

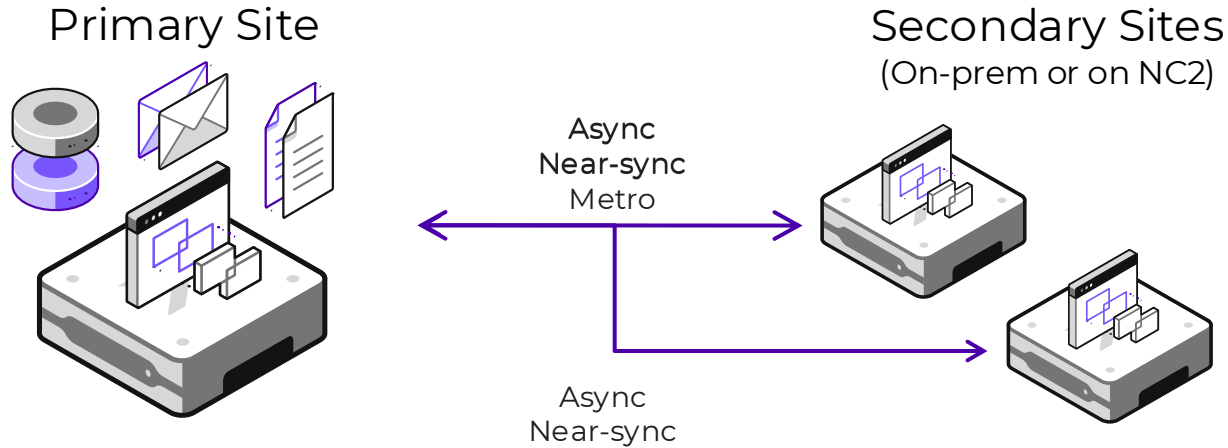
NUTANIX

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

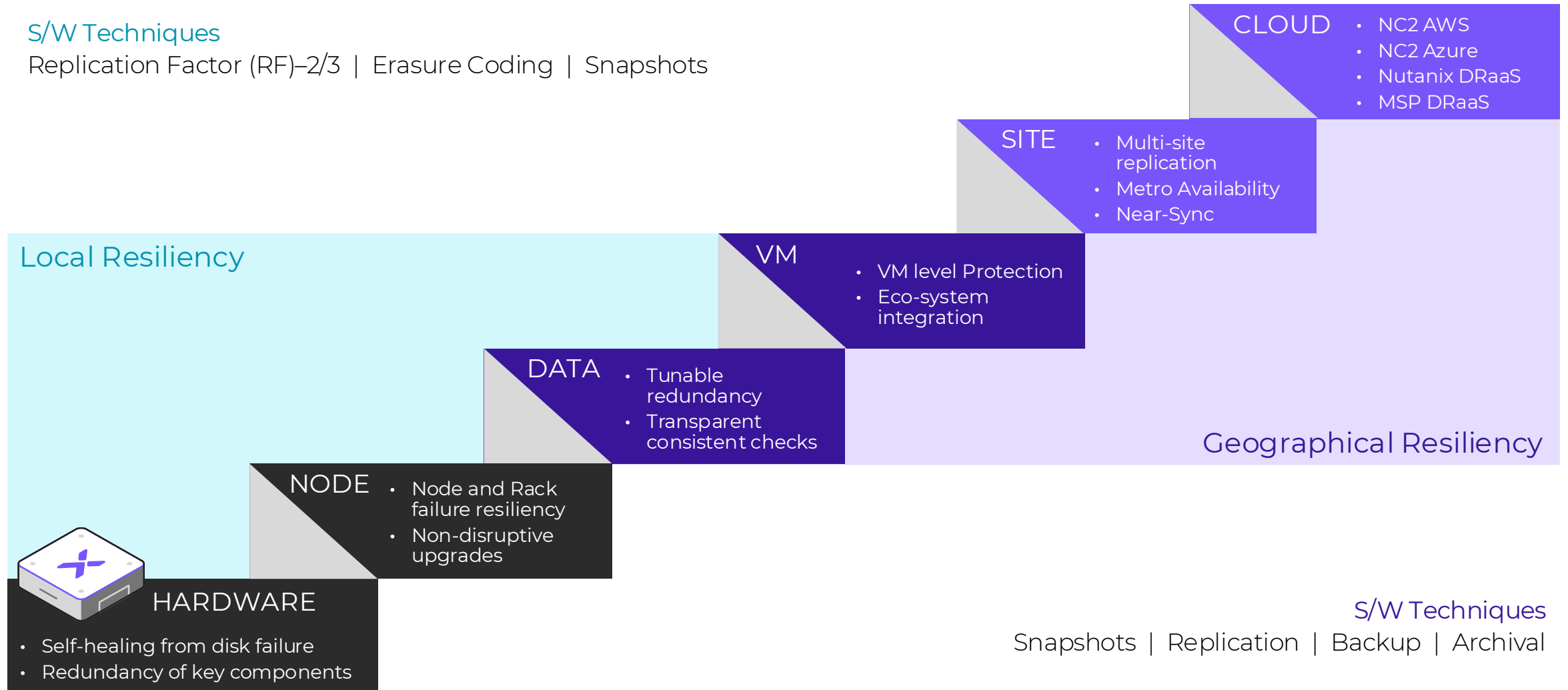


- Backup & archive data
- Use popular data protection software

True Resiliency From A to Z and Beyond

S/W Techniques

Replication Factor (RF)-2/3 | Erasure Coding | Snapshots



Comparing our Solutions

*NDR = Nutanix DR = Leap

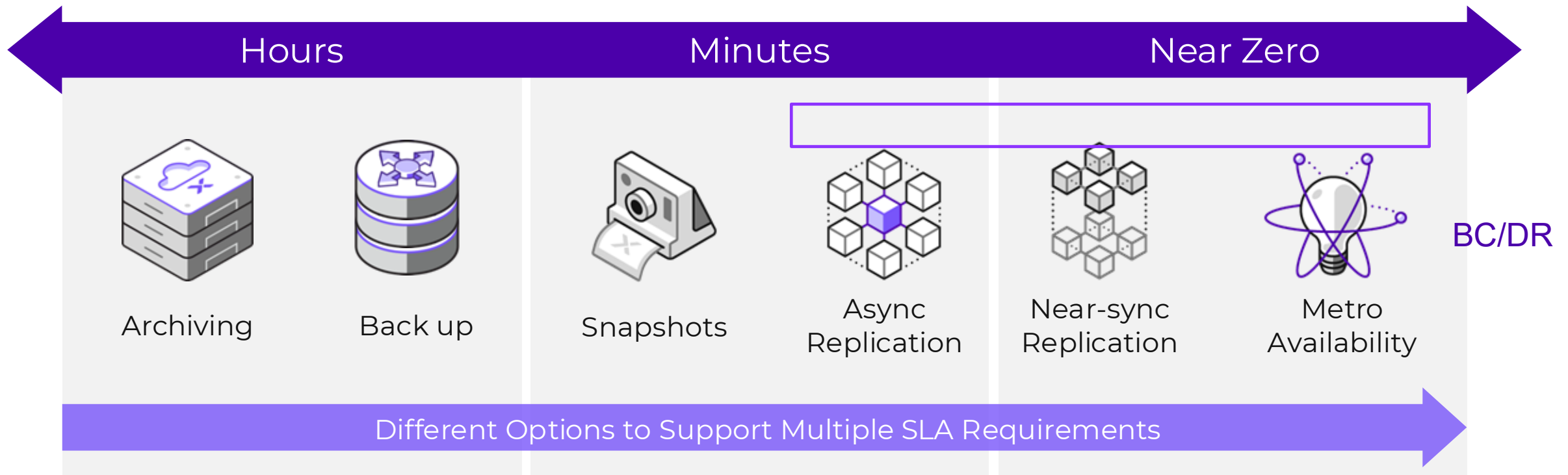
	Metro AHV	Metro ESXi	Sync Rep	Near Sync Rep	Async Rep
RPO	0	0	0	20 sec < RPO < 15 min	1 hour < RPO < some days
RTO	Minutes (automated)	Minutes (automated)	Minutes to hours (manual)	Minutes to hours (manual)	Minutes to hours (manual)
Distance	Limited distance (latency < 5ms RTT)	Limited distance (latency < 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

Nutanix Data Protection Strategy



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.

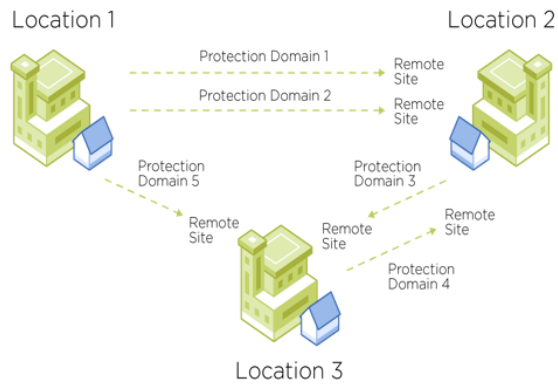
[Data Protection](#) is natively integrated into the Nutanix software stack, and offers customers the following benefits on a per-application basis:

- 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

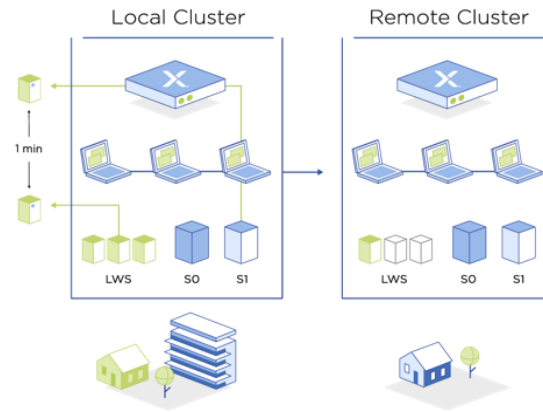
Asynchronous Replication

RTO: Minutes
RPO: 1 Hour



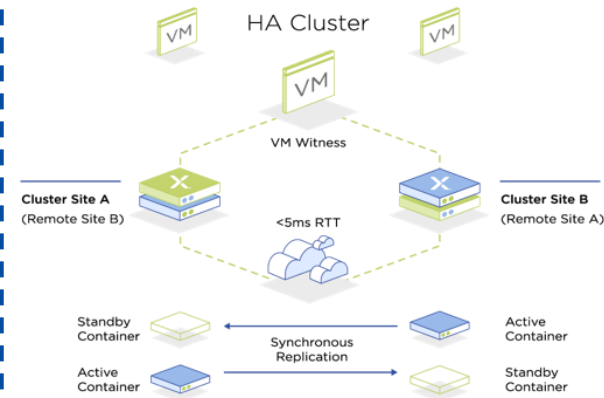
Near-Sync Replication

RTO: Minutes
RPO: 1-15 minutes



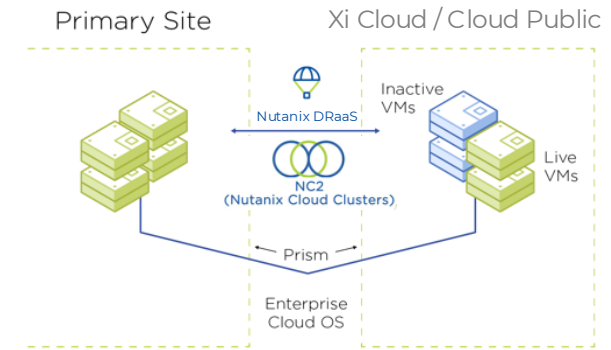
Metro Availability (Synchronous)

RTO: Minutes
RPO: Zero



DRaaS/NC2 (Cloud public)

RTO: Minutes
RPO: 1 Hour



Protection Domain or NDR

Protection Domain



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

Protection Domain or NDR



NDR

Protection Domain



NDR



Native Snapshots

True Immutability

Re-direct on Write

- Space Efficient
 - Performant
-

Policy Based

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

Multicloud Snapshot Technology™

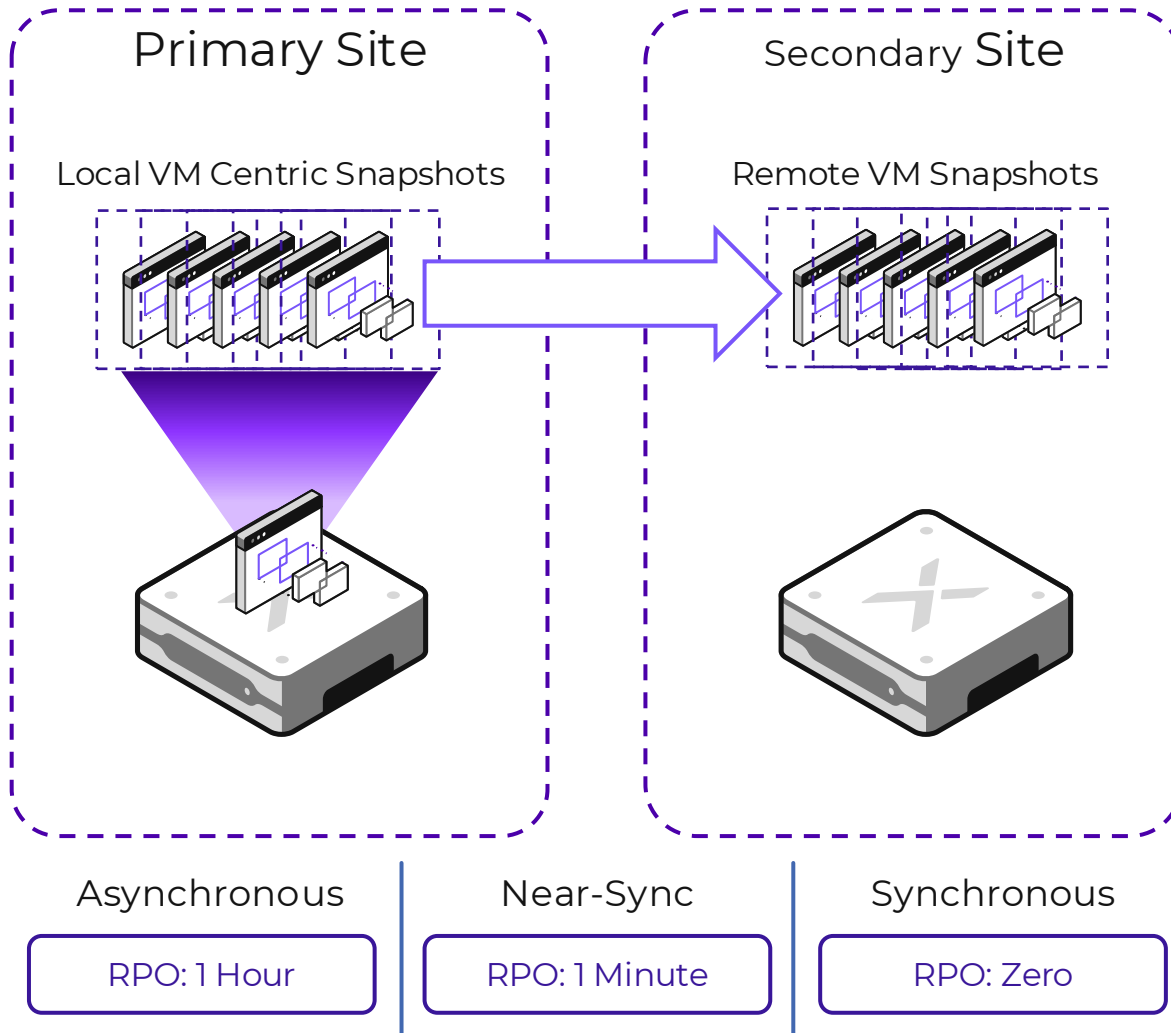
Primary Storage Optimization

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

Coming
Soon



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

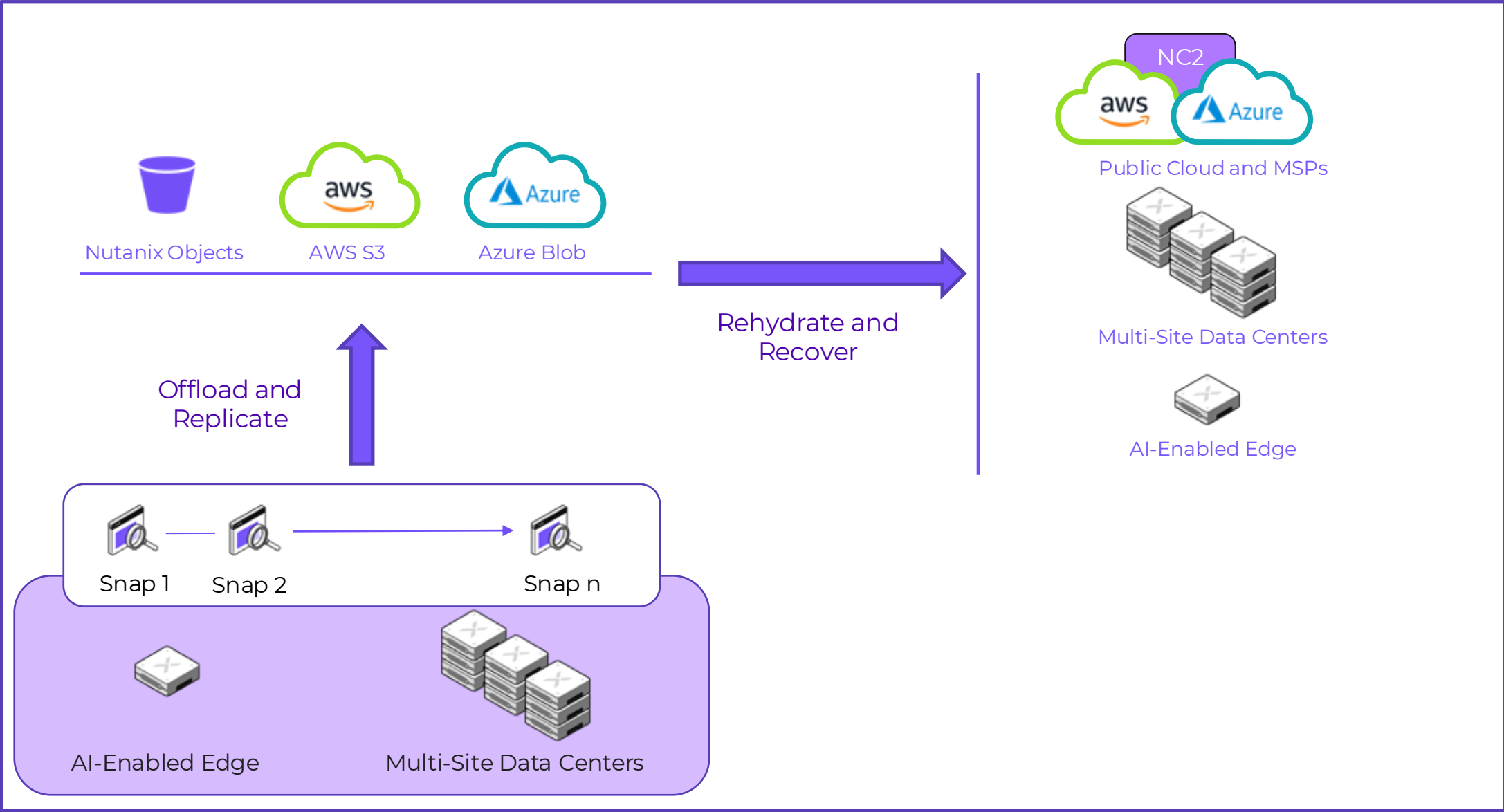
Retain snapshots for **longer periods of time** without bogging down storage performance

Cost Optimization

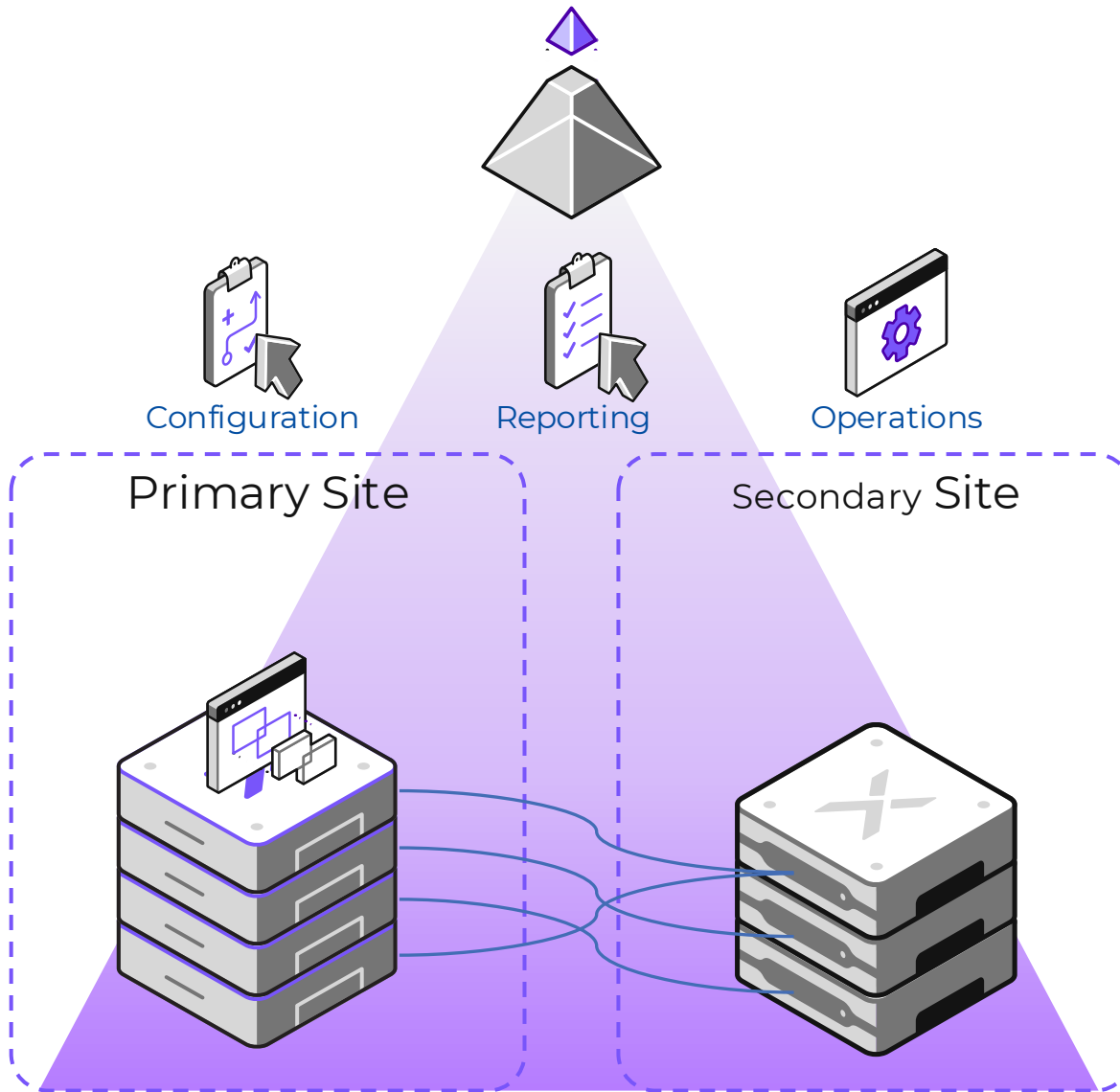
Reserve **primary storage** for high performance

Store snapshots **in low-cost secondary storage**

Nutanix Multicloud Snapshot Technology



Disaster Recovery Orchestration



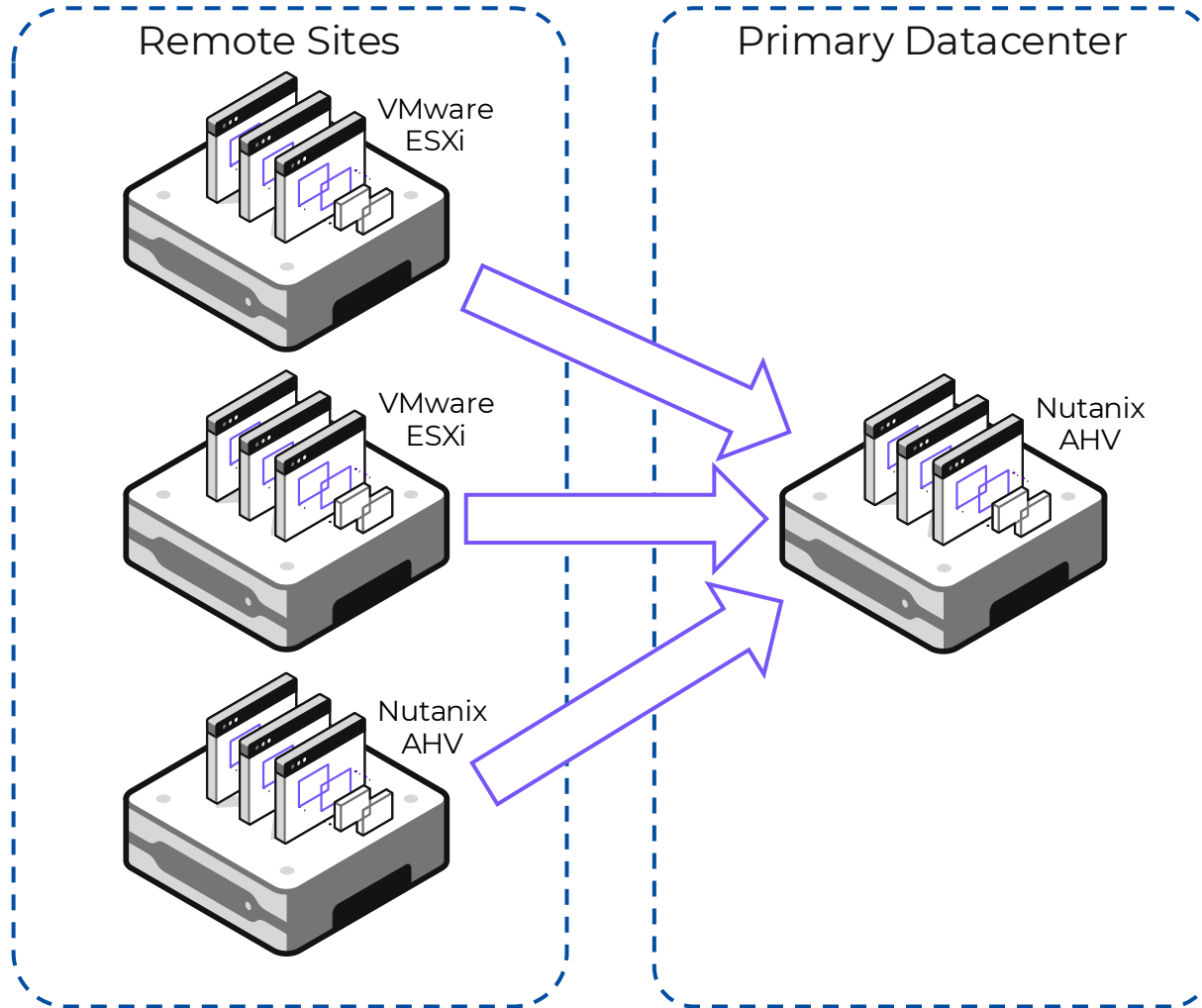
HIGHLIGHTS

- 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

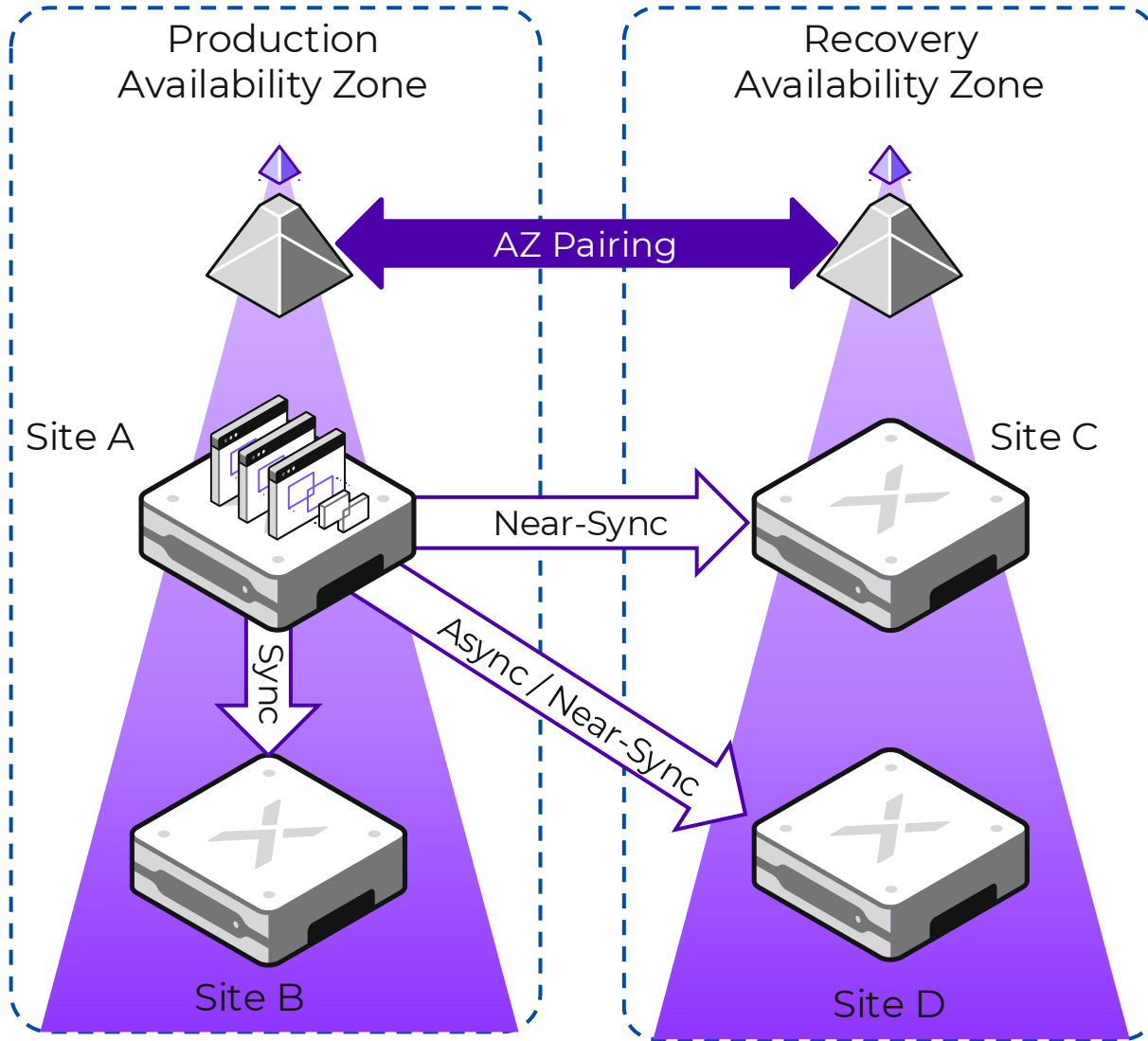
SOLUTION

- 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

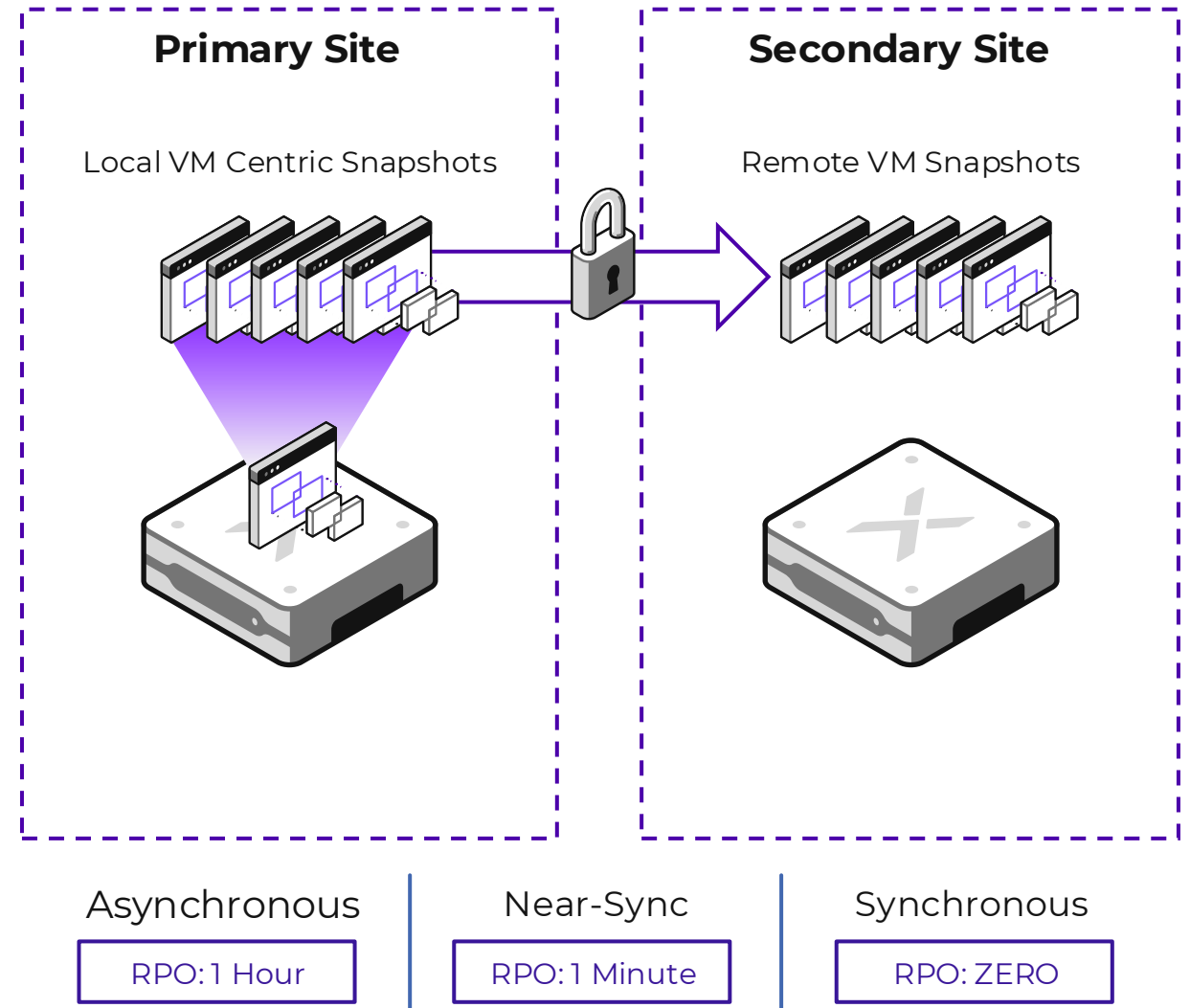
- Addresses zero data loss DR, DR testing, datacenter migration, and data corruption restore

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



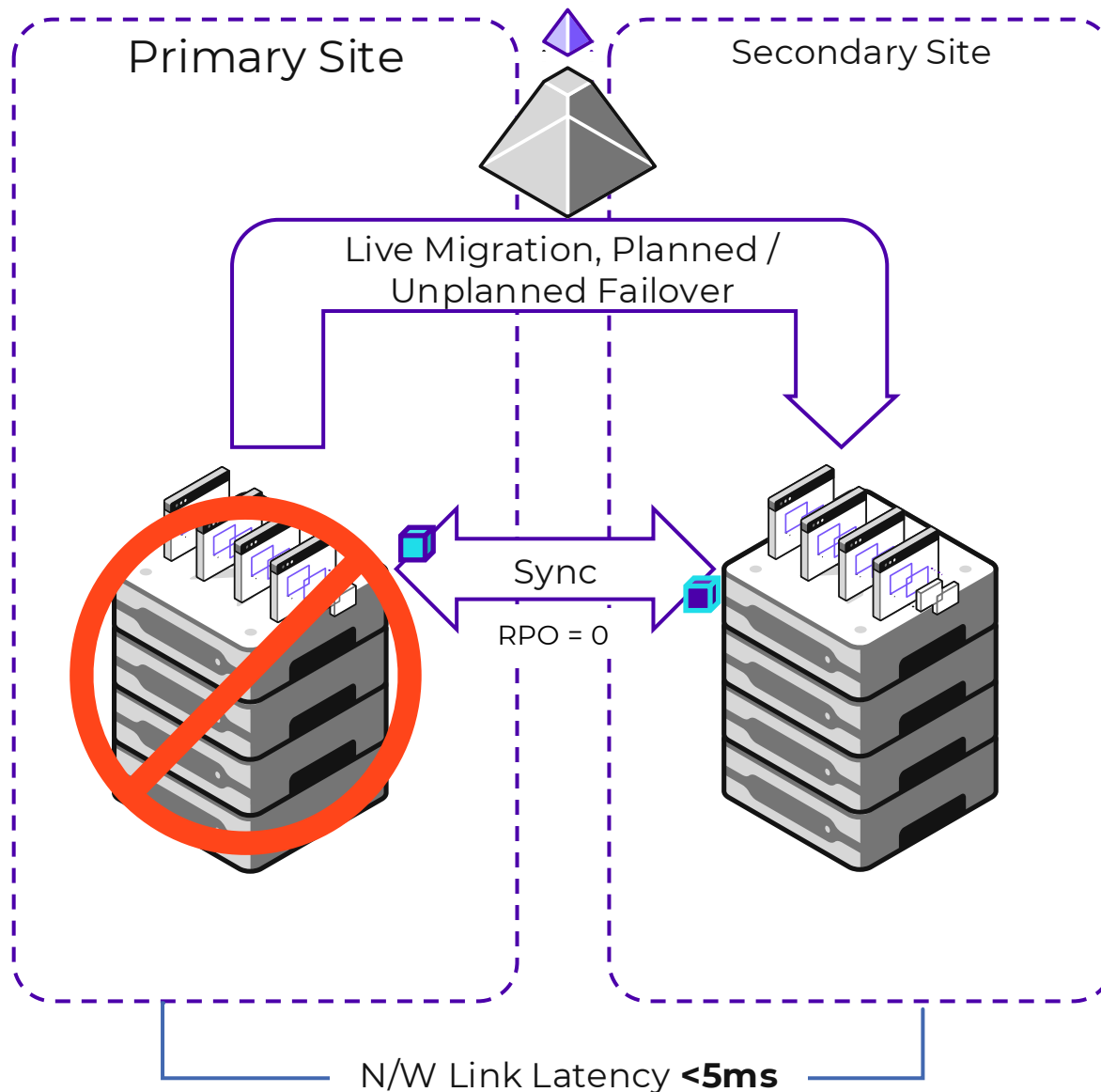
0 TOUCH

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

The screenshot displays the 'Edit Schedule' dialog for a protection policy named 'PP_SyncRep212'. The dialog is divided into several sections:

- Primary Location:** Local AZ : PHX-POC212
- Recovery Location:** PC_10.38.214.39 : PHX-...
- Protection Type:** Synchronous (selected), Asynchronous
- Failure Detection Mode:** Automatic (selected), Manual
- Timeout after:** 10 secs

At the bottom of the dialog, there are 'Cancel' and 'Save Schedule' buttons. The background shows a policy configuration page with a 'Start Protection Immediately' button and a 'Policy name' field containing 'PP_SyncRep212'.

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

1 General 2 Power On Sequence 3 Network Settings

Static IP addresses will be preserved post recovery. Dynamic IPs will not be preserved for VMs on ESX or VMs using non-IPAM networks.

Network Type
Are all L2 production networks in the recovery plan, stretched? If networks are stretched, then live migration of VMs is possible.

Non-stretch networks Stretch networks ?

[How it works?](#) + [Add Network Mapping](#)

Local AZ (Primary)		PC_10.38.214.39 (Recovery)	
Production	Test Failback	Production	Test Failover
Virtual Network or Port Group Secondary-2123	Virtual Network or Port Group Select	Virtual Network or Port Group Secondary-2123	Virtual Network or Port Group Select
Gateway IP / Prefix Length 10.38.212.129 / 25	Gateway IP / Prefix Length Enter Gateway IP /	Gateway IP / Prefix Length 10.38.212.129 / 25	Gateway IP / Prefix Length Enter Gateway IP /

[← Back](#) [Done](#)

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 `mccli` 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.

Failure Execution Mode

Manual

Execute failover manually in case of cluster or location failure.

Automatic

Execute failover automatically for metro availability protected VMs using a witness in case of cluster failure.

Witness

PC_10.136.112.37 (Cluster: PC-vTeam-1)

Execute failover after disconnectivity of

10

second(s) ±

In case of failure of one or more clusters, auto failover will be executed for VMs from failed clusters only.

Settings

- General
- Capacity Configurations
- Entity Sync
- Licensing
- Prism Central Management
- Upgrade Prism Central
- Witness**
- Xi Cloud Services

Introducing Witness



The Witness service continuously monitors clusters, nodes etc. to provide automatic failure handling. This Prism Central can act as a witness service and can be used to:

Enable auto failover in Recovery Plans (Within PC only)

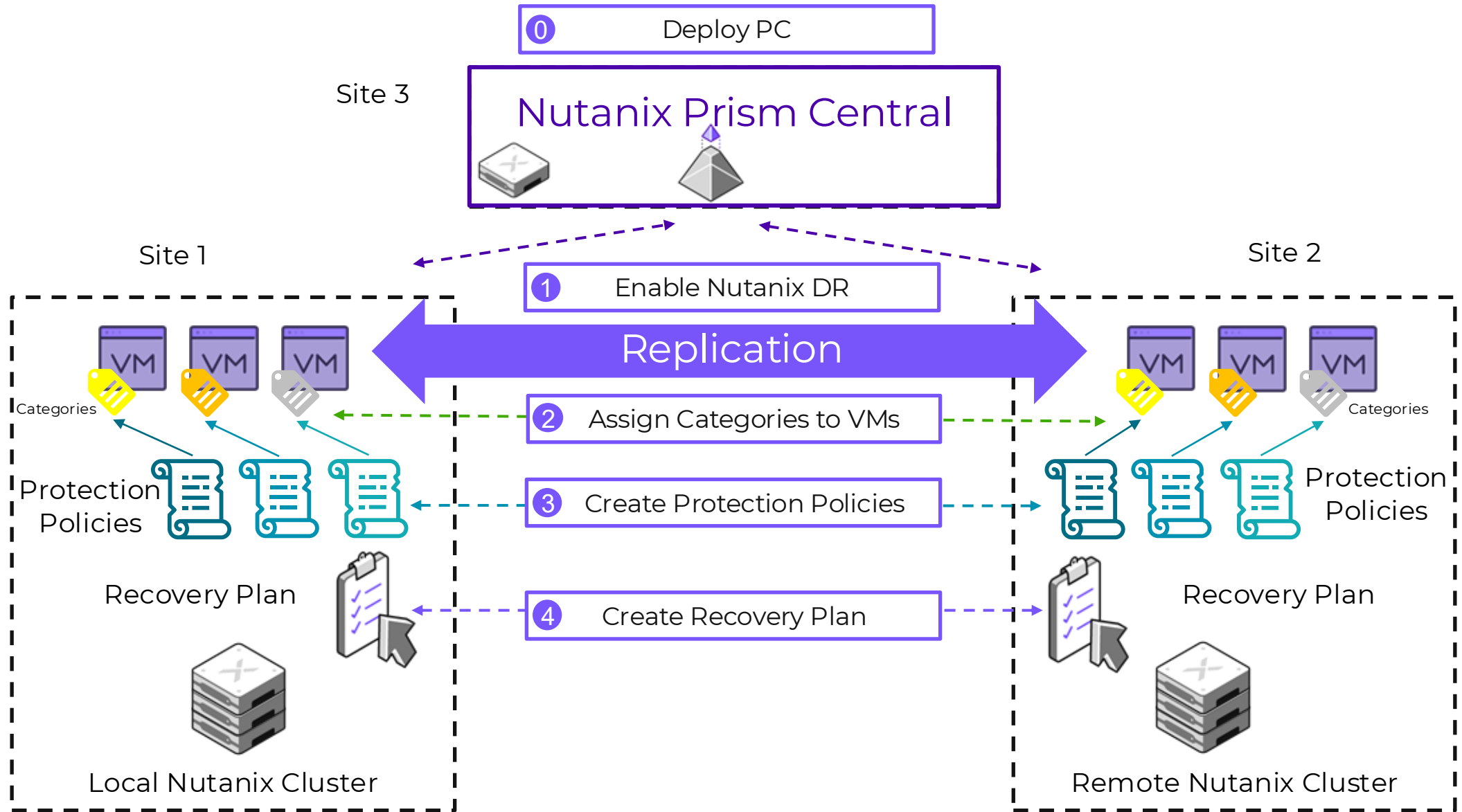
Best practices to ensure before setting up witness.

- Prism Central instance for witnesses is running as a separate failure domain.
- Prism Central and Prism Element instances are upgraded to compatible versions.

1 Witness available

Name	Cluster	IP Address	Monitoring (On this PC)	
PC_10.136.112.37	PC-vTeam-1	10.136.112.138	2 Recovery Plan(s)	View Usage History

Setting Up Metro AHV



Failover / Cross-Cluster Live Migration

✓ Failover per Recovery Plan →

or

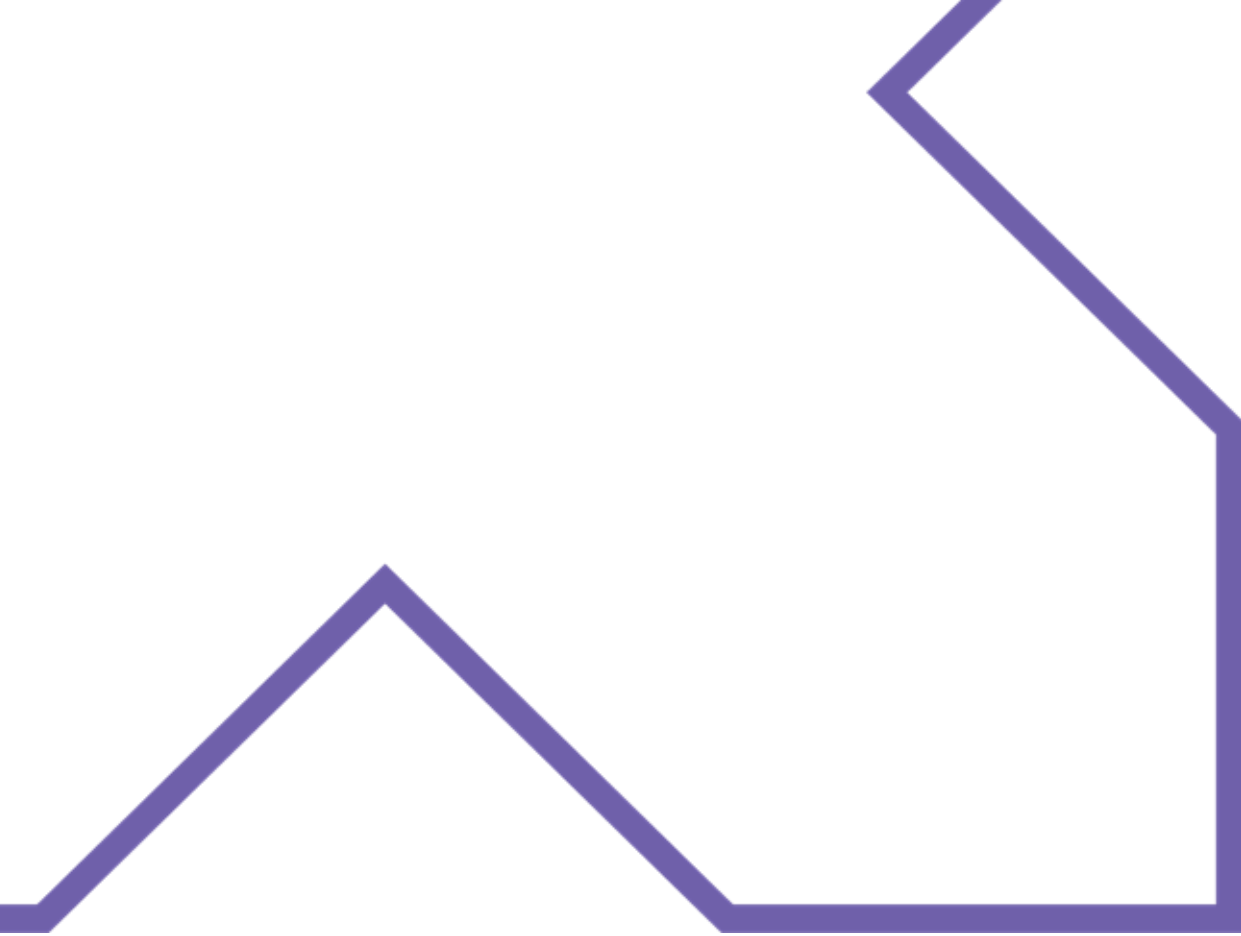
✓ Migrate single VM(s)

The screenshot shows a two-step wizard. Step 1, 'Destination Cluster', is active. It contains a 'Cluster Information' section with 'Source Location' (Local AZ) and 'Destination Location' (PC_10.46.144.15). Below, 'Source Cluster' (auto_cluster_prod_vinaya_khandelw...) and 'Destination Cluster' (Please Select) are shown. A dropdown menu for the destination cluster is open, showing 'auto_cluster_prod_vinaya_khandelwal_1ac118c14f53'. The 'Selected VMs' section shows 'VMs that can be migrated (1 Total)' with a table containing one entry: 'sync-rep-pfo-migrate'. 'Cancel' and 'Next' buttons are at the bottom.

The dialog box is titled 'Failover from Recovery Plan'. It has a 'Failover Type' section with 'Planned Failover' selected and 'Live Migrate VMs' checked. Below, 'Failover From' and 'Failover To' sections show 'Location' dropdowns with values 'PC_10.38.212.39' and 'Local AZ'. A link '+ Add target clusters to failover to specific clusters' is present. The 'Recovery Status' section contains a table:

VM failing over from	Total 3 VMs
PC_10.38.212.39 to Local AZ	3

Below the table is a note: 'VM host affinity needs to be reconfigured manually post failover.' 'Close' and 'Failover' buttons are at the bottom right.



Nutanix Security

Nutanix Vulnerability Database (NXVD)

How can I get CVE information for the Nutanix Platform?

- NXVD can be found in the Nutanix Support Center (Documentation > Software Documentation > Security > NXVD)
- Ability to get status of any published vulnerability
- Available for
 - AOS (NCI)
 - AHV (NCI)
 - PRISM (NCM)
 - Karbon (NCI)
 - MSP (NCI)
 - Objects (NUS)

CESA	CVE	CVSS Score	Package	Severity	Product Release	Status
<input type="checkbox"/> CESA-2020-3915	CVE-2019-87498	6.5	libssh2	Medium		Pending Release
<input type="checkbox"/> CESA-2020-3911	CVE-2019-86935	6.1	python	Medium		Pending Release
<input type="checkbox"/> CESA-2020-3908	CVE-2019-34866	6.7	cpio	Medium		
<input type="checkbox"/> CESA-2020-3901	CVE-2017-12652	3.7	libpng	Low		
<input type="checkbox"/> CESA-2020-3898	CVE-2018-10896, CVE-2020-8631, CVE-2020-8632	8.1	cloud-init	High		
<input type="checkbox"/> CESA-2020-3888	CVE-2019-86935, CVE-2020-8492	6.5	python	Medium		
<input type="checkbox"/> CESA-2020-3864	CVE-2017-18190, CVE-2019-8675, CVE-2019-8696	5.8	cups	Medium		Pending Release
<input type="checkbox"/> CESA-2020-3861	CVE-2019-19126	2.9	glibc	Low		Pending Release
<input type="checkbox"/> CESA-2020-3848	CVE-2019-8010305	2.5	libmspack	Low		Pending Release
<input type="checkbox"/> CESA-2020-3220	CVE-2019-19527, CVE-2020-10757, CVE-2020-12653, CVE-2020-12654	7.8	kernel	High	5.18.1, 5.15.3, 5.18.0.5	Released

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

	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



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.

System Accounts | Prism Central | Controller VM (CVM) | **Hypervisor (AHV)**

You can only view and change passwords for AHV accounts on clusters running AOS 7.3 or greater and AHV 10.3 or greater. AHV a level and password changes apply only to the selected hosts. Non-Nutanix and mixed-hypervisor clusters are not shown.

[Change Password](#)

☆ Type text to filter by

1 selected out of 6 grouped AHV Accounts [Export](#)

Cluster	Account	Host Count	Status
<input checked="" type="checkbox"/>	root	6	Secure

Host Name	Last Password Change	Status
<input checked="" type="checkbox"/> [redacted] 03-2	Jul 28, 2024	Secure
<input type="checkbox"/> [redacted] 02-1	Jul 28, 2024	Secure

Role Based Access Control (RBAC) and Logging

Implementing least privilege : Fine-grained access control

- **RBAC**

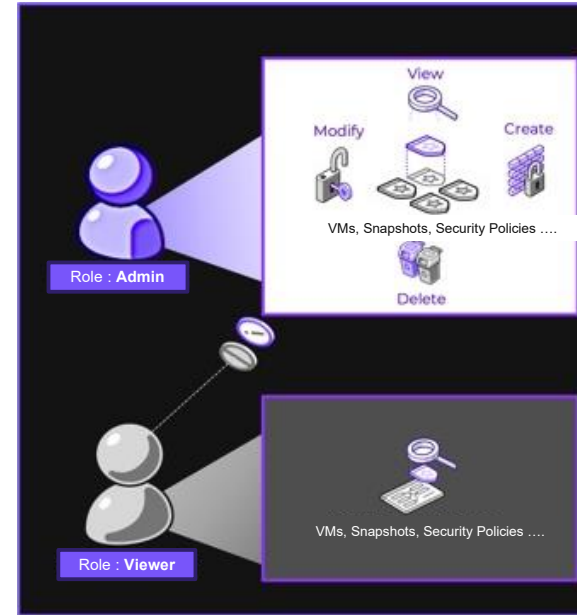
Least-privileged roles and permissions

Named accounts for traceability and auditing

- **Logs**

Logging of all activities

Log export to SIEM platform

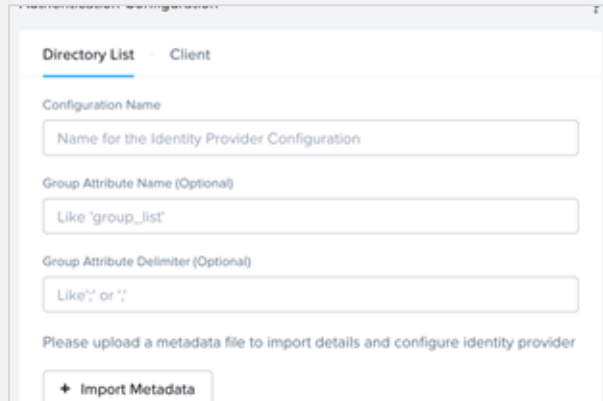


Title	Create Time
User admin failed to log in from 10.66.24.6	03/15/24, 11:38:22 PM
User admin failed to log in from 10.66.24.6	03/14/24, 03:08:07 PM
User admin@ntnxlab.local failed to log in from 10.66.24.6	03/14/24, 02:26:03 PM
User admin failed to log in from 10.66.24.6	03/14/24, 02:25:58 PM



Access Denied : Restrict access to Data and Services

Use the AAA framework to protect your hybrid cloud infrastructure



Directory List - Client

Configuration Name
Name for the Identity Provider Configuration

Group Attribute Name (Optional)
Like 'group_list'

Group Attribute Delimiter (Optional)
Like ';' or ':'

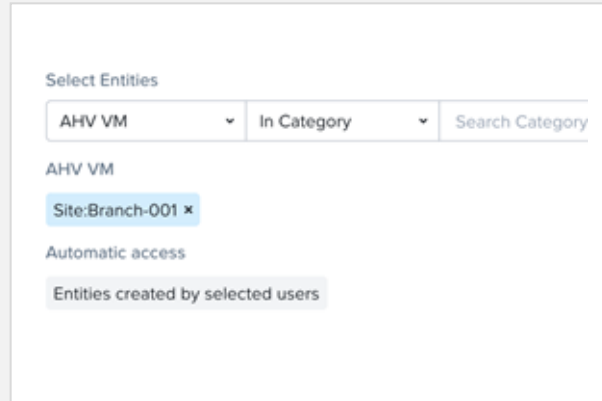
Please upload a metadata file to import details and configure identity provider

+ Import Metadata

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



Select Entities

AHV VM In Category Search Category

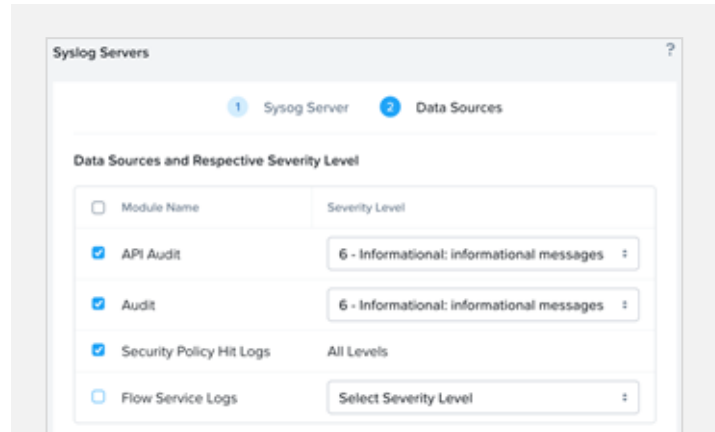
AHV VM
Site:Branch-001 x

Automatic access
Entities created by selected users

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



Syslog Servers

1 Syslog Server 2 Data Sources

Data Sources and Respective Severity Level

Module Name	Severity Level
<input checked="" type="checkbox"/> API Audit	6 - Informational: informational messages
<input checked="" type="checkbox"/> Audit	6 - Informational: informational messages
<input checked="" type="checkbox"/> Security Policy Hit Logs	All Levels
<input type="checkbox"/> Flow Service Logs	Select Severity Level

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

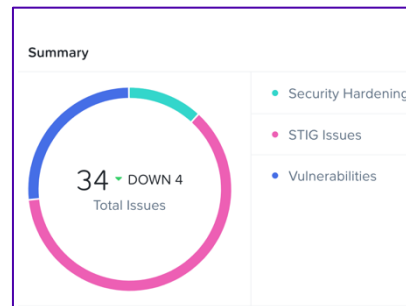
Regular software and hardware updates
(BIOS, firmware, etc.)

1-Click Upgrade / Automated Inventory

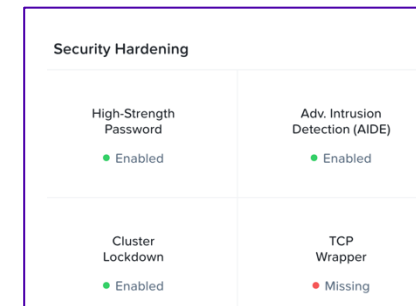
Automate compatibility checks SW/ HW



Prism Security Dashboard



Detailed Security Posture Summaries



Enabled Security At-A-Glance

Vulnerabilities for 6.6

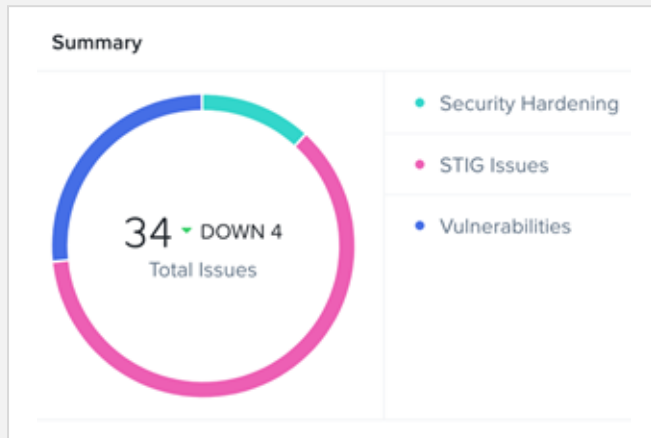
Summary	Vulnerabilities
1 Critical Vulnerabilities	CVE-2018-1270
9 Total Vulnerabilities	CVE-2022-21540
	CVE-2022-21541
	CVE-2022-21549
	CVE-2022-22950

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

Vulnerabilities for 6.6

Summary	Vulnerabilities
1 Critical Vulnerabilities	CVE-2018-1270
	CVE-2022-21540
9 Total Vulnerabilities	CVE-2022-21541
	CVE-2022-21549
	CVE-2022-22950

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**

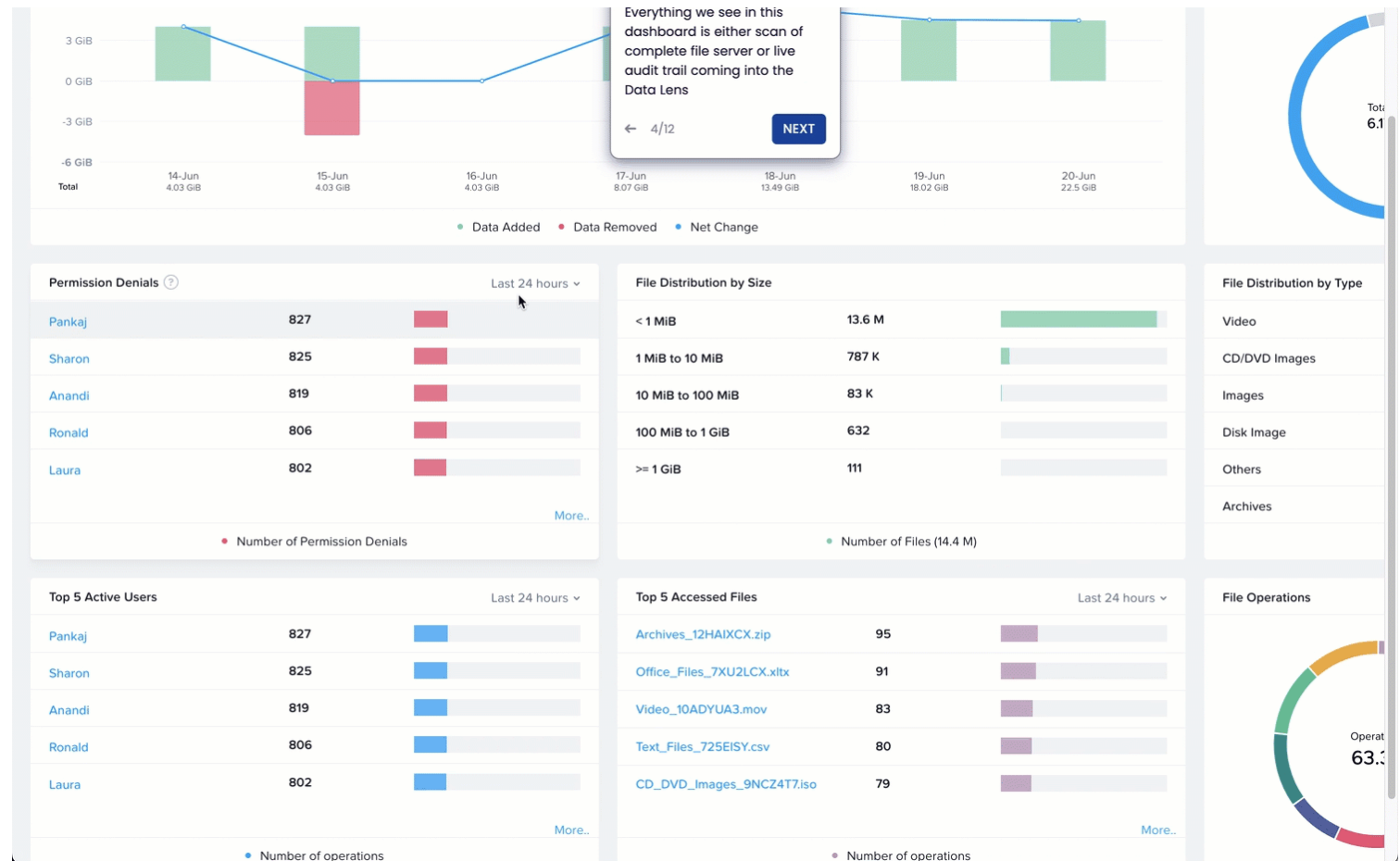
Detect and block Ransomware (5000+ signatures)

Auditing and Anomaly Detection

- **Objects (S3)**

Write Once, Read Many (WORM)

Object Lock

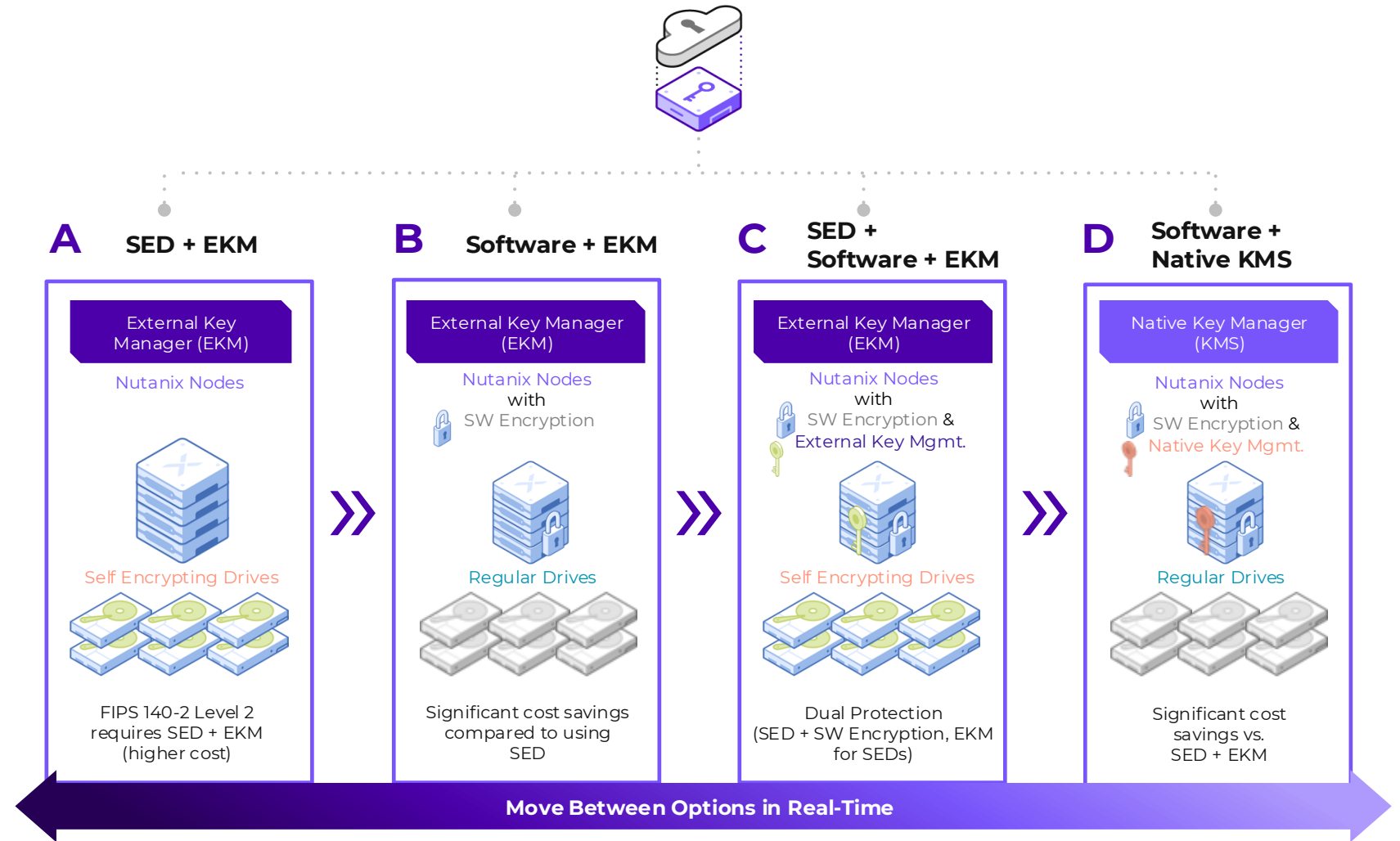


Data-at-Rest Encryption Made Easy

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.

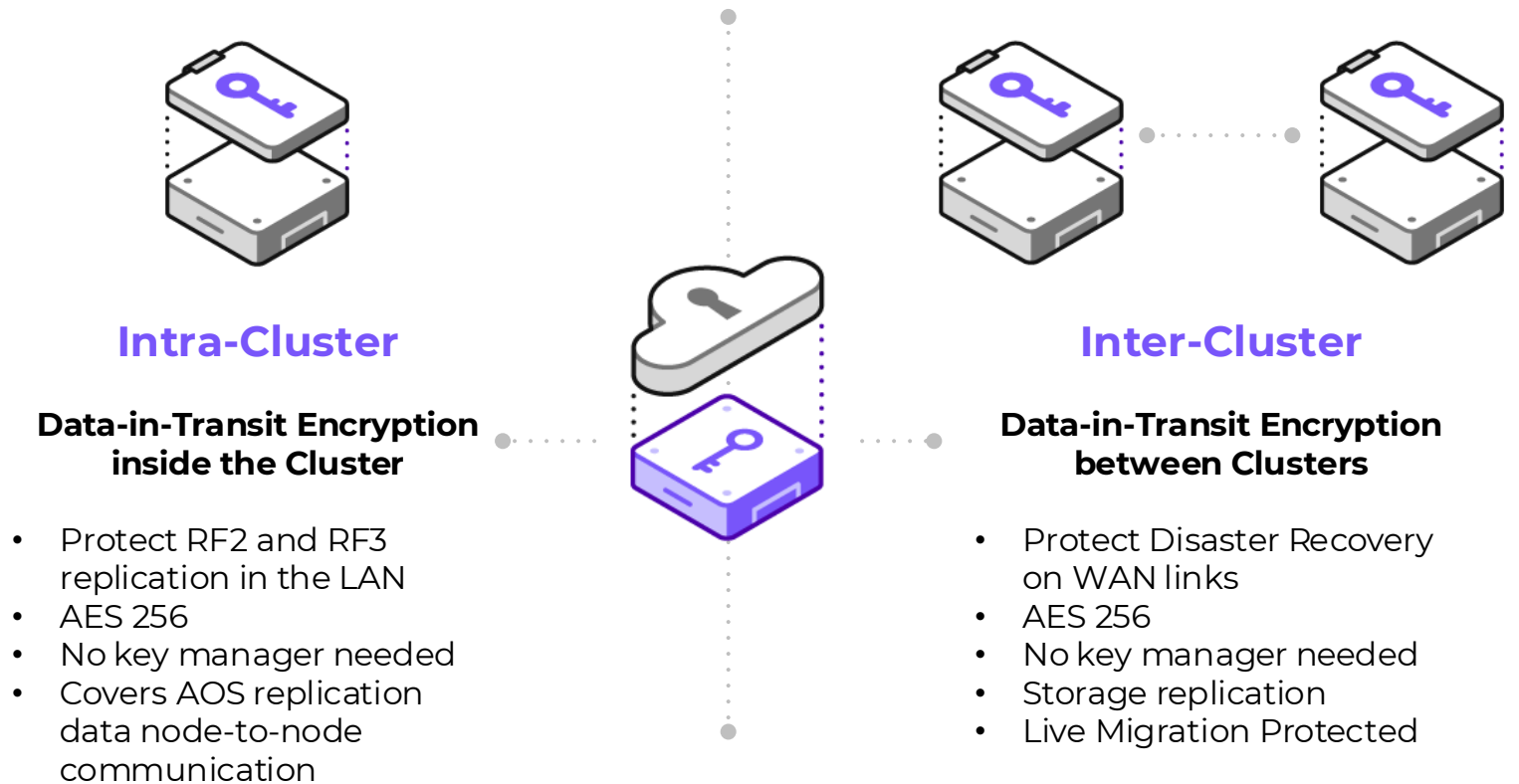


Data-In Transit Encryption

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



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**

Approver Set 1 Done

Set Name
Approver Set 1

Approvers Add Approver

Prism Username	Email Address	
triyasha.ghosh	triyasha.ghosh@nutanix.com	🗑️
prerna.garg	prerna.garg@nutanix.com	🗑️
admin	admin@nutanix.com	🗑️

Approval Rule
All need to approve before the Request Expiry. Any reject or no answer cancels the request

Request Expiry
48 hours

Actions Filters

Type text to filter by

25 entities (1.2 GiB) Export 1 - 20 of 100 20 per page

Create time (name)	Location	Secure	Available Space	Type	Owner
<input checked="" type="checkbox"/> 1:53 PM, 28 Apr 2022 (Test-point)	Local AZ: PC-A-PE-1	Secure		Application Consistent	admin
<input checked="" type="checkbox"/> 1:42 PM, 29 Apr 2022 (Trial-point)	Local AZ: PC-A-PE-1	Secure		Application Consistent	admin
<input checked="" type="checkbox"/> 1:41 PM, 29 Apr 2022 (Trial-point)	Local AZ: PC-A-PE-1	Secure		Application Consistent	admin
<input checked="" type="checkbox"/> 1:40 PM, 29 Apr 2022 (Trial-point)	Local AZ: PC-A-PE-1	Secure		Application Consistent	admin
<input type="checkbox"/> 1:39 PM, 29 Apr 2022 (Trial-point)	Local AZ: PC-A-PE-1	Secure		Application Consistent	admin
<input type="checkbox"/> 2:00 PM, 15 Apr 2022 (abc-point)	Local AZ: PC-A-PE-1	Secure		Application Consistent	admin
<input type="checkbox"/> 1:00 PM, 15 Apr 2022 (abc-point)	Local AZ: PC-A-PE-1			Crash Consistent	admin
<input type="checkbox"/> 10:00 AM, 10 Apr 2022 (abc-point)	Local AZ: PC-A-PE-1			Crash Consistent	admin
<input type="checkbox"/> 10:00 AM, 10 Apr 2022 (abc-point)	Local AZ: PC-A-PE-1		4 GIB	Crash Consistent	admin
<input type="checkbox"/> 9:00 AM, 10 Apr 2022 (abc-point)	Local AZ: PC-A-PE-1		4 GIB	Crash Consistent	admin

Delete Recovery Points?

Are you sure you want to delete Recovery Points '1:53 PM, 28 Apr 2022 (Test-point)', '1:42 PM, 28 Apr 2022 (Test-point)', '1:41 PM, 28 Apr 2022 (Test-point)', '1:40 PM, 28 Apr 2022 (Test-point)'?

These Recovery Points are secured by an Approval Policy and will be deleted once approved.

Cancel Delete

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

BIOS vs UEFI

Credential & Device Guard

TPM vs vTPM

SecureBoot

- On
- Off

AHV

Boot Configuration

Legacy BIOS Mode

Set Boot Priority

Default Boot Order (CD-ROM, Disk, Networks)

UEFI BIOS Mode ?

UEFI BIOS Mode supports enhanced Shield VM security settings.

Shield VM Settings

Secure Boot

IDE disks are not supported by Secure Boot.

Windows® Defender Credential Guard ?

Attach vTPM

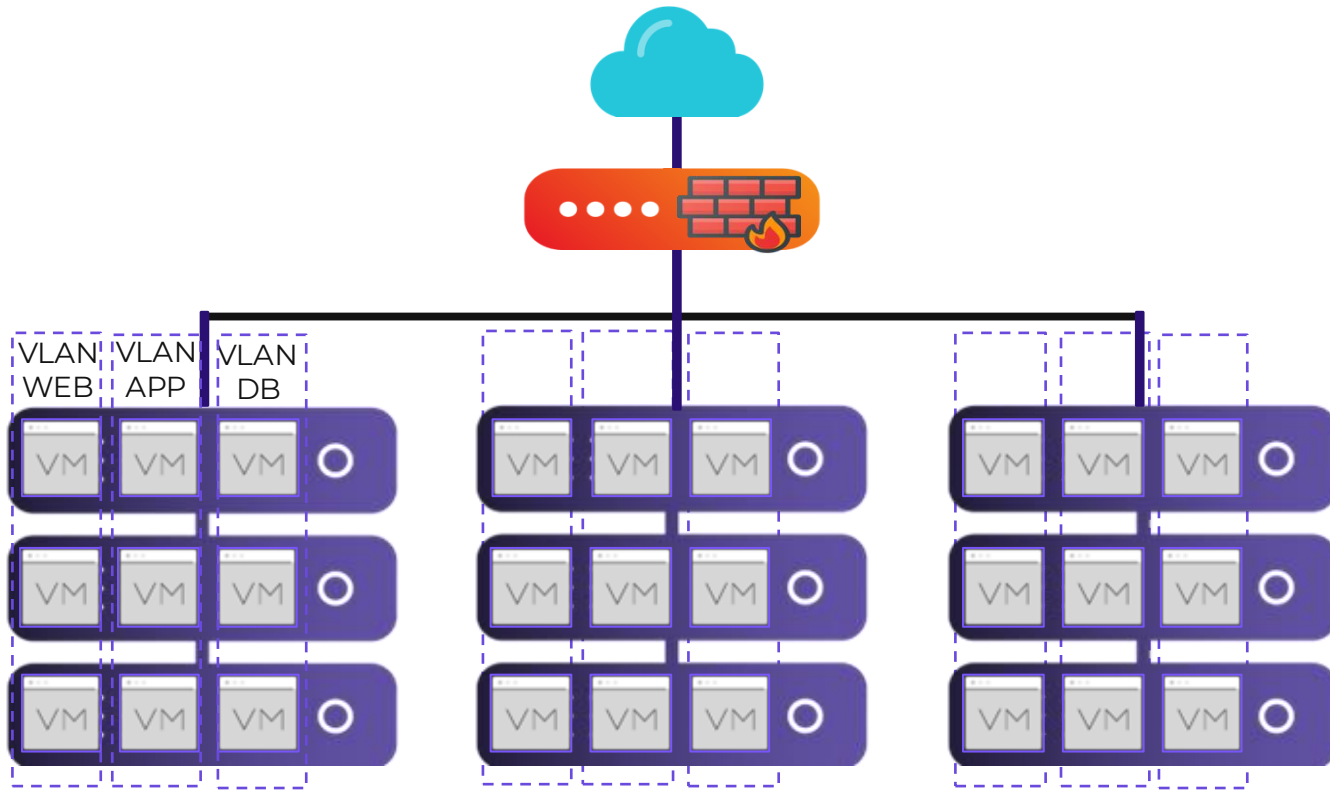
NCI
AHV Virtualization
(AHV)



Flow Security

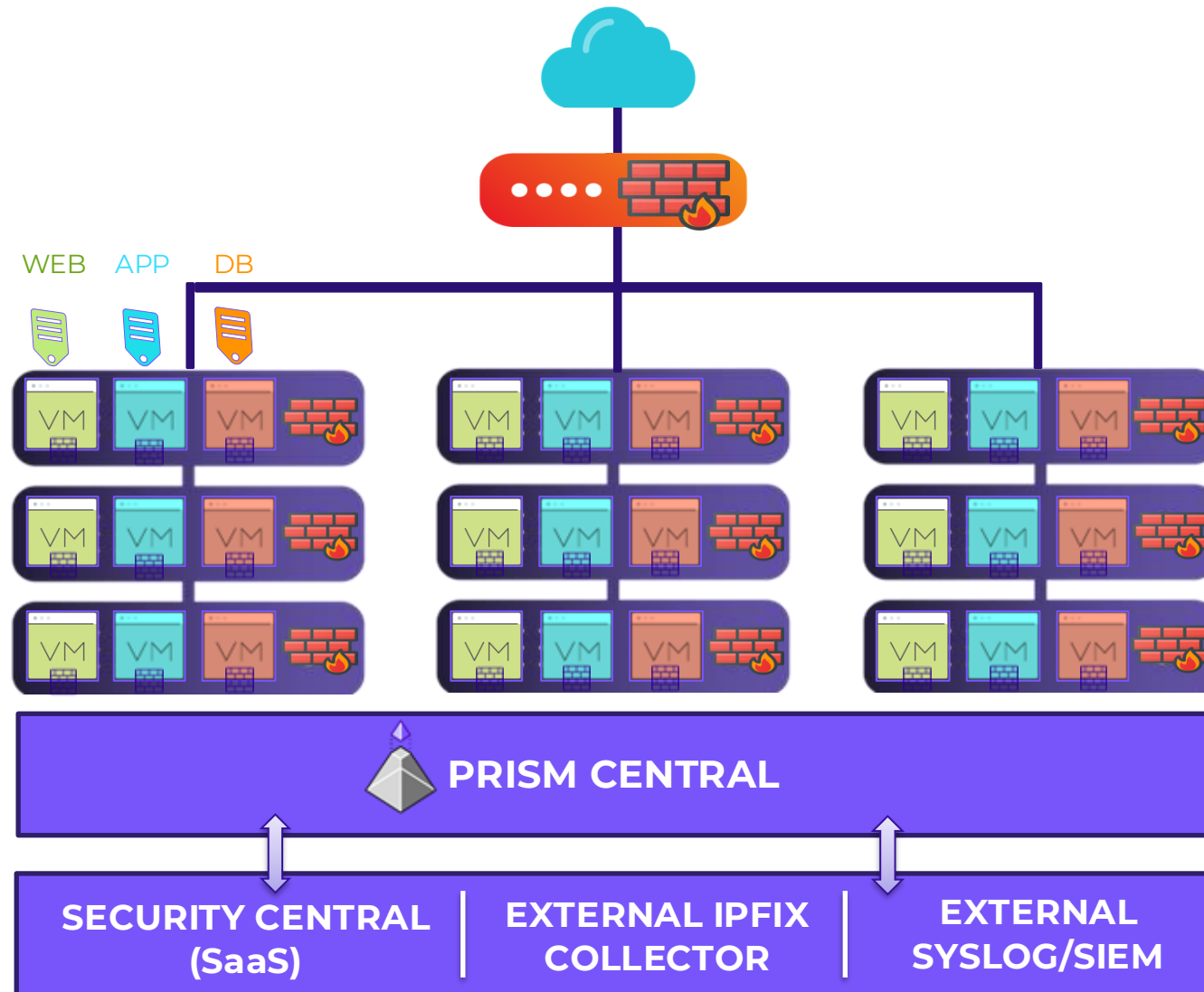
NUTANIX

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**

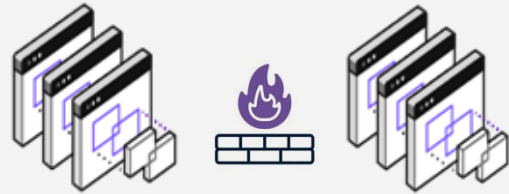
Zero Trust Microsegmentation for protecting East-West traffic



- **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



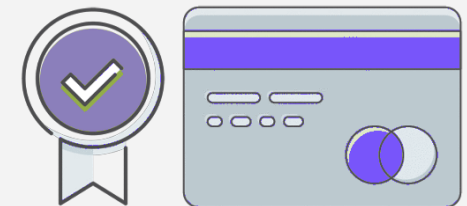
Isolating Environments



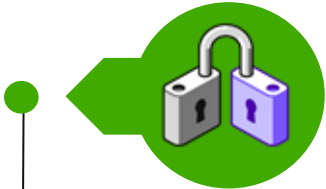
Securing VDI Environments



Strengthening Regulatory Compliance



Complete Visibility Of Workloads And Flows



Visualize Application Traffic



Explore External Traffic

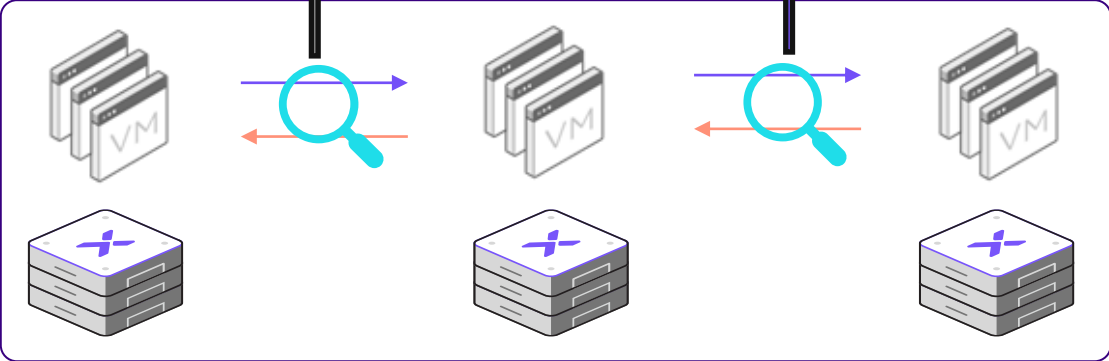
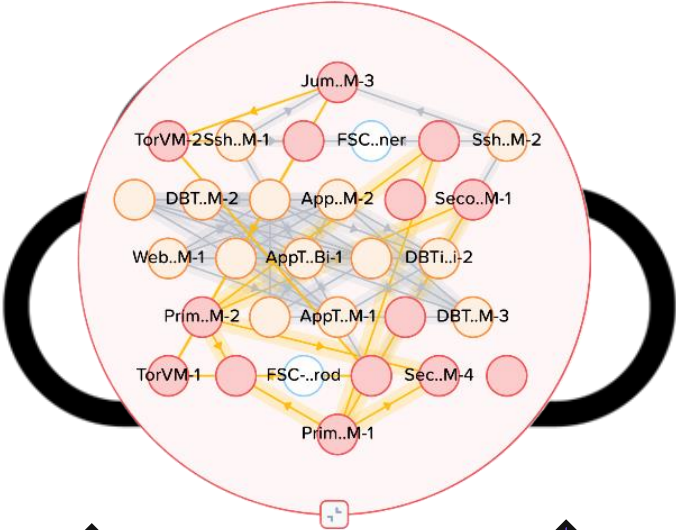


Detect Lateral Movements

Identify with Color Coded Flows

Report VM Security Status

Export Traffic Flows as CSV

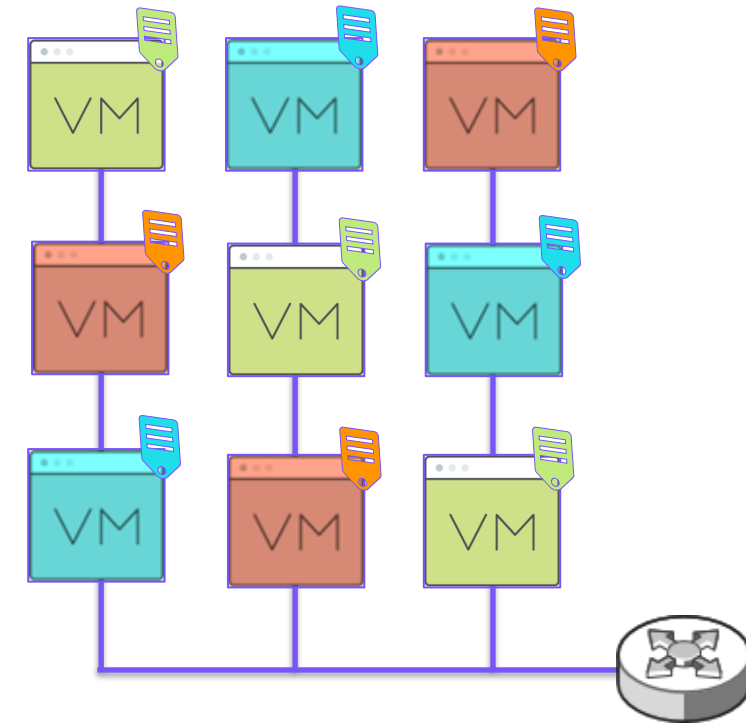


Identify and Group VMs with Categories

- 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.




Environment: Production

App: MyApp1

Tier: Web

PROD-MyApp1-Web



Environment: Development

App: MyApp2

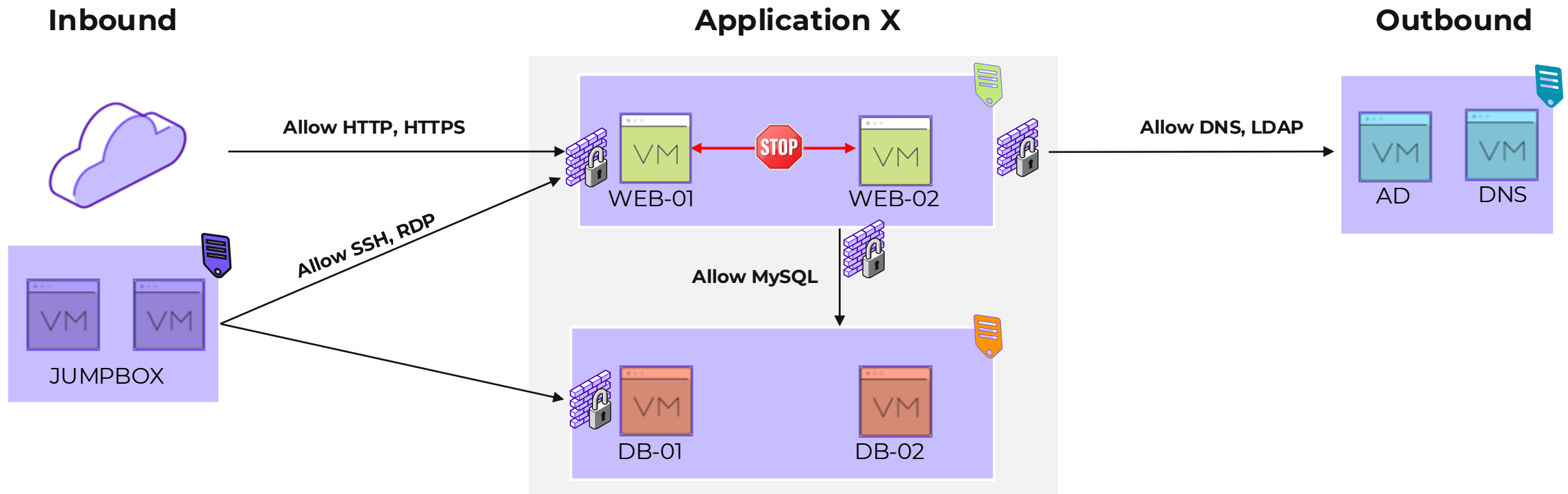
Tier: DB

DEV-MyApp2-DB

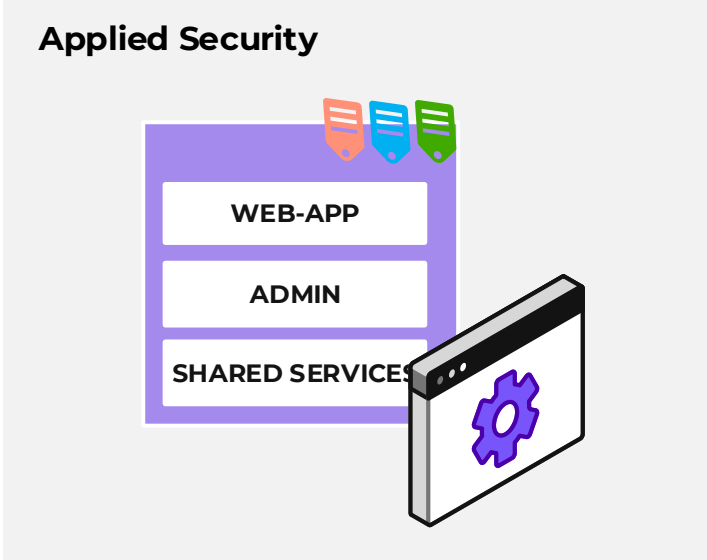
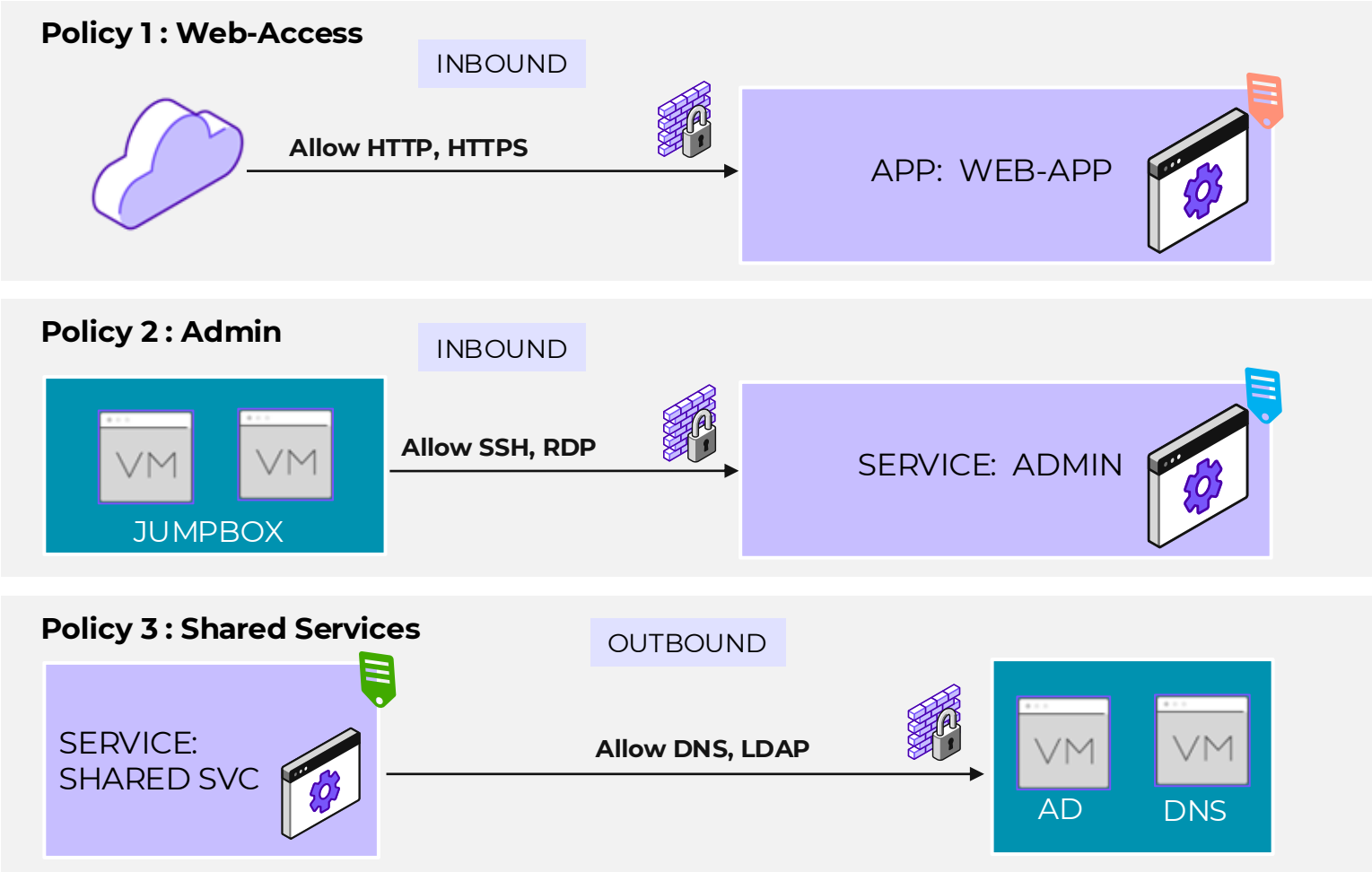


* Requires NCM Starter

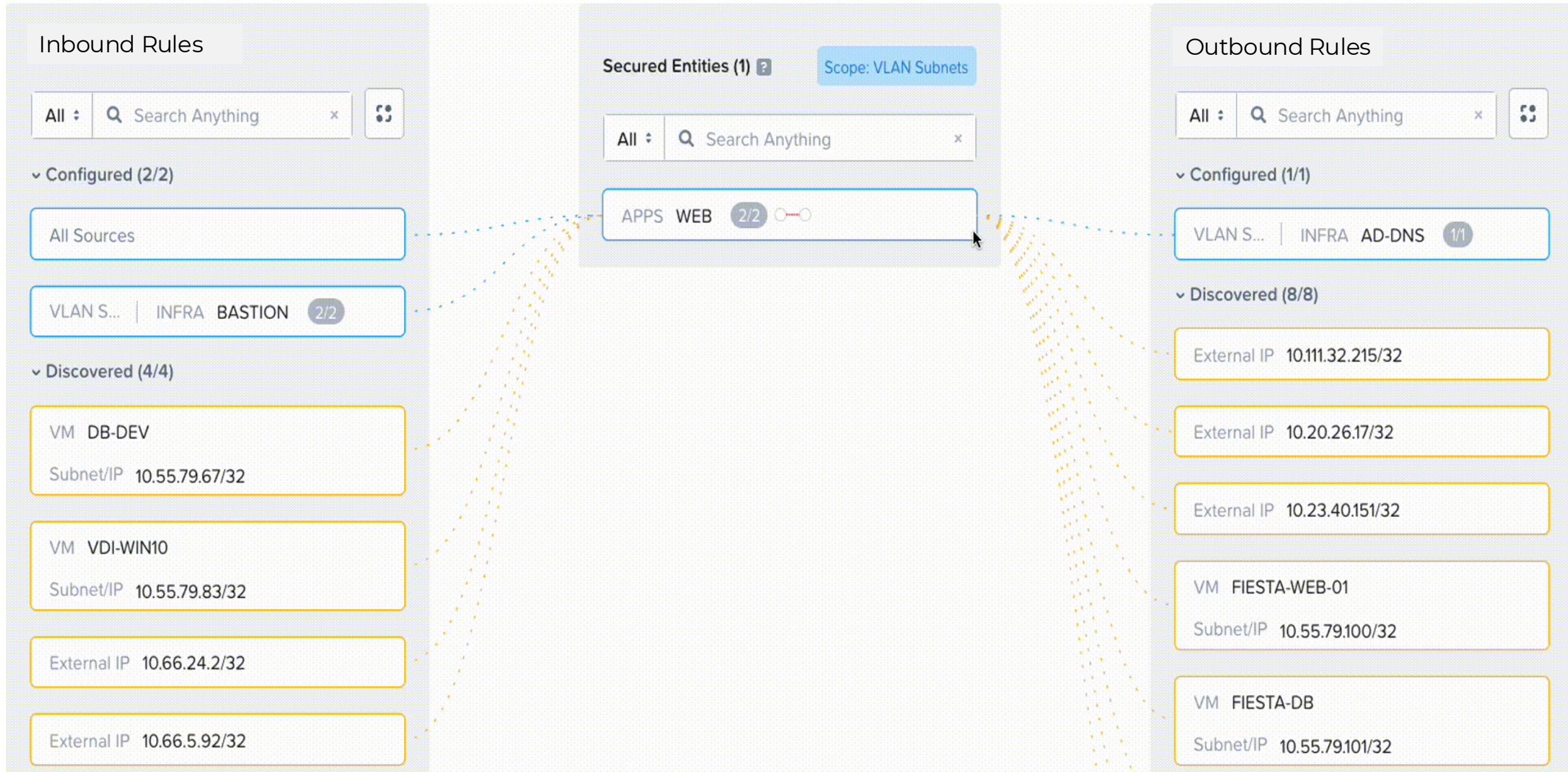
Protecting Apps with App-centric Policy



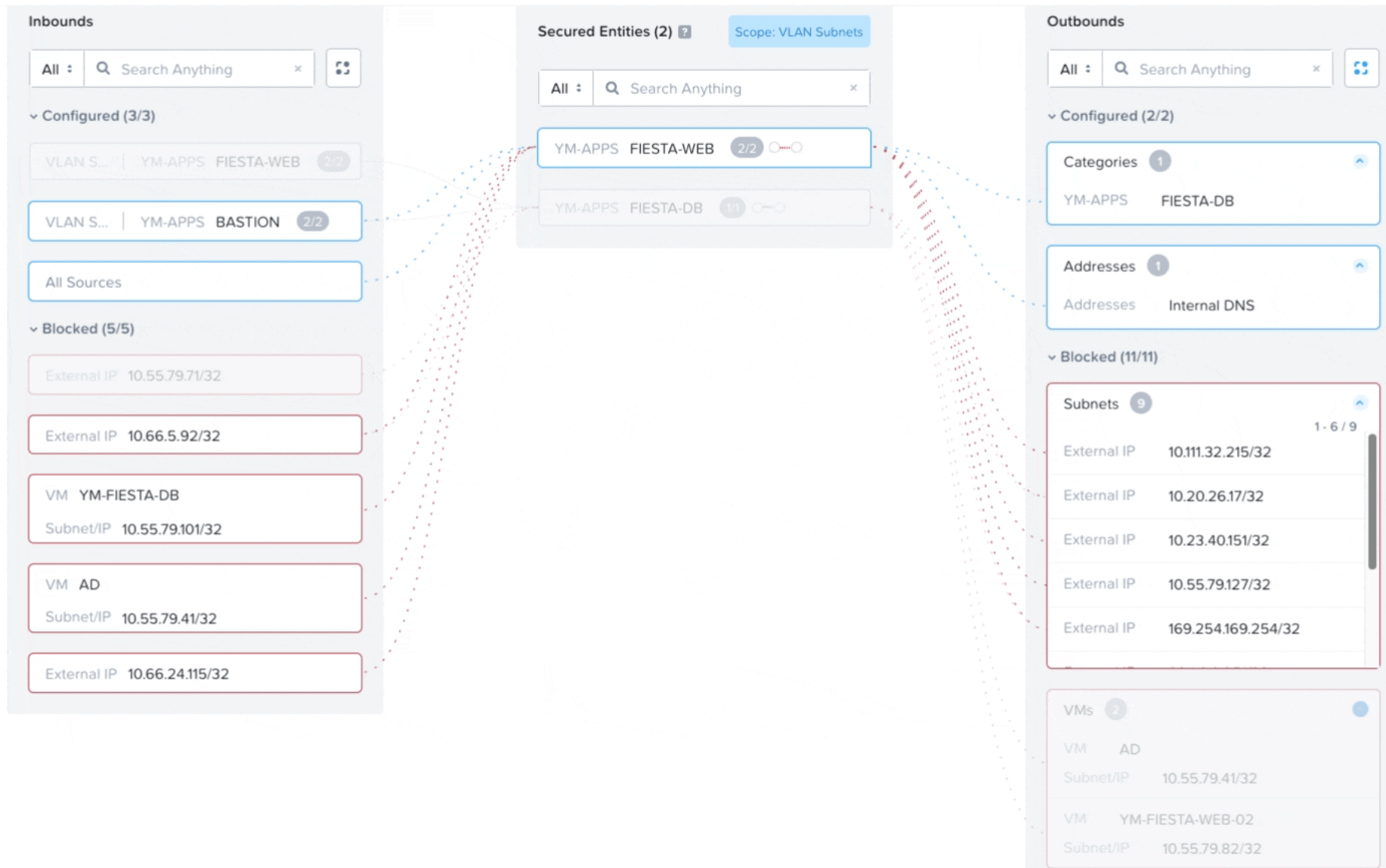
Flexible Mapping Between VMs And Policies



Live Traffic Analysis - Monitor



Live Traffic Analysis - Enforce



Toggle between Visual and List View

Inbound Rules



Inbound Rules		Outbound Rules	All	Search Anything
^ Configured Rules (2)				
Source	Secured Entity	Scope: VLAN Subnets	Services	
VLAN Sub... INFRA BASTION	APPS WEB	Scope: VLAN Subnets	ssh	
All Sources	APPS WEB	Scope: VLAN Subnets	https http	
^ Blocked Traffic (4)				
Source	Secured Entity	Scope: VLAN Subnets	Services	
Subnet/IP 10.55.79.67/32 (VM: DB-DEV)	APPS WEB	Scope: VLAN Subnets	ICMP 8,0	
Subnet/IP 10.55.79.83/32 (VM: VDI-WIN10)	APPS WEB	Scope: VLAN Subnets	ICMP 8,0	
External IP 10.66.24.2/32				
External IP 10.66.5.92/32				

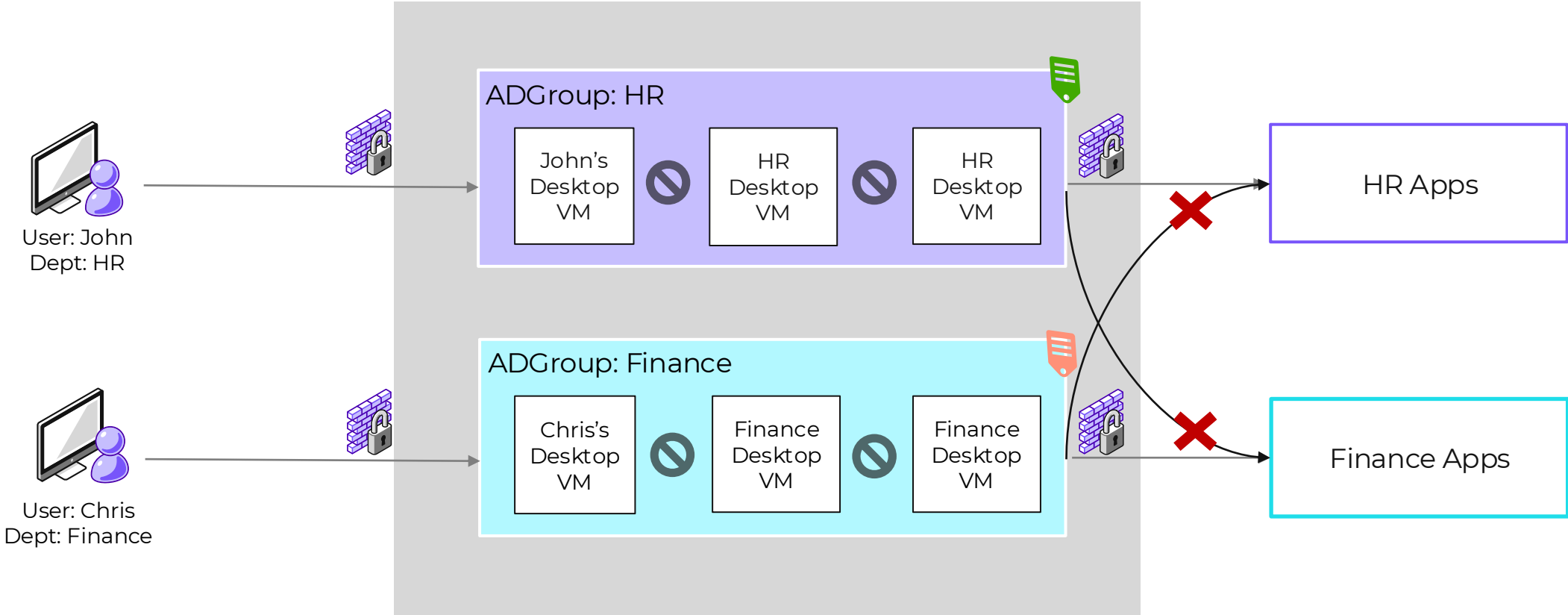
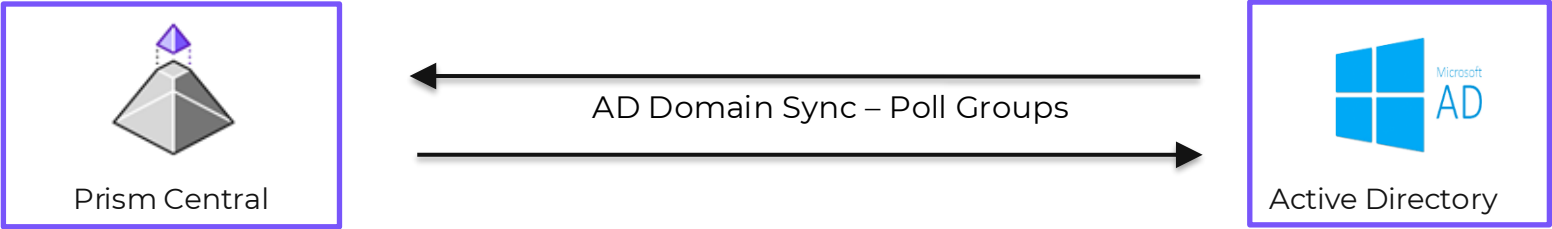
Outbound Rules



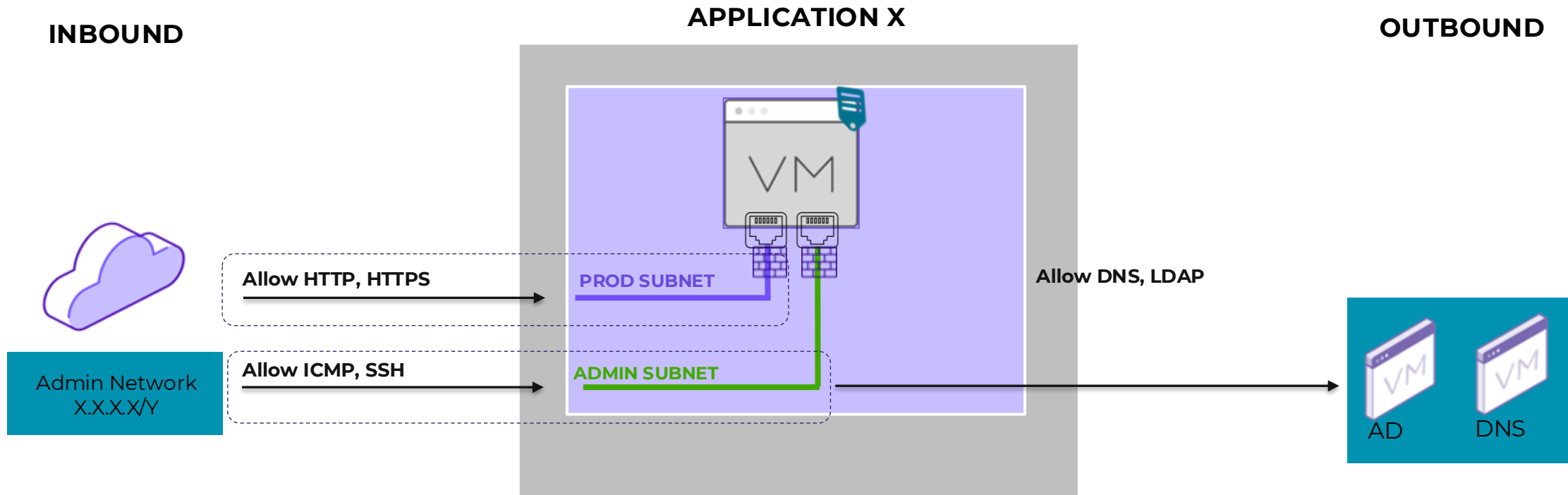
Inbound Rules		Outbound Rules	All	Search Anything
^ Configured Rules (1)				
Secured Entity	Scope: VLAN Subnets	Destination	Services	
APPS WEB	Scope: VLAN Subnets	VLAN Sub... INFRA AD-DNS	domain ldap	
^ Blocked Traffic (8)				
Secured Entity	Scope: VLAN Subnets	Destination	Services	
APPS WEB	Scope: VLAN Subnets	External IP 10.20.26.17/32	TCP 2074	
APPS WEB	Scope: VLAN Subnets	External IP 10.23.40.151/32	TCP 443 ICMP 8,0	
APPS WEB	Scope: VLAN Subnets	Subnet/IP 10.55.79.100/32 (VM: FIESTA-WEB-01)	UDP 137-138	



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.

