

Threat Prevention in the Data Center

Speaker Name (Insert Pronouns)

Roll / Division at VMware

February 26, 2024

Current Threat Landscape



44%
of breaches
reported lateral
movement¹

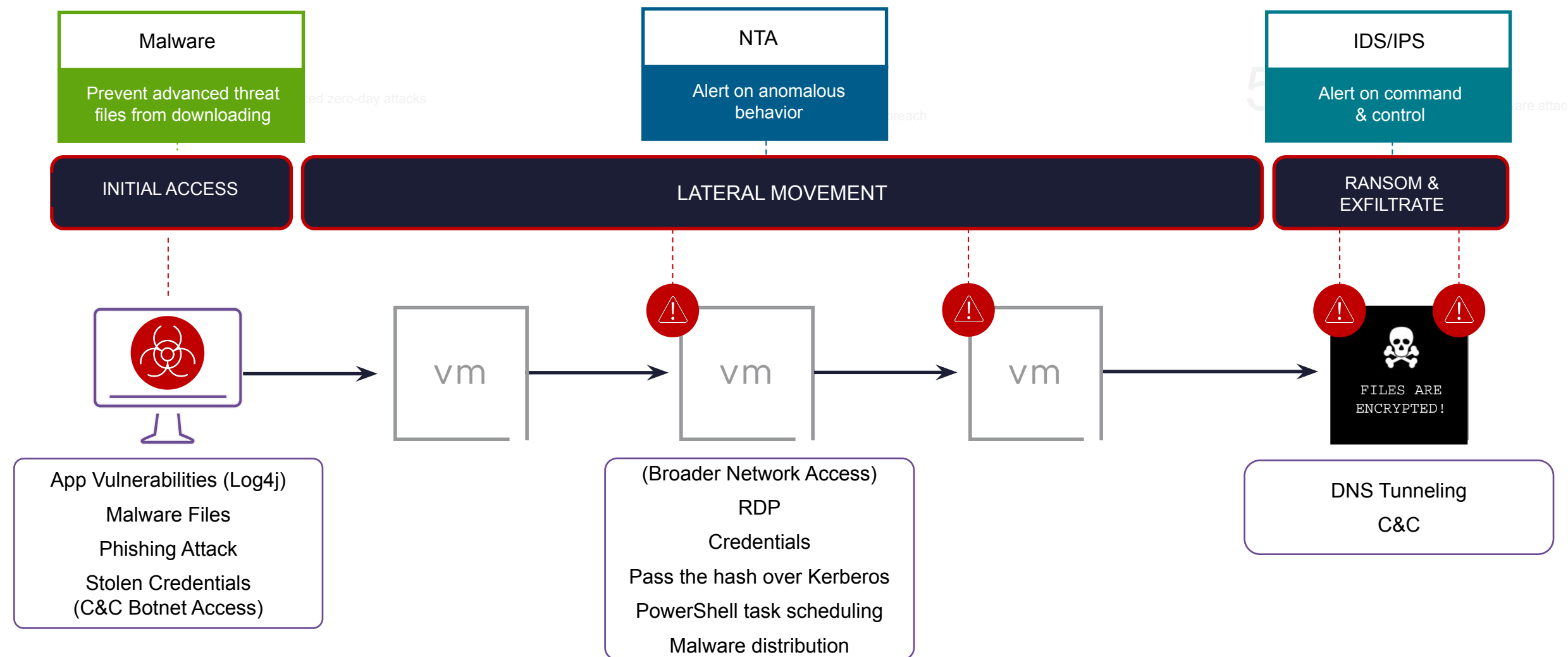


204
Days to detect
a breach²

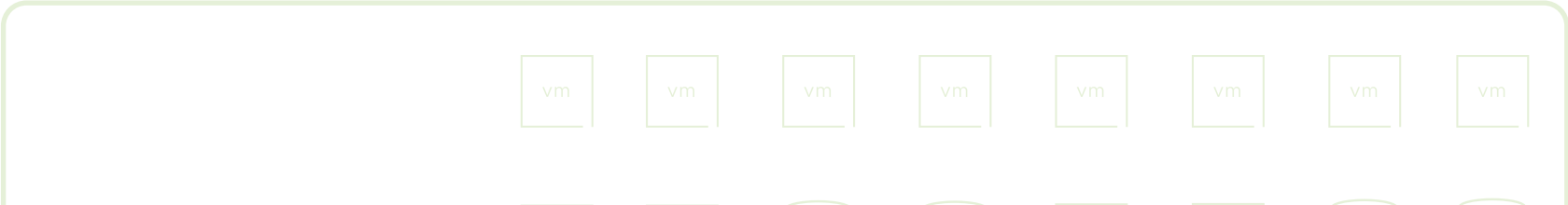


\$4.35M
Average cost
of a data breach³

Typical Advanced Persistent Threat (APT) Scenario



Securing Just at the Perimeter Isn't Enough



You should be worried about Lateral Security



Traditional Architecture for East-West Security

Challenges

Throughput Constraints

Customers are forced to choose what needs to be secured. This is made worse when customers choose not to protect potentially critical workloads due to network constraints

Topology Constraints

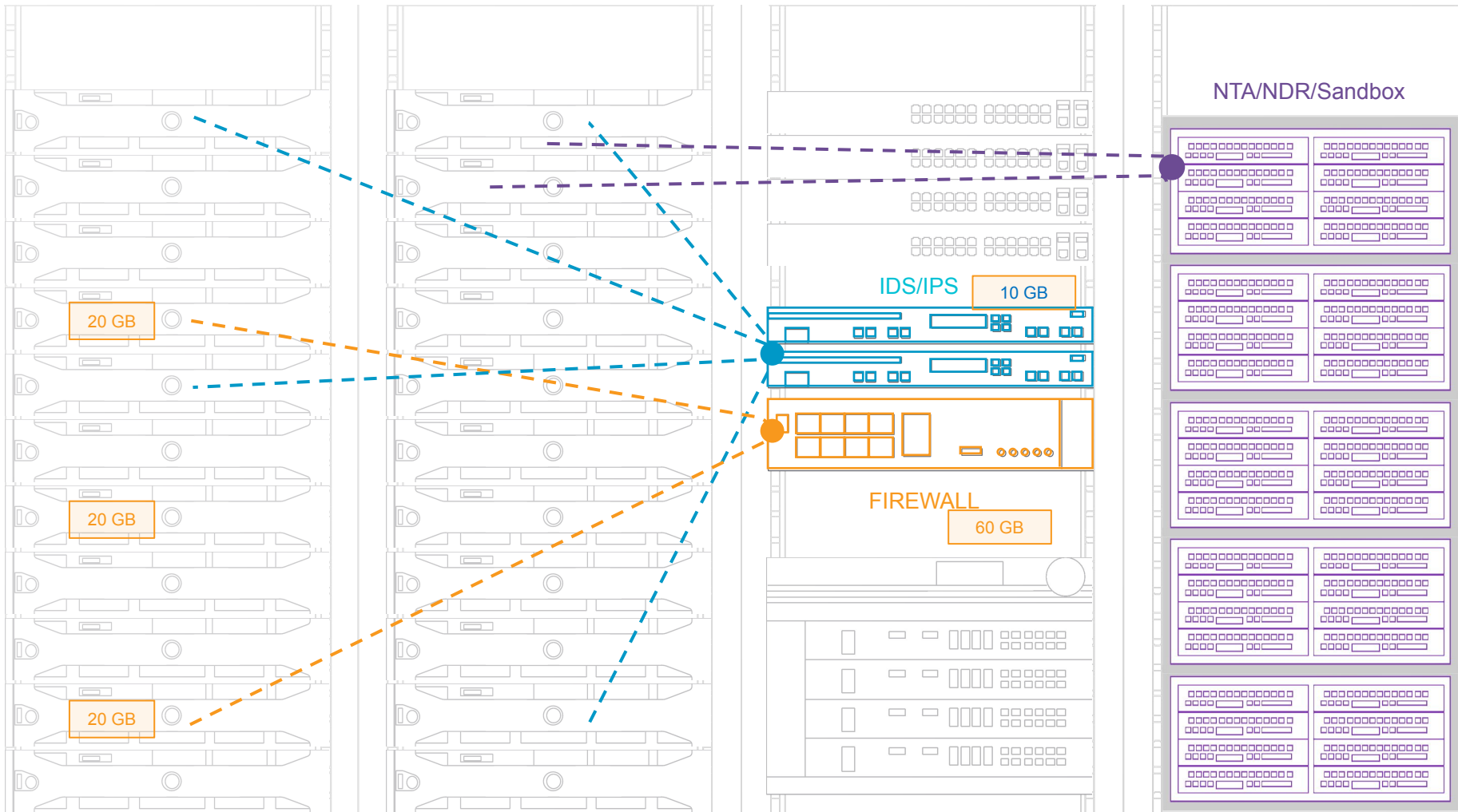
No Protection for critical workloads due to network topology constraints

Complexity

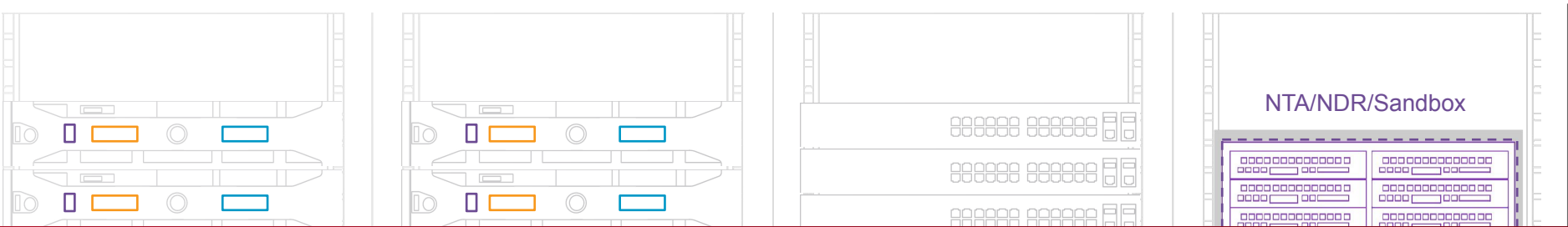
Complex to insert and causes sub-optimal traffic flows

True Visibility

The VMware solution is unique in that you can inspect all traffic regardless of network topology



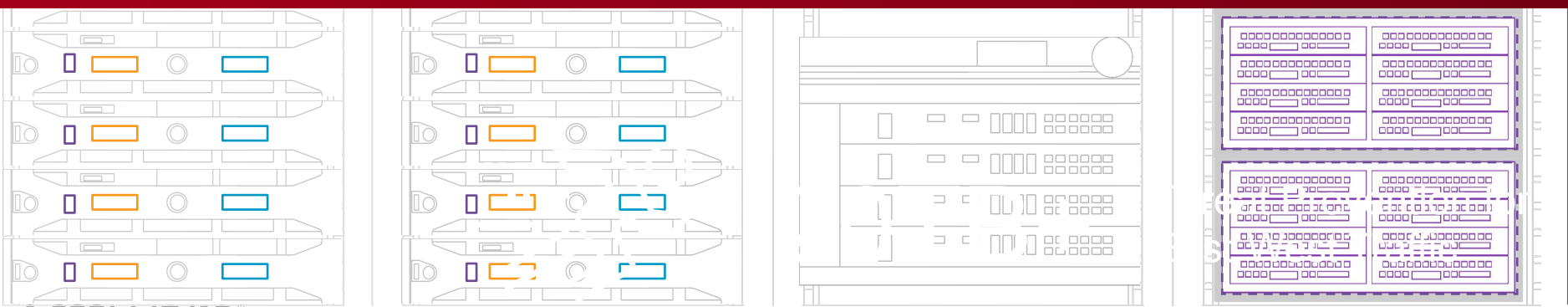
Modern Distributed Architecture for East-West Threat Prevention



Benefits

Security Everywhere

Enforce Security Controls Laterally
No Network Changes

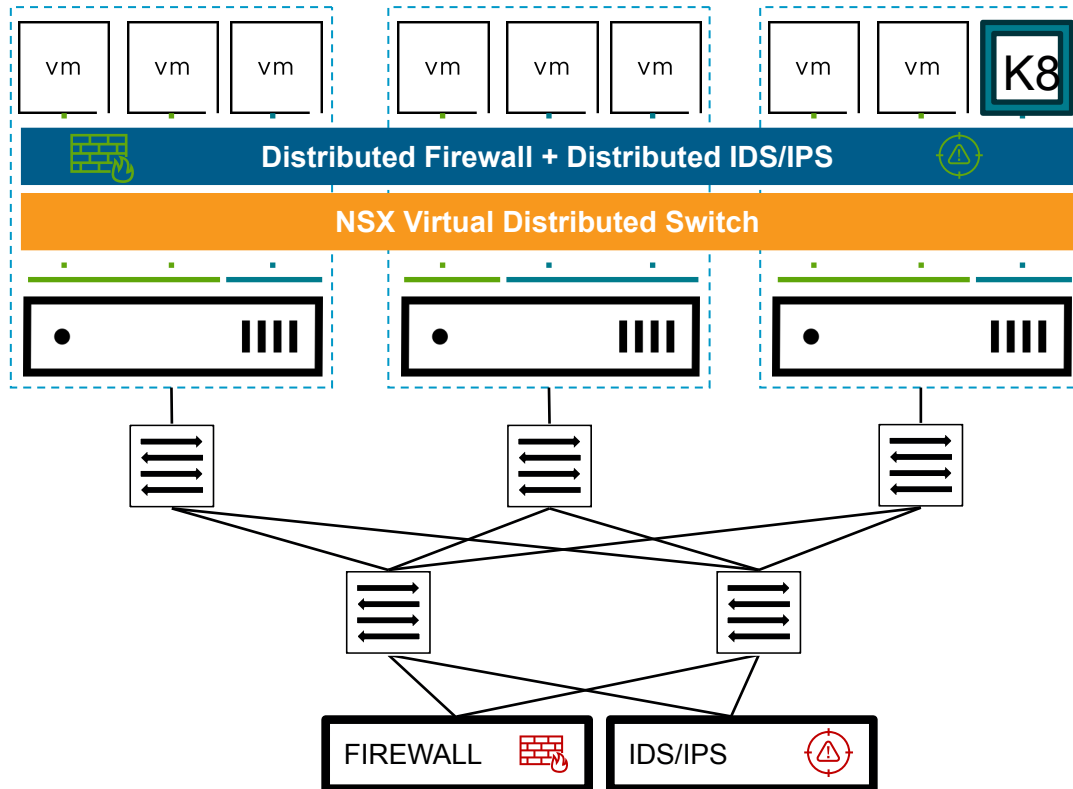


Scale Horizontally

Security scales with applications
ensuring no blind spots

NSX Distributed IDS/IPS

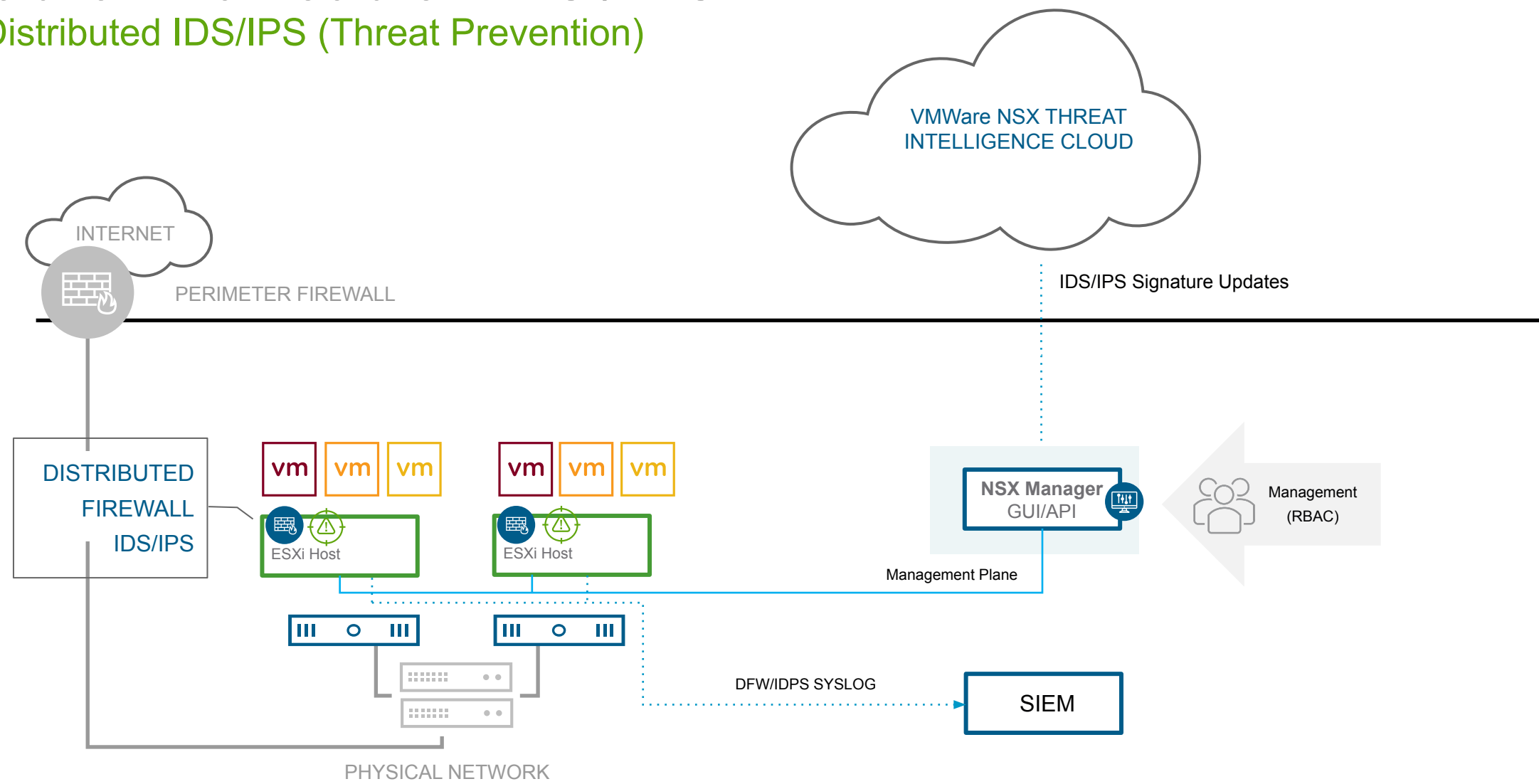
Application-specific Intrusion Detection and Prevention enforced at the Hypervisor



- ✓ Distributed & Built-in Analysis – scales linearly with workloads, no blind-spots for VMs and Containers
- ✓ Curated Signature Distribution – fewer false positives, lower computational overhead on host
- ✓ Context-based Threat Detection – reduced need for signature tuning, better alert prioritization
- ✓ Policy & State Mobility - simplify operations, eliminate stale / redundant policies

Solution Architecture – IDS / IPS

Distributed IDS/IPS (Threat Prevention)



Solution Architecture - Malware

Distributed Malware Detection and Prevention



Malware Prevention the Data Center

Feature Details

Distributed

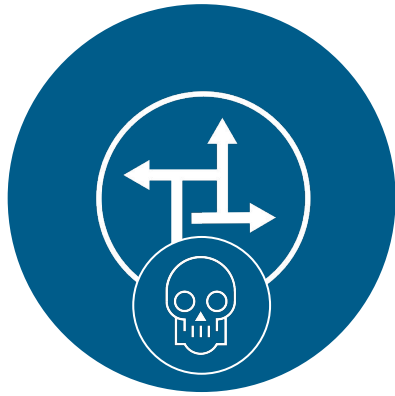
- Detection and Prevention
- Windows and Linux VMs
- Executable file types (PE files)
- Intercept File Operations on Guest VM
- Static analysis on-premises
- Dynamic analysis requires sending files to cloud (Opt-In)

Gateway

- Detection only
- Endpoint agnostic
- Intercept File transactions over HTTP and FTP
- Multiple file types
 - Executables, Document types, media types, archives, scripts, other

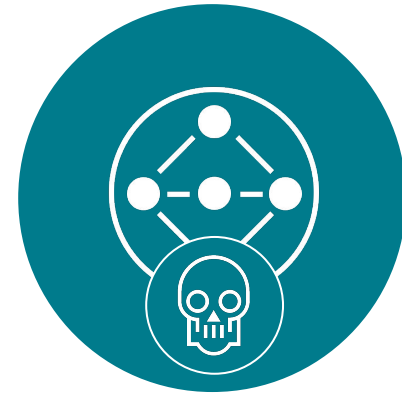
Solution Architecture - Malware

Two Enforcement Points



Gateway Malware
Detection

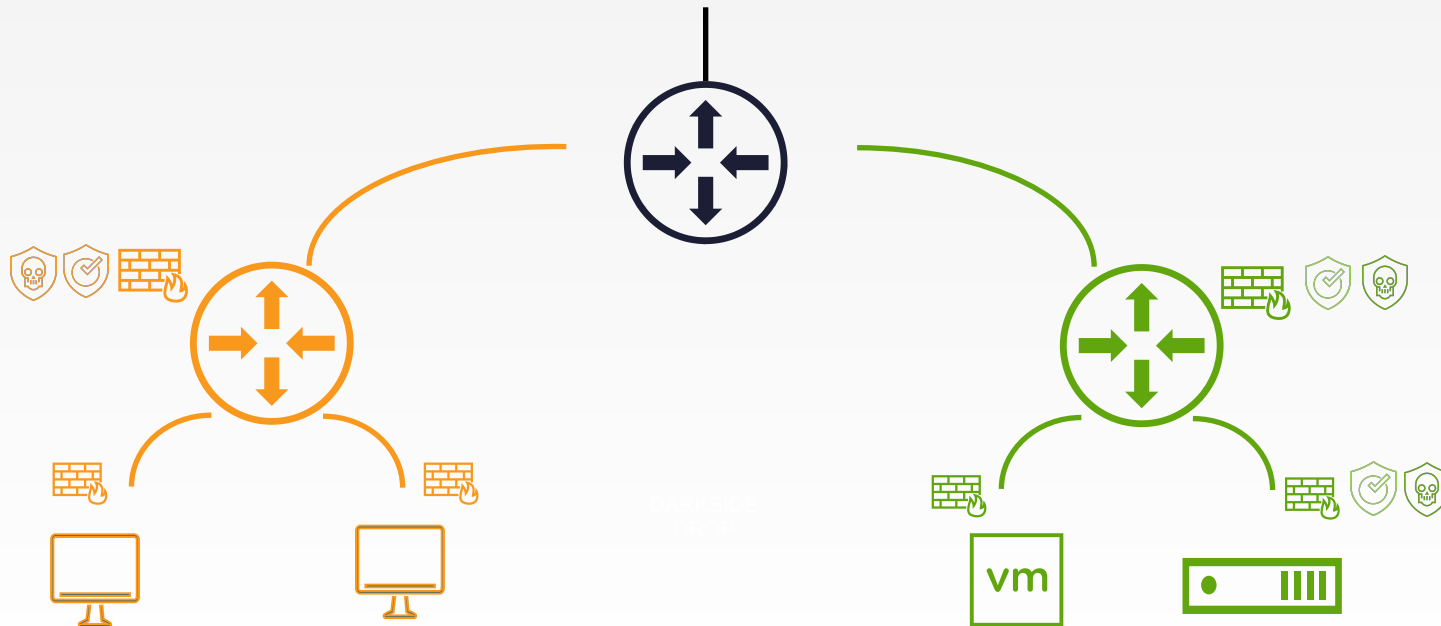
- Malware Detection on Gateway
- Malware Prevention on Hosts
- Can prevent known and unknown Malware from being executed in the Data Center
- Can be used even when Encryption or obfuscation is being used
- Broader Perspective on overall lateral movement of potentially malicious artifacts.



Distributed Malware
Prevention

Solution Architecture - Malware

Gateway Malware Protection



- Malware Detection
- Detect known and previously unseen malicious files at the network/zone perimeter
- Supported on T1 (Uplink and Service Interface)
- Hash lookup, local (static) analysis and cloud-based dynamic analysis
- Leverages GFW-IDPS for file extraction
- Once detected at the GFW, malicious file can be blocked at DFW

Solution Architecture - Malware

Distributed Malware Prevention

The screenshot displays the 'Analysis Overview' window for a submission dated 2021-06-11 16:47:33 UTC. The file 9d418ecc0f3bf45029263b0944236884 is identified as MALICIOUS. The risk assessment shows a Maliciousness score of 100/100, a High Risk estimate, and detected malicious behavior. The antivirus class is RANSOMWARE (TROJAN) and the family is DARKSIDE (AGEN). The analysis overview table lists two findings: a Signature (Identified ransomware code) and a Family (Ransomware specific behavior) both with a severity of 100.

Analysis Overview

Overview Report

SUBMISSION 2021-06-11 16:47:33 UTC

Threat Level

The file 9d418ecc0f3bf45029263b0944236884 was found to be **MALICIOUS**.

RISK ASSESSMENT

Maliciousness score: 100/100
Risk estimate: High Risk - Malicious behavior detected
Antivirus class: RANSOMWARE TROJAN
Malware: DARKSIDE
Antivirus family: AGEN DARKSIDE

ANALYSIS OVERVIEW

Rows to display: 25 Showing page 1/1

SEVERITY	TYPE	DESCRIPTION	ATT&CK TACTIC(S)	ATT&CK TECHNIQUE(S)
100	Signature	Identified ransomware code		
100	Family	Ransomware specific behavior	Impact	Data Destruction

CLOSE

- Malware Detection and Prevention
- Block known and previously unseen malicious files
- Hash lookup, local (static) analysis and cloud-based dynamic analysis (Sandbox)
- Guest-introspection based file-extraction and blocking for DFW
- Intercept files even if they came in over an encrypted connection
- No hair-pinning, network-latency or re-architecture

VMware Threat Prevention Use Cases

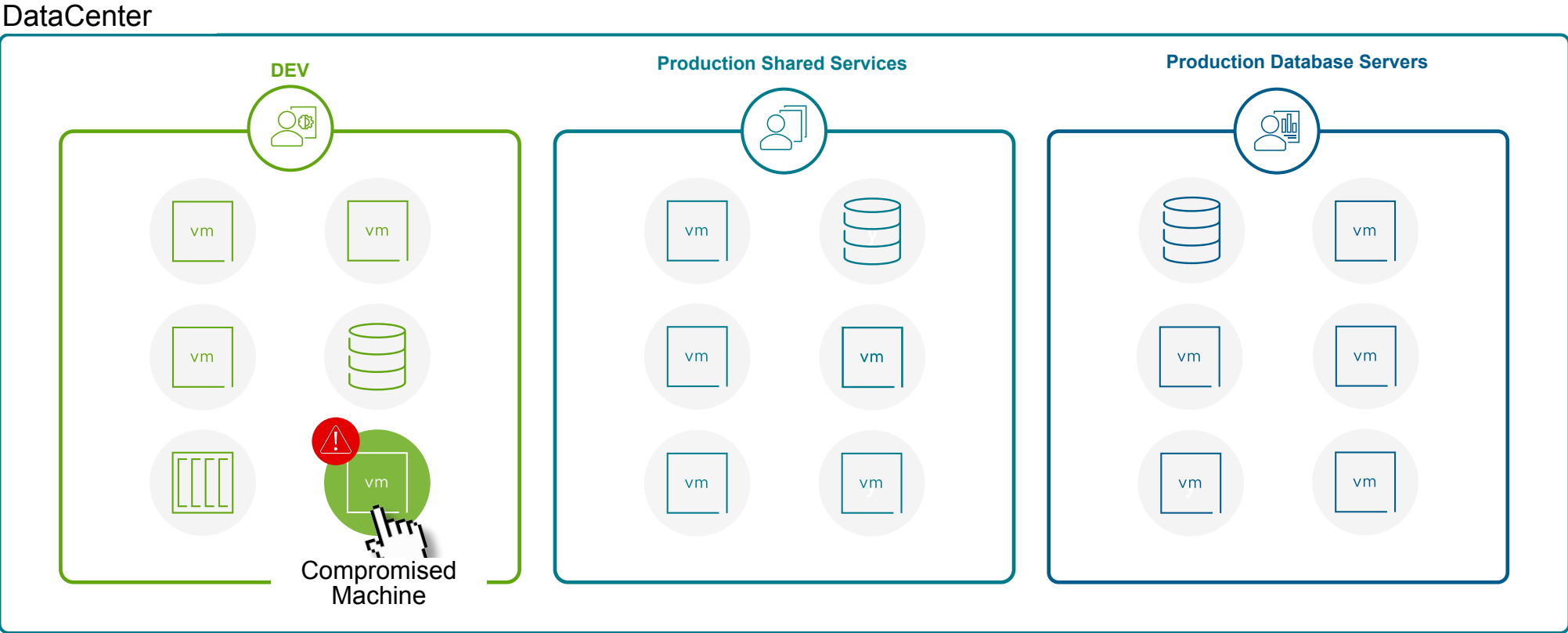
Threat Prevention

- Once the security perimeter is breached, there are fewer and fewer controls in place for attackers to work against. What's worse is that they will start to use your own tools like RDP and SMB to move around laterally inside your network.
- It is desirable to be able run Threat Prevention (TP) as many workloads as possible as it will detect and prevent against known threats in the data center.
- This has been extremely difficult until now.
- VMware's Threat Prevention is easy to deploy and becomes very useful inside the datacenter
- Using TP here will ensure that well known attacks are detected and / or prevented
 - Attackers will use your own tools against you "Living off of the land"
 - Attackers will almost never use highly valuable exploits after the initial compromise / attack
- This is where the attackers advantage starts to erode and the opportunity to detect the attackers starts to become ours.
- Attackers will often avoid the use of obfuscation and encryption in these intermediate steps



VMware Threat Prevention

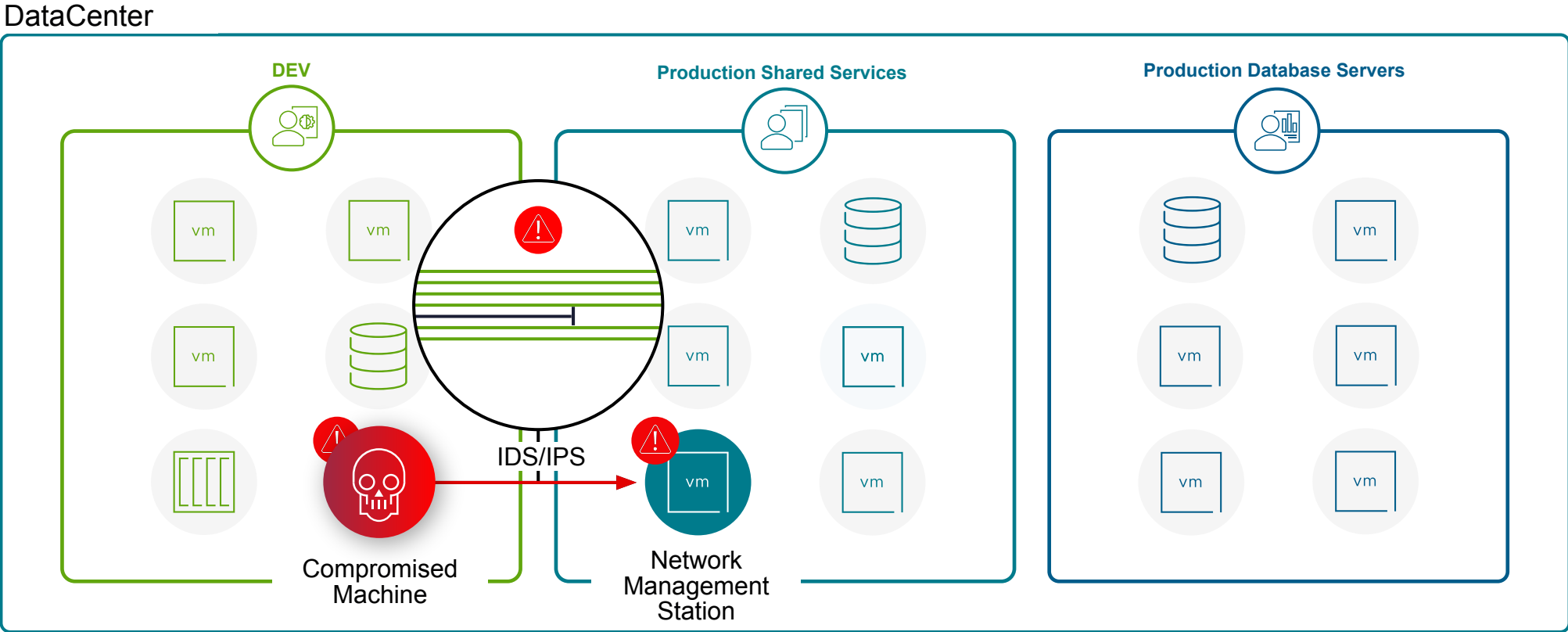
Distributed Malware Prevention



Prevent Malicious
File Download over SMB Session

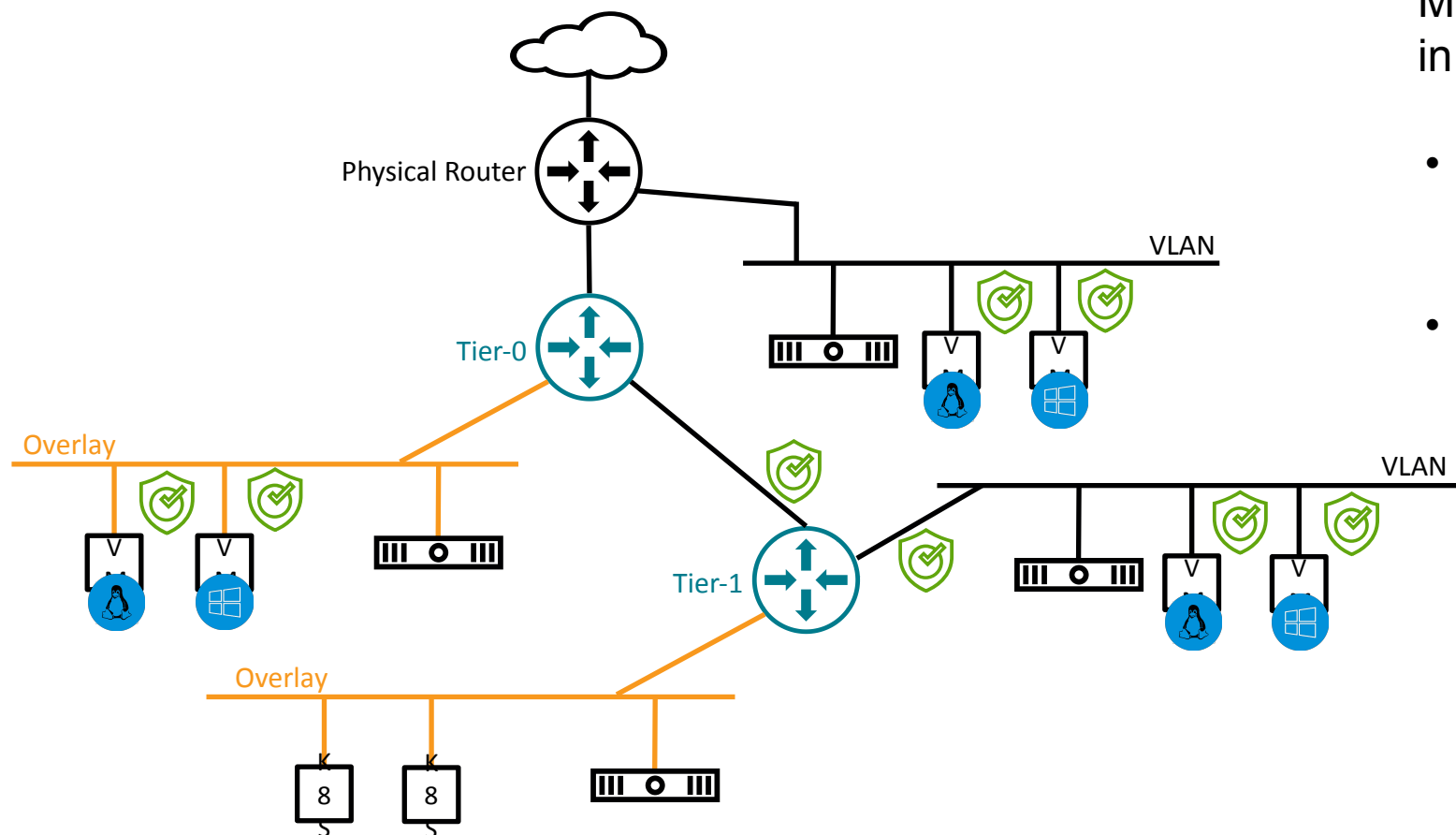
VMware Threat Prevention

Intrusion Detection and Prevention



When and Where to deploy Malware Prevention?

Gateway (Detect) and Distributed (Detect and Prevent)

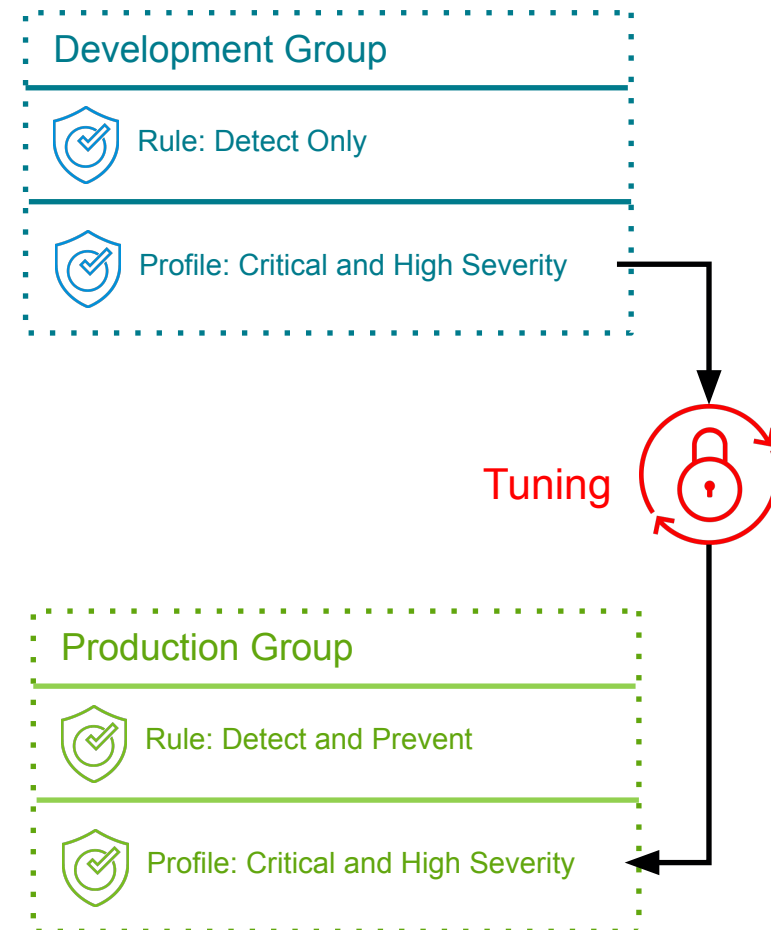
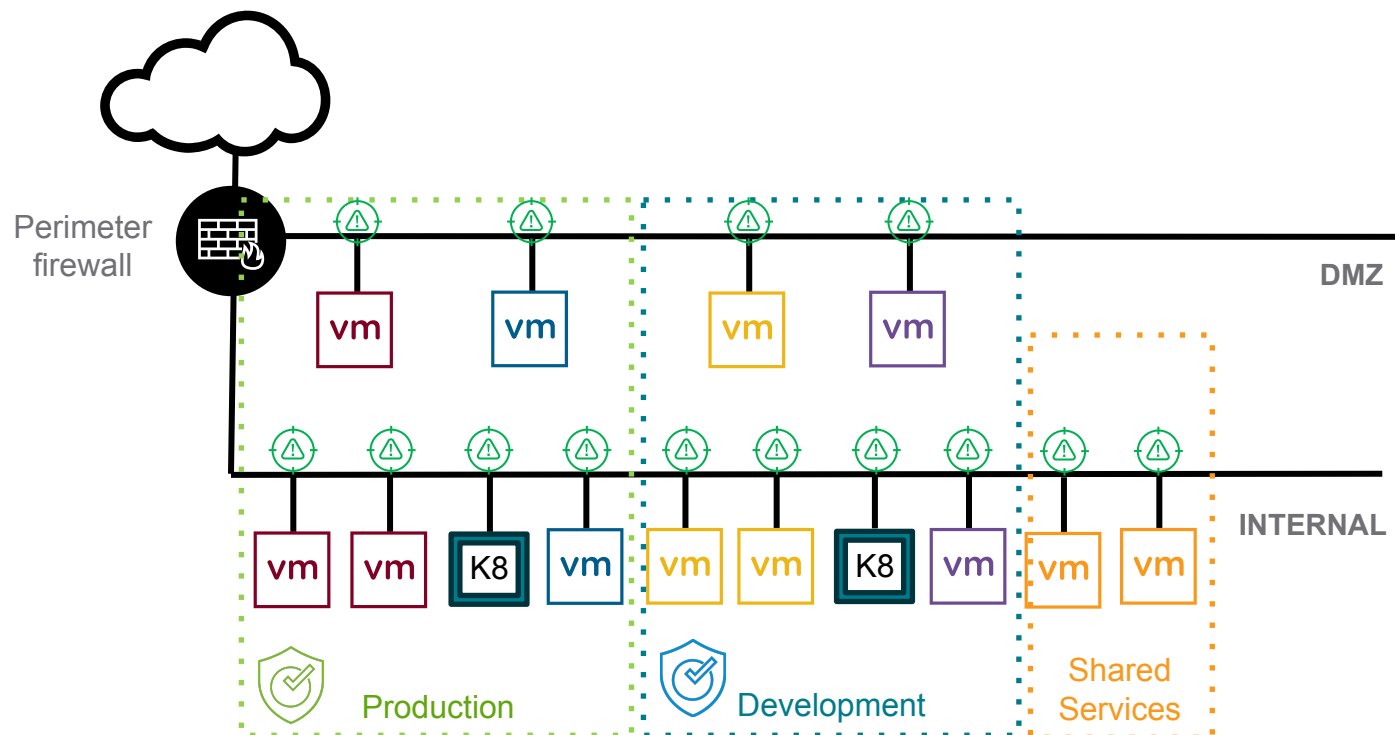


Malware Detection/Prevention is enforced in 2 points:

- Central
On T1 Uplinks and Service Interfaces
Malware Detection only
- Distributed
On Windows and Linux VM
Malware Detection
Malware Prevention

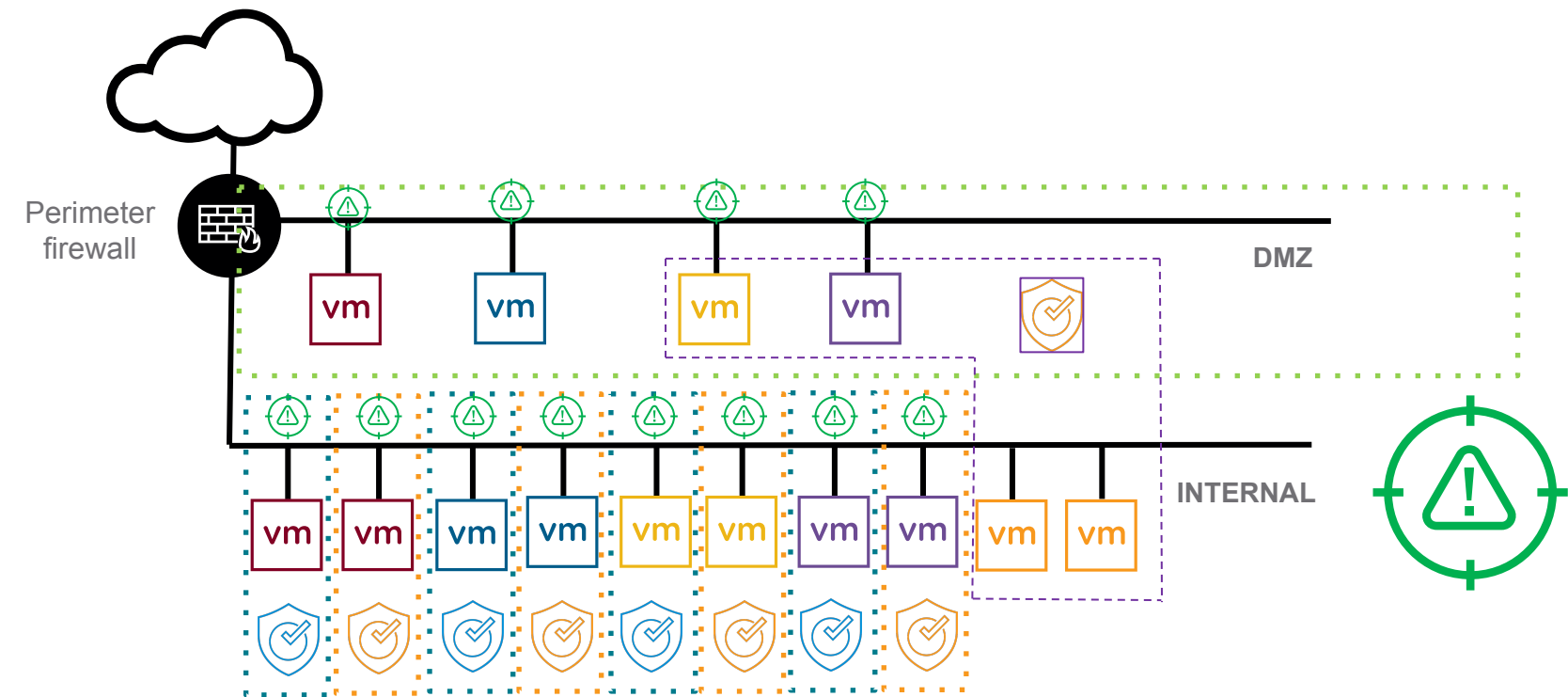
When and Where to deploy IDS/IPS ?

No Blind Spots – At the VNIC level of every workload



When and Where to deploy IDS/IPS ?

Not bound by traditional Networking Boundaries



Web-Servers Group

Rule: Detect and Prevent

Profile: Attack Targets: Web Server

App-Servers Group

Rule: Detect and Prevent

Profile: Products Affected: Drupal, WordPress, ...

DB-Servers Group

Rule: Detect and Prevent

Profile: Products Affected: CouchDB, MsSQL, MySQL, ...

Two Threat Prevention Use Cases



Virtual Patching

- Ability to provide a compensating control when a known threat is present in the Data Center
- Not always possible to apply patches in a time effective manner
 - Testing
 - Downtime
 - Risk
 - Compliance
- Does not patch the vulnerable code but rather uses the TP functionality to ensure that the threat is detected and prevented before it reaches the workload

Compliance

- Regulatory compliance often requires the use of technology like TP to be in use in the environment
- Auditors will seek a clear understanding of what is in scope and how the workloads are being treated
- The creation of Compliance Zones that are inclusive of any in scope workload regardless of network construct is easiest done using NSX
 - PCI Zone
 - SWIFT Zone
- The newly created group receives the correct TP policy to ensure threats are mitigated and compliance is maintained

Patching Dilemma

To Patch or not to Patch – Why is that even a Question?

- What to Patch ?
 - Patching everything is very difficult and resource intensive
 - Customer will often Patch Externally Facing assets first (Most Risk)
 - CVSS (Common Vulnerability Scoring System) is often the basis for a patching strategy
 - Patching internal only assets can often be deprioritized.
- When to patch ?
 - Prioritize systems based on risk (value of data / business criticality of service,...)
 - Maintenance Window/downtime
- How to patch ?
 - Patching Cycle
 - Evaluate/test the patch
 - Rolling Updates to reduce downtime
 - Compliance assessment
- What if no patch is available?
 - Older Systems like Windows 2008 / 2012 and RHEL 5 no longer get patches
 - Many applications are in the same predicament

The patching dilemma

Risk and Cost



Vulnerability
may be exploited

Unpatched
Vulnerability

The patching dilemma

Risk and Cost



Patch is Available



Maintenance Window/Downtime



Applying the patch



Compliance and Regression testing

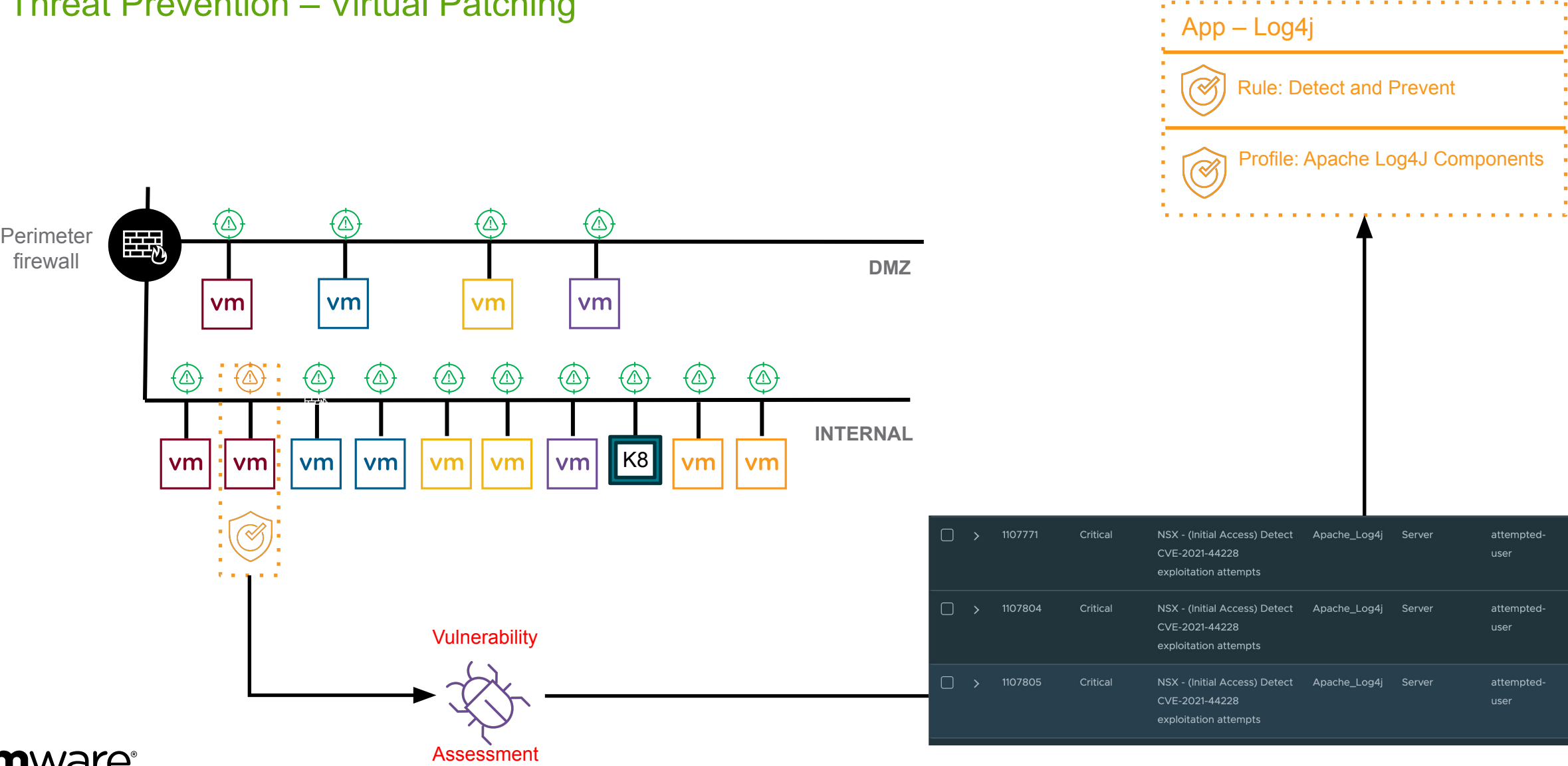
The Patching dilemma

Virtual Patching - Mitigating the Risk without downtime

- Signature-based prevention of vulnerability exploitation applied outside of the vulnerable asset
 - Ensures that risks are mitigated yet assets remain available
 - Often implemented temporarily, until system can be patched
 - Allows organizations maintain normal patching cycle
 - Significantly reduces the risk of a patch causing new software issues
 - Signature may be available before a real patch is
- Benefits of using NSX Distributed IDS/IPS as a Virtual Patching Solution
 - A minimal or targeted set of signatures can be applied to vulnerable workloads to cover unpatched vulnerabilities
 - Minimal Risk of False Positives
 - Low Noise
 - Not just applied at the perimeter/network segment but at the vNIC of every vulnerable workload
 - No tuning requirement

The Patching dilemma

Threat Prevention – Virtual Patching



The Patching dilemma

Create a Compensating Control

- Create a Dynamic group **Vulnerable Workloads** , matching workloads with a **Vulnerability Scope**

Criteria 1

Virtual Machine

Tag

Equals

Scope

Vulnerability

+ -

- Create a IPS profile **Virtual Patching** with **ALL** signatures enabled with alert-only action * and apply it to the **Vulnerable Workloads** group in **detect/prevent mode**

Virtual Patching

(1)

In Progress

Virtual Patching	10216	Any	Any	Any	Virtual Patching	Vulnerable Workloa...	Detect & Prevent	<div></div>	
------------------	-------	-----	-----	-----	------------------	-----------------------	------------------	-------------	--

- *Run Vulnerability scan/assessment*
- Apply **Vulnerability** tag to vulnerable workload for each identified vulnerability
i.e. “Scope: Vulnerability | Tag: CVE-2021-44228”

Tag	Scope	Assigned To
CVE-2020-14008	Vulnerability	1

- Manage signatures for the **Vulnerability Patching** profile, filter based on **Name** or **CVE** and change action for filtered signatures to **Reject**

<input type="checkbox"/>	>	1107771	Critical	NSX - (Initial Access) Detect CVE-2021-44228 exploitation attempts	Apache_Log4j	Server	attempted-user	10.0
<input type="checkbox"/>	>	1107804	Critical	NSX - (Initial Access) Detect CVE-2021-44228 exploitation attempts	Apache_Log4j	Server	attempted-user	10.0
<input type="checkbox"/>	>	1107805	Critical	NSX - (Initial Access) Detect CVE-2021-44228 exploitation attempts	Apache_Log4j	Server	attempted-user	10.0

Compliance

Maintaining and Demonstrating Compliance for PCI-DSS

- **Compliance**

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards and best practices that are designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

- PCI-DSS Section 11.4 states:

- **Use intrusion detection (IDS) or intrusion prevention (IPS) techniques to detect or prevent intrusions on the network.**

All traffic in the cardholder data environment and critical points should be monitored. Using intrusion detection or intrusion prevention techniques (IDS / IPS), network traffic should be compared with known “signatures” or the behavior of the type of attack activity. Alerts should be sent to relevant personnel, or such harmful activities should be blocked automatically.

- PCI-DSS Section 5 states:

Use and regularly update anti-virus software. Anti-virus software needs to be installed on all systems commonly affected by malware. Make sure anti-virus or anti-malware programs are updated on a regular basis to detect known malware should be blocked automatically.

Compliance

Maintaining and Demonstrating Compliance for SWIFT

- **Compliance**

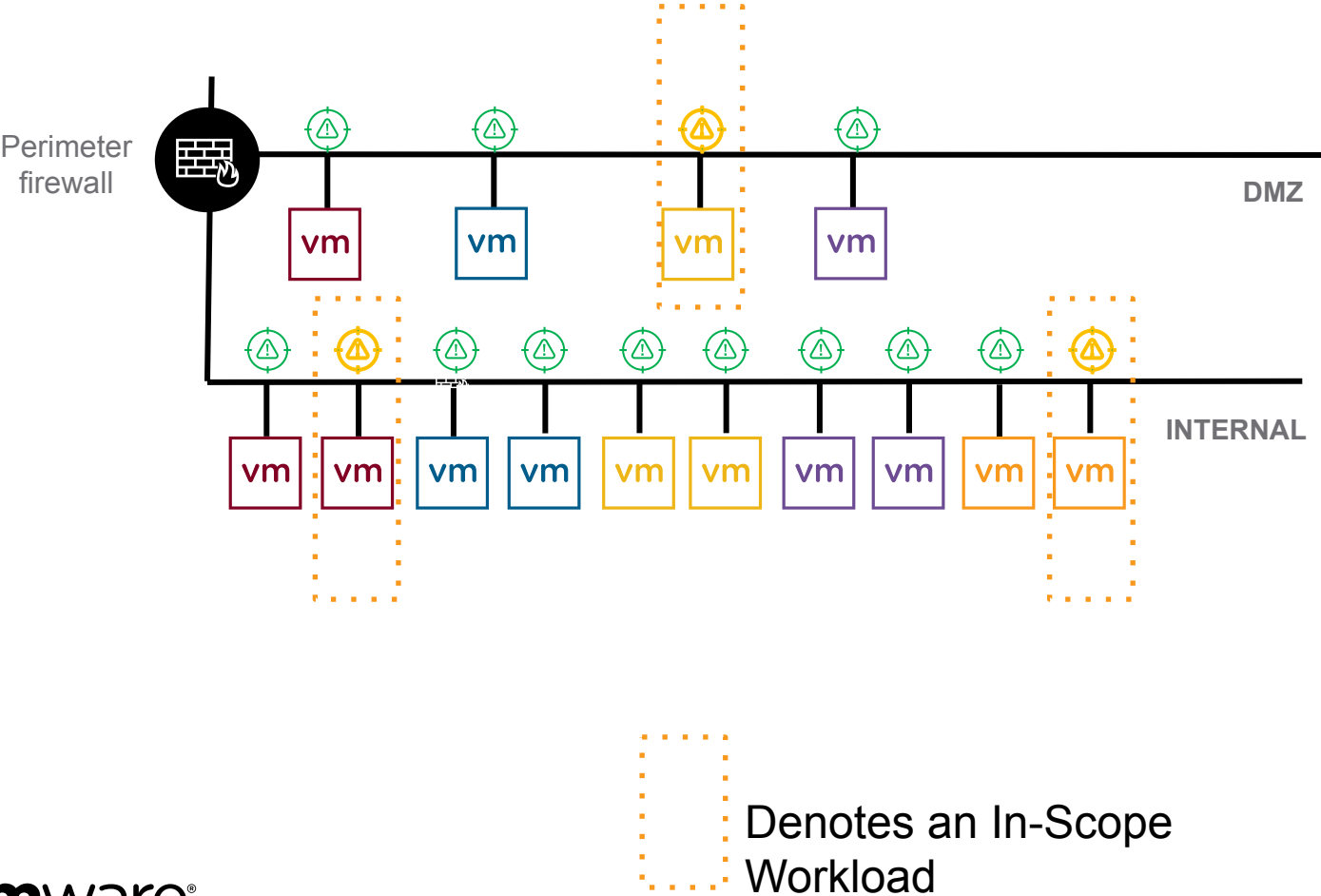
SWIFT (Society for Worldwide Interbank Financial Telecommunication) Customer Security Controls Framework v2024 details what protections shall be in use for all Banking Transfer Systems.

- SWIFT Section 6.5A states:

- **Use intrusion detection (IDS) or intrusion prevention (IPS) techniques to detect or prevent intrusions on the network.**
 - Detect and contain anomalous network activity into the on-premises or remote Swift environment. In-scope components:
 - network (data exchange layer reaching the Swift-related components)
 - remote (that is hosted or operated by a third party, or both) virtualisation or cloud platform supporting the user Swift environment


Compliance


Ensure Compliance no matter the location of the VM



Identify All In Scope Workloads – Create a Dynamic Group based on tags.

All In-Scope PCI Workloads

 Rule: Detect and Prevent

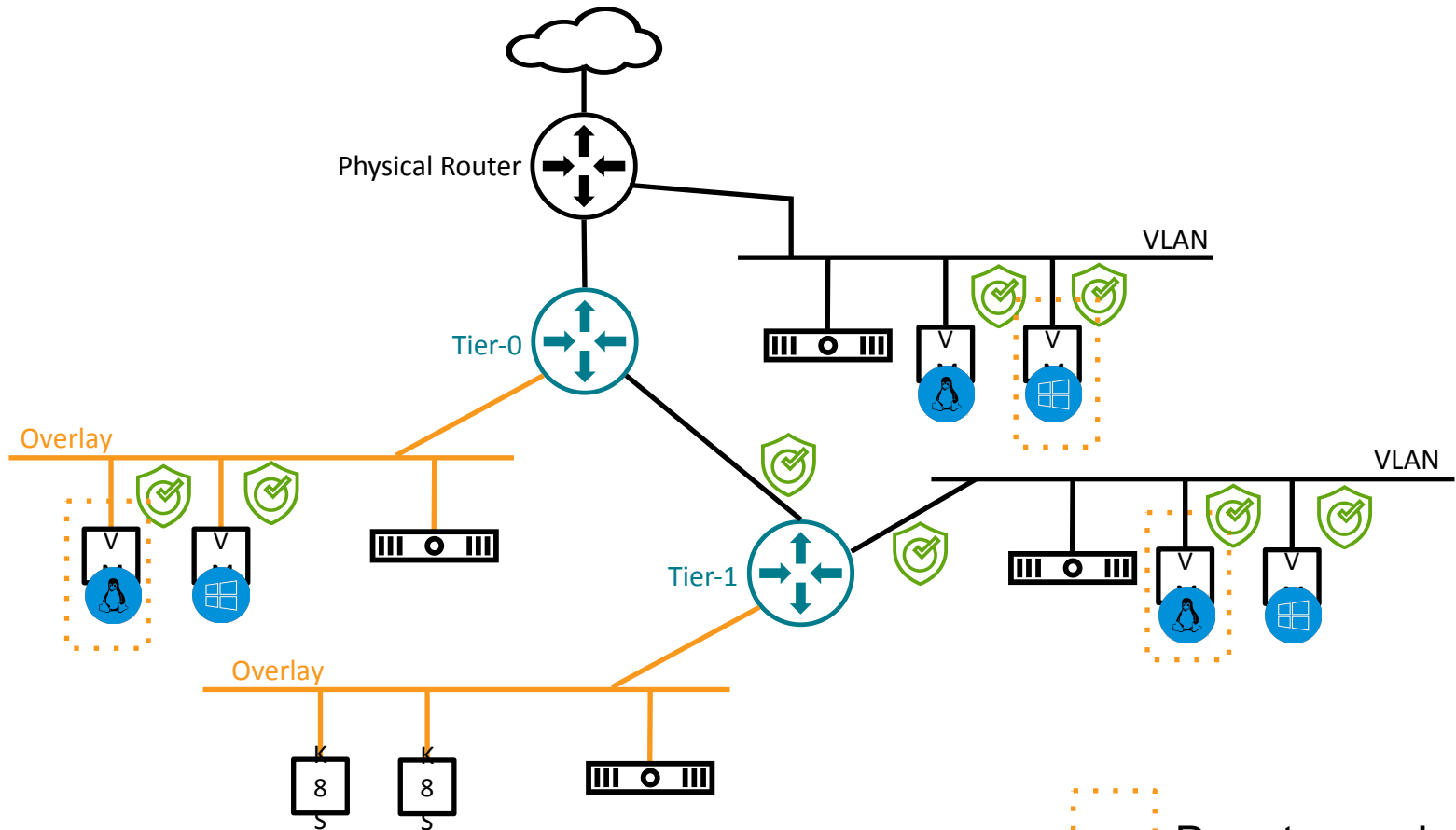
 Profile: Critical and High Vulnerabilities

Assign a Profile to that Group which meets that the Appropriate IDS Policy is always being enforced.



Compliance

Ensure Compliance no matter the location of the VM



Denotes an In-Scope Workload

Identify All In Scope Workloads – Create a Dynamic Group based on tags.

SWIFT Transfer Terminals

Rule: Detect and Prevent

Profile: Malware Prevention Executables and Documents

Assign a Profile to that Group which add Malware Prevention to the appropriate In Scope Workloads



Thank You