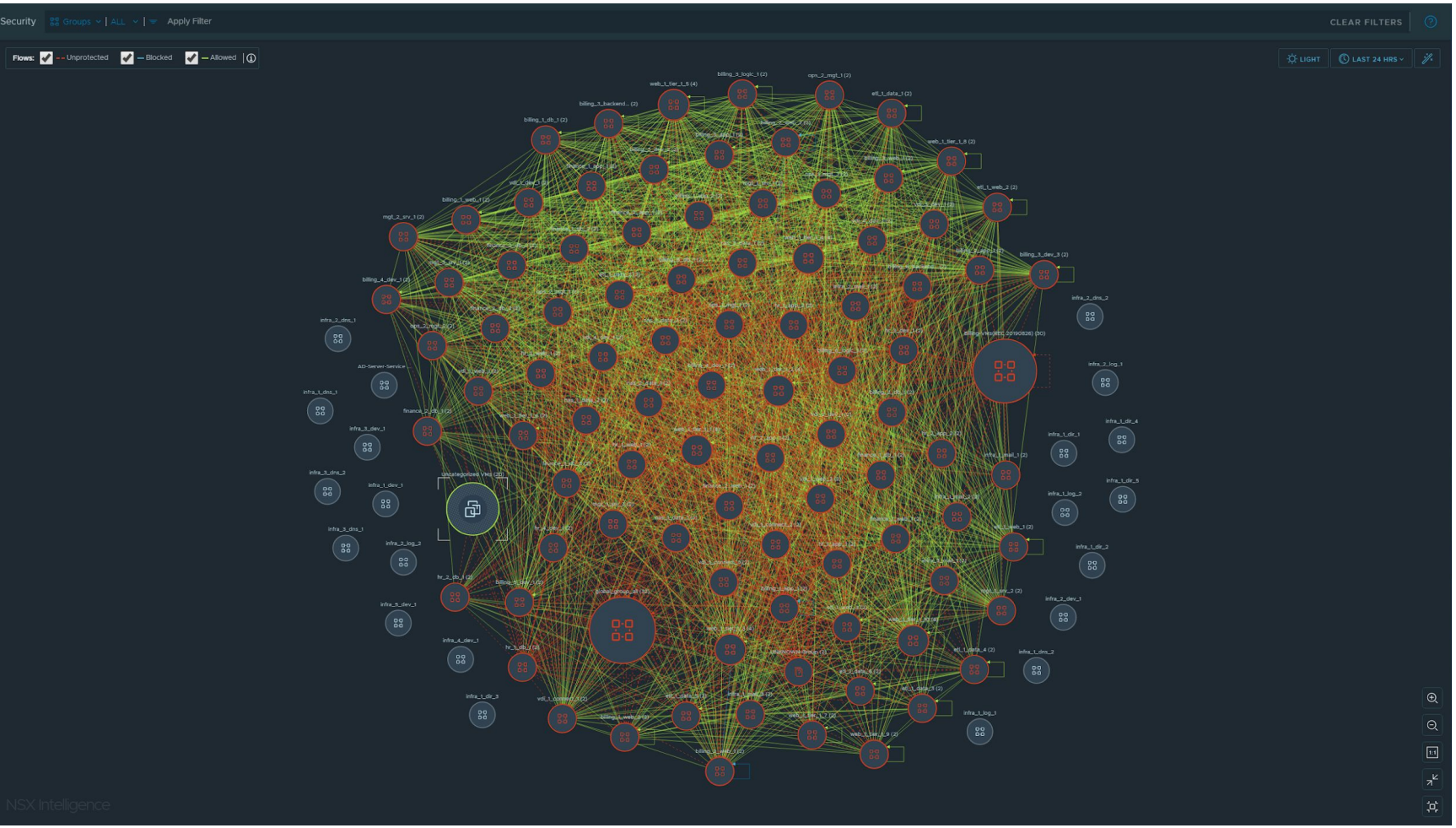
1. Src: [Any] to Dst: [Any] [TELNET] Action: Drop
2. Src: [Any] to Dst: [Any] [FTP] Action: Drop
2. Src: [Any] to Dst: [Any] [SMBv1] Action: Drop
2. Src: [Any] to Dst: [Any] [TLS1.0] Action: Drop

BEFORE AFTER



Visibility and Analytics within a VI WLD

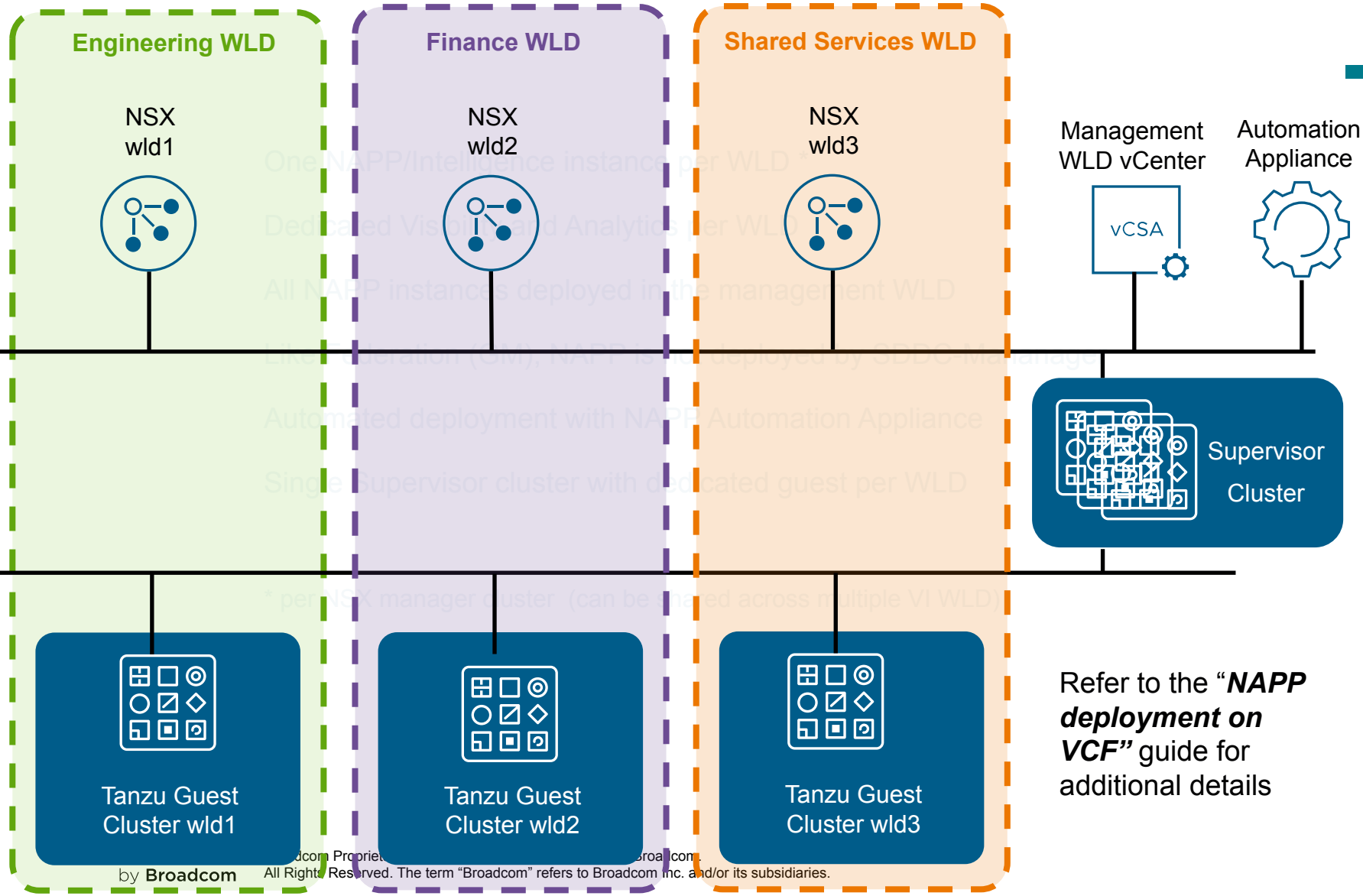
VMware Security Intelligence



- Visibility
- Policy Recommendations
- Network traffic Analysis
- Collection of events from WLD
  - Flow (L4/L7)
  - Context
  - Inventory

Visibility and Analytics within a VI WLD

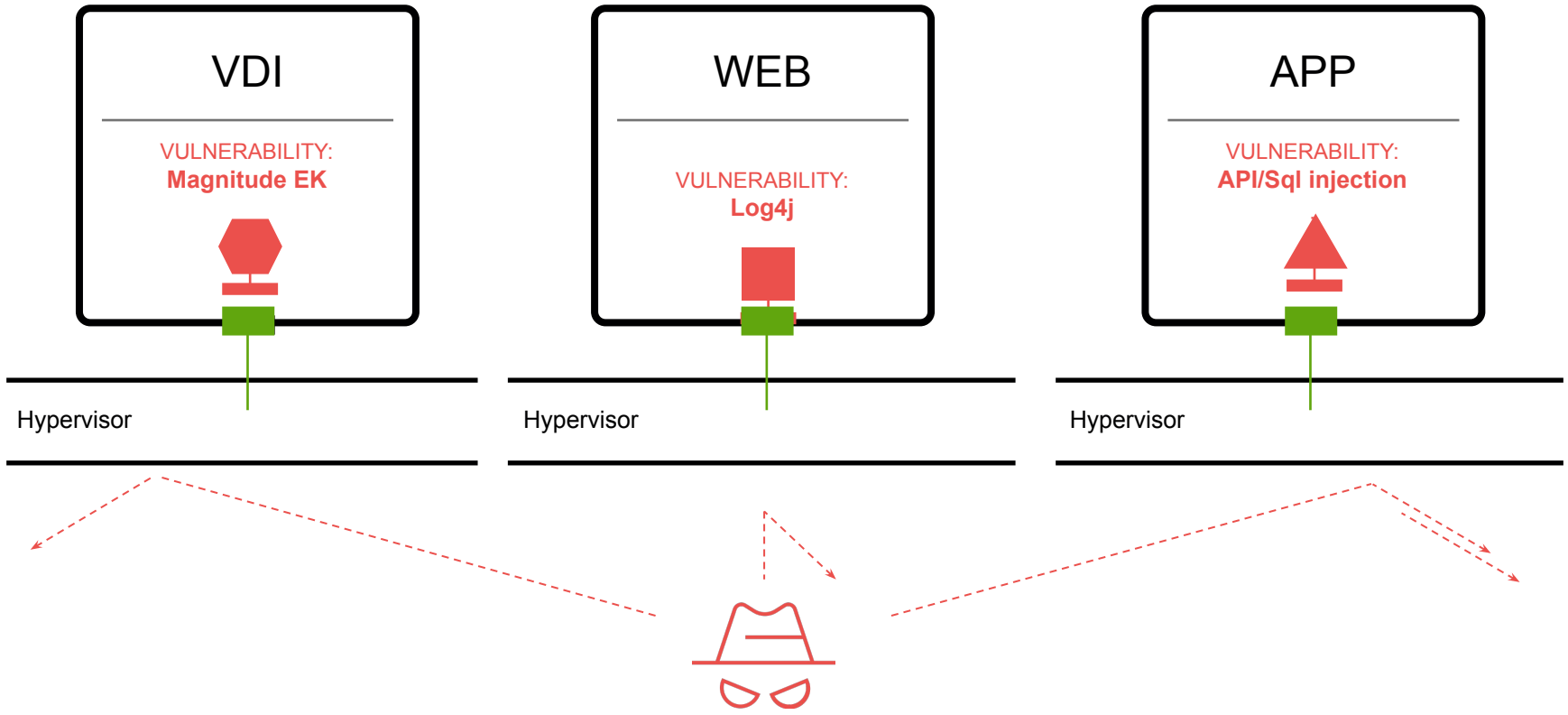
VMware Security Intelligence/NAPP



Refer to the "***NAPP deployment on VCF"*** guide for additional details

Ransomware Protection & Threat Investigation within a VI WLD

Virtual Patching with the Distributed IDS/IPS



Patching cycles are lengthy and often require maintenance window/downtime

Patches may not be available for older systems

Compensating control by intercepting vulnerable workloads with a dedicated IDPS signature set

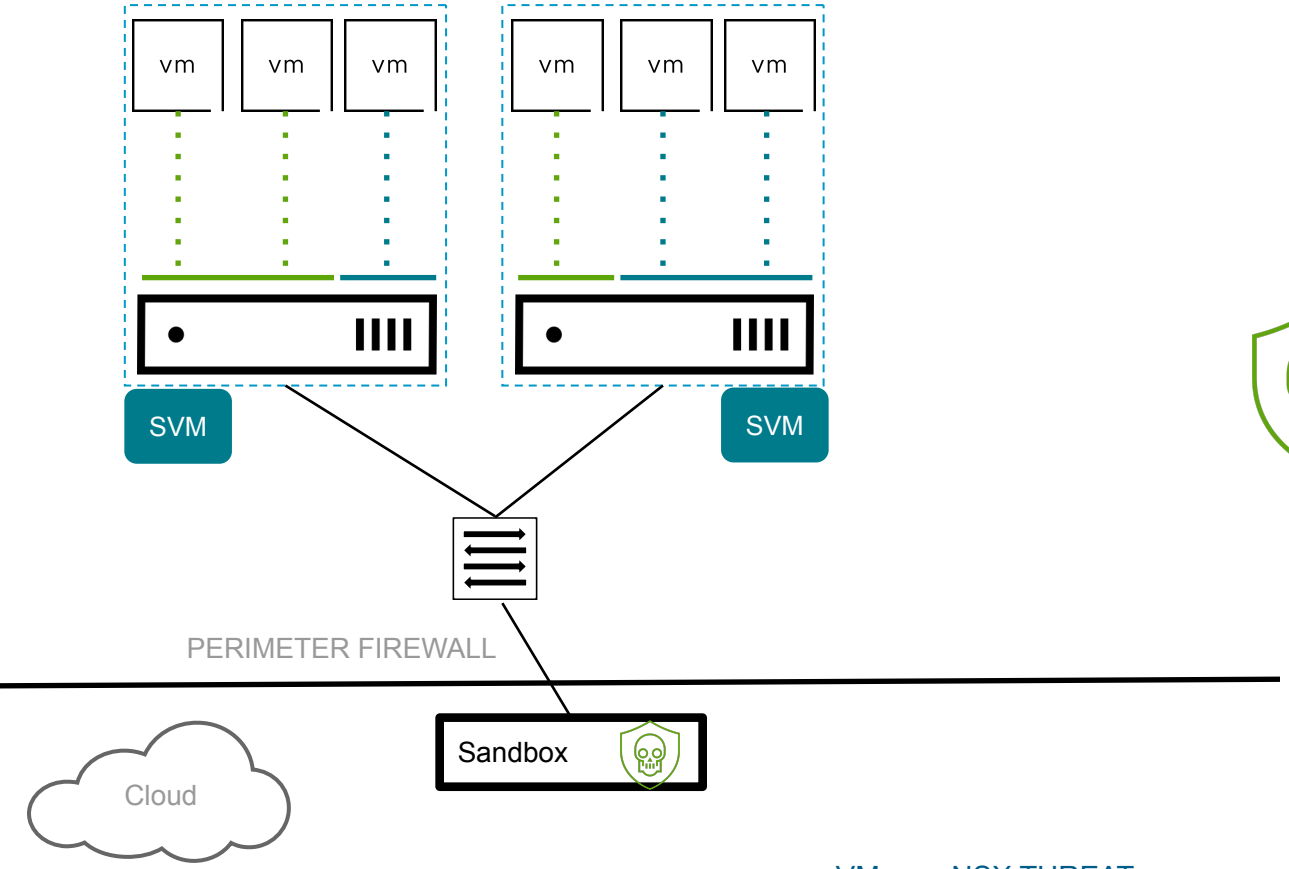
Protection regardless of where the attack comes from

Provides protection from network exploits until actual software patch is applied

Virtual Patching

Ransomware Protection & Threat Investigation within a VI WLD

Distributed Malware Detection and Prevention



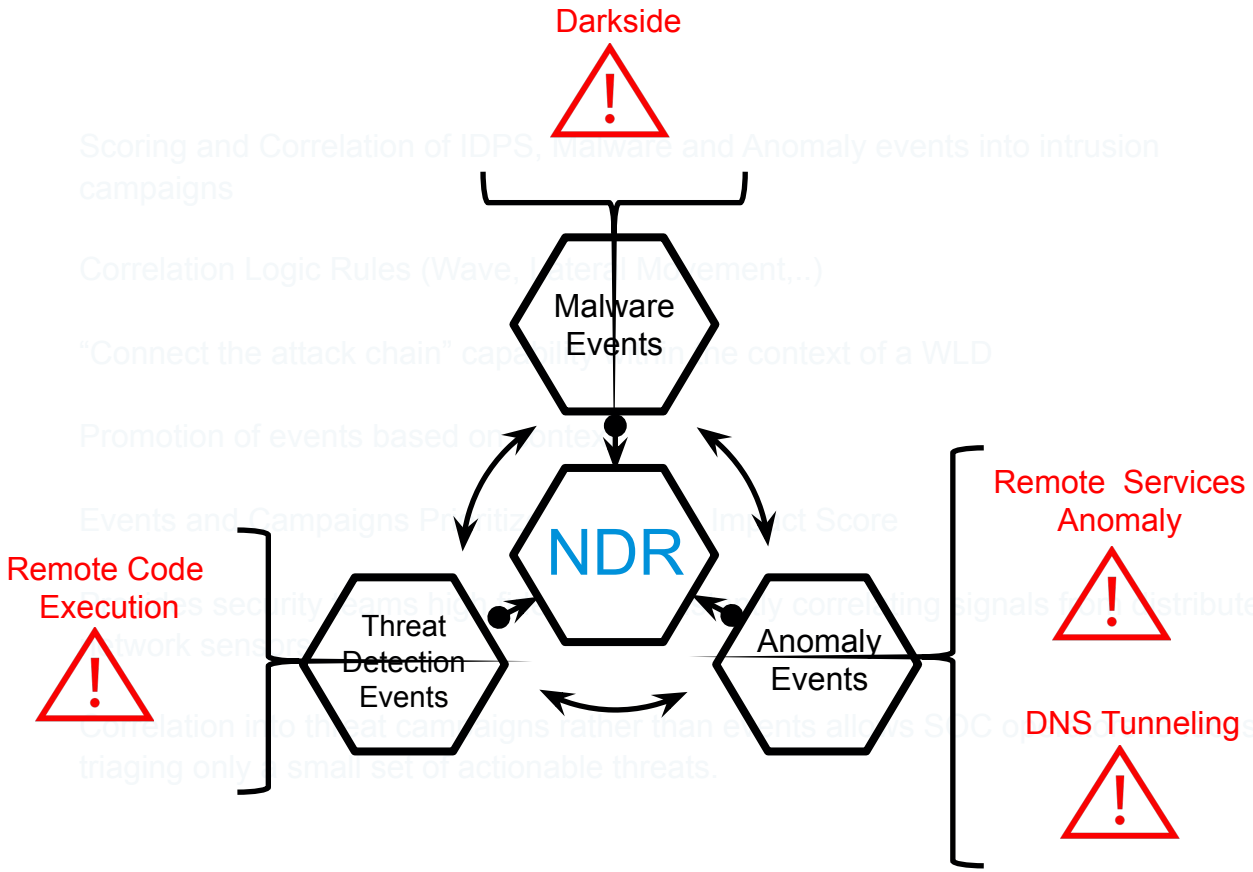
- Ability to analyze Files using Static and Dynamic techniques in the Data Center
- Can prevent known and unknown Malware from being executed in the Data Center
- Can be used even when Encryption or obfuscation is being used
- Uses Vmtools and Guest Introspection for file interception

VMware NSX THREAT INTELLIGENCE CLOUD

Your computer files have been encrypted. _

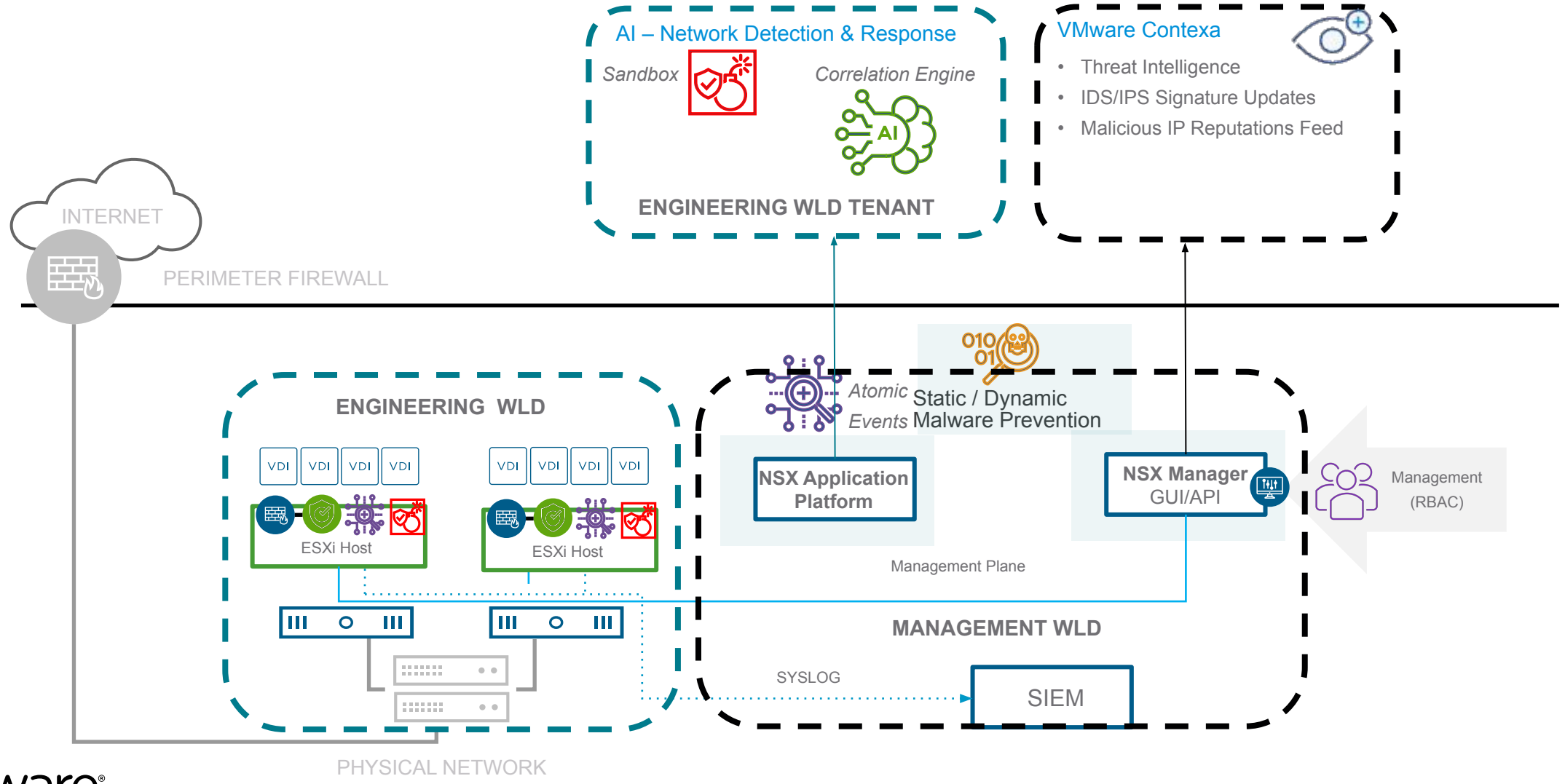
Ransomware Protection & Threat Investigation within a VI WLD

Threat Investigation with Network Detection & Response



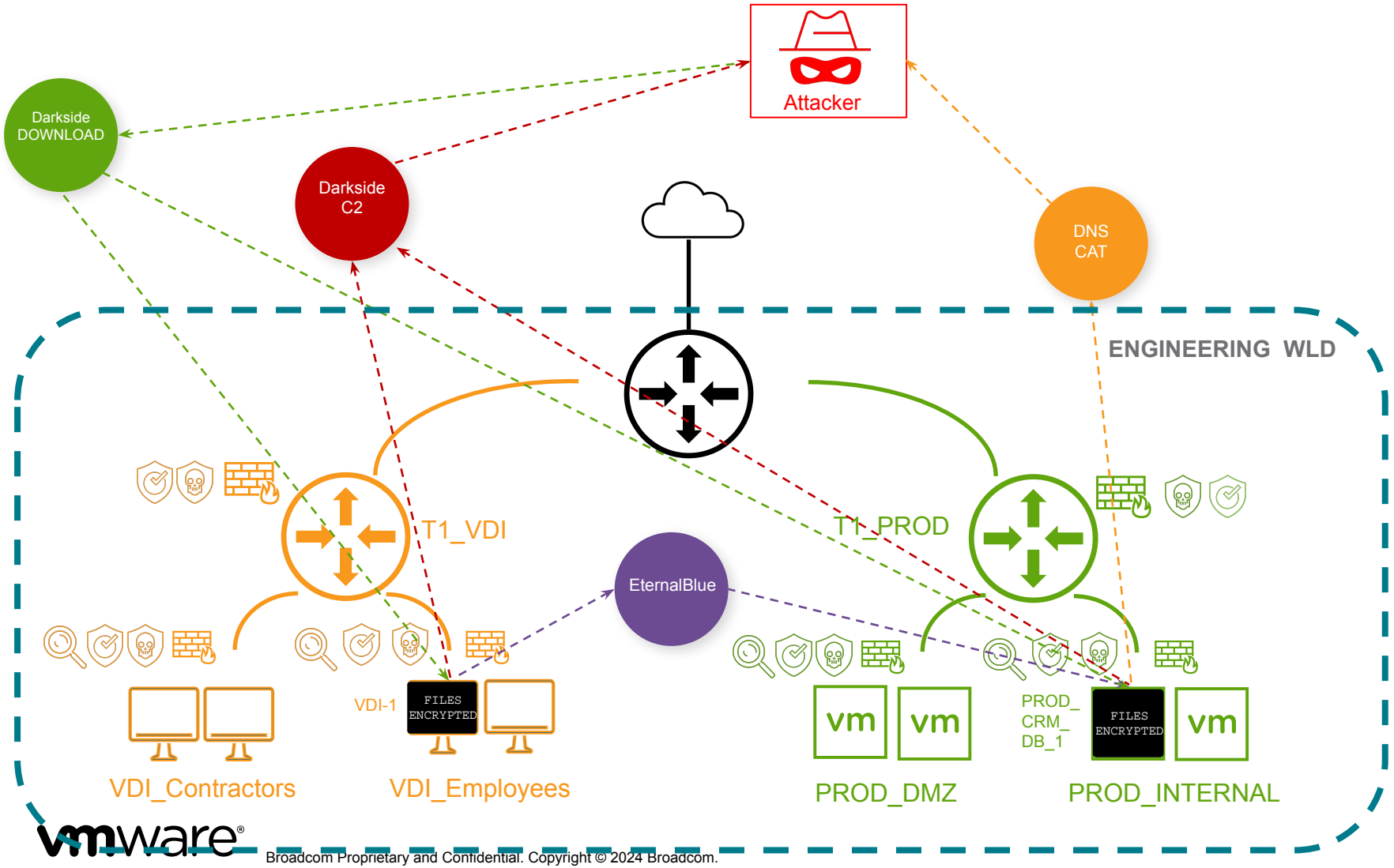
Ransomware Protection & Threat Investigation within a VI WLD

Threat Investigation with Network Detection & Response



Ransomware Protection & Threat Investigation within a VI WLD

Demo



Attack Stages

- Delivery
- Exploitation
- Command and Control
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Exfiltration

Demo

VMware Firewall with Advanced Threat Prevention

Security across Sites with NSX Federation

Federation Use Cases

NSX Federation Use Cases:

Operational simplicity

Common policy configuration

Global networking

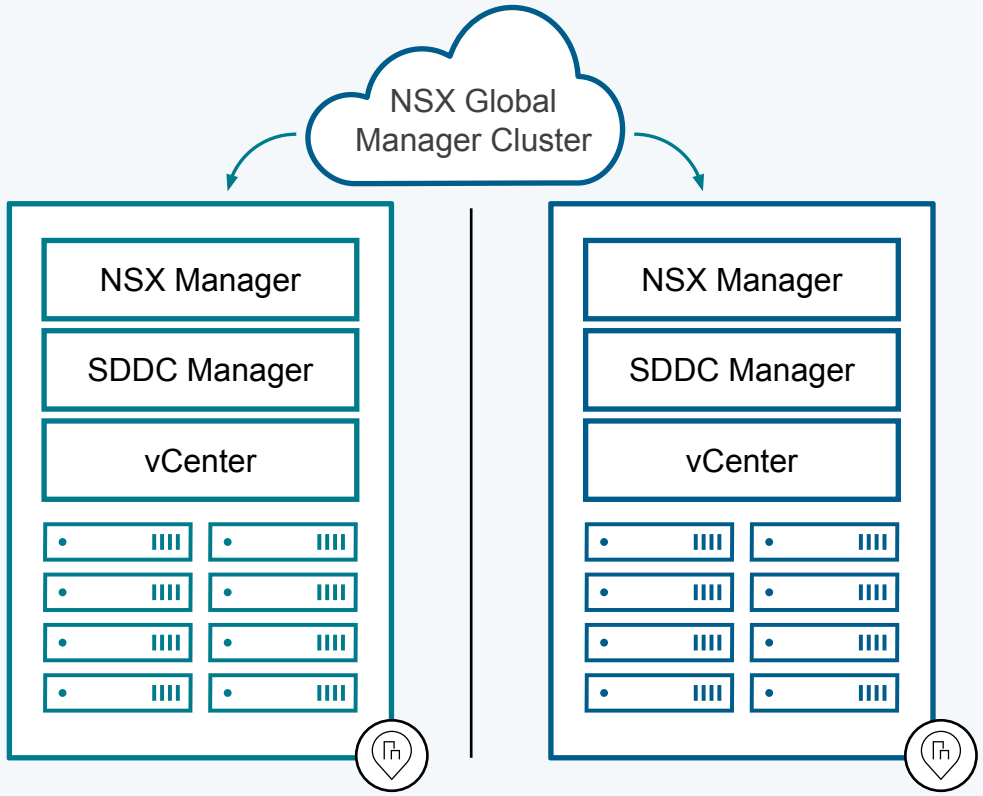
Simplified disaster recovery

Additional features provided by NSX Global Manager:

Password management

Certificate management

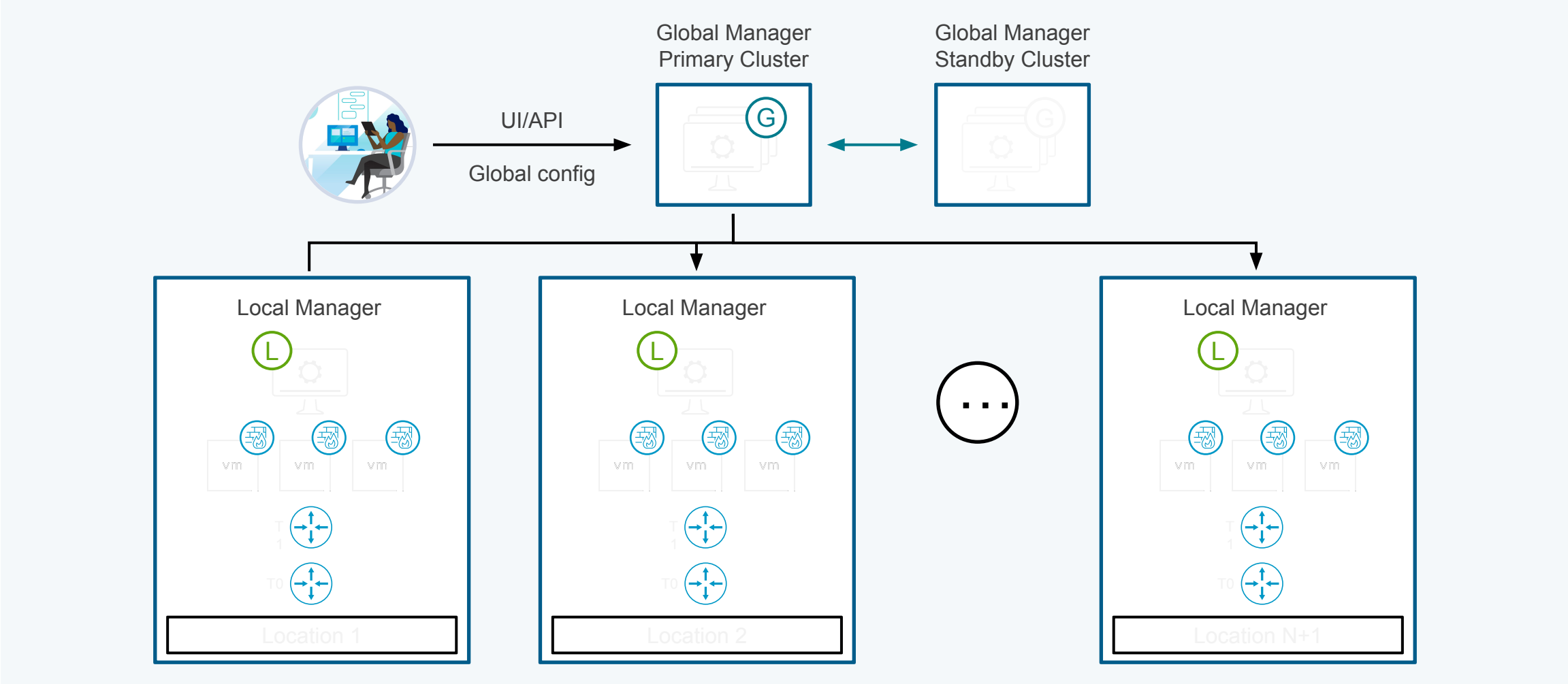
Backup and restore of Global Managers



NSX Federation Support is provided in Cloud Foundation as manual guidance

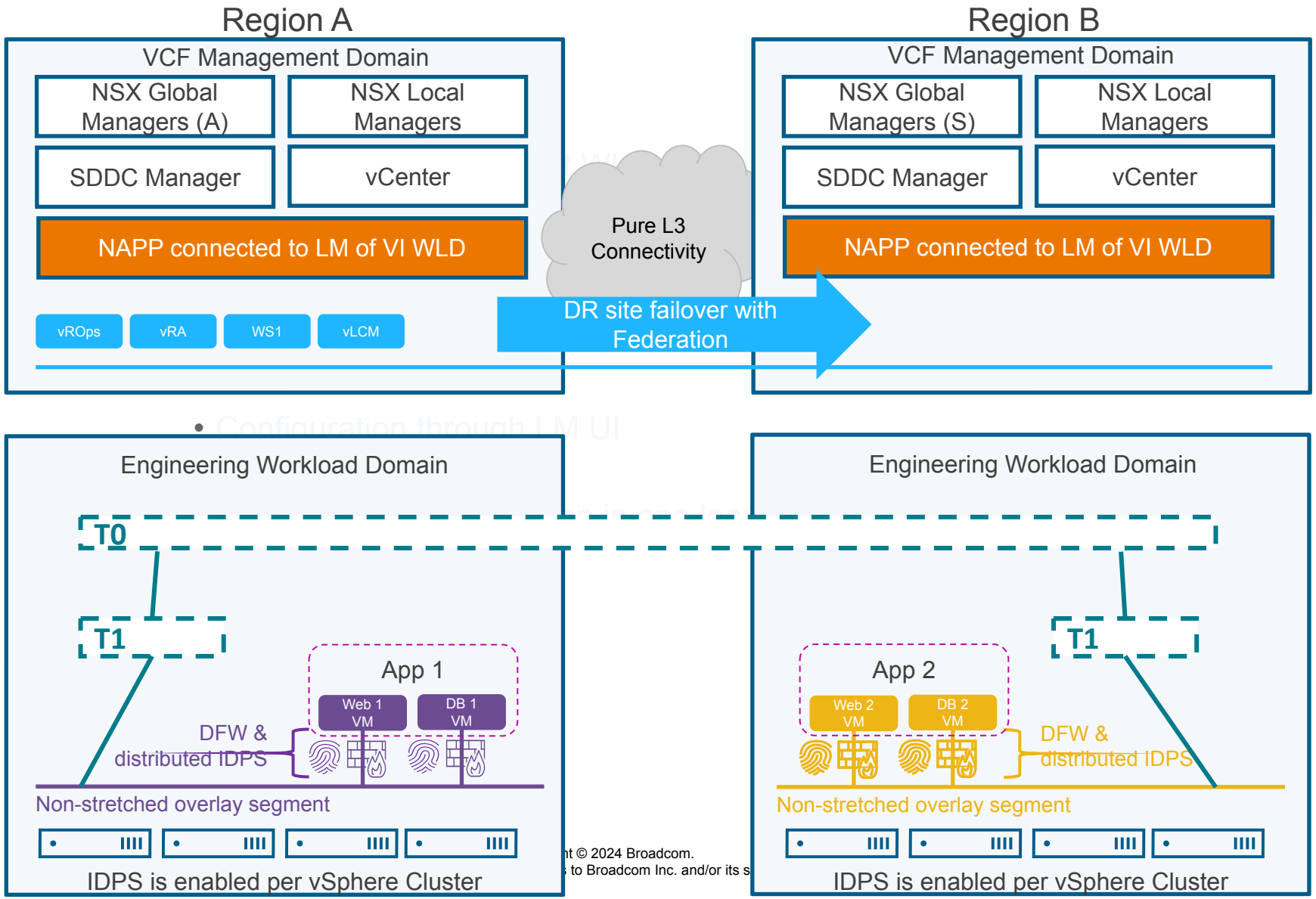
Security across Sites with NSX Federation

Manage multiple NSX Data Center environments



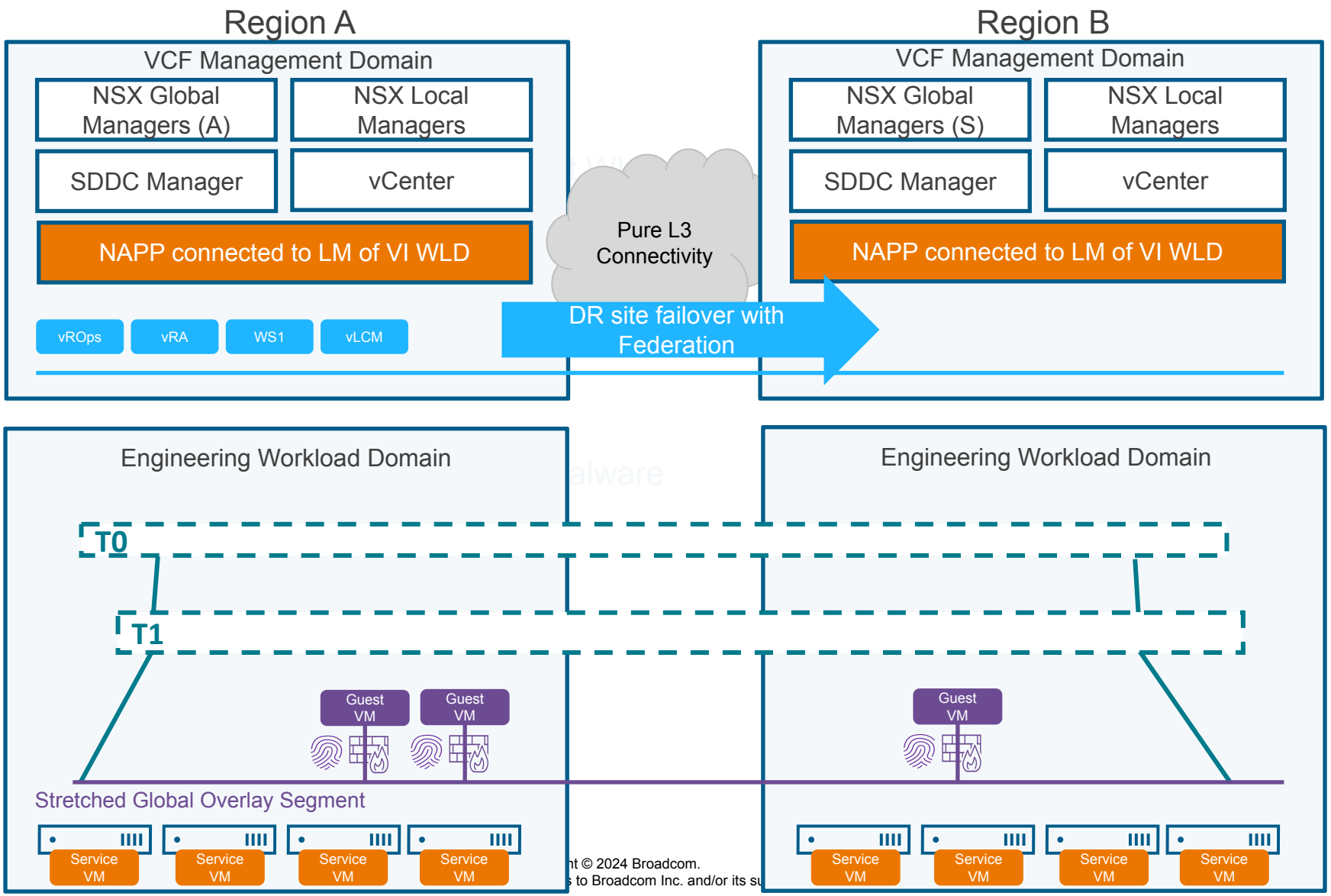
Security across Sites with NSX Federation

Security Intelligence / NDR – Recommended Deployment



Security across Sites with NSX Federation

Distributed Malware Prevention – Recommended Deployment



Security across Sites with NSX Federation

Supported VMware Security Services with VCF 4.5, 5.0 and 5.1

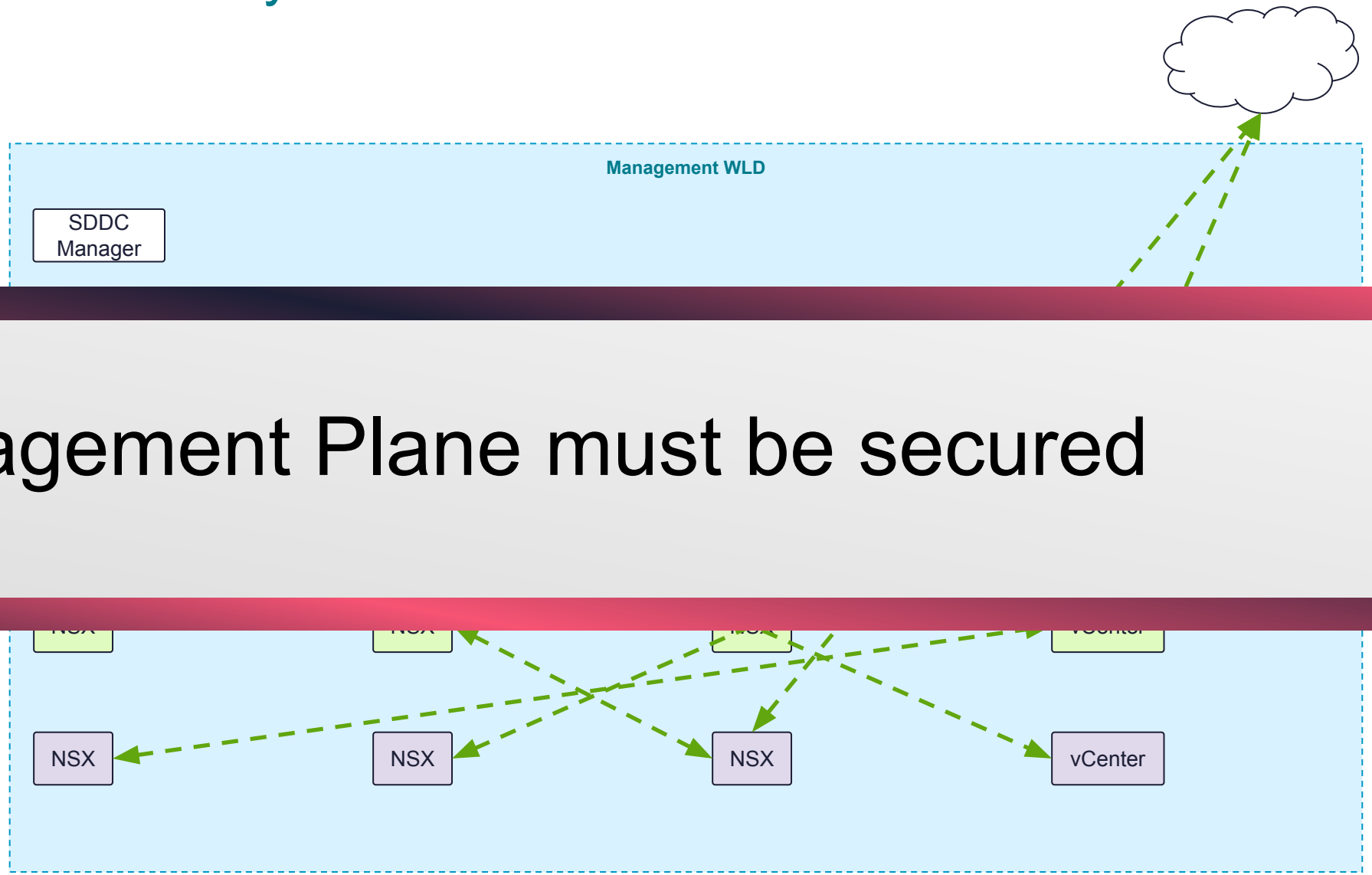
Feature	
Security Intelligence for Visibility & Micro-Segmentation Planning	Supported from LM UI. NAPP on each location • Local recommendations • For best experience, use on non-stretched segments
Advanced Threat Prevention - Intrusion Detection and Prevention System (IDS/IPS) – Distributed and Gateway	Supported from LM UI. No NAPP Dependency • IDS/IPS (classification-rules) using LM Groups • Members of LM Group can be any LM object or GM segment
Advanced Threat Prevention - Network Traffic Analysis (NTA)	Supported from LM UI. NAPP on each location
Advanced Threat Prevention – Distributed Malware Detection and Prevention with Sandboxing *	Supported from LM UI. NAPP on each location. *NSX 4.1.2 required*
Advanced Threat Prevention - Network Detection and Response (NDR)	Supported from LM UI. NAPP on each location. *NSX 4.1.2 required*

Management WLD Security

Default State

All traffic within the Management WLD is

Managers and vCenters are put on Management NSX Exclusion List and connected to vSphere dvpg



Management Plane must be secured

Securing VCF with VMware Firewall

VI and MGMT WLDs

Securing VI WLD

Zero-Trust / Secure Apps with Security Intelligence and DFW

Ransomware Protection & Threat Investigation with NSX ATP

Secure Virtual WLD zones using the GFW or DFW

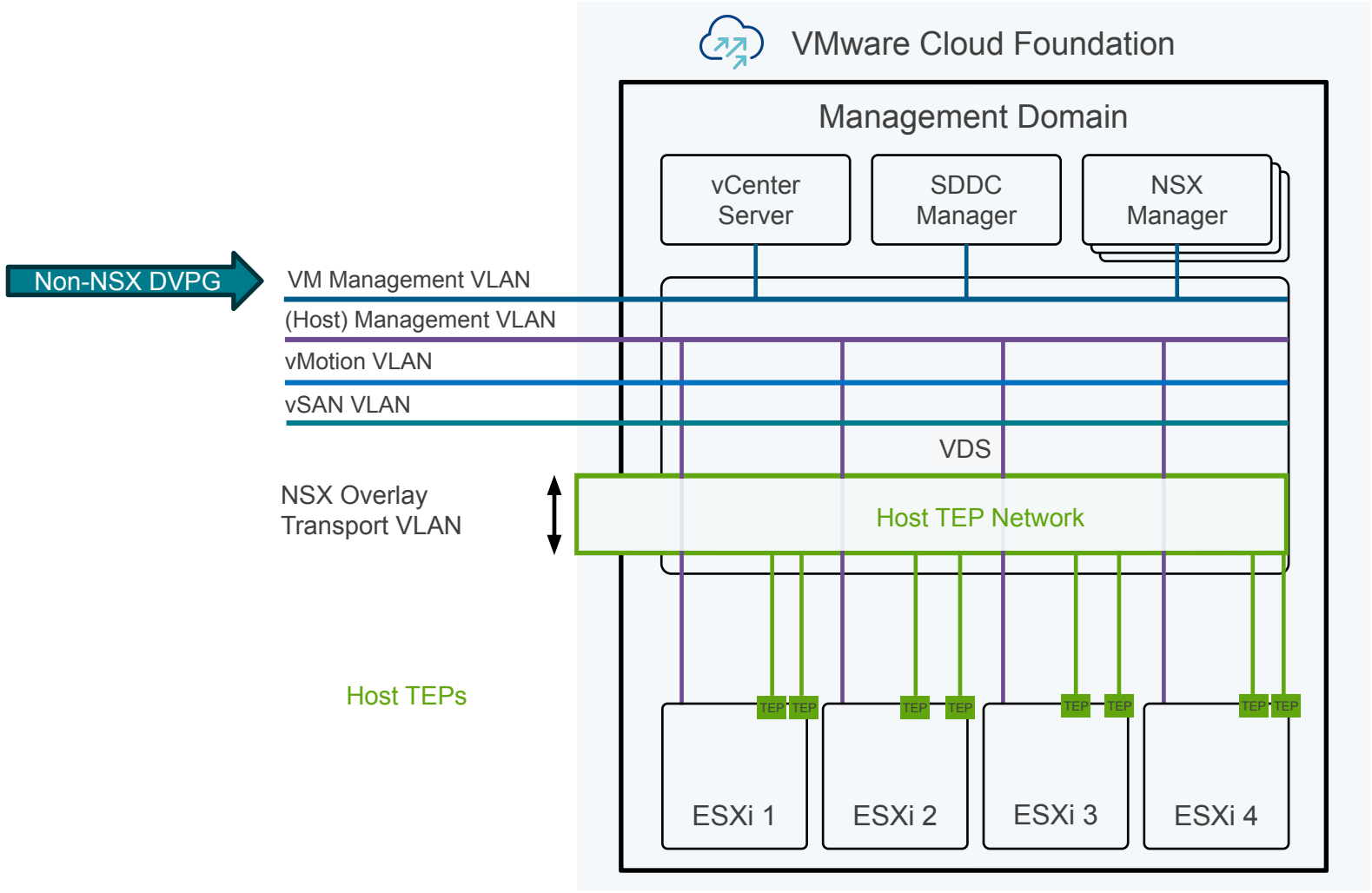
Securing MGMT WLD

Secure Infrastructure / Functional Segmentation using the Distributed Firewall

Visibility and Analytics with Security Intelligence

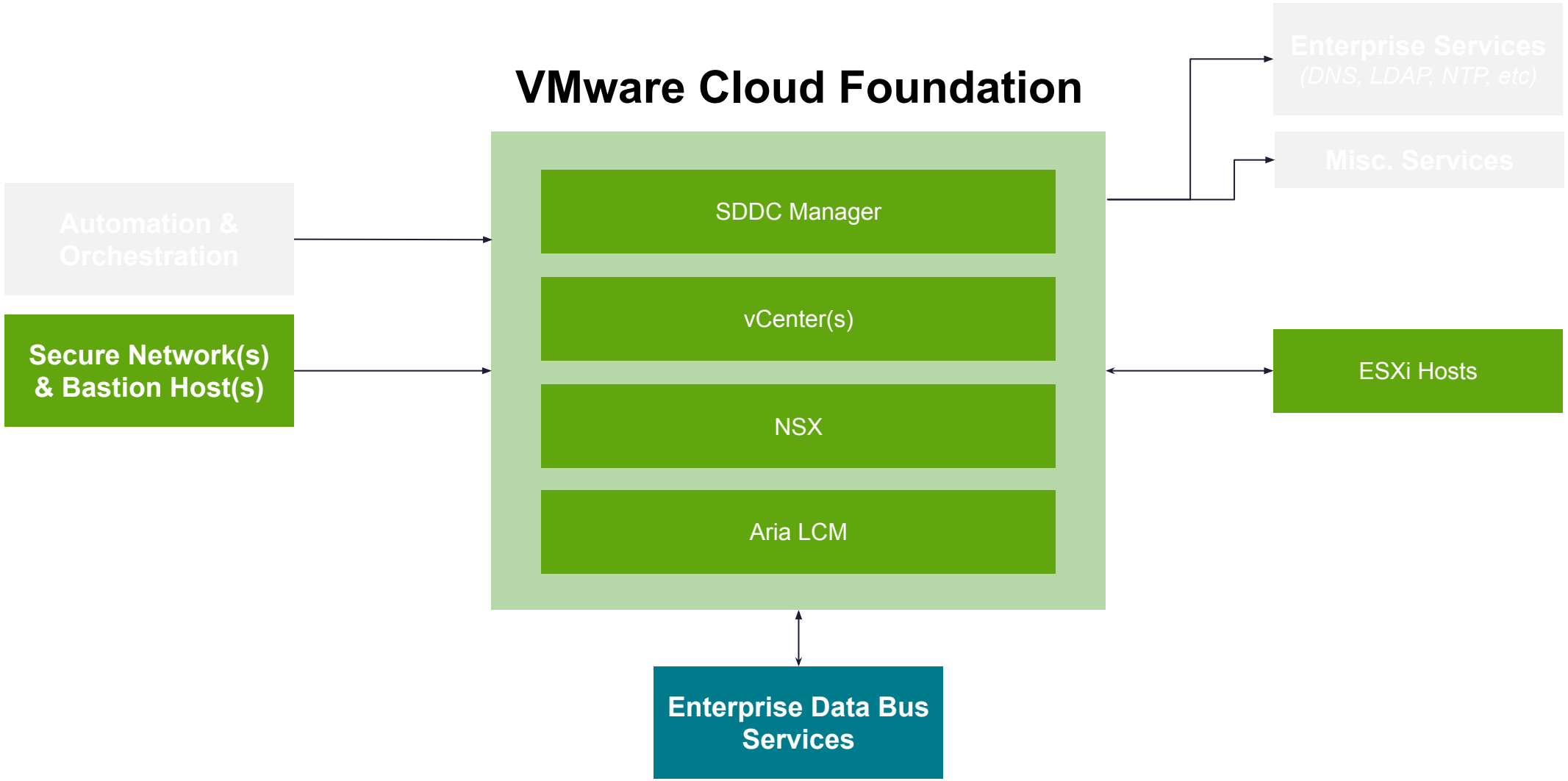
Management WLD Security

Functional Segmentation: Out of the box VCF MGMT WLD Networking



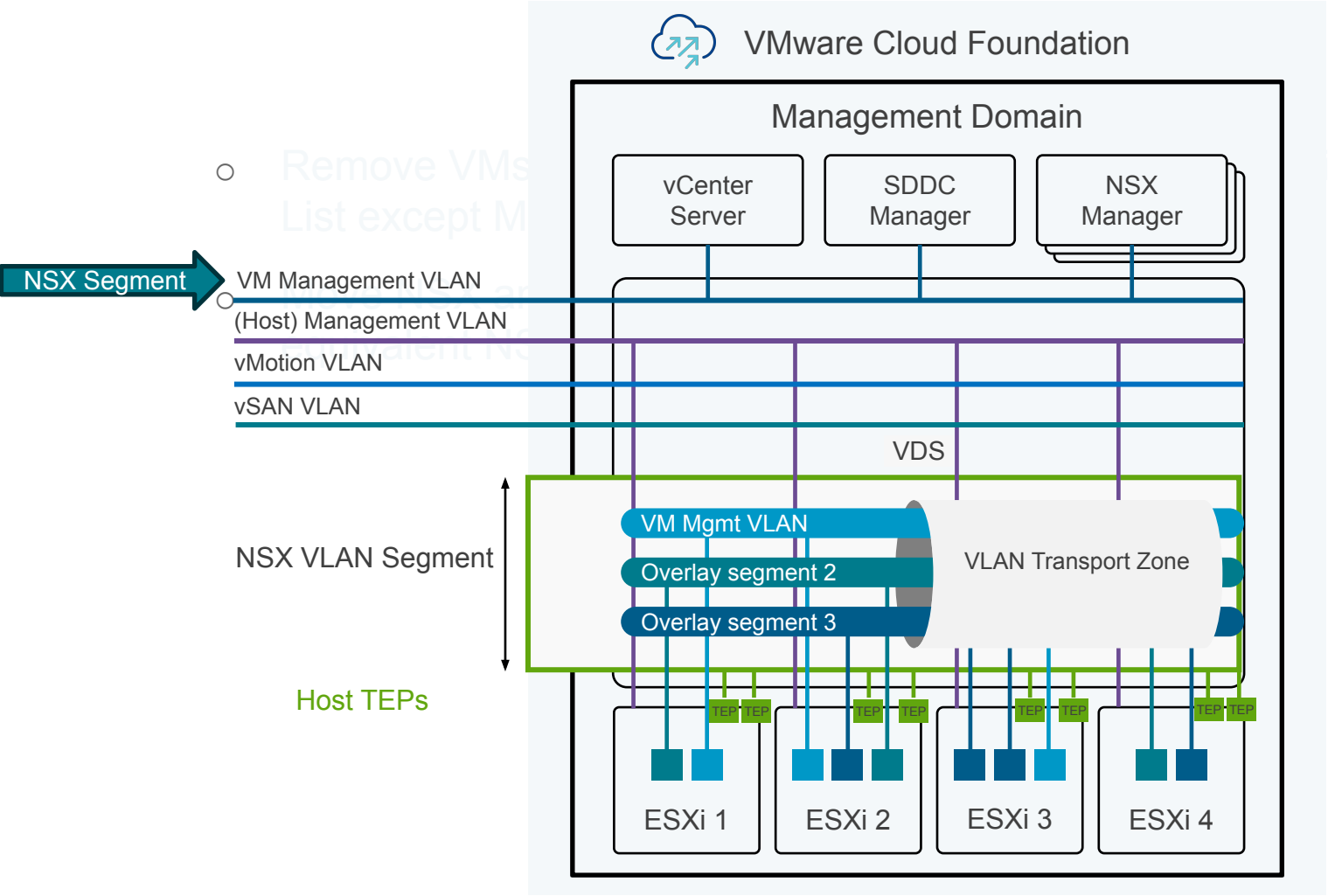
Management WLD Security

Functional Segmentation: Example System Communication



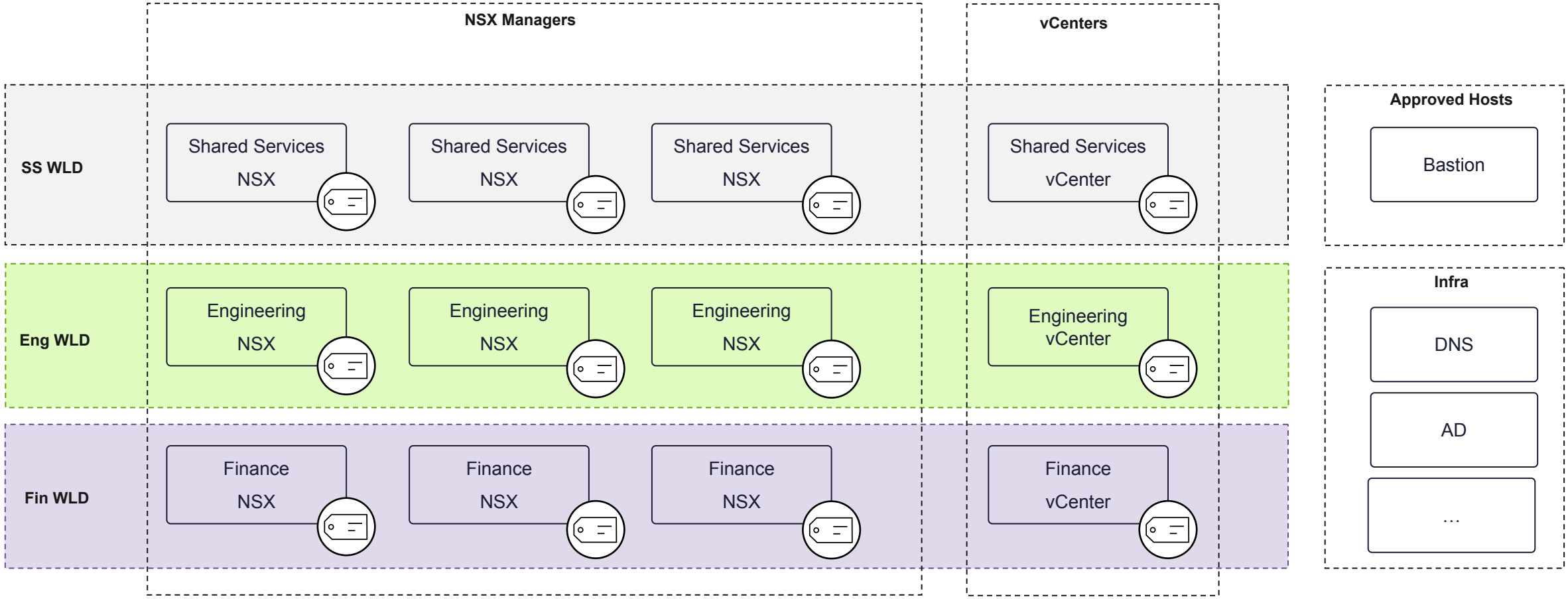
Management WLD Security

Functional Segmentation: Pre-Requisites



Management WLD Security

Functional Segmentation: Create NSX Groups and Tag VMs



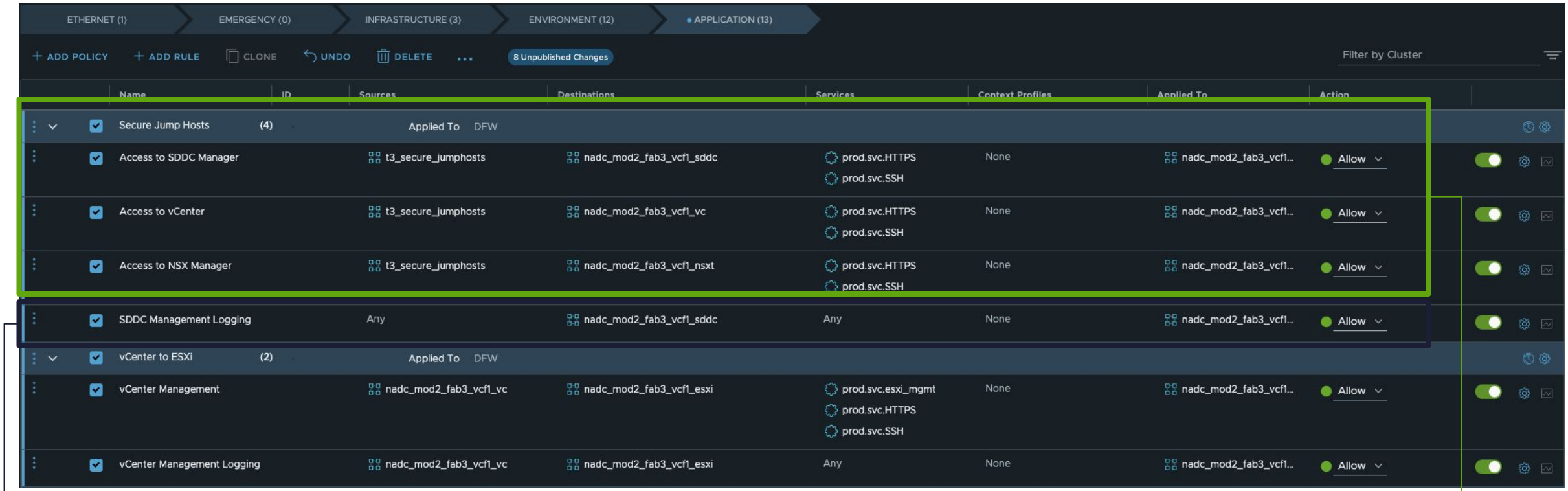
Management WLD Security

Functional Segmentation: Define the security policy

- Start with a macro-segmentation policy
  - Allow vCenters to vCenters Linked Mode
  - Allow NSX Managers to NSX Managers within a WLD
  - Allow Bastion hosts to vCenters and NSX Managers
  - Enable Logging with log-tags
- Deepen the security policy
  - Increase granularity (micro-segmentation) based on logs or Security Intelligence
  - Use L7 App-ID
- Use https://ports.esp.vmware.com as a reference

Management WLD Security

Functional Segmentation: Define the security policy

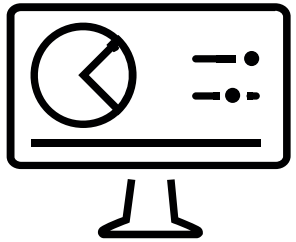


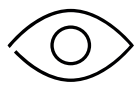
logging/audit > deny

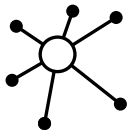
secure/trusted traffic

Management WLD Security

Visibility and Analytics







- Deploy NAPP and NSX Intelligence in the management WLD
- Use NAPP Automation Appliance for a quick and simple deployment (Multi-WLD support)
- Analyze traffic patterns
- Use the recommendation engine
- Leverage NSX Network Traffic Analysis to detect any suspicious management traffic

Demo

WLD Security with VMware Firewall

Thank You

vmware by Broadcom