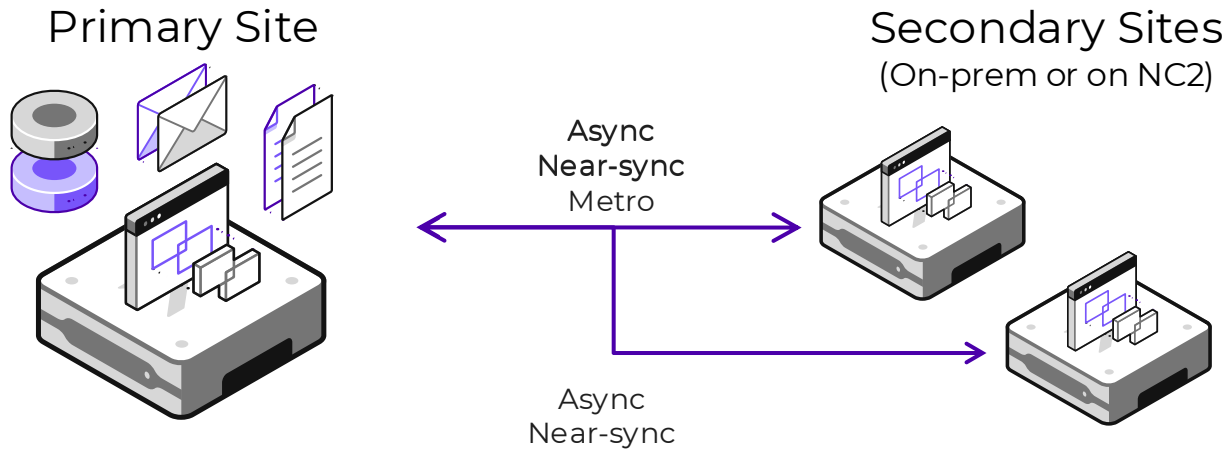
NUTANIX

Metro Availability

Comprehensive BC/DR Solution

Integrated 1-Click Disaster Recovery



- 1-click failover, failback and test
- Automatically orchestrate recovery plans
- Multi-Site Replication

One User Interface for Management & Operations

Integrated Best-in-Class Backup Rich Partner Ecosystem

Arcserve | Commvault | HYCU | Veeam

Nutanix Mine

Cohesity | Rubrik | Veritas | and More...

- Backup & archive data
- Use popular data protection software

True Resiliency From A to Z and Beyond

S/W Techniques
Replication Factor (RF)–2/3 | Erasure Coding | Snapshots

CLOUD
- NC2 AWS
- NC2 Azure
- Nutanix DRaaS
- MSP DRaaS

SITE
- Multi-site replication
- Metro Availability
- Near-Sync

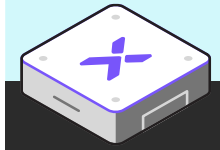
Local Resiliency

VM
- VM level Protection
- Eco-system integration

DATA
- Tunable redundancy
- Transparent consistent checks

Geographical Resiliency

NODE
- Node and Rack failure resiliency
- Non-disruptive upgrades



HARDWARE
- Self-healing from disk failure
- Redundancy of key components

S/W Techniques
Snapshots | Replication | Backup | Archival

Comparing our Solutions

*NDR = Nutanix DR = Leap

	Metro AHV	Metro ESXi	Sync Rep	Near Sync Rep	Async Rep
RPO	0	0	0	20 sec < RPO < 15 min	1 hour < RPO < some days
RTO	Minutes (automated)	Minutes (automated)	Minutes to hours (manual)	Minutes to hours (manual)	Minutes to hours (manual)
Distance	Limited distance (latency < 5ms RTT)	Limited distance (latency < 5ms RTT)	Limited distance (latency < 5ms RTT)	Longer distance	Longer distance
Granularity	VM centric	Storage container centric	VM centric (AHV) Storage centric (ESX)	VM centric	VM centric
Failover	Automated failover (witness)	Automated failover (witness)	Manual runbook failover	Manual runbook failover	Manual runbook failover
Number of failure domains	3	3	2	2	2
Performance impact	IO write latency	IO write latency	IO write latency	No impact	No impact
App Dependencies	Orchestration possible	No (HA priority)	Orchestration possible	Orchestration possible	Orchestration possible
Data Corruption (virus, ransomware...)	Hard to recover	Hard to recover	Hard to recover	Recoverable (snapshots)	Recoverable (snapshots)
Hypervisor	AHV	ESXi	AHV (NDR) & ESXi (PD)	AHV & ESXi	AHV & ESXi
Management	PC (NDR)	PE (PD)	PC or PE	PC or PE	PC or PE
Support Hybrid Cloud	No	No	No	Yes	Yes

Disaster Recovery

Nutanix Data Protection Strategy

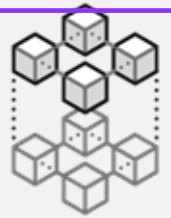
Hours | Minutes | Near Zero

Archiving

Back up

Snapshots

Async Replication



Near-sync Replication

Metro Availability

BC/DR

Different Options to Support Multiple SLA Requirements

Data Protection & Disaster Recovery

 Integrated

 Simple

 1 Clic Test/Failover

DR is generally made up of two key elements, Data Protection (DP) and Disaster Recovery (DR) orchestration.

Data Protection is natively integrated into the Nutanix software stack, and offers customers the following benefits on a per-application basis:

- Data Protection
- Multi-site replication
- Tailored RPO (Recovery Point Objective)

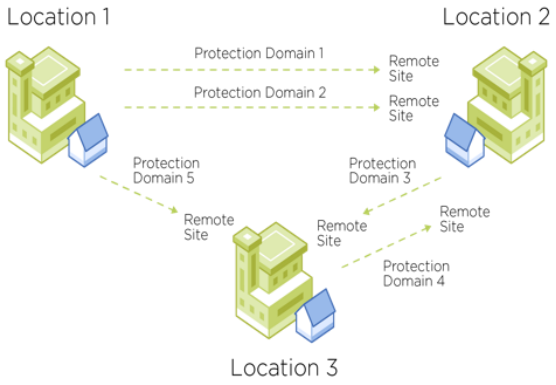
→ 2 protection methods are offered: historically, Protection Domain (via Prism Element) vs Protection Policies (via Prism Central and Nutanix Disaster Recovery (ex Leap)).

Choose the best solution for your DRP/BCP

Asynchronous Replication

RTO: Minutes

RPO: 1 Hour



AHV · vmware vSphere · Microsoft Hyper-v

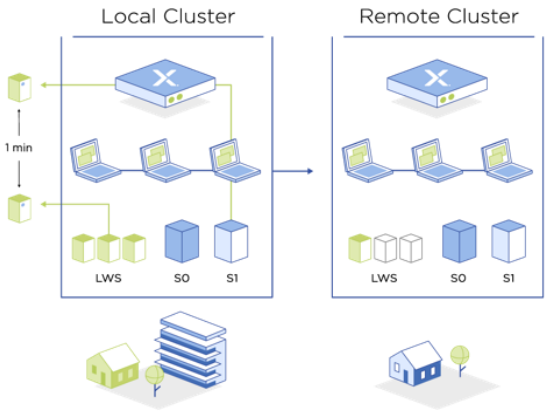
Protection Domain or NDR

Protection Domain

Near-Sync Replication

RTO: Minutes

RPO: 1-15 minutes



AHV · vmware vSphere

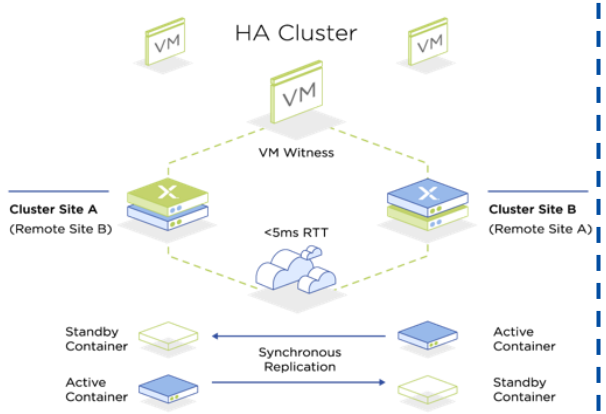
AHV (20 sec. In 6.6) (20 sec.)

Protection Domain or NDR

Metro Availability (Synchronous)

RTO: Minutes

RPO: Zero



AHV · vmware vSphere · Microsoft Hyper-v

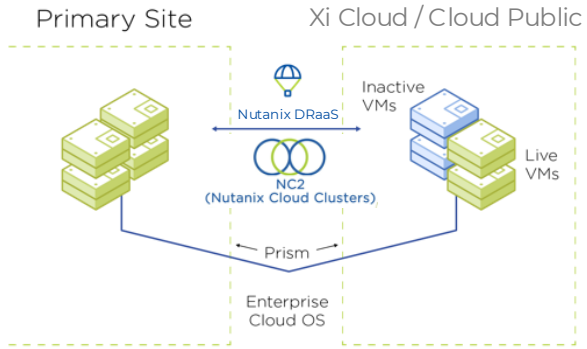
NDR

Protection Domain

DRaaS/NC2 (Cloud public)

RTO: Minutes

RPO: 1 Hour



AHV · vmware vSphere

NDR

Native Snapshots

True Immutability

Re-direct on Write

- Space Efficient
- Performant

Policy Based

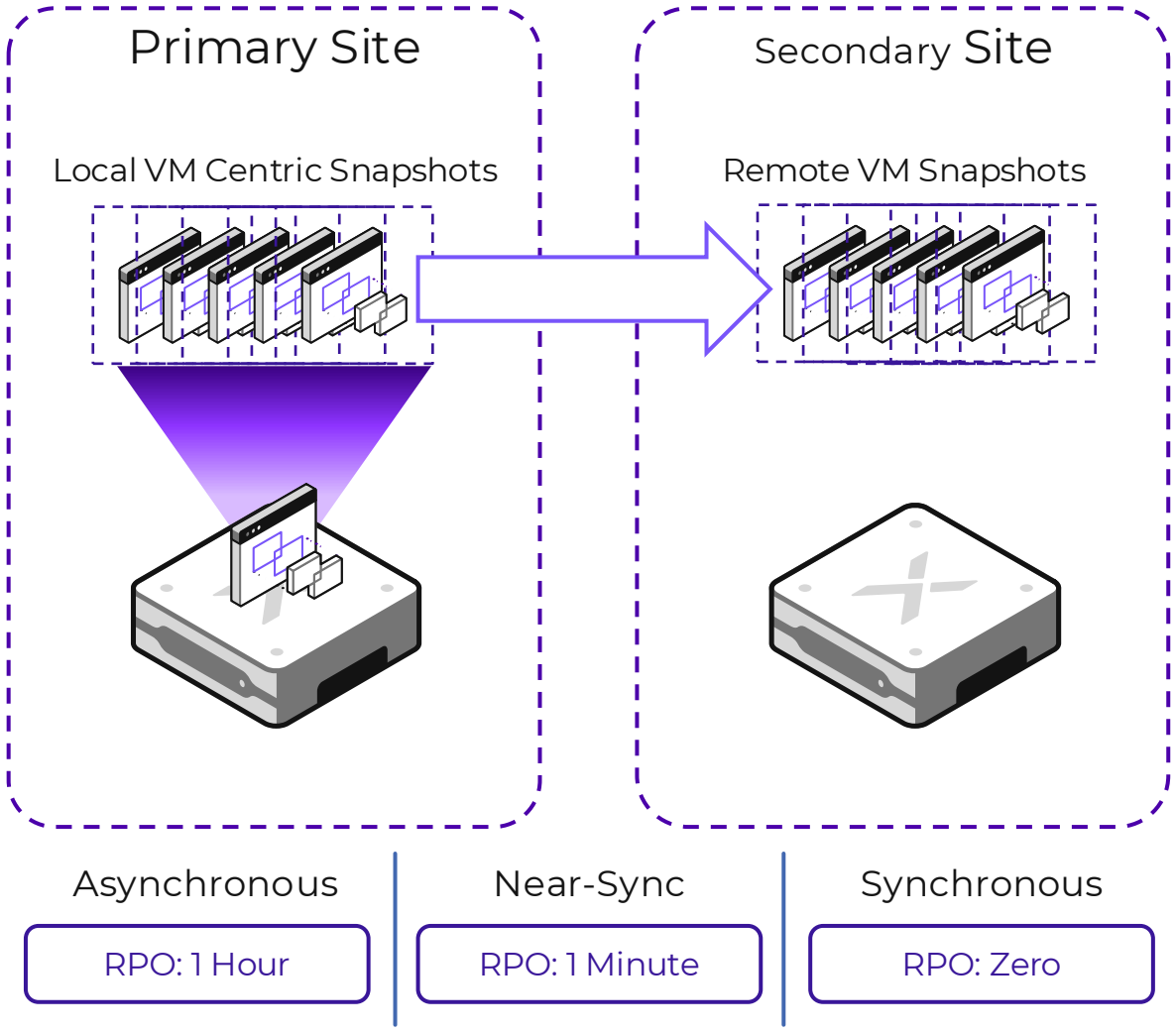
- Categories
- Schedules: RPO, Retention
- Local/Remote

Multicloud Snapshot Technology™

Coming Soon

- Primary Storage Optimization
- Ease of Mobility between on prem and cloud
- Long Term Retention

Nutanix Local and Remote Snapshots



HIGHLIGHTS

- Create unlimited local VM snapshots
- Policy-based snapshot management
- App- and Crash- consistent policies
- Support multiple hypervisors
- **Support replication across hypervisors**

BENEFITS

- Self-service file restore
- No performance impact through redirect on write
- Efficient storage utilization
- **Reduced virtualization licensing costs**

Multicloud Snapshot Technology

Mobility

Store snapshots outside of Nutanix (i.e., AWS, Azure)

Fluid movement between sites (on prem and cloud)

Long-Term Retention

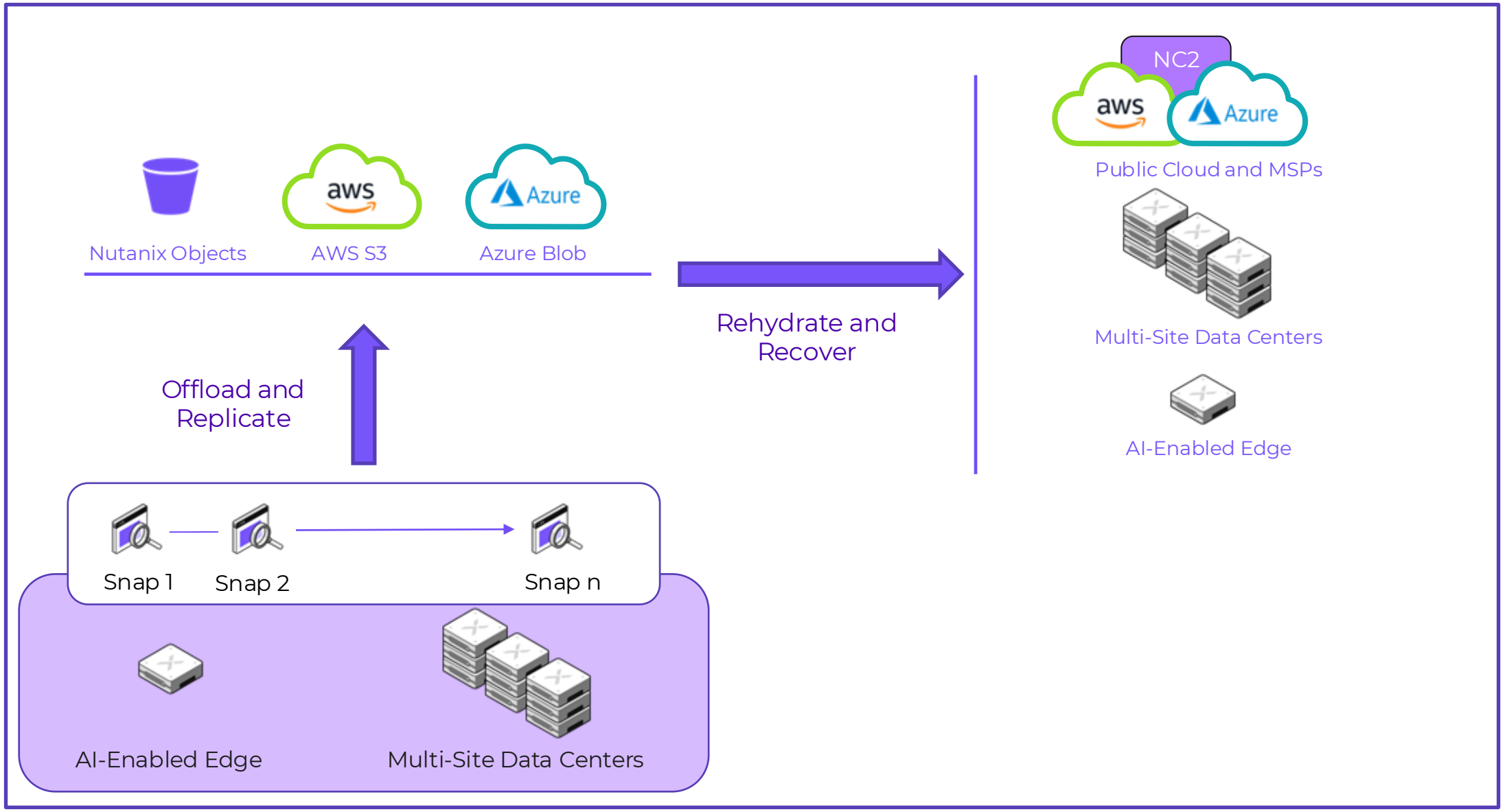
Retain snapshots for longer periods of time without bogging down storage performance

Cost Optimization

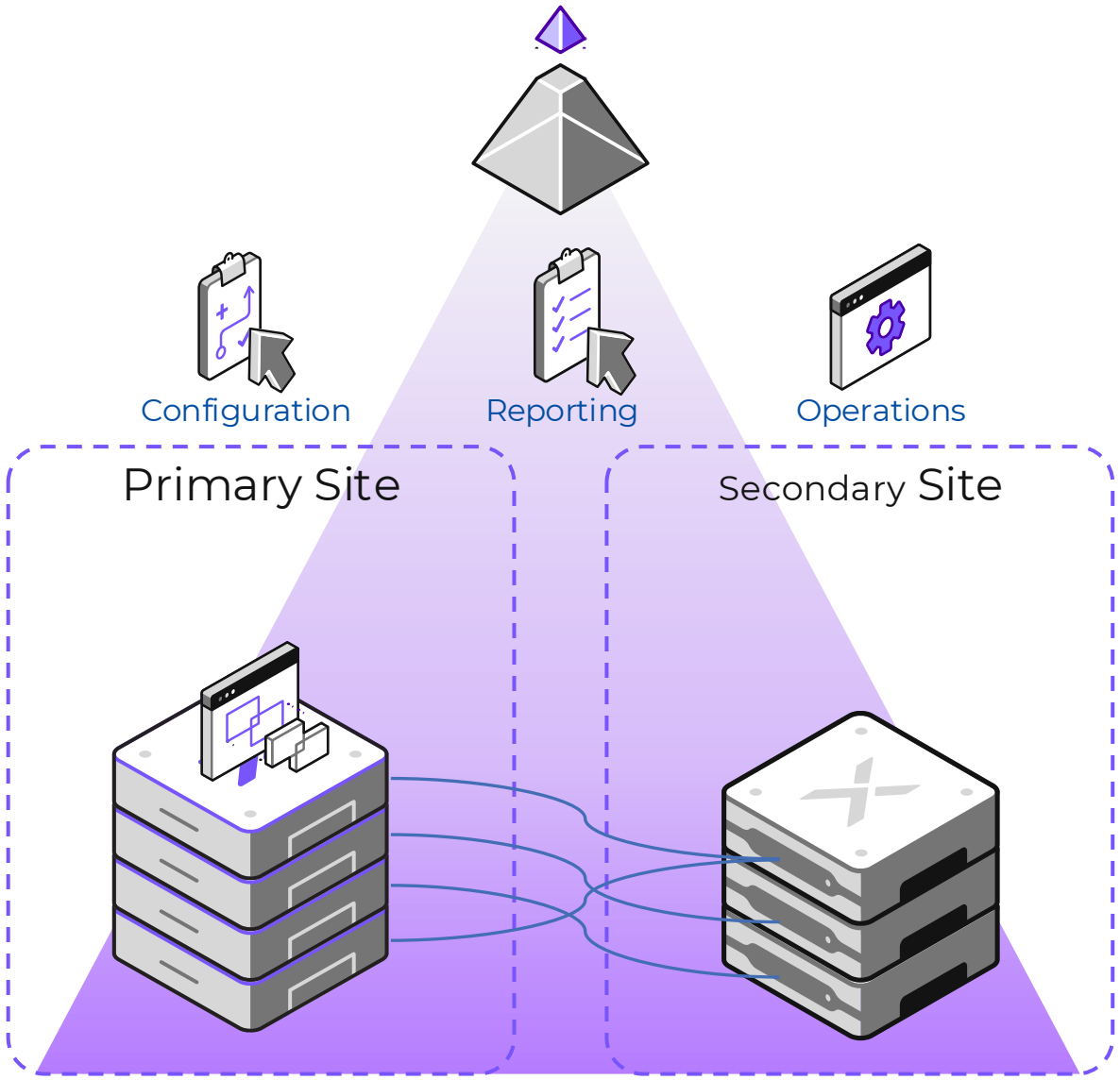
Reserve primary storage for high performance

Store snapshots in low-cost secondary storage

Nutanix Multicloud Snapshot Technology



Disaster Recovery Orchestration



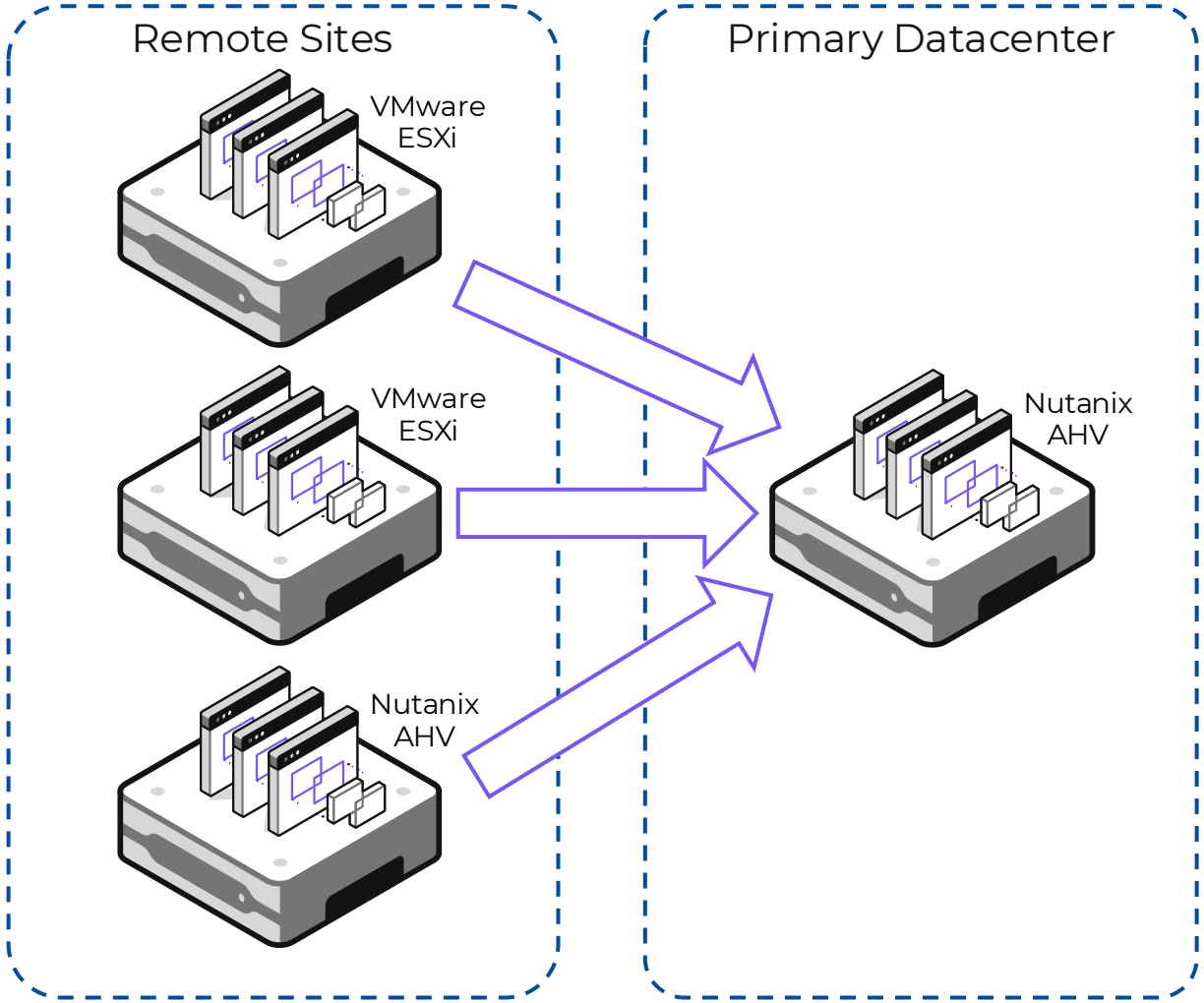
HIGHLIGHTS

- 1-Click Failover, Failback, and Testing
- Auto-protect Applications using Nutanix Categories and Protection Policies
- Orchestrate Recovery Plans (runbooks)
- Restore apps selectively or site-wide
- Unified consumer grade interface through Prism
- Recover from the latest recovery point or a previous point in time

BENEFITS

- Reduce risk with an easy-to-use policy-based approach to DR
- Recover from a disaster immediately or days after a ransomware attack

vSphere ⇨ AHV Cross-Hypervisor DR!!



OVERVIEW

- U.S.-based Agriculture Firm with >40 sites
- Mix of AHV & ESX Hypervisor

CHALLENGES

- Needed a single solution to backup and recover all sites centrally

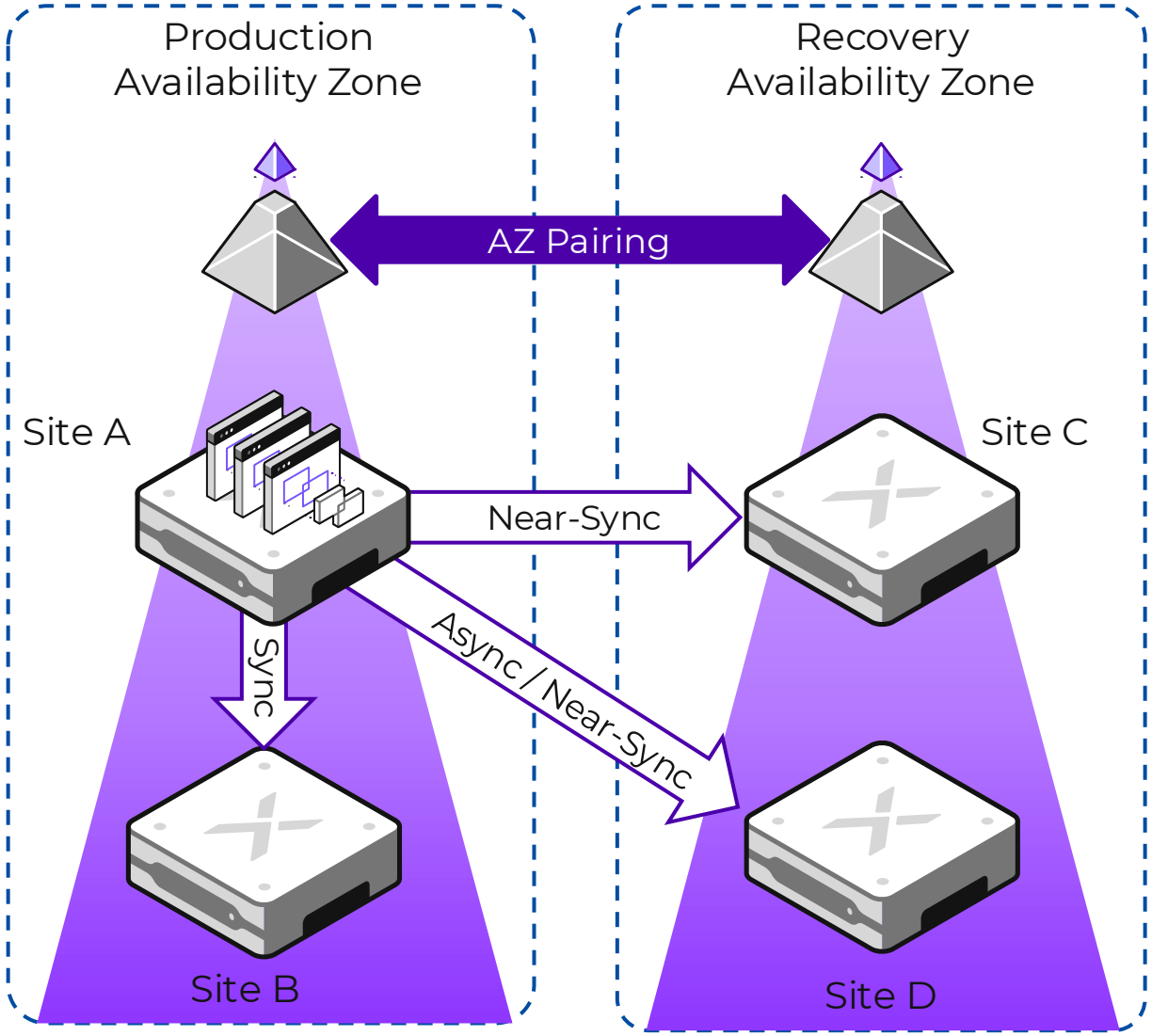
SOLUTION

- Cross-Hypervisor DR allows hypervisor choice while providing ability to restore any of the VMs to Primary Datacenter on AHV

BENEFITS

- Lower TCO from AHV
- Ability to restore entire site locally
- Standardization across the environment

Nutanix Multi-Site Disaster Recovery



HIGHLIGHTS

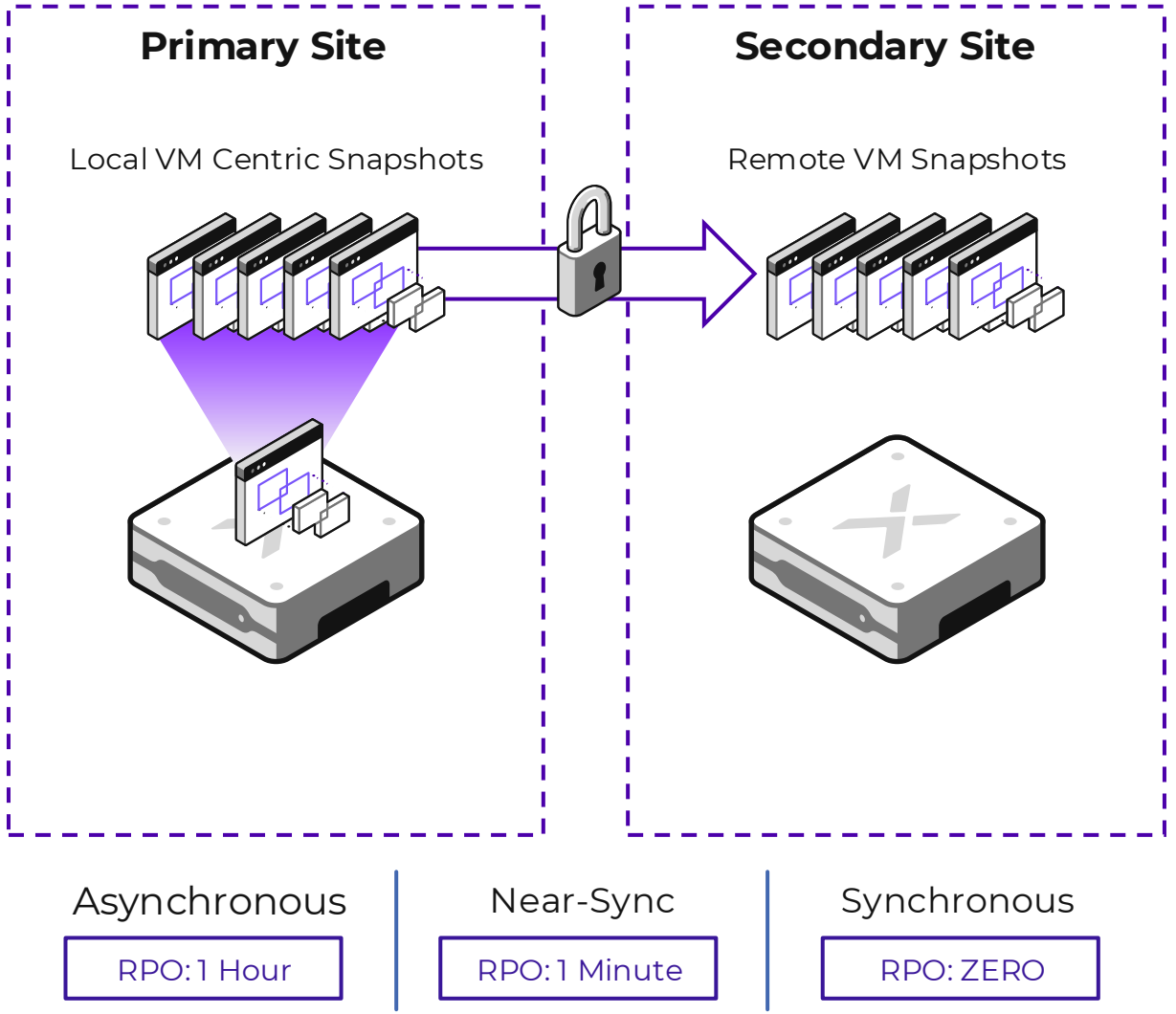
- Addresses zero data loss DR, DR testing, datacenter migration, and data corruption restore

BENEFITS

- Eliminates complex installation and administration
- Avoids vendor and hypervisor lock-in

DR Replication Encryption

- This is an enterprise readiness feature for competitive parity and help bolster our security story.
- Easy-to-use replication traffic encryption feature that is hypervisor agnostic and uses system managed keys.
- Uses gRPC TLS for control path and TCP TLS for data path.
- Will be enabled by default in 6.8



Nutanix Metro Availability for AHV

aka Metro AHV

NUTANIX

What is Metro Availability?

0 RPO

No data loss for business-critical applications

0 RTO

No downtime during planned maintenance

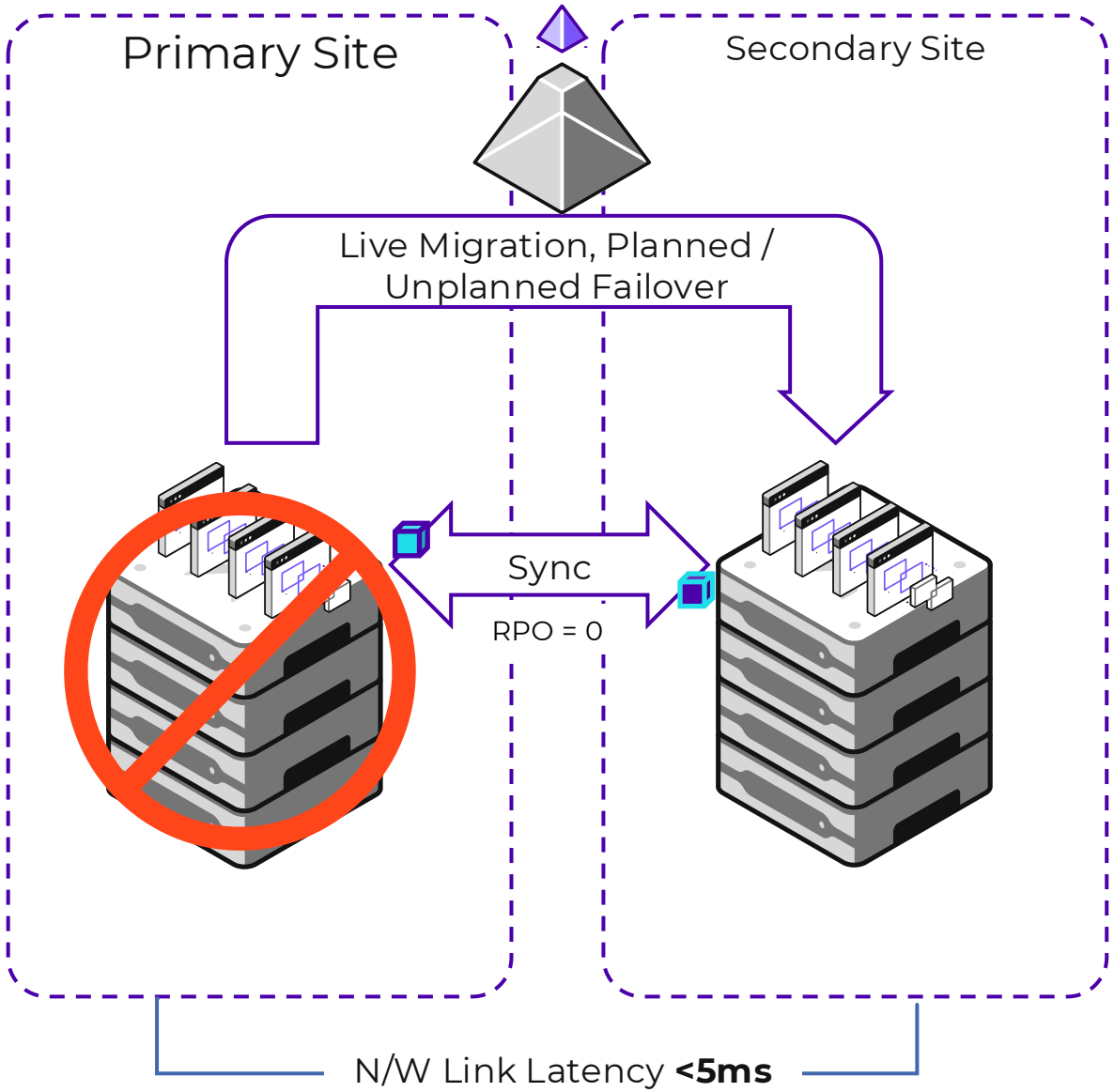
0 TOUCH

Automated application recovery orchestrated by Witness.

Metro AHV is not a Stretched Cluster, but a Sync DR with automated Failover (via Witness).

It achieves the same objectives with a mix of BC & DR, giving best of both worlds.

AHV Metro Availability and Synchronous Replication



HIGHLIGHTS

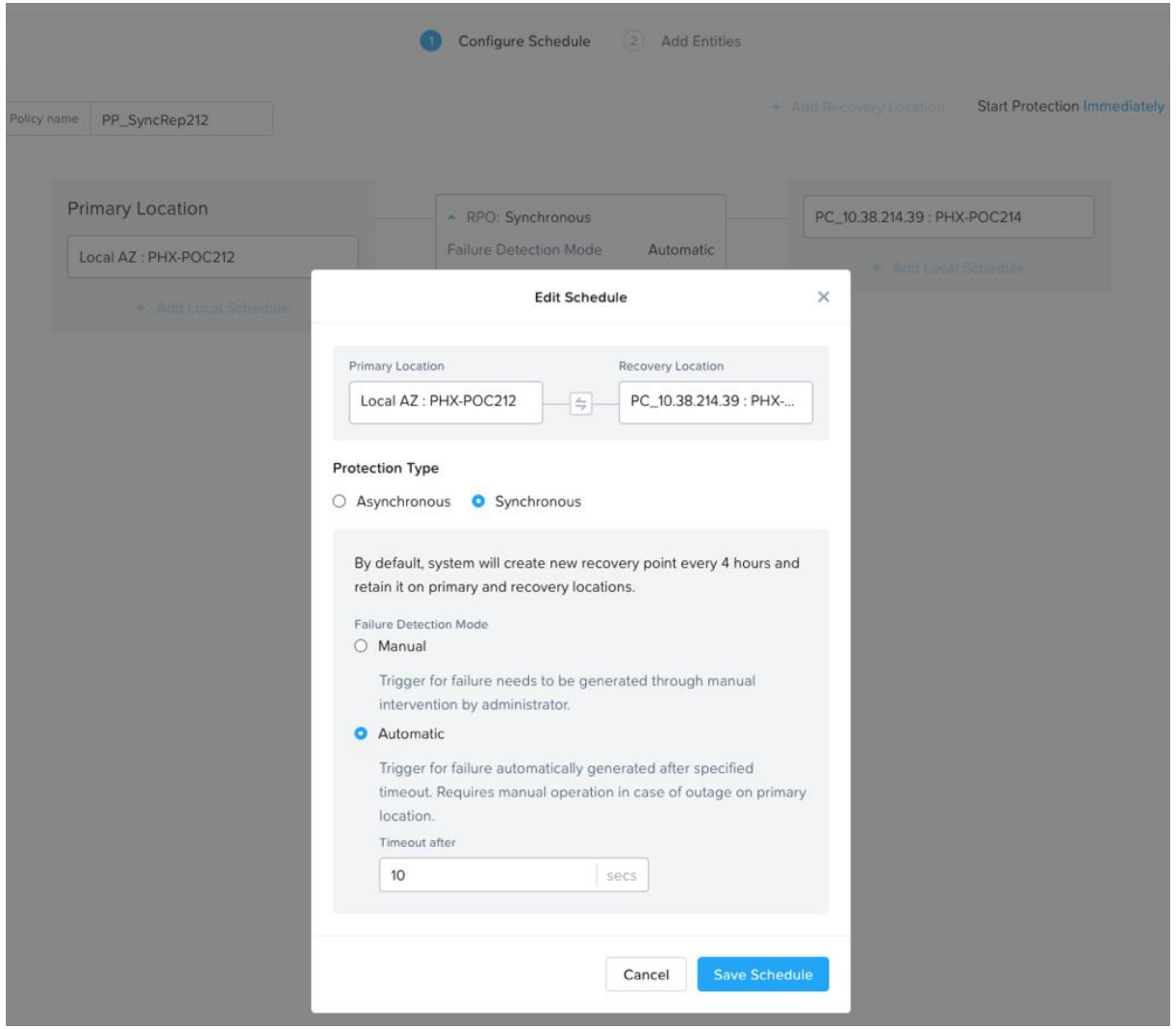
- Policy-based for predictable outcomes
- Protect mission-critical applications against complete site failure
- Support for bi-directional synchronous replication and failover.
- Zero Touch automated witness-based failover.

BENEFITS

- Easy to setup and manage which removes the burden of specialized personnel and equipment.
- 0 RPO and near 0 RTO using synchronous replication and the witness capability which provides the highest level of availability for the business
- 1-Click live migration of VM's between sites allows greater flexibility for tasks like DC maintenance or Disaster Avoidance
- REST-API Driven allowing our workflows to be included as a part of a larger DR runbook.

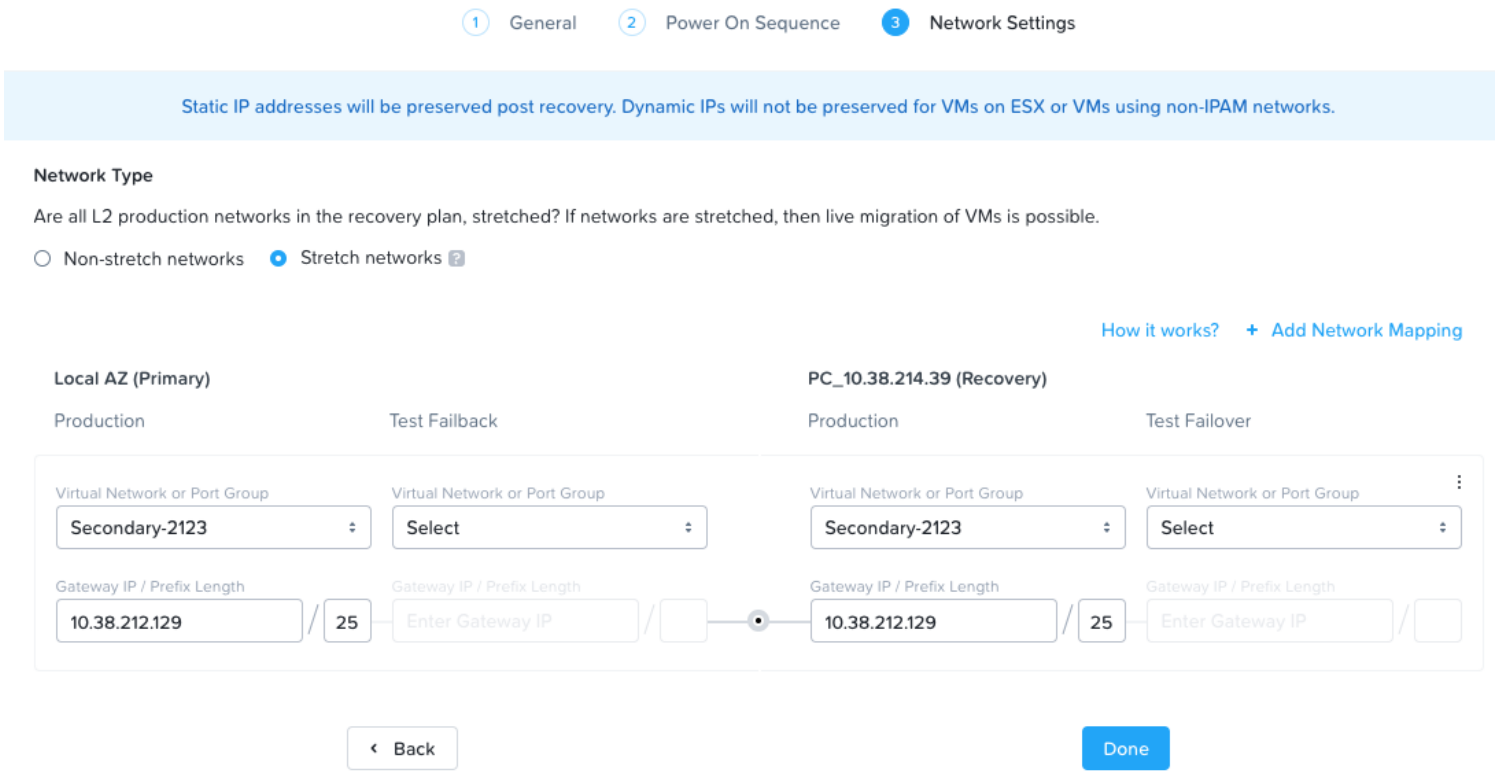
Protection Policies for Sync Rep

- ✓ Define Recovery Cluster
- ✓ Define RPO
- ✓ Define Failure Handling
- ✓ Usage of Categories for automatic Protection
- ✓ Define VMs that will be protected



Define Recovery Plans

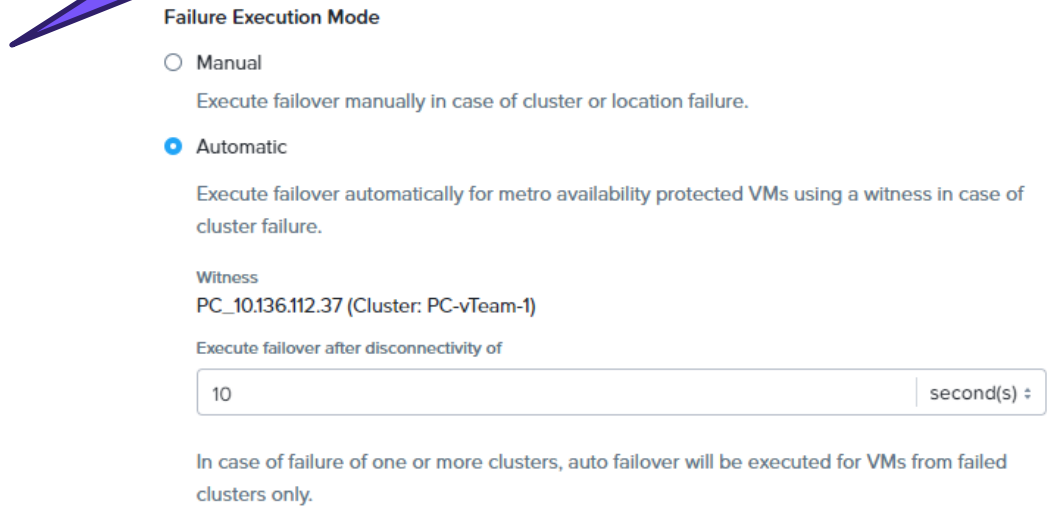
- ✓ Add VMs
- ✓ Define bootorder of VMs with stages
- ✓ Define delays between stages
- ✓ In-Guest Skript-Execution for Recovery
- ✓ Network Mapping for Production and Test Failover

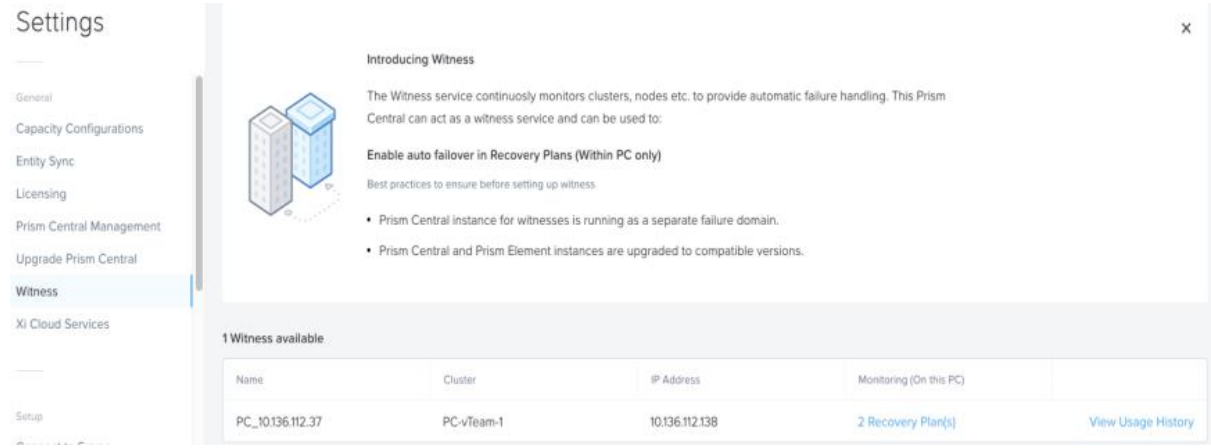


Witness for AHV (inside PC)

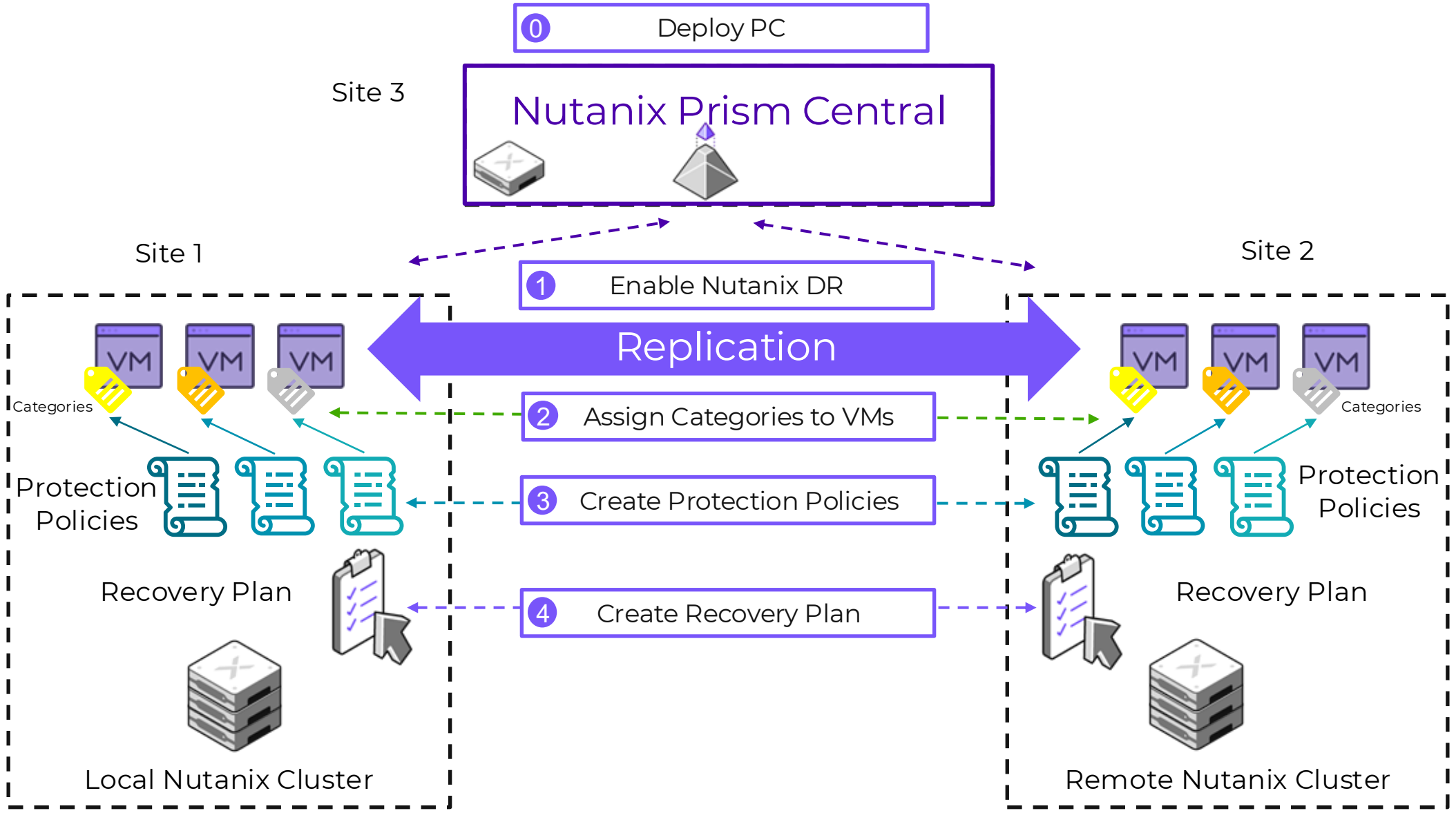
FEAT 14033 – 6.9 / pc.2024.2

- Witness-as-a-Service is deployed as a container in PC. => It needs persistent storage (Data Services must be set in AOS). That's why AOS is actually mandatory.
- Witness service is hosted in Magneto service inside PC.
  `nutanix@pcvm:$ cluster status | grep magneto`
- It resides on a separate domain failure (3rd site).
- Witness in PC is easy to upgrade, only need to upgrade PC via LCM.
- Controls Failover for one or more clusters via Recovery Plan.
- Used only with « Automatic » failure execution mode (setup in RP). Service starts only if used in at least one RP. Witness periodically ping Cerebro service of each pair clusters.
- Use `mcli` commands: disable entities with witness lock, or bypass witness locks in KB14030
- Some info are visible in PC (Settings > Witness), but do not contain service health.





Setting Up Metro AHV

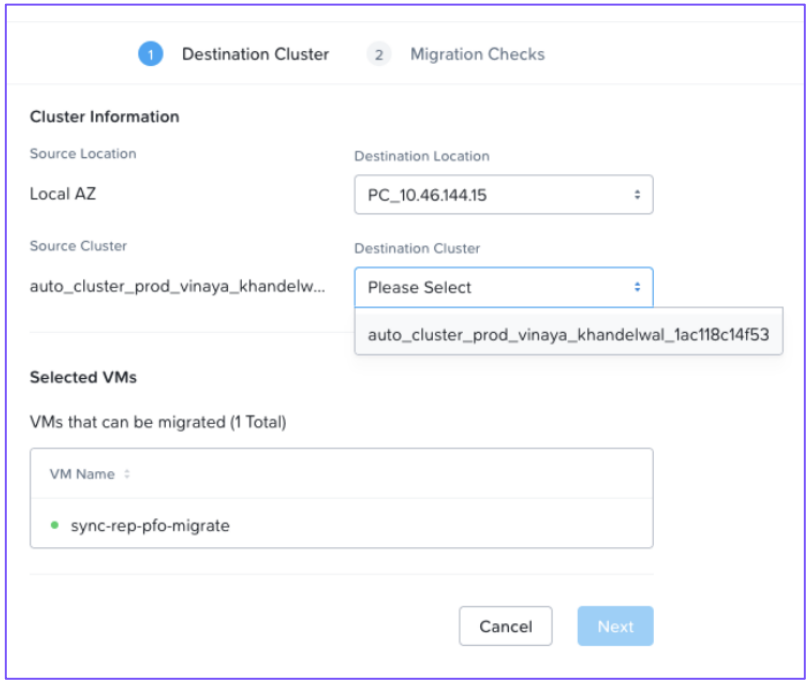


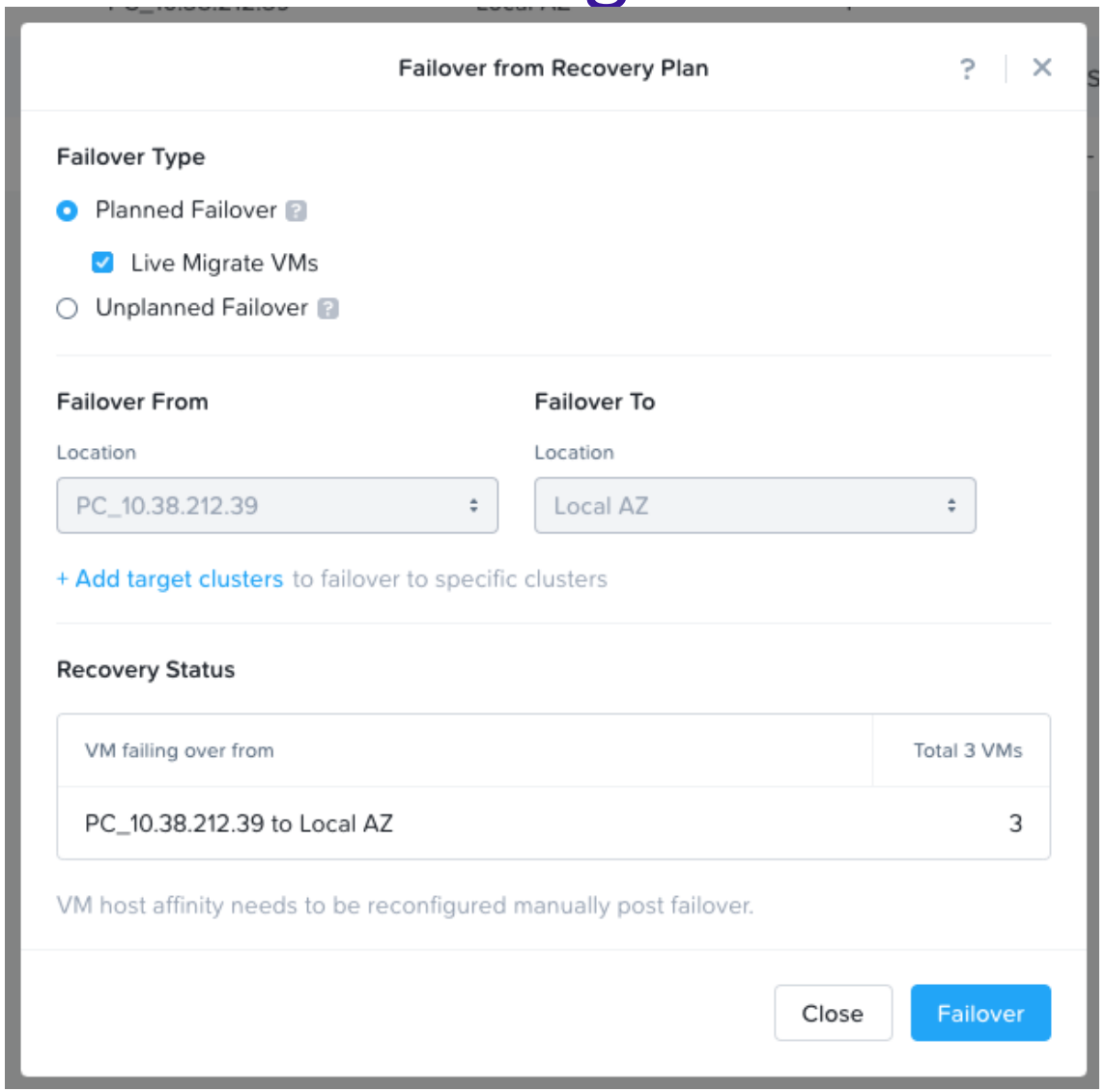
Failover / Cross-Cluster Live Migration

- ✓ Failover per Recovery Plan →

or

- ✓ Migrate single VM(s)

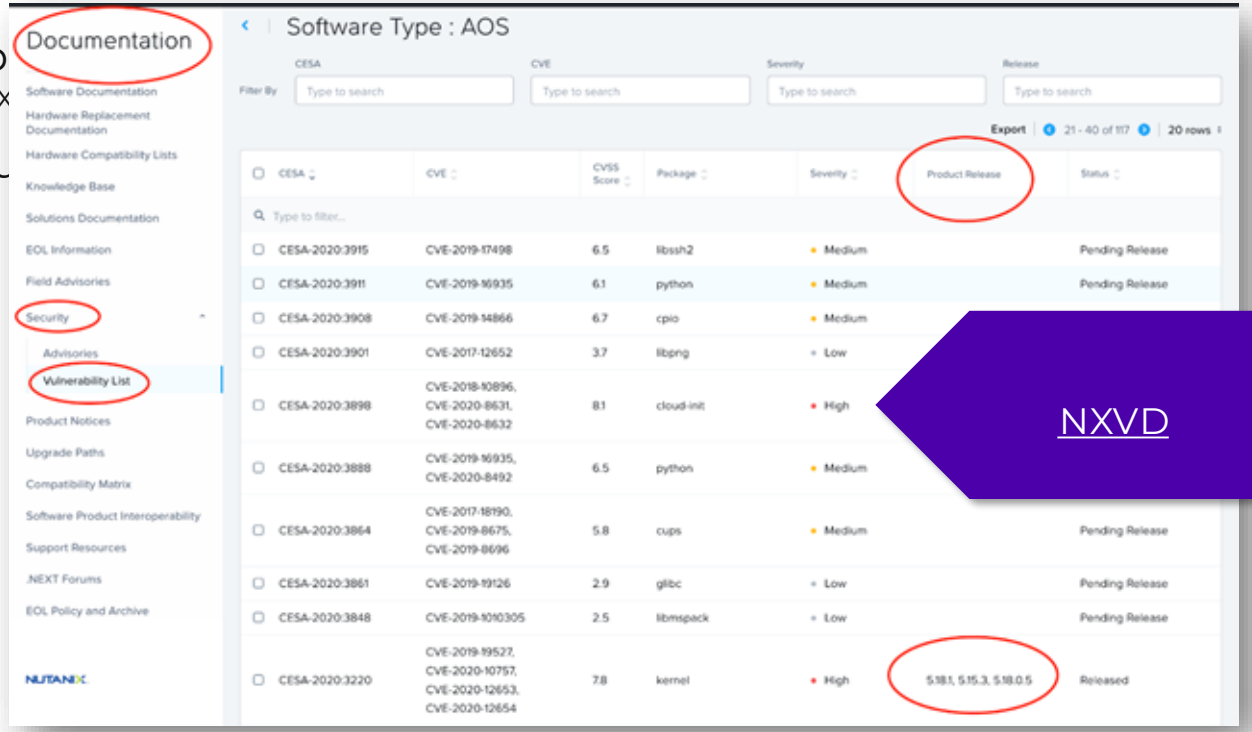




Nutanix Security

Nutanix Vulnerability Database (NXVD)

- **How can I get CVE information for the Nutanix Platform?**
  - NXVD can be found in the Nutanix Sup
    (Documentation > Software Documentation > Security > NX
  - Ability to get status of any published vu
  - Available for
    - AOS (NCI)
    - AHV (NCI)
    - PRISM (NCM)
    - Karbon (NCI)
    - MSP (NCI)
    - Objects (NUS)



Authentication and Auditing

Blocking brute force attacks :
Prevention & awareness

- Strong password policy (+10 chars)
- Default password alert
- Multi-Factor Authentication (MFA) via SSO / SAML 2
- Automatic account locking
- Integration with PAM solutions

Time it would take a computer to crack a password with the following parameters

Number of characters	Lowercase letters only	At least one uppercase letter	At least one uppercase letter +number	At least one uppercase letter +number+symbol
1	Instantly	Instantly	-	-
2	Instantly	Instantly	Instantly	-
3	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 min	6 min
8	Instantly	22 min	1 hrs	8 hrs
9	2 min	19 hrs	3 days	3 wks
10	1 hrs	1 mths	7 mths	5 yrs
11	1 day	5 yrs	41 yrs	400 yrs
12	3 wks	300 yrs	2,000 yrs	34,000 yrs

Source: Security.org

Account	Component	Cluster		Status	Last Password Change
admin	AOS	DM3-POC079-DC1	High-strength policy	Secure	Feb 28, 2024
nutanix	AOS	DM3-POC079-DC1	High-strength policy	Secure	Apr 04, 2023
admin	AOS	DM3-POC079-DC2		Secure	Dec 27, 2023
nutanix	AOS	DM3-POC079-DC2		Secure	Apr 04, 2023
nutanix	PC	_		Default Password	Jun 02, 2022
admin	PC	_		Secure	Feb 28, 2024

Password Manager increases AHV account security

7.3

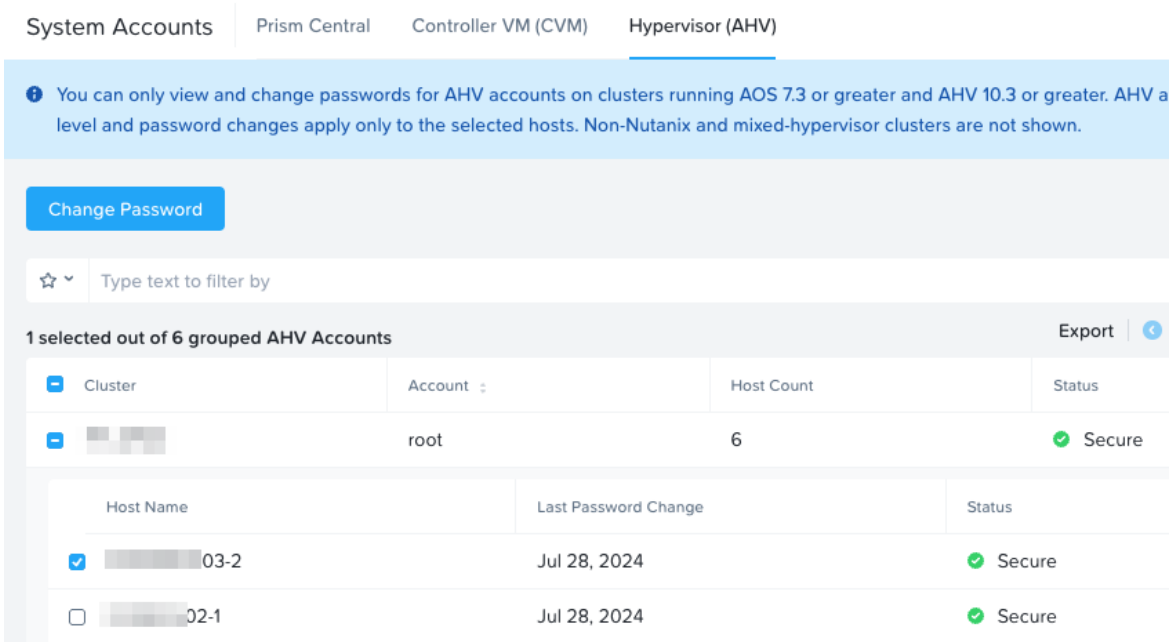
Benefit

Easily change AHV system account passwords

Added AHV accounts to existing password manager.

Prism Central UI and API-based centralized password management for all system accounts across clusters.

Warnings for default passwords.



Role Based Access Control (RBAC) and Logging

Implementing least privilege :
Fine-grained access control

- **RBAC**

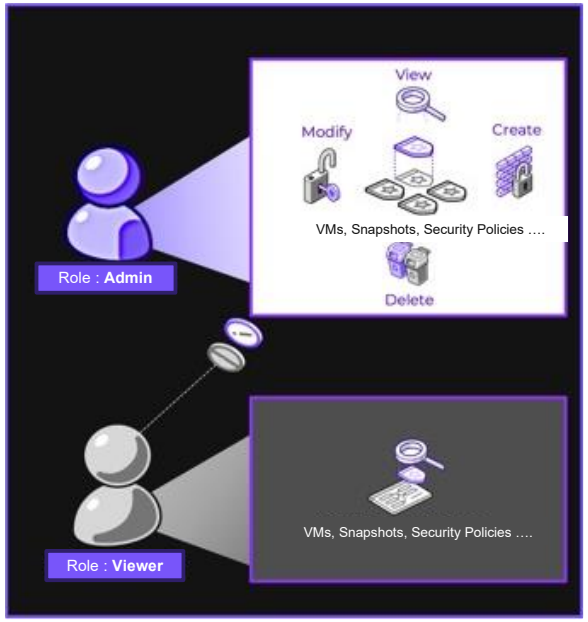
Least-privileged roles and permissions

Named accounts for traceability and auditing

- **Logs**

Logging of all activities

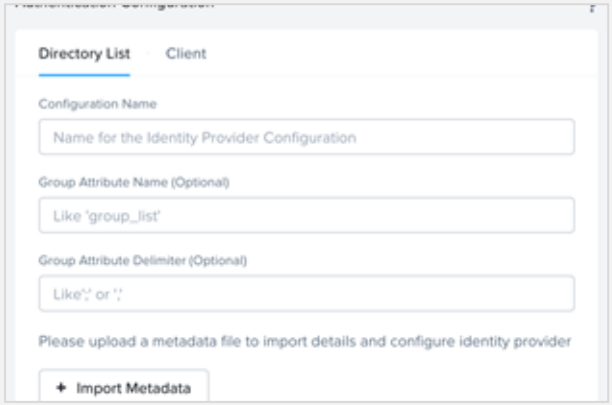
Log export to SIEM platform



Title	Create Time
User admin failed to log in from 10.66.24.6	03/15/24, 11:38:22 PM
User admin failed to log in from 10.66.24.6	03/14/24, 03:08:07 PM
User admin@ntnxlab.local failed to log in from 10.66.24.6	03/14/24, 02:26:03 PM
User admin failed to log in from 10.66.24.6	03/14/24, 02:25:58 PM

Access Denied : Restrict access to Data and Services

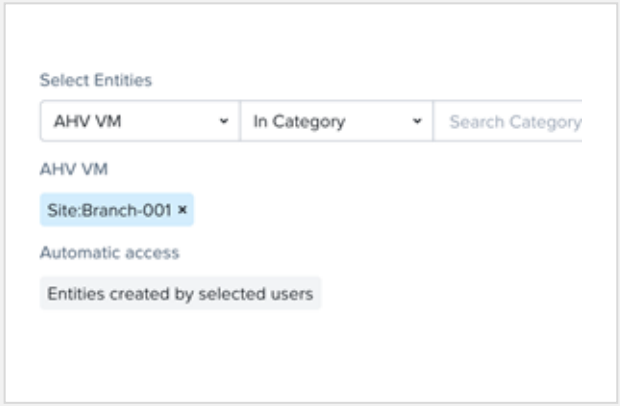
Use the AAA framework to protect your hybrid cloud infrastructure



Authentication (AuthN)

Who are you?

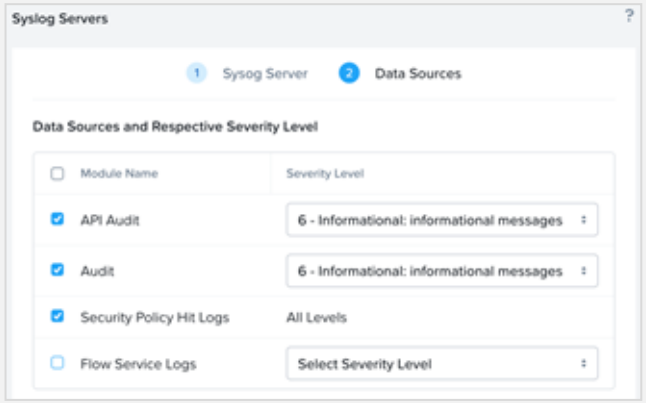
- Identity and Access Management
- LDAP or SAML integration for users
  - SAML for Multi-factor auth
- Use SSH keys and disable passwords for admin



Authorization (AuthZ)

What can you access?

- Cluster RBAC
  - Least privilege admin access to infrastructure
- Project RBAC
  - Least privilege access to VMs and apps
  - Define tenant boundaries



Accounting (Auditing)

What did you do, and when?

- Syslog
  - Capture logins and admin activity
- IPFix Network Info
  - New in AOS 6.6

LCM & Security Hardening

Limiting vulnerabilities exploitation :
Staying up-to-date / informed

- **Prism Security Dashboard**

Unified view of your security posture

Monitor CVEs Vulnerabilities

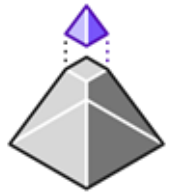
Scanning and applying STIGs

- **LCM**

Regular software and hardware updates (BIOS, firmware, etc.)

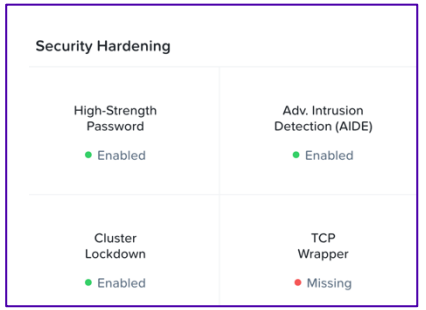
1-Click Upgrade / Automated Inventory

Automate compatibility checks SW/ HW



Prism Security Dashboard

Detailed Security Posture Summaries



Enabled Security At-A-Glance

Vulnerability Analysis & Recommendations

Prism Security Dashboard

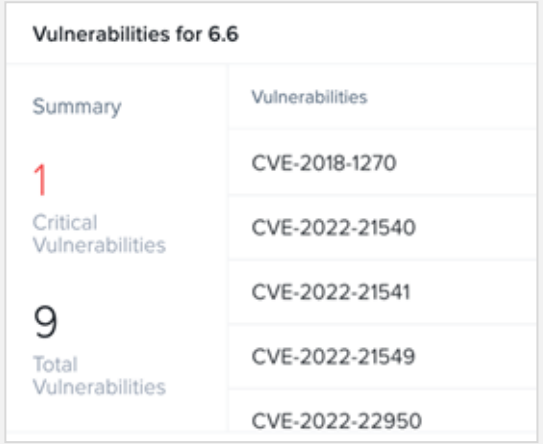
Visibility and Configuration of AOS Platform Security

Finding Summary

- Daily summarized view
- See issues by type
- Refreshes daily or manual
  - Track progress!

Visibility and Config

- One-click toggle vs CLI!
- Easily view status.
- Hide tiles you don't need



Vulnerability Analysis

- See impacted clusters
- Updates with PC
- Future: LCM

Data Security

Keeping your Data safe and secure : protect from malicious deletion

- **AOS**

Data at Rest Encryption with Native KMS

Secure Snapshot

- **Data Lens**

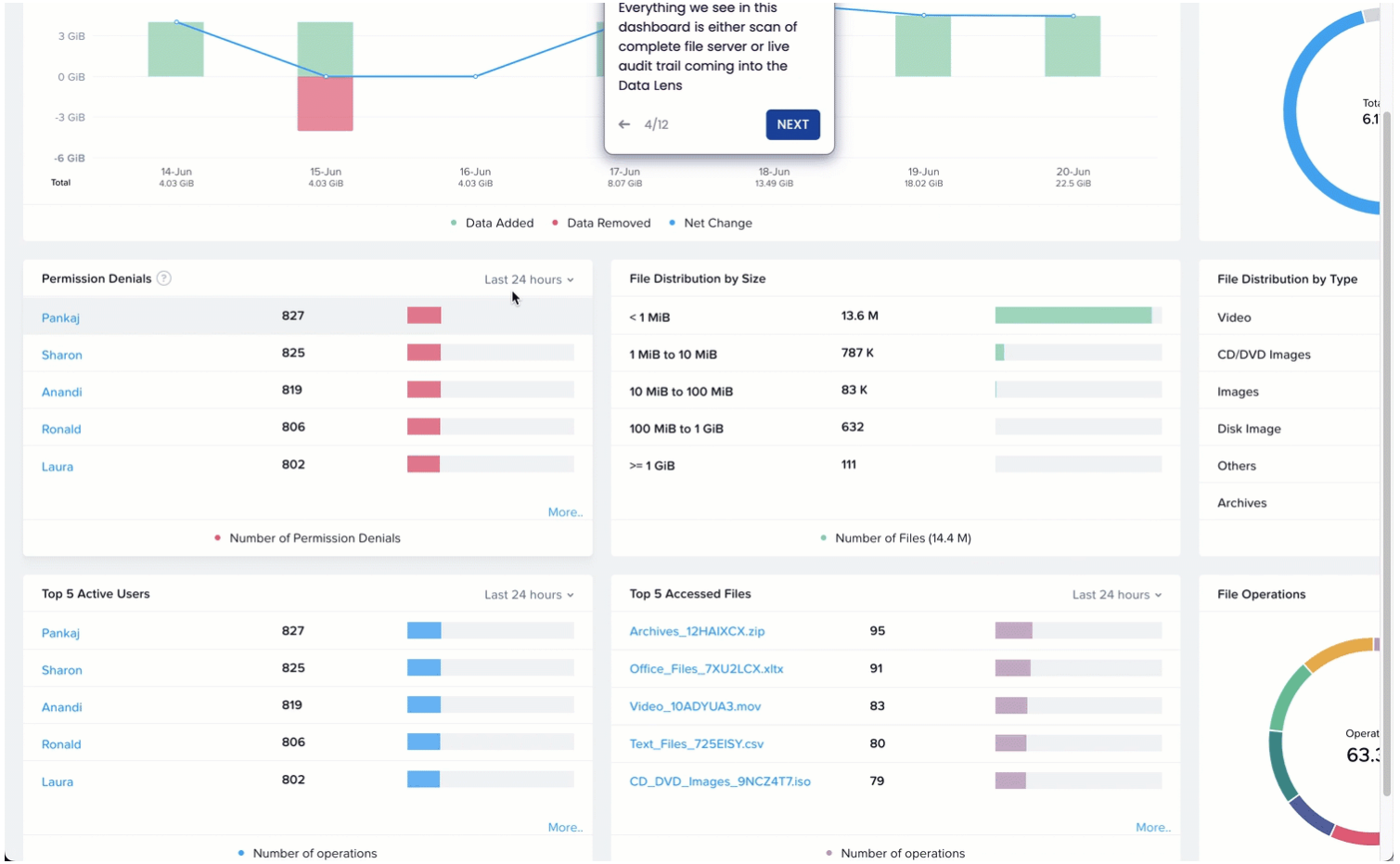
Detect and block Ransomware (5000+ signatures)

Auditing and Anomaly Detection

- **Objects (S3)**

Write Once, Read Many (WORM)

Object Lock

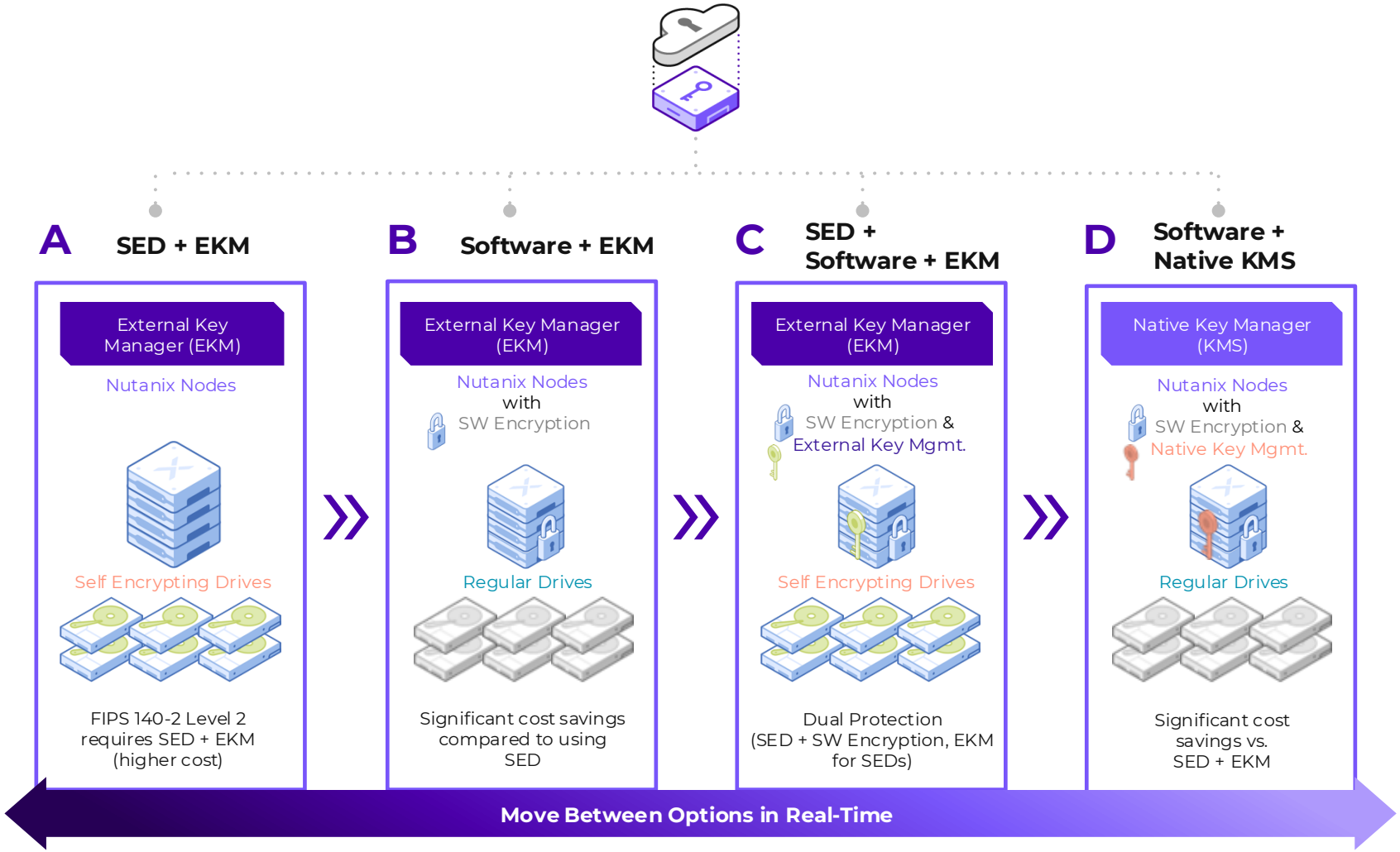


Data-at-Rest Encryption Made Easy

Quickly encrypt all your data on Nutanix Cloud Platform using one of the following options.

Why is Data-at-Rest Encryption Important?

- Keeps data confidential and prevents loss, theft, end-of life recycling, RMA replacement
- Ensures Regulatory compliance, like HIPAA, PCI-DSS, NIST
- Nutanix makes it easy! With operational simplicity.



Data-In Transit Encryption

Nutanix encrypts data-in-flight inside and between your Nutanix clusters.

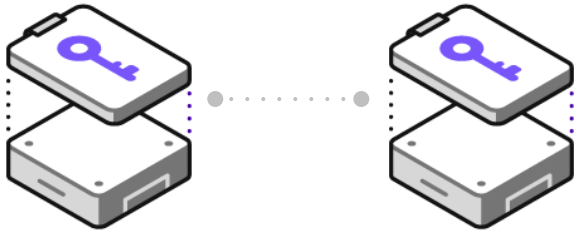
Why is Data-In-Transit Encryption Important?

- **Keeps data safe** from MITM attacks
- **Ensures an end-to-end encryption** method
- **Removes complexity** using built-in Nutanix security without the hassle of external management

Intra-Cluster

Data-in-Transit Encryption inside the Cluster

- Protect RF2 and RF3 replication in the LAN
- AES 256
- No key manager needed
- Covers AOS replication data node-to-node communication



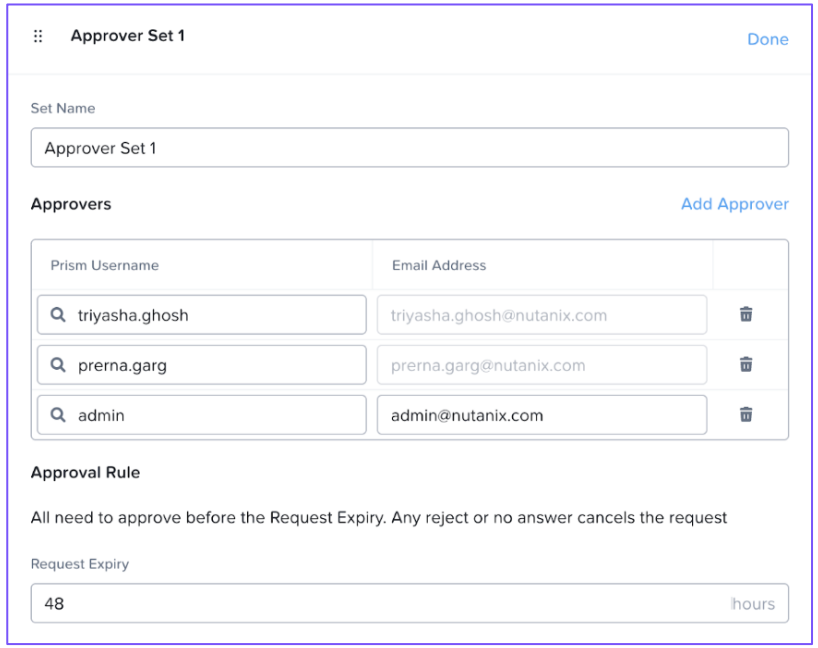
Inter-Cluster

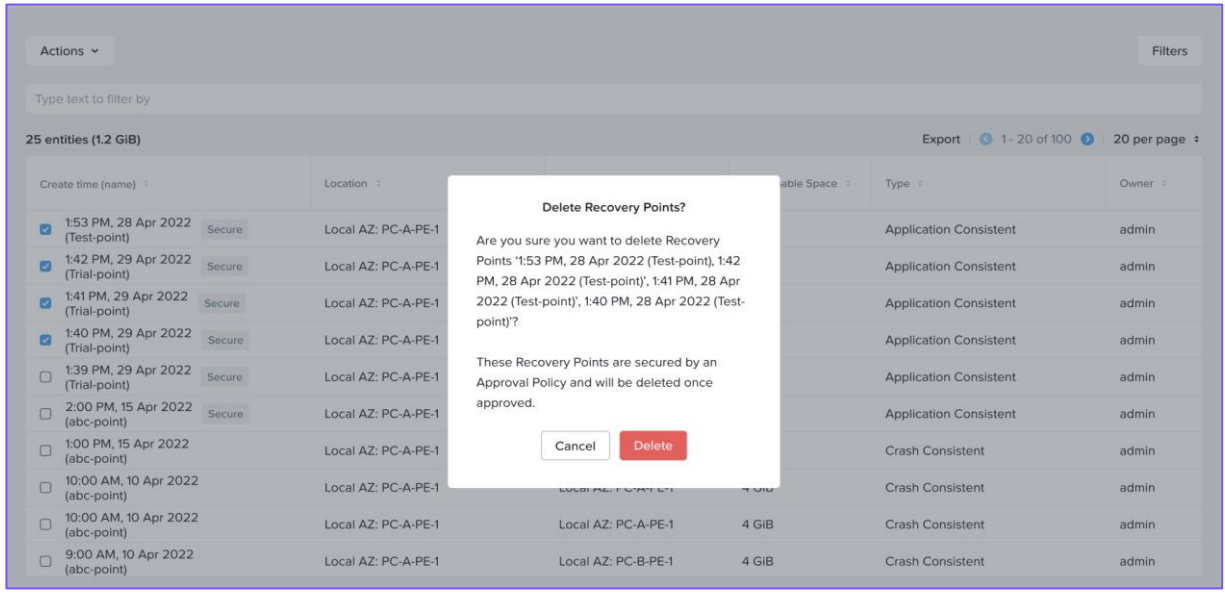
Data-in-Transit Encryption between Clusters

- Protect Disaster Recovery on WAN links
- AES 256
- No key manager needed
- Storage replication
- Live Migration Protected

Secure Snapshot

- Provide additional protection for snapshots
- Ensure that Nutanix snapshots for AOS are **immutable and cannot be deleted** by a single compromised admin.
- Set up a **Multi-party Policy Approval** to protect critical actions, like deleting Recovery Points.
- Protect against **human error**

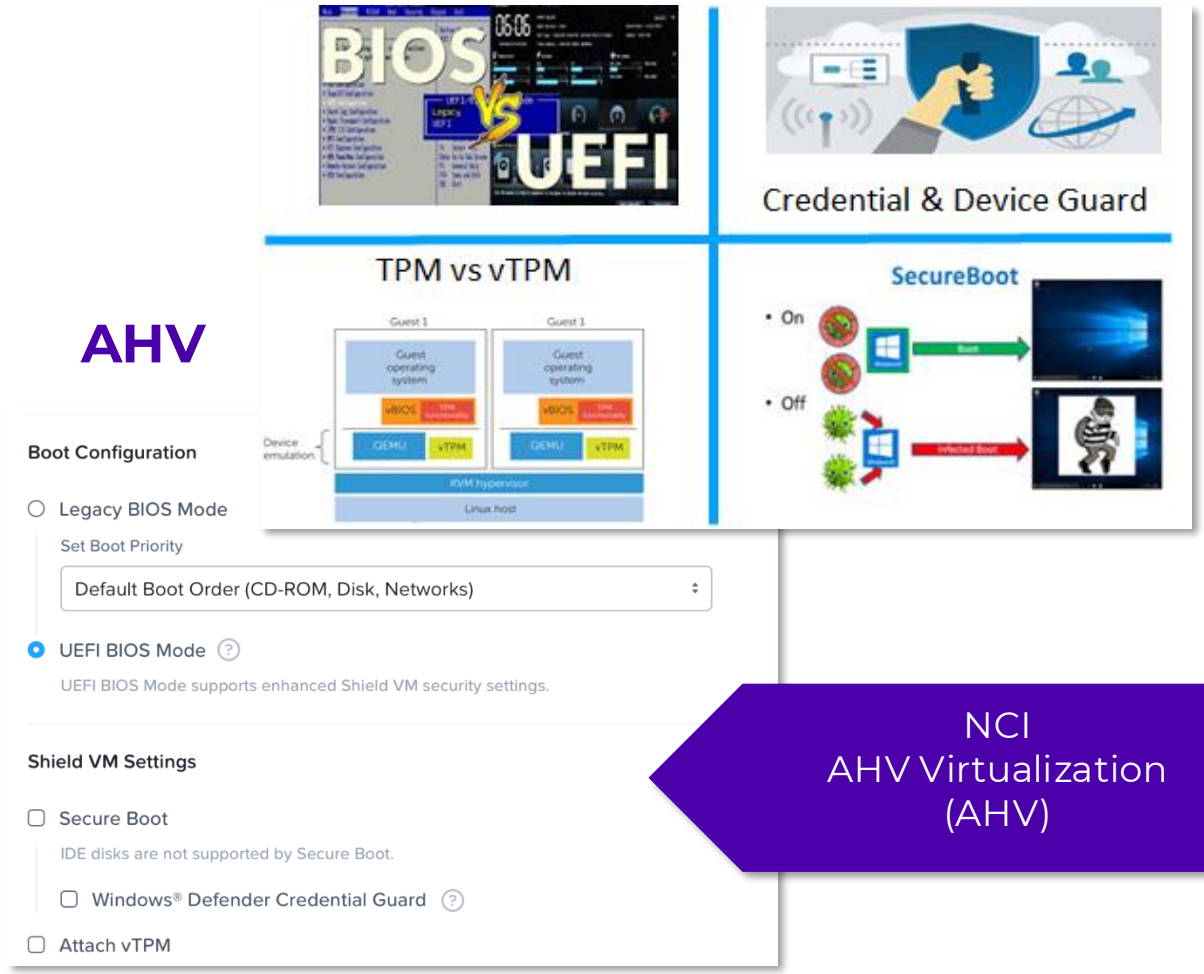




AHV Workload Security

- **Platform-Level**
  - Standardized and Secure UEFI replaces traditional BIOS
  - Secure Boot ensures hardware root during boot
  - TPM provide secure key storage and functions. vTPM is a software implementation of TPM for virtualization
- **OS-Level**
  - Microsoft Credential Guard protects security credentials and tokens outside of running Windows system

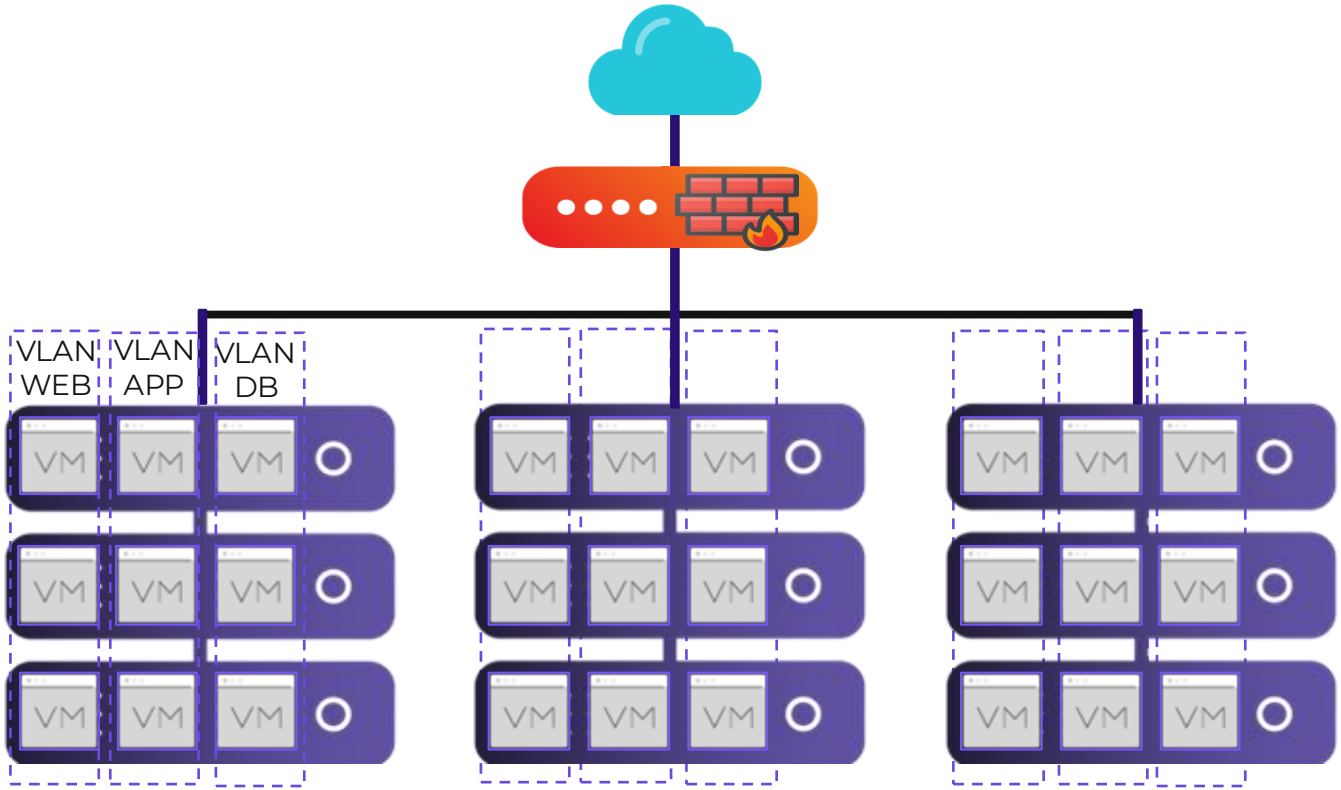
Important
→ Windows 11 requires UEFI, Secure Boot, and vTPM



NCI
AHV Virtualization
(AHV)

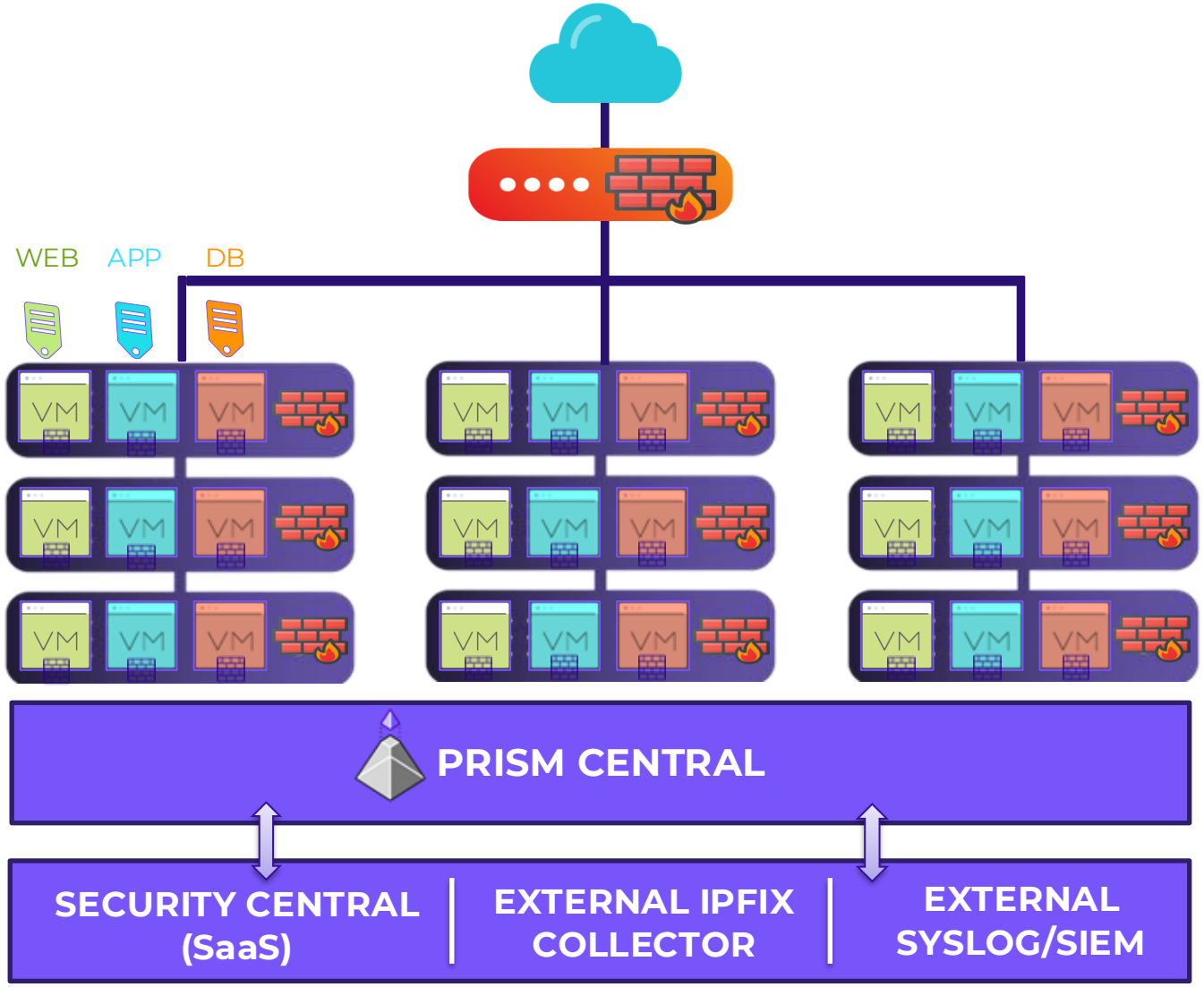
Flow Security

Traditional perimeter firewalls are becoming obsolete for protecting East-West traffic



- **Only broader Segmentation**
- **Traffic Hairpinning/Tromboning**
- **Limited Capacity/Scale**
- **Static IP Based Security Rules**

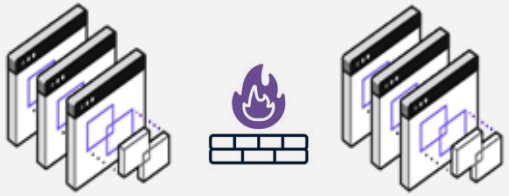
Zero Trust Microsegmentation for protecting East-West traffic



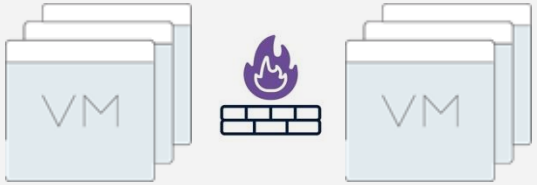
- **Built-in AHV Hypervisor**
- **Centrally managed from unified console**
- **Scalable and Distributed E/W Firewalling**
- **Tag/Category based Security Rules**
- **Agentless enforcement at each vNIC**
- **Security Rules moves along with VM**
- **Rich Visualization and Monitoring**

How Customers Are Using Microsegmentation

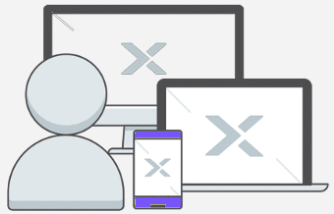
Segmenting and Protecting High-Value Applications



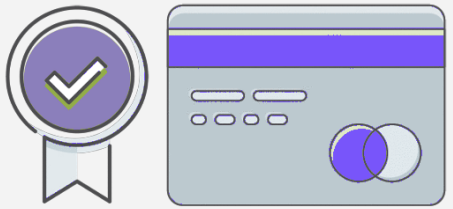
Isolating Environments



Securing VDI Environments



Strengthening Regulatory Compliance



Complete Visibility Of Workloads And Flows

Visualize Application Traffic

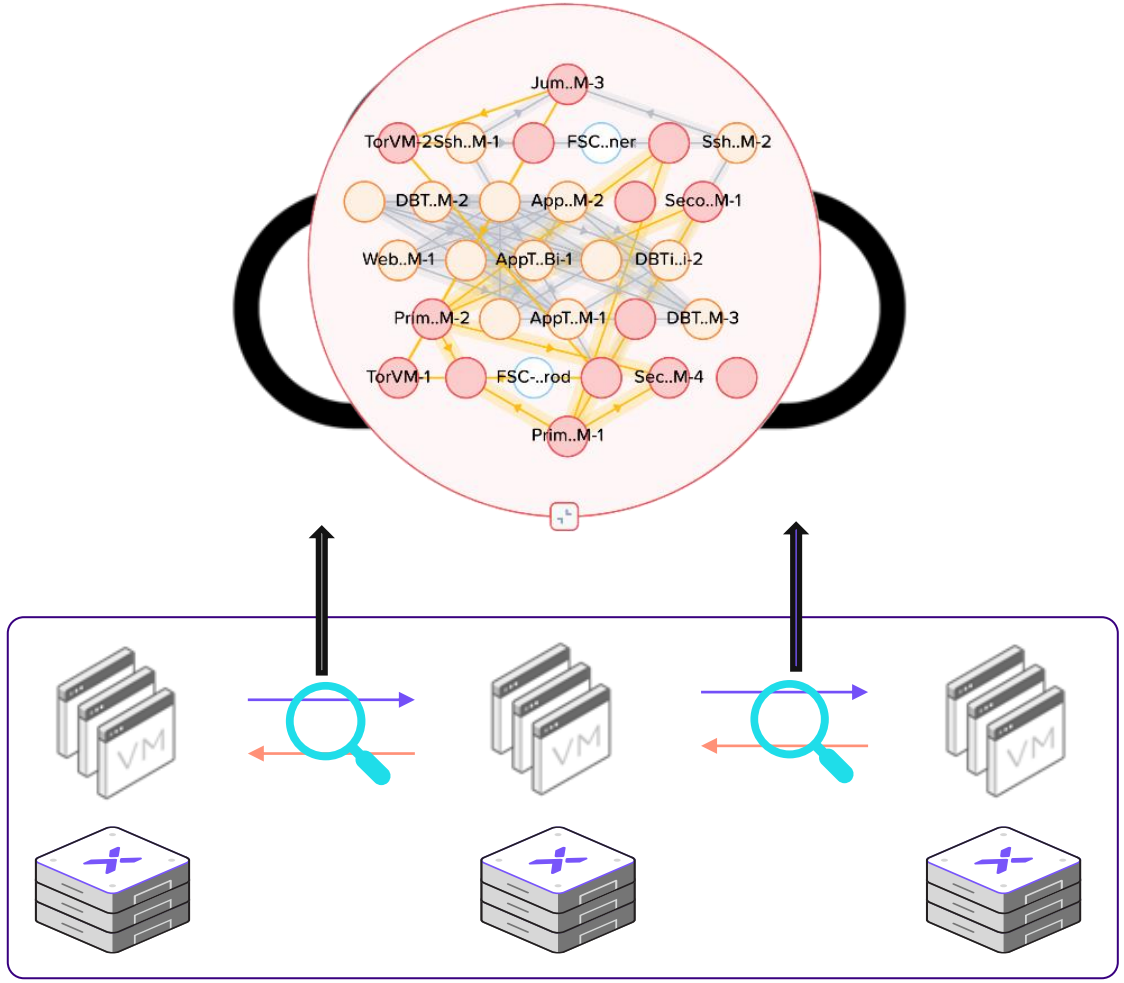
Explore External Traffic

Detect Lateral Movements

Identify with Color Coded Flows

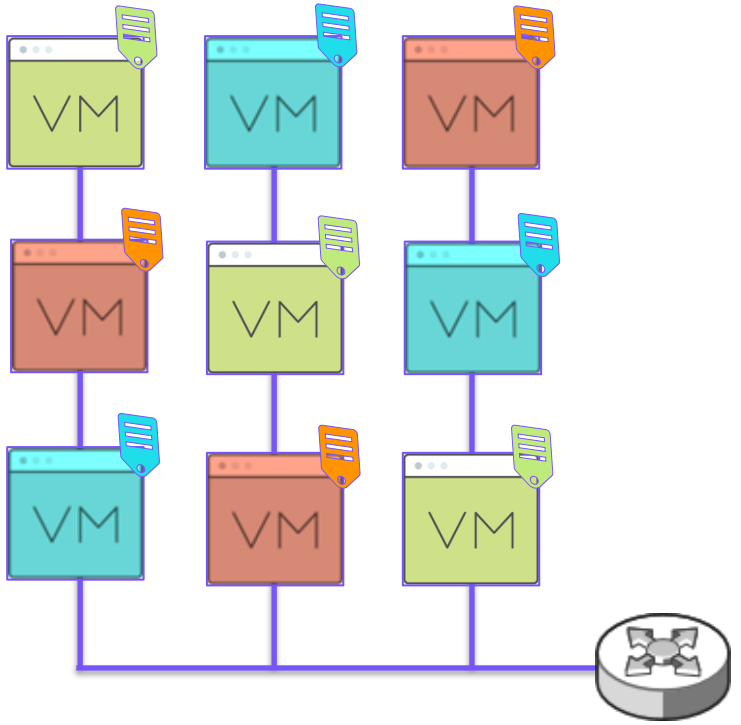
Report VM Security Status

Export Traffic Flows as CSV



Identify and Group VMs with Categories

- The categories attached to the VM determine its membership in the Security Policies
- Define a strategy to tag (categorize) the existing and new applications workloads

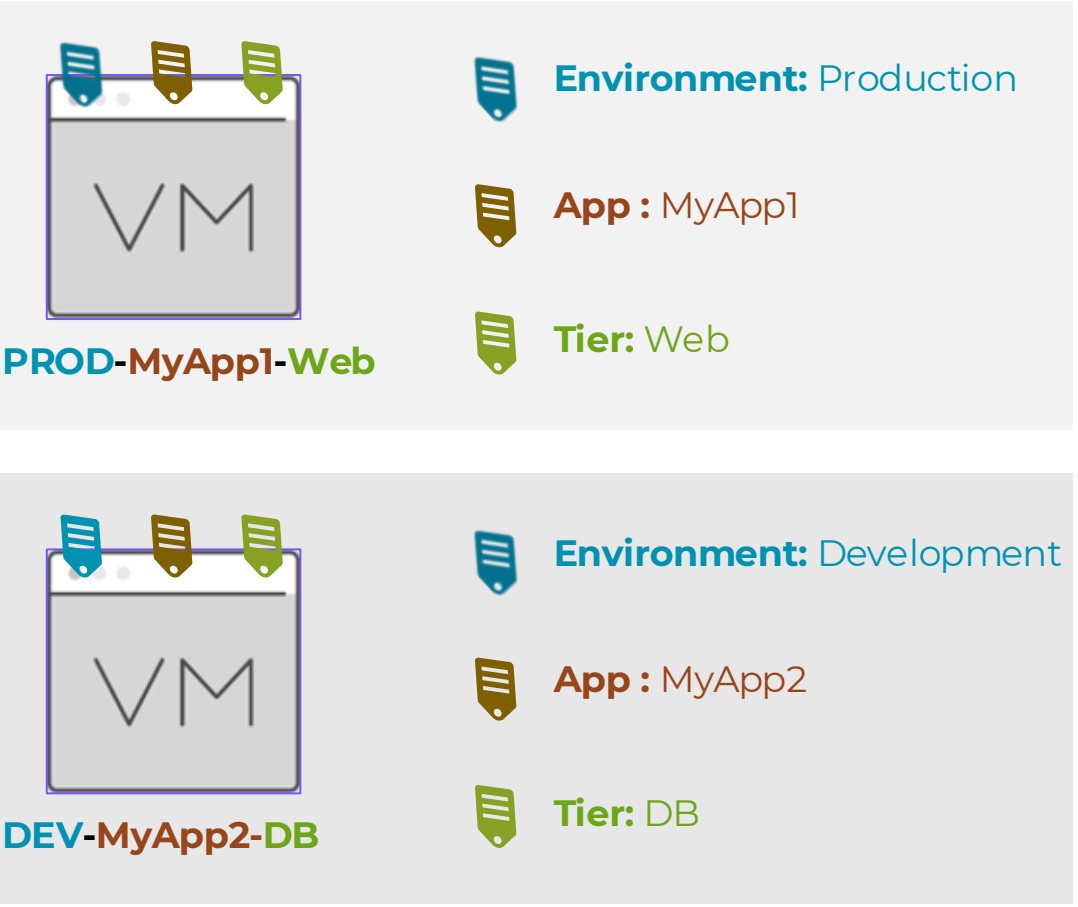


Common categories

Category	Example Values
Environment	Production, Dev, Test
Application	CRM, ERP, Intranet, ECM
Tier	Web , App, DB
Classification	Level-1, Level-2, Secret
Compliance	PCI, SWIFT, HIPAA

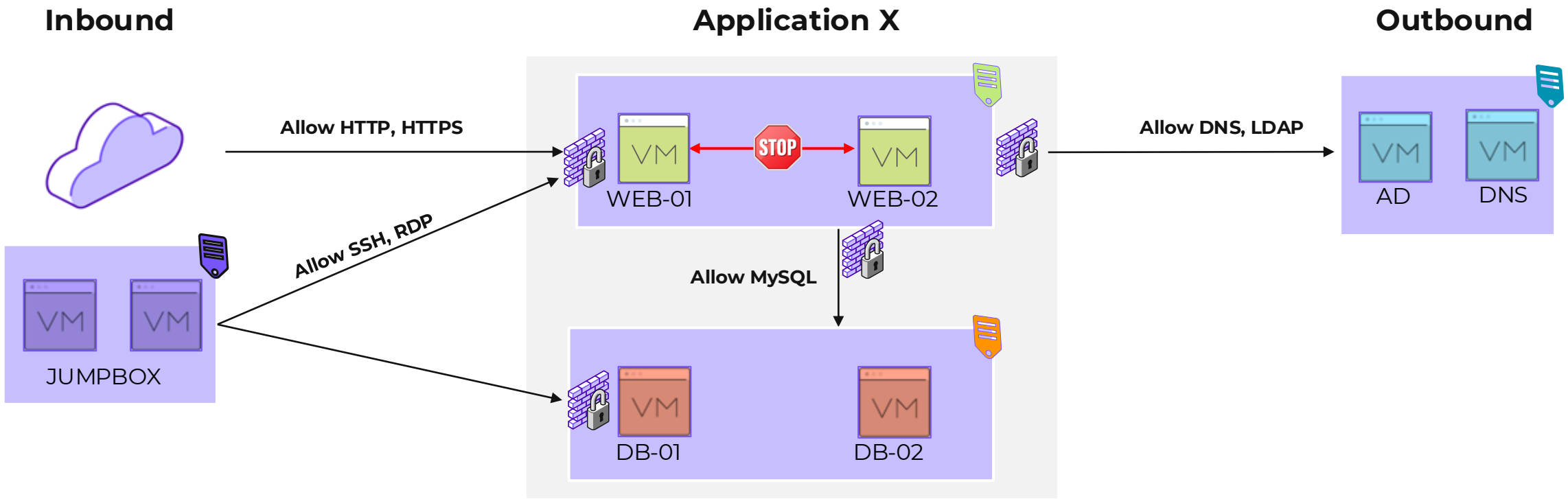
Automated Categorization Of New VMs

- Auto-categorization via Playbooks* allows VMs to be included automatically in existing security policies
- Example of inclusion criteria: VM naming convention, VM OS (Windows, Linux), etc.

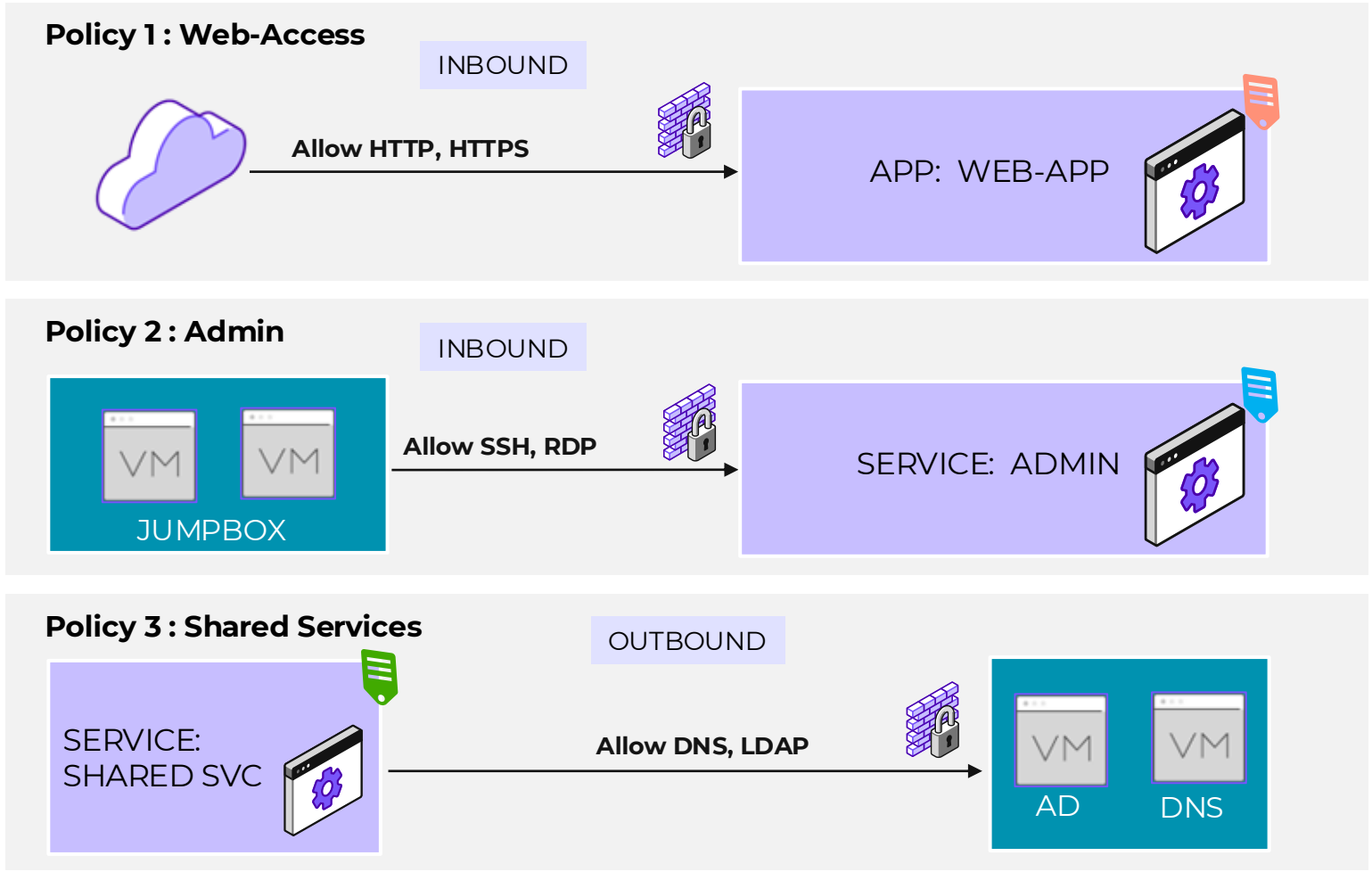


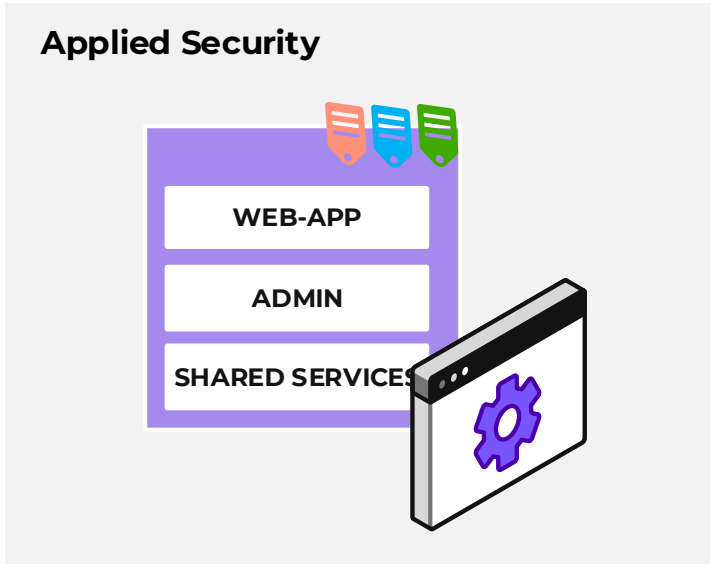
* Requires NCM Starter

Protecting Apps with App-centric Policy

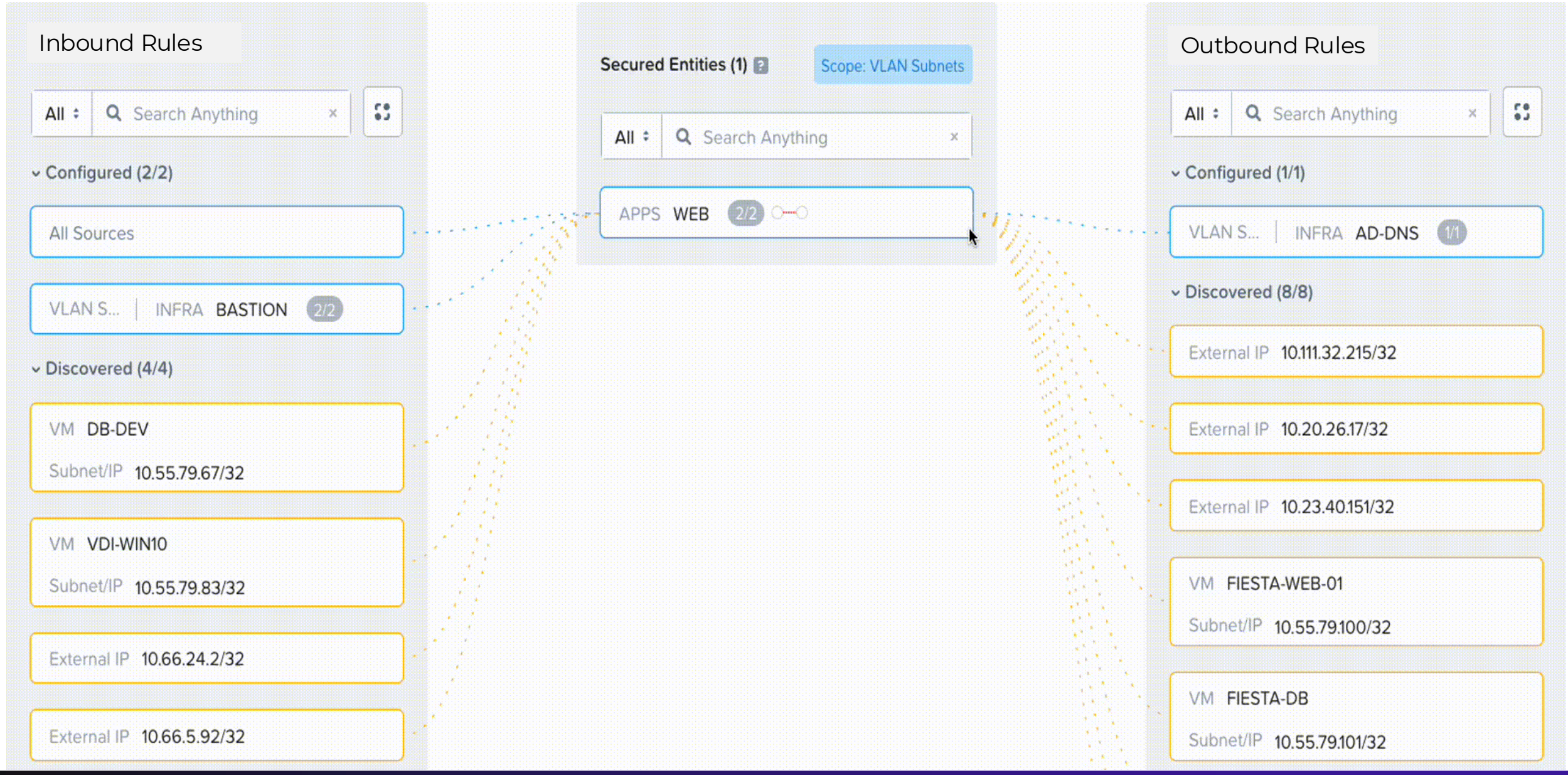


Flexible Mapping Between VMs And Policies

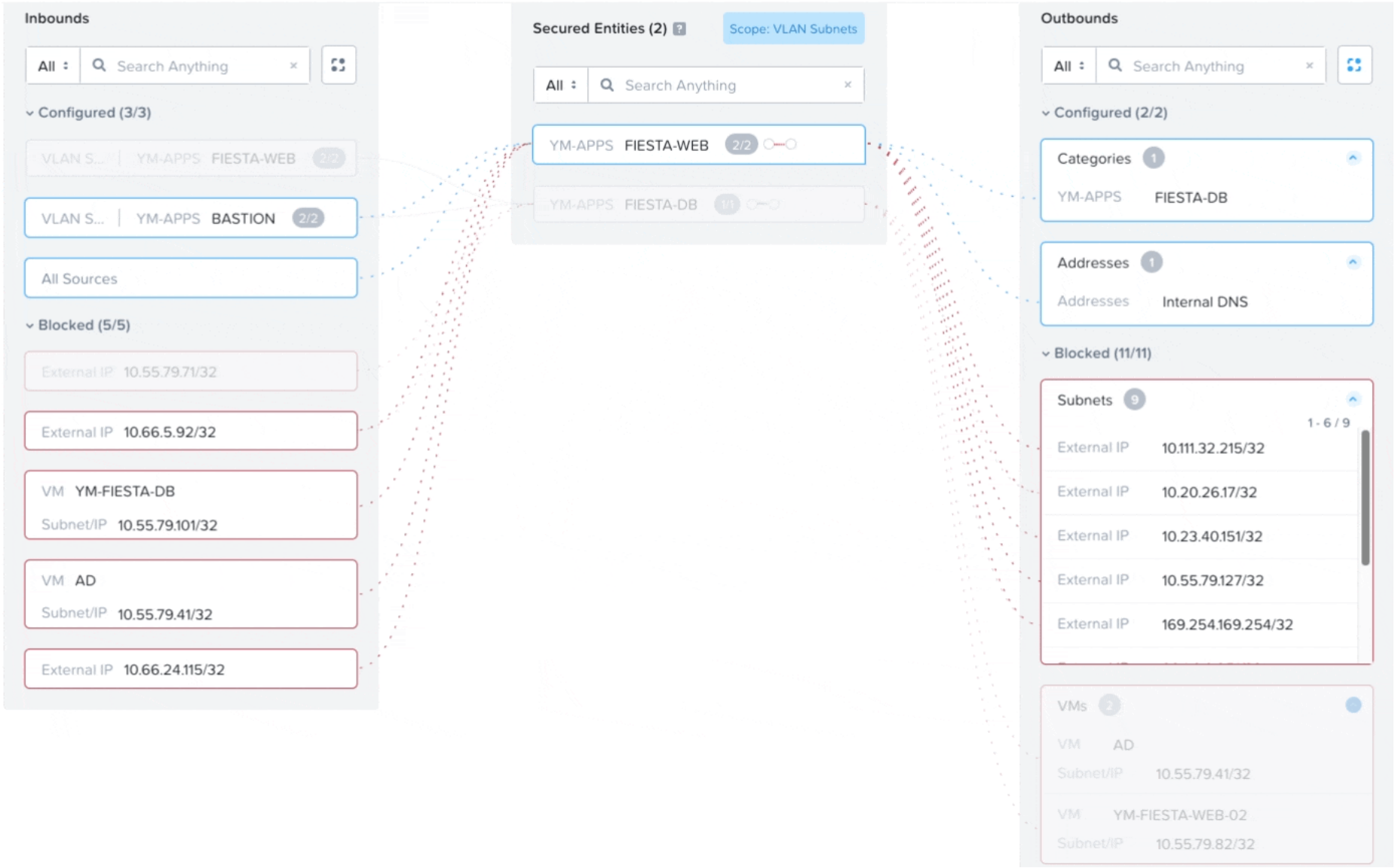




Live Traffic Analysis - Monitor

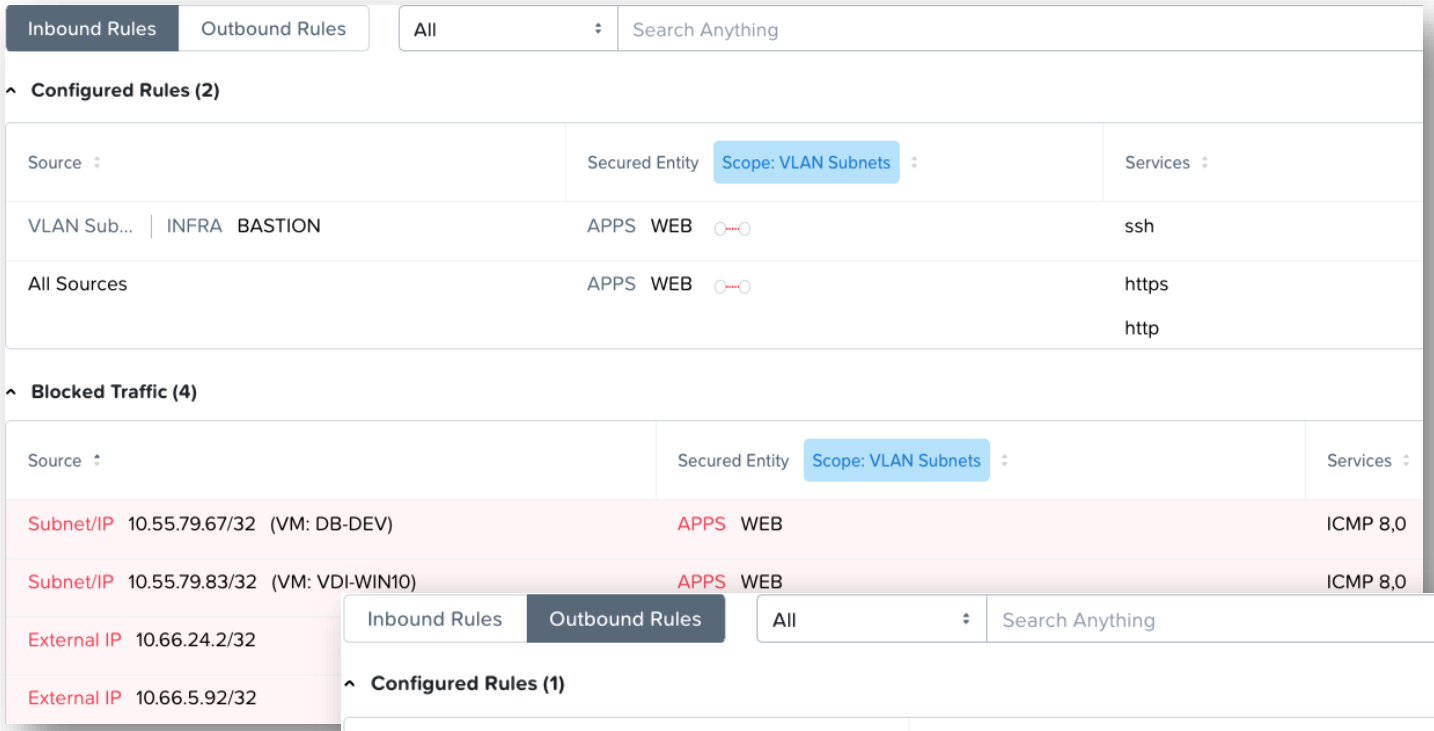


Live Traffic Analysis - Enforce

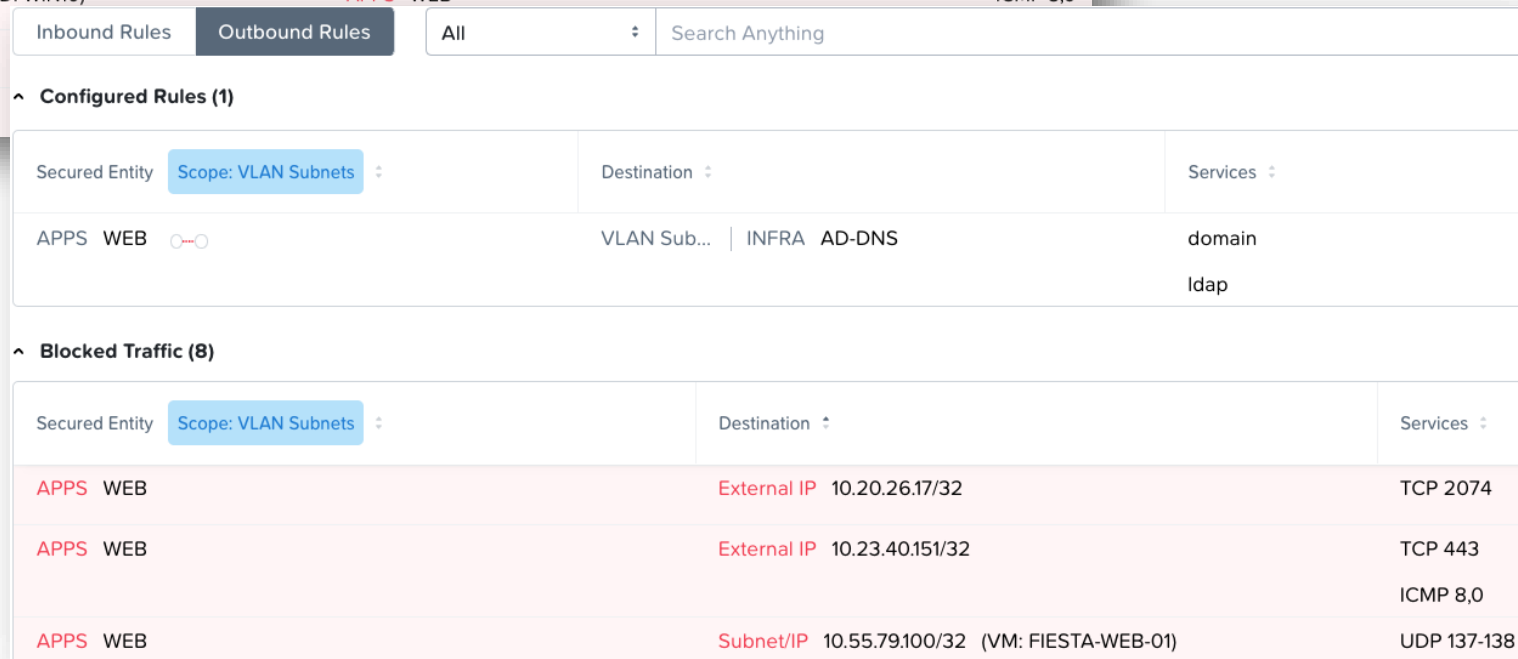


Toggle between Visual and List View

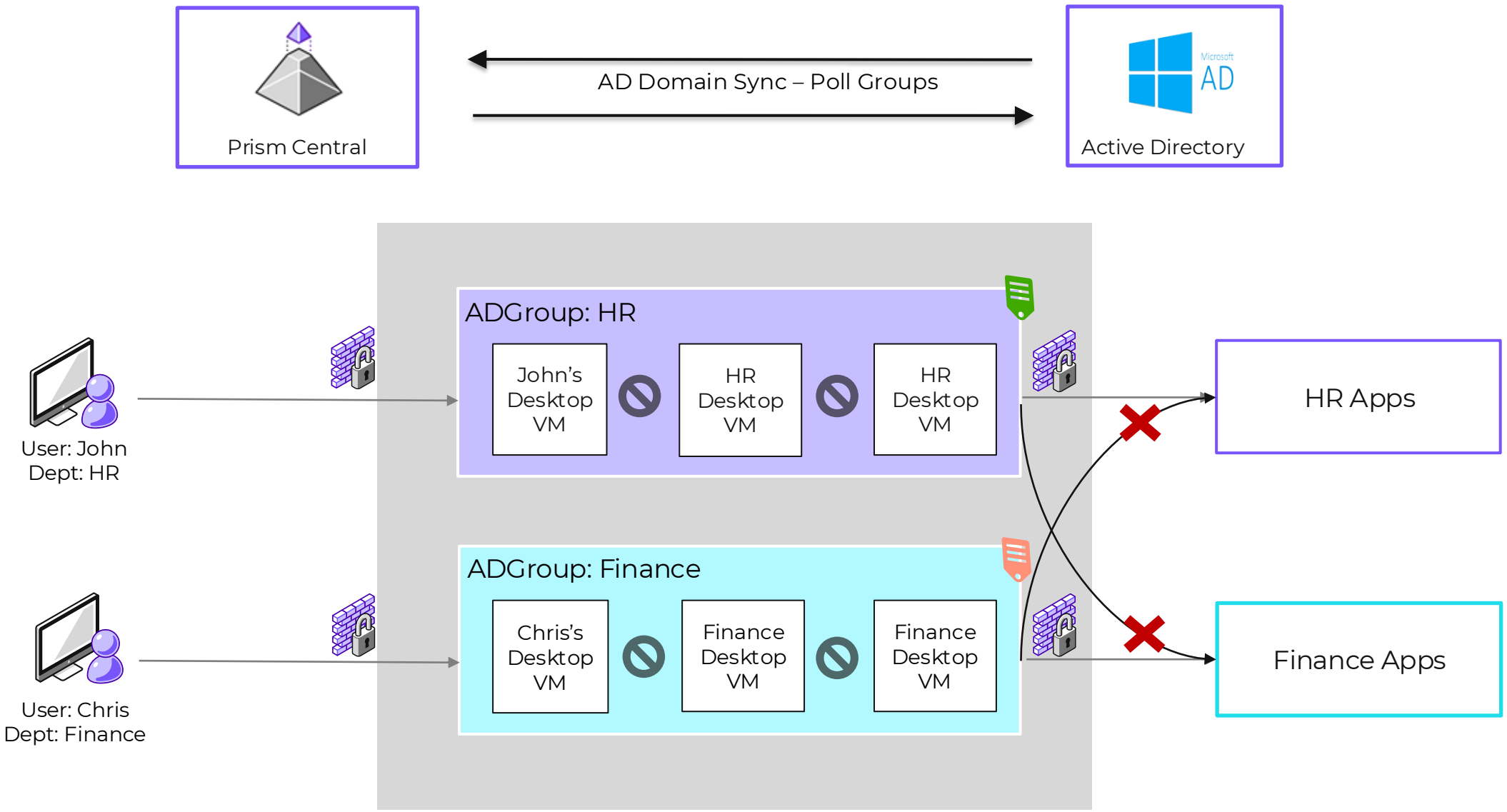
Inbound Rules



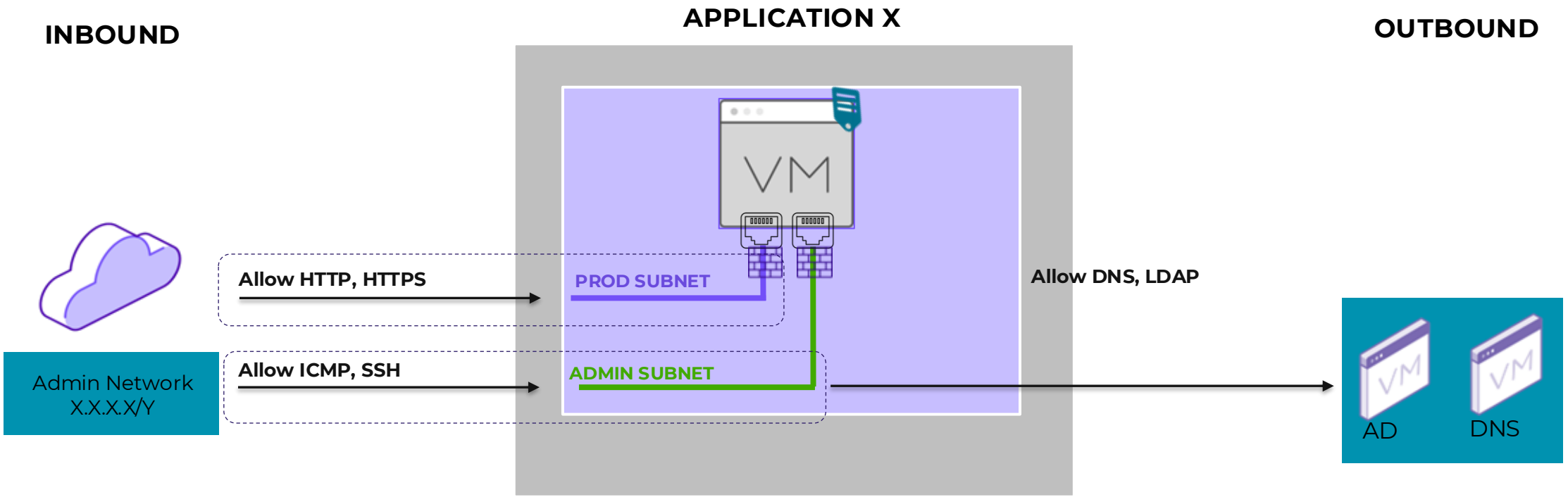
Outbound Rules



Secure Virtual Desktops with ID Firewall



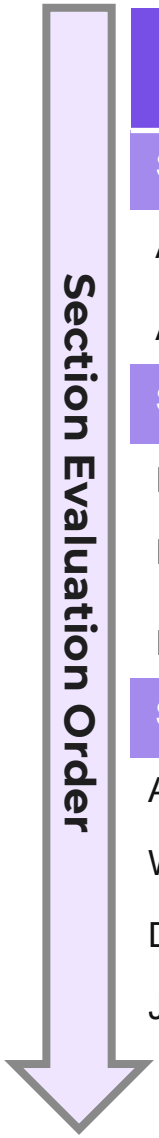
Per vNIC Granular Control



Based on Subnet Categorisation : PROD/ADMIN ...etc

* Tech Preview Feature

Evaluation order



Source	Destination	Protocol+ Ports	Allow/ Deny	Status
Section: **Quarantine**				
Any, Except Forensics	Malware VM	Any	Deny	Enforced
Any	Bad VM	Any	Deny	Enforced
Section: **Isolation**				
Isolate: Dev, Prod, Staging			Isolate	Monitored
Isolate: HR, Sales, Marketing, Dev, IT			Isolate	Saved
Isolate: Non-PCI, PCI			Isolate	Enforced
Section: Application				
Any	Web	TCP 80, 443	Allow	Saved
Web	DB	TCP 3306	Allow	Monitored
Dev-Users	DevFiler VM	TCP 445, 2049	Allow	Saved
JumpBox	DB	TCP 22	Allow	Enforced

Security Policies Sync 2 PCs

- The security policy and categories replicated via the Entity Sync framework
- Bi-directional synchronization between PC AZ1 and PC AZ2
- No lapse in security posture during or after a planned or unplanned failover across PC instances.