



Protecting Your Workloads and Data

Effective risk reduction strategies
for Building and Operating a Secure
Hybrid Cloud Platform with Nutanix

Forward-Looking Statements: This presentation contains forward-looking statements about, among other things: our business plans, initiatives and objectives; the benefits and capabilities of our platform, products, services and technology; our plans or expectations regarding product releases and enhancements, as well as the impact of including additional solutions in our product portfolio; trend analyses and statements regarding future events; and anticipated growth and industry prospects. These forward-looking statements are based on current expectations and beliefs of our management, current information available to our management, and current market trends and market conditions. The achievement or success of the matters covered by such forward-looking statements involves risks, uncertainties and assumptions, and if any such risks or uncertainties materialize or if any of the assumptions prove incorrect, actual results or outcomes could differ materially from those expressed or implied by these forward-looking statements. Accordingly, undue reliance should not be placed on such statements. Our filings with the SEC, which are available without charge at <https://www.sec.gov>, discuss some of the risk factors that may affect our business plans, initiatives and objectives, results of operations and financial condition. We undertake no intent or obligation to publicly update or revise any of the forward-looking statements made in this presentation, whether as a result of new information, future events or otherwise, except as required by law.

Product or Roadmap Information: Any future product or roadmap information included in this presentation is intended to outline general product directions, and is not a commitment, promise or legal obligation for us to deliver any material, code, or functionality. This information should not be used when making a purchasing decision. Further, note that we have made no determination as to whether separate fees will be charged for any future products, product enhancements and/or functionality which may ultimately be made available. We may, in our own discretion, choose to charge separate fees for the delivery of any future products, product enhancements and/or functionality which are ultimately made available.

Trademark Disclaimer: © 2026 Nutanix, Inc. All rights reserved. Nutanix, the Nutanix logo and all Nutanix product and service names mentioned herein are registered trademarks or trademarks of Nutanix, Inc. in the United States and other countries. Nutanix, Inc. is not affiliated with VMware by Broadcom or Broadcom. VMware and the various VMware product names recited herein are registered or unregistered trademarks of Broadcom in the United States and/or other countries. All other brand names mentioned herein are for identification purposes only and may be the trademarks of their respective holder(s). Certain information contained in this presentation may relate to, or be based on, studies, publications, surveys and other data obtained from third-party sources and our own internal estimates and research. While we believe these third-party studies, publications, surveys and other data are reliable as of the date of this paper, they have not independently verified unless specifically stated, and we make no representation as to the adequacy, fairness, accuracy, or completeness of any information obtained from third-party sources.



John Dodds

Director, Product
Management

Nutanix



Bill O'Donnell

Sr. Principal Product
Manager

Nutanix



Jon Cosson

Head of IT & CISO

JM Finn

The Nutanix logo, a stylized 'X' shape composed of four interlocking geometric blocks, is centered in the background of the slide. It has a blue-to-purple gradient and a 3D effect.

Agenda

Nutanix Cloud Platform

- 01** Secure Your Nutanix Cloud Platform
- 02** Secure Your Data
- 03** Secure Your Network and Applications

Secure Resilient Platform for Apps & Data

Aligned with the NIST Cybersecurity Framework

Return to normal as fast as possible

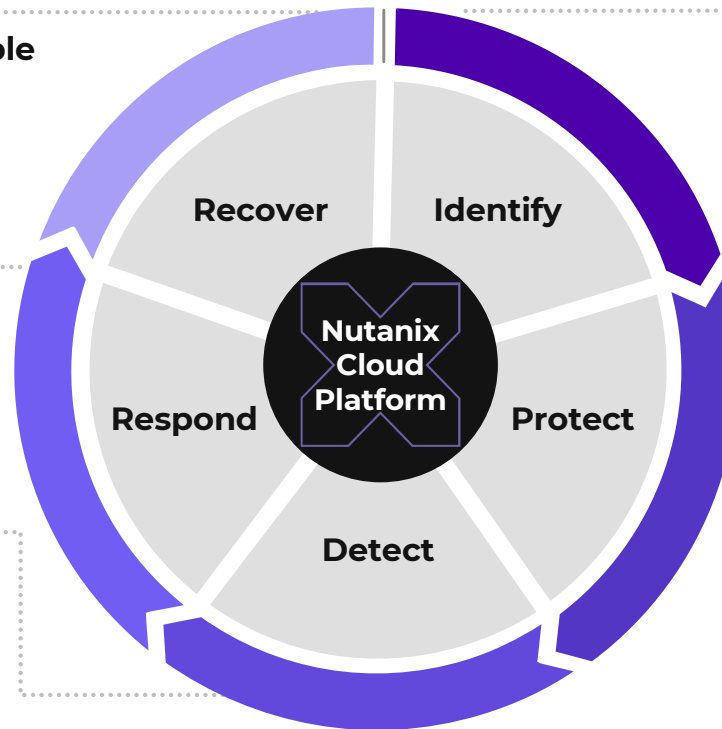
- Immutable snapshots
- Cyber and Disaster Resilience
- Data protection ecosystem

Policy-based automated response rules

- Alerts, Host, or VM actions
- Unstructured data blocking
- 3rd party integrations

Detect anomalous activity in near real-time

- Ransomware detection (Data Lens)
- Network threats (Security Central)



Certifications and Trust

[Nutanix.com/trust](https://nutanix.com/trust)

Global certifications

- **FIPS 140-3** 
Federal Information Processing Standard 140-2 validating cryptographic modules
- **Common Criteria EAL 2+** 
An evaluation of IT products to maintain high and consistent security standards
- **ISO 27001 + 27017 + 27018 + 27701 + 28000** 
An independent organization that publishes best-practice standards. (SaaS Focused)

Government certifications (USA)

- **DoDIN APL (Department of Defense)**
Cybersecurity certification for exclusive purchase by the DoD
- **National Institute of Standards and Technology (DISA)**
An evaluation, assigned controls, and approve of Nutanix STIGS

NIST frameworks

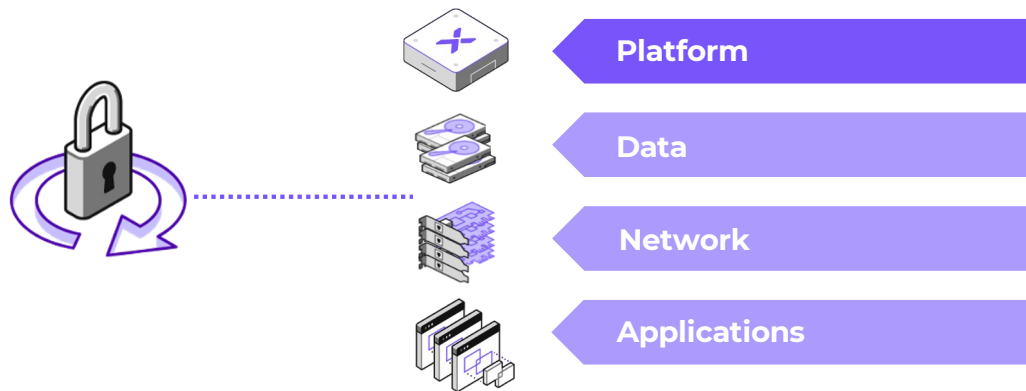
- **NIST Cybersecurity Framework**
Organized by five key Functions — Identify, Protect, Detect, Respond, Recover. These five terms, when considered together, provide a comprehensive view for managing cybersecurity risk over time
- **NIST Zero Trust Architecture (ZTA)**
Cybersecurity paradigms that moves defenses from static, network-based perimeters to focus on users, assets, and resources

Information security frameworks

- **Authentication, Authorization, Accounting Framework (AAA)** Control and track access within a network
- **Confidentiality, Integrity, Availability Framework (CIA Triad)** Data handling designed to guide policies for information security within an organization

Platform:
NCI, AOS, AHV

Build Your Cloud Securely



Zero Trust Platform

Prove It's You

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

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

What are you allowed to do?

Select Entities

AHV VM In Category Search Category

AHV VM

Site:Branch-001 x

Automatic access

Entities created by selected users

Authorization

What can you access?

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

Track who did what

Syslog Servers

1 Syslog Server 2 Data Sources

Data Sources and Respective Severity Level

Module Name	Severity Level
☒ API Audit	6 - Informational: informational messages
☒ Audit	6 - Informational: informational messages
☒ Security Policy Hit Logs	All Levels
☐ Flow Service Logs	Select Severity Level

Accountability

What did you do, and when?

- Syslog / rsyslog
 - Capture logins and admin activity
- IPFix Network Info

Nutanix Secure Administration

Platform Security: Prism Security

Authentication, Role-Based Access Control (RBAC), Auditing

- Fine-grained delegation of control and responsibility

Fast Risk Indicators

- Quickly identify Common Vulnerabilities and Exposures (CVEs)

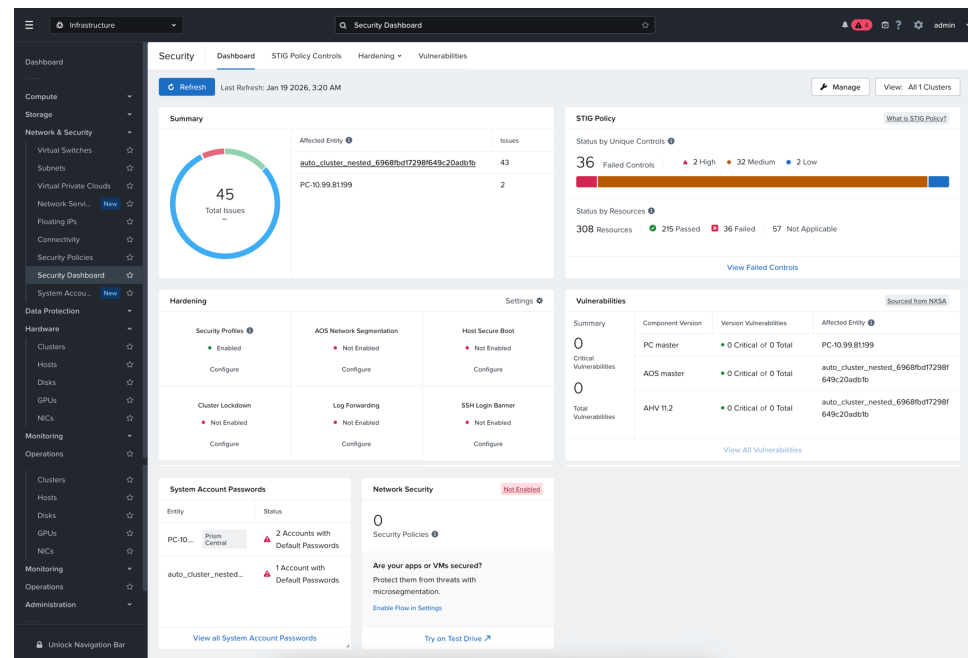
Customized Security Focus

- Get info on what's most critical for your security posture
- Easy one click config toggles
- New (3QCY26) Platform Security Profiles

View, Understand, and Track Security Gaps

- Infrastructure security posture at-a-glance
- System password Management
- Easy access to Flow network Security Management

Prism Security



Vulnerabilities and Upgrades



Nutanix Vulnerability Database



How can I get CVE information for my Nutanix Platform?

- NXVD can be found in the Nutanix Support Portal
- Ability to get status of any published vulnerability
- Available for:
 - AOS
 - MSP
 - AHV
 - Objects
 - Prism
 - BIOS/Firmware (HW)
 - NKP

New Nutanix is a CVE Numbering Authority (CNA)

Nutanix can assign and publish CVEs directly

- Reducing third-party dependency
- Enabling faster, clearer, and more consistent vulnerability disclosure information.

Combined with Easy LCM Upgrades

Component	Available Version	Current Version	Last Updated	Release Notes
Software	3.6.0	3.5.2	Transition update	
Cats	3.6.0	3.5.2	Transition update	
Epsilon	2.4.2.1	2.4.2	Transition update	
MSP	4.6.0.1	4.5.0	Transition update	View Release Notes
NCC	pc-2022.6.01	pc-2022.6	Release Date: October 13, 2022	View Release Notes
PC	Transition update			



Transitioning to Remove Bash Shell Access

Improve security cyber resiliency, stability, and supportability

What does this mean to me

- Transitioning over time in disabling SSH Bash shell access
- Automation leveraging V4 API
- Prism Web Interface will continue to be available
- PowerShell will be enhanced to support Nutanix CLI
- **Under Development** — SSH Service Menu
 - Able to access any of the existing Nutanix CLI
 - Able to execute any self-service scripts that exist today in the support KB articles
 - Ability to view logs
 - Ability to access support only Bash Shell to solve critical support issues



New SSH Service Menu

Auth with admin account or LDAP

Under Development

```
DEMO>su - admin
Last login: Thu Nov  6 17:03:14 UTC 2025 on pts/1

=====
LDAP Authentication Required
Domain: qa.nutanix.com
=====

LDAP Username: Administrator
LDAP Password:
Authenticating...
✓ Authentication successful!
Welcome, Administrator

=====
NuService Support
Logged in as: Administrator
=====
Option 1: Run Allowed Commands
Option 2: Launch Admin Shell
Option 3: Enable/Disable Nutanix Account
Option 4: Exit
=====
Choice: █
```

Current Target Transition Plan

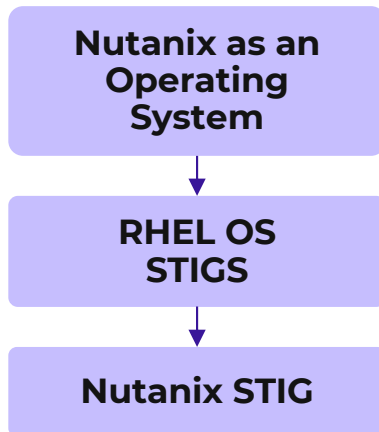


See Bash shell transition FAQ in KB article KB-20212

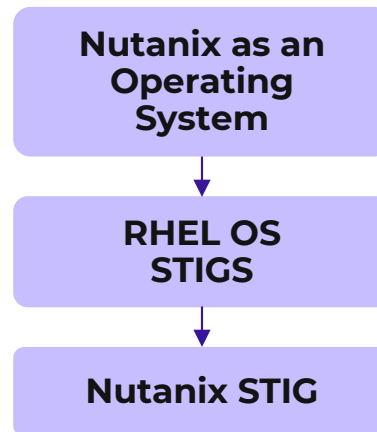
Transition to DISA Approved Nutanix STIGs

Improve security cyber resiliency, stability, and supportability

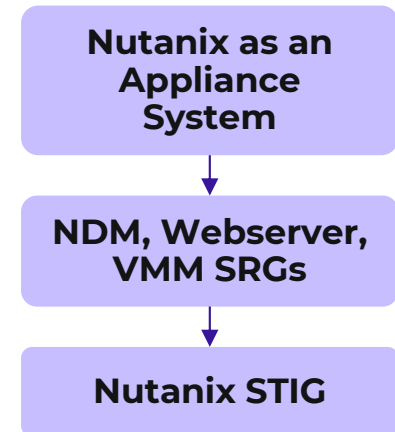
AOS/AHV 7.3



AOS 7.5 (AOS only)



AOS/AHV (Under Development)



FIPS 140-3 Complete

AOS/AHV Release

Note: DoDin APL Certified and will be listed until 9/2027 as the program will transition to DISA STIGs

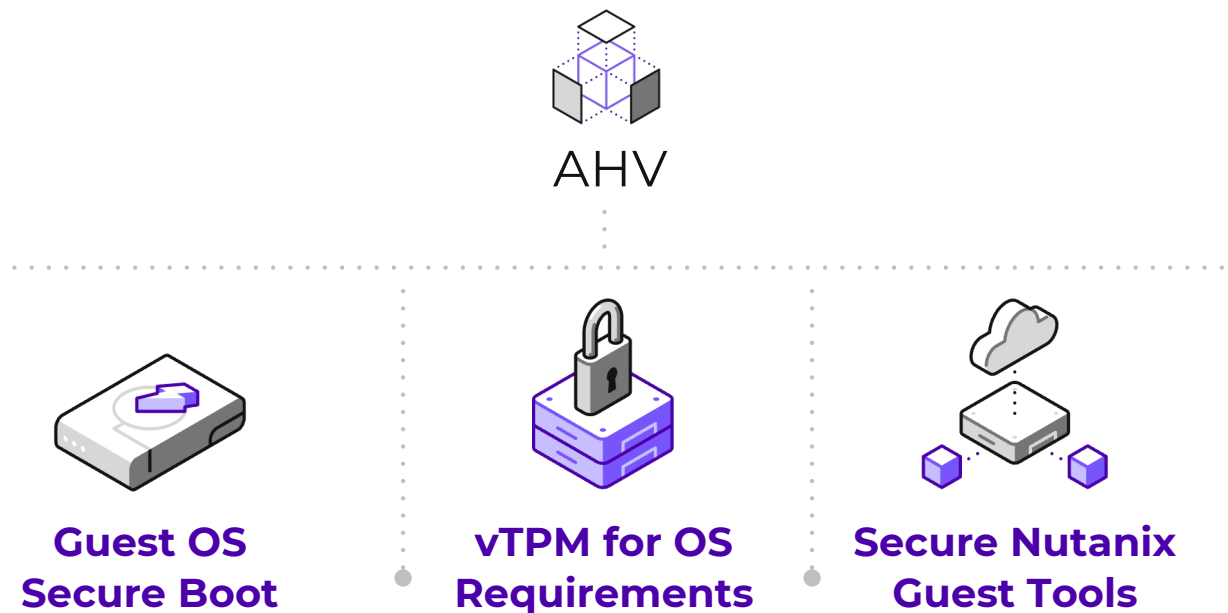
Note: Requires Opting into support only access to the Bash Shell

Nutanix + Cloud Virtualization Security



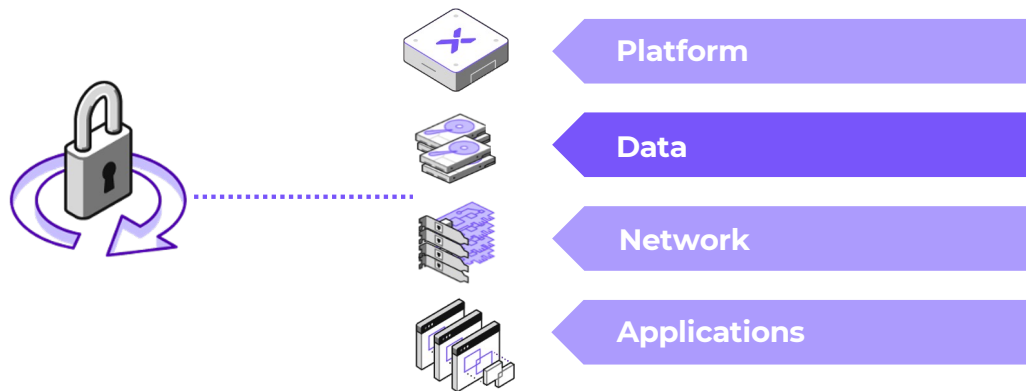
Cloud Virtualization Security: AHV

- **Run VMs with Cryptographic Confidence** — Boot only trusted, 'signed' OSes; replaces the traditional BIOS model with UEFI that's DOD compliant
- **Create a Virtual Vault without New Hardware** — Virtual TPM Stores encrypted functions and keys including Microsoft Credential Guard and BitLocker (now required by Windows 11)
- **Virtual TPM Encrypted Storage** — Each VM vTPM instance is encrypted with unique key stored in Nutanix built-in KMS or **NEW** in 3rd party KMS
- **Secure Virtual Tool Communication** — Tunnel communication through virtual serial ports eliminating open ports of Nutanix Guest Tools (NGT)



Platform:
NCI, AOS, AHV

Build Your Cloud Securely



Encrypt Your Data

Nutanix + data encryption



Data encryption: Data-at-rest encryption

Operational simplicity

Nothing to manage once enabled, set it and forget it.

Performance agnostic

Enable without a performance hit.

Keeps data confidential

Prevents loss/theft.

Regulatory alignment

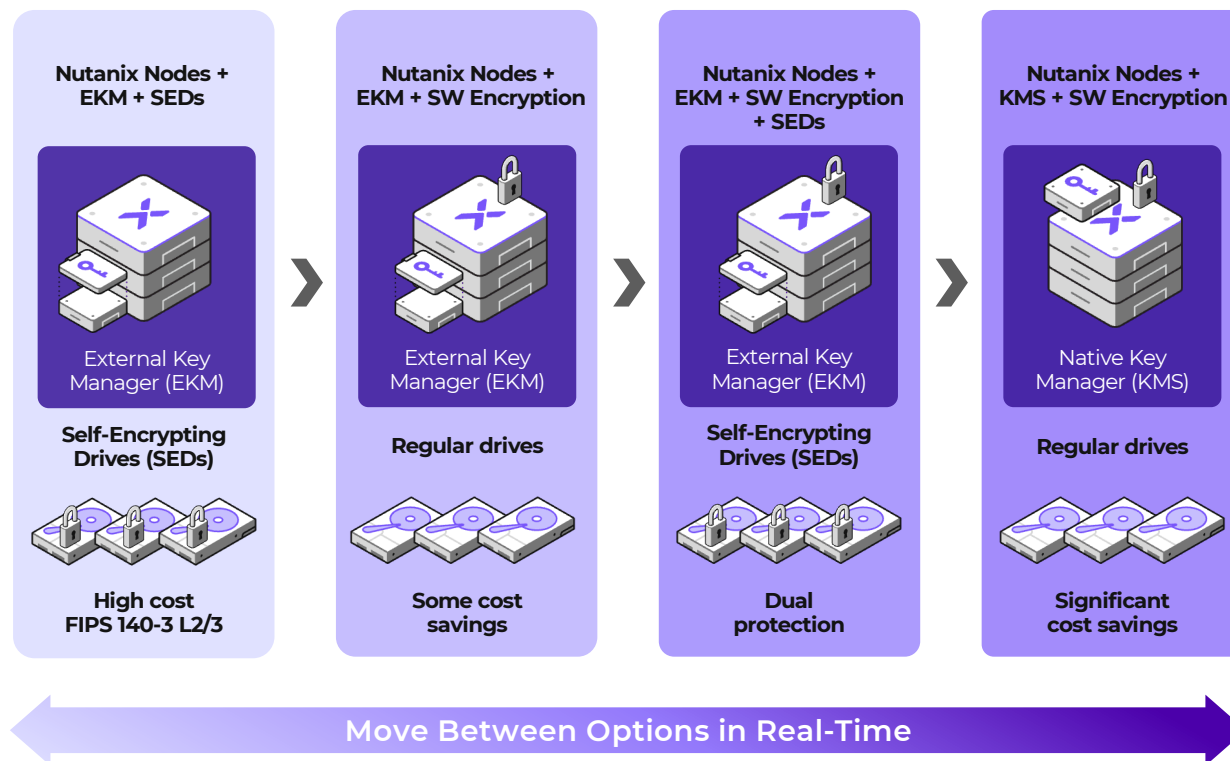
Align to HIPAA, PCI-DSS, NIST.

Nutanix makes change easy!

Move between options simply.

Wide range of Key Manager

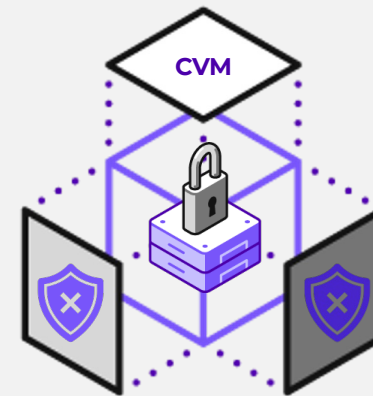
- Nutanix Build-in KMS
- 3rd Party KMIP KMIS
- **New** — Azure as an EKM



CVM Advance Security Prevention



- **Prevents** malicious CVM attacks from compromising AOS Data and system state information
- **Only Nutanix signed code** can change AOS data and state
 - Example: A compromised admin ID or compromised process **can not** update or delete AOS data, snapshots, or system state information
- All malicious attempts are logged



Nutanix Secure Snapshot

A Nutanix customer reported that Secure Snapshot gave them early notification of an attempted and failed ransomware attack

Immutable Snapshots: Nutanix Secure Snapshot*

Zero Admin Compromise

Denies changing or deleting Nutanix snapshots/snapshot policies even if the administrator ID has been compromised.

Automate and Move On

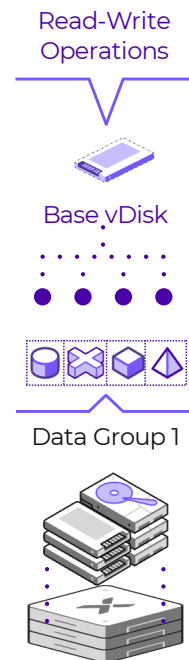
Automatically take regular immutable Snapshots with a configurable Secure Snapshot retention period of 1–31 days.

Ransomware Recovery

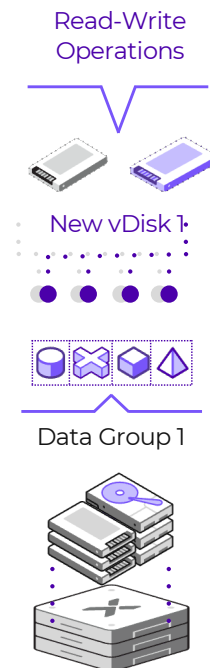
Support fast recovery without having to pay malicious attackers' ransoms.

**Applies to NCI AOS Storage
and NUS Files and Objects**

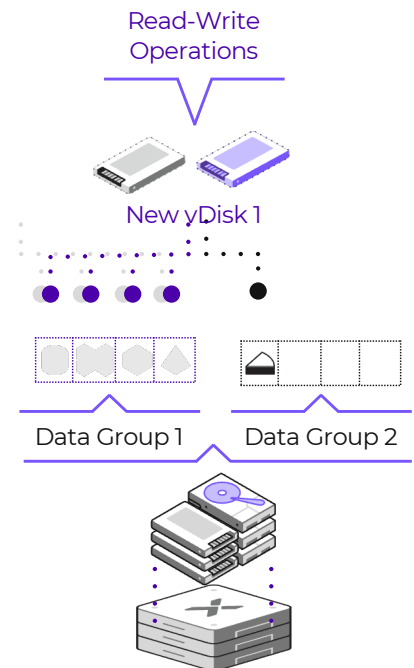
1. Before Snapshot



2. During Snapshot



3. After Snapshot



Data Lens: Global Visibility and Front-line Defense



Nutanix Data Lens

Flexible deployment options

- **New** Deploy in your infrastructure on-premises or leverage a Nutanix-hosted service

Ransomware Protection Detect and block

- **New** 2 minutes or less threat containment window (with On-Prem)

Intelligent Ransomware Recovery

- 1-click recovery

Anomaly Detection and Alerting

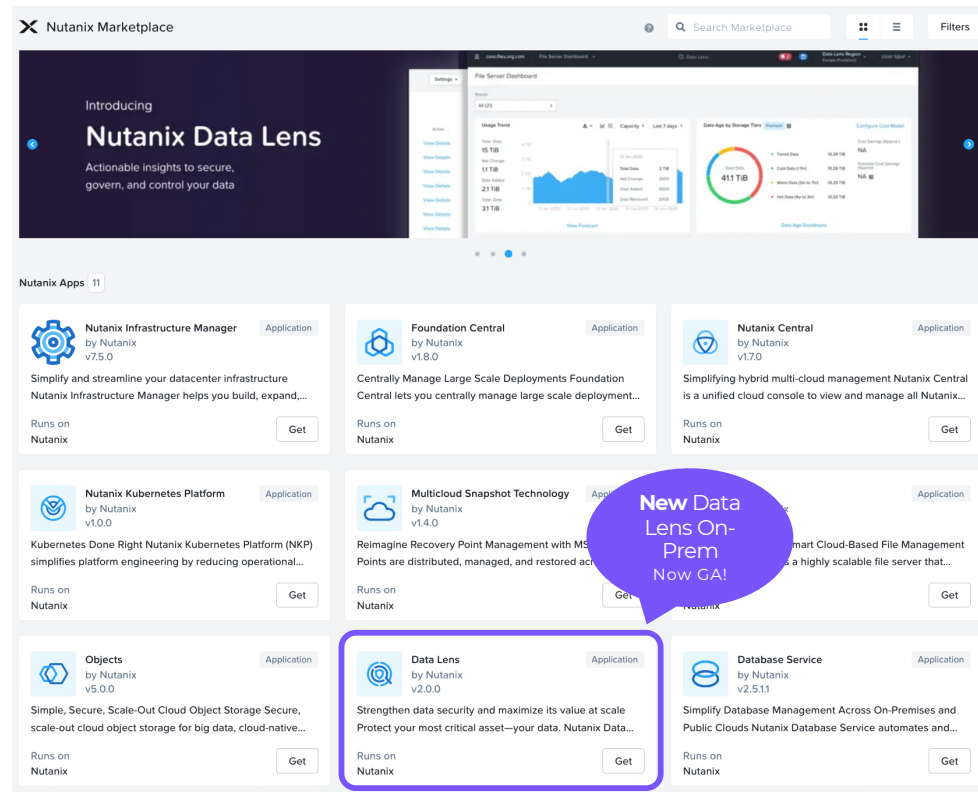
- Warn potential NUS or AWS data exfiltration

Audit Trails

- Who, what, and when
- Comply with audit controls

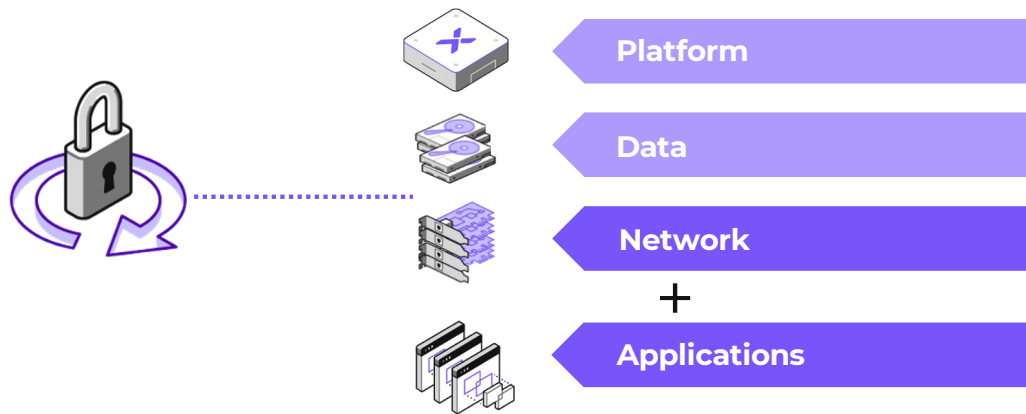
Permissions Risk Analysis

- Scoring based on policy



Platform:
NCI, AOS, AHV

Build Your Cloud Securely



Network Security — What Has Been Said

Status Quo

**We have Edge
Firewalls**
Our OS is secured
We are good!



Living on the Cutting Edge

**Our Environment is
very dynamic, it
won't scale.**



Stumble and Fail

**Microseg is too
complex. We tried it
before and it
didn't work.**



Flying Blind

**We don't have the
visibility into our
environments. It
may break our
critical apps.**



Security Models Must Evolve

COMPLEX INFRASTRUCTURE + TRADITIONAL SECURITY APPROACHES = **INCREASED RISK**

- **Hybrid Cloud:** New application and deployment architectures require new security strategies. Requires cloud domain knowledge.
- **Blind Spots:** Multiple products and manual efforts to implement and maintain increasing complexity without removing security gaps.
- **New Application factoring:** VMs, Containers, on-prem, in the Cloud.
- **Lack of unified solutions:** multi-product strategies can be complex and resource-intensive in a traditional, multivendor infrastructure stack.

Zero Trust is the **ONLY** way forward



Ensure Application & Network Security in AHV

Application Security:

Flow

Reduce Your Blast Radius

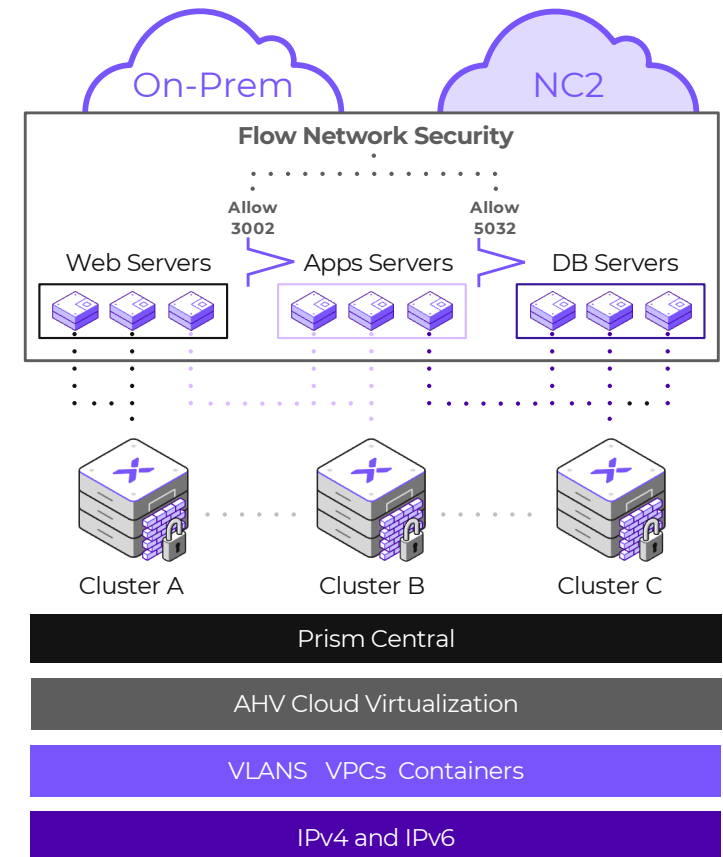
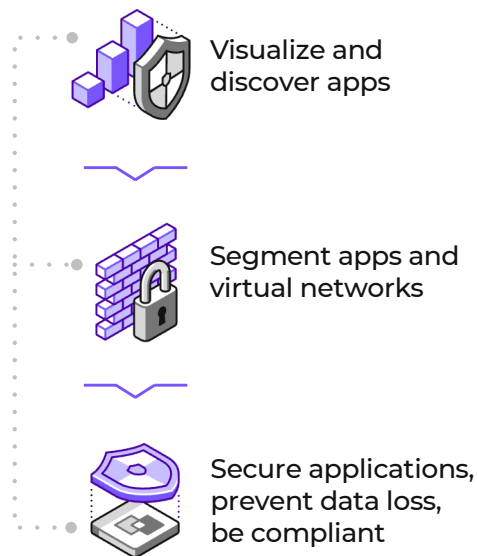
Flow Network Security simply creates policy-based Micro-segmentation between your apps.

Software Defined Networking (SDN) without the Headaches

Flow Virtual Networking enables cloud-like networking access controls with virtual private clouds (VPCs).

Build the Foundations of Zero Trust

Enable Zero Trust segmentation and reduce risk through controlled access of apps and data.

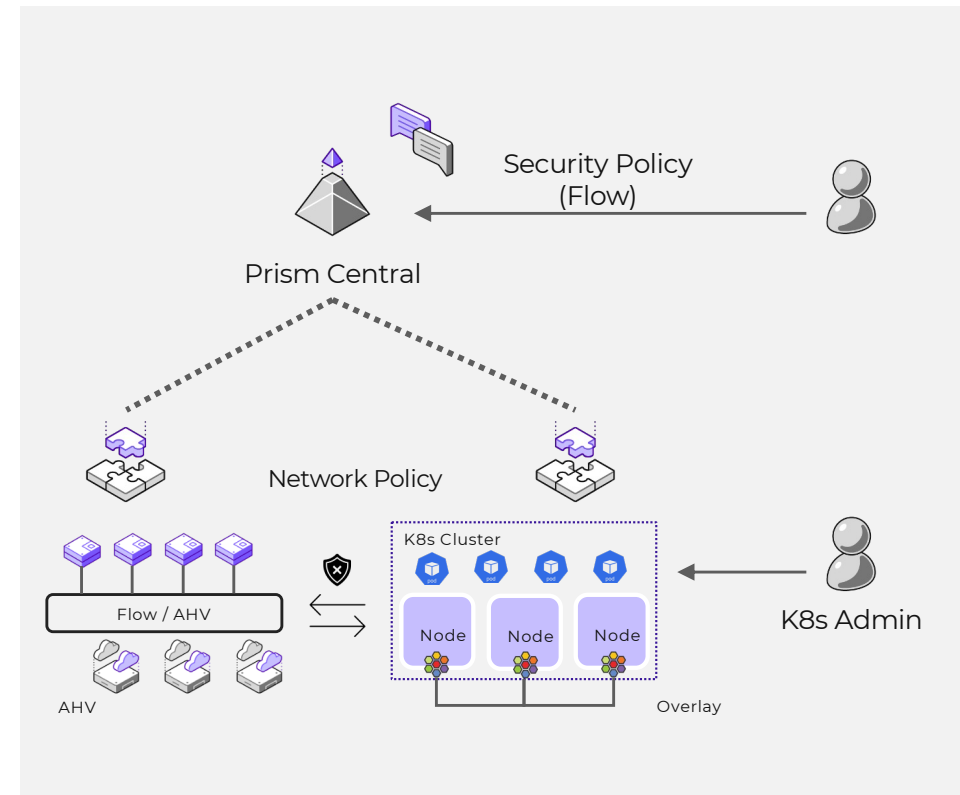


Zero Trust for Modern Applications



Securing containers and Virtual Machines every where with **Flow**

- One management solution securing Containerized and VM Applications
- Centralized visibility and compliance
- Network/Security admins manage segmentation policies for K8s workloads
- Flexible Design:
 - Policy Enforcement via Cilium CNI
 - Uses Standard K8s Network Policies

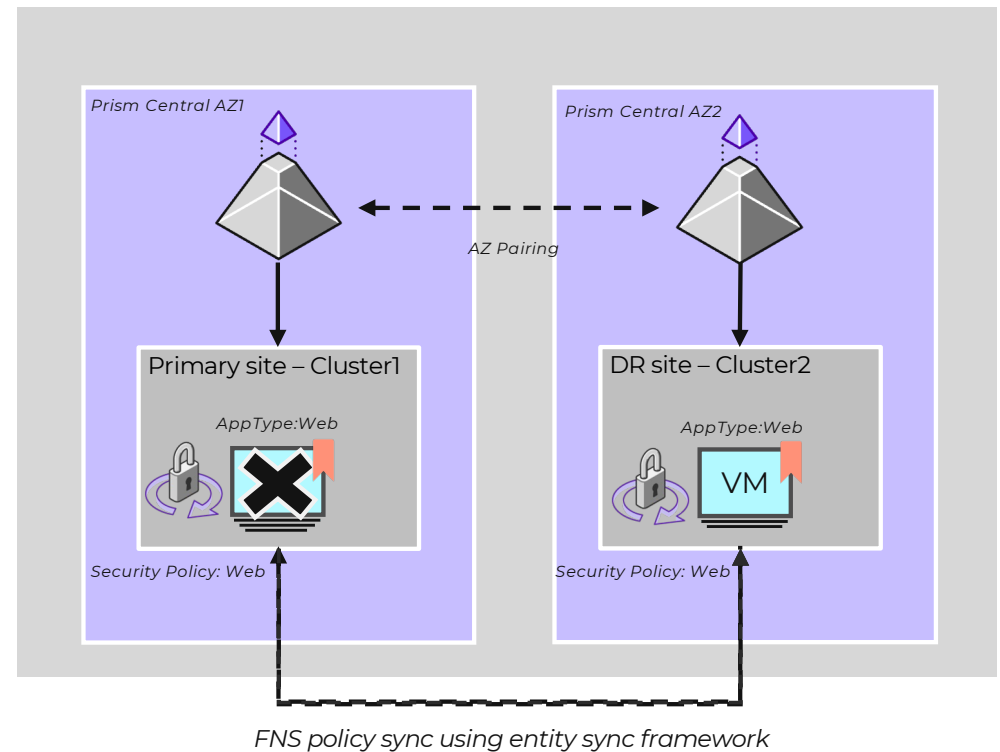


Security Policies + DR

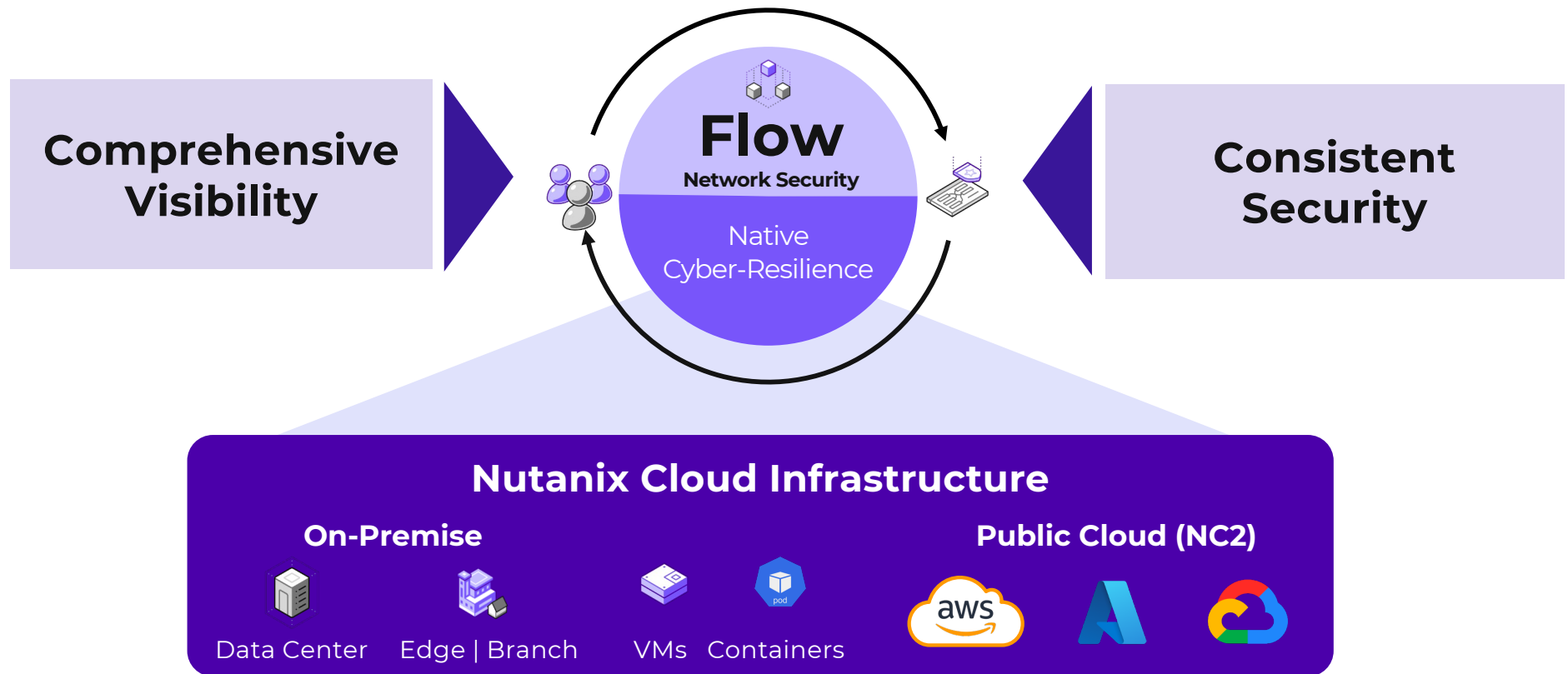


Replicate Security Policies across Availability Zones

- CCLM across all network types preserving security policies
- All Security Policy constructs are replicated
- VPC , VLAN and NC2
- Bi-directional
- No security posture lapse during or after a planned or unplanned failover across PC instances
- Sync up to 1,000 FNS Policies (VLAN or VPC)



Native Lateral Defense for Nutanix with Flow



Summary

NUTANIX

Defense in Depth with Partners

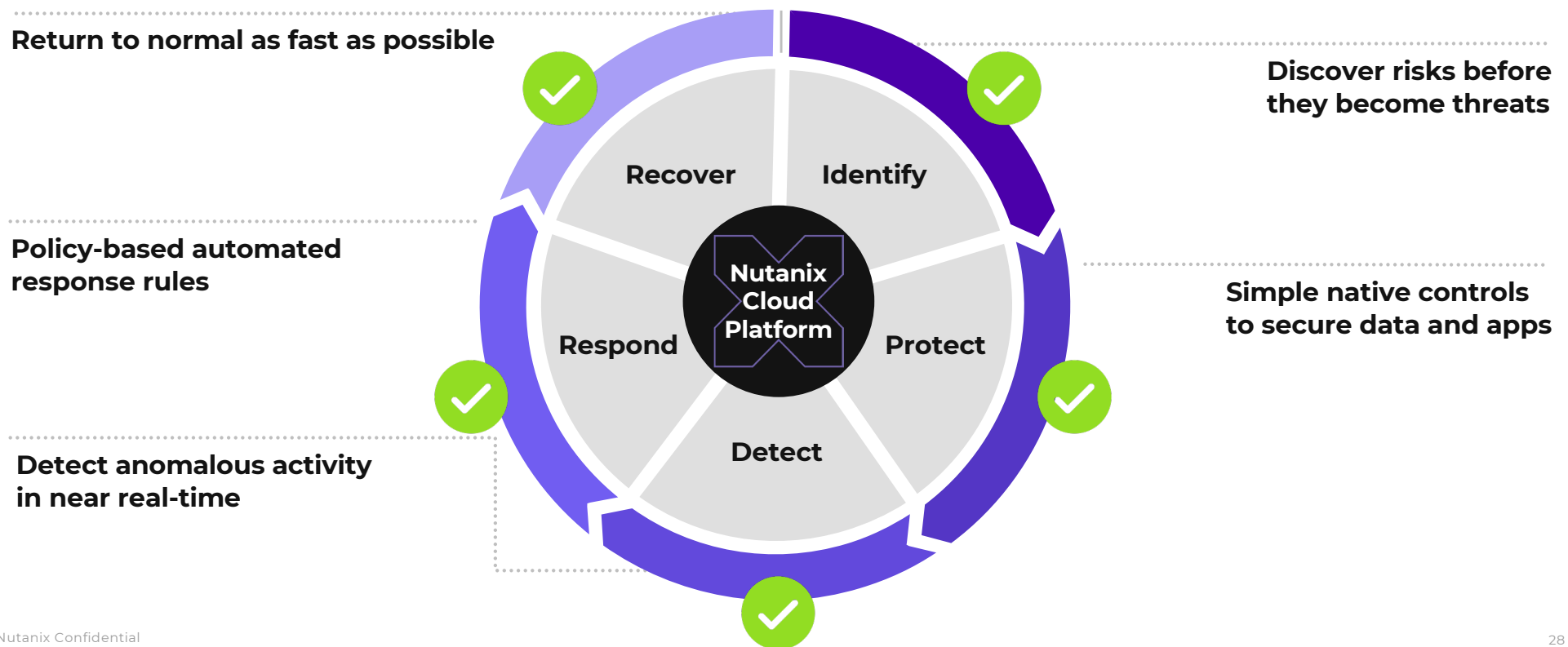
200+ Best of Breed Solutions that work with Nutanix.

Preserve and expand security investments into virtual and multi-cloud environments.



Nutanix Is a Valuable Security Partner

Aligned with the NIST Cybersecurity Framework





Complete your
session surveys in
our mobile app for
a chance to win.

Your feedback could win
you a pair of Apple AirPods
Pro 3, an iPad mini, or a
Lands' End gift card!



Consider attending these other Security Sessions

Sessions	Time	Room
Fortifying Data Security: Proactive Ransomware Defense with Nutanix Data Lens	Wed: 2:00-3:00	W184c
Flow at Scale: Production-Ready Networking and Security	Wed: 3:30-4:40pm	W184c
How to Automate cloud Native Security with K8s	Wed: 3:30	W184d
K8s networking on Nutanix: Security and Advance Architecture	Wed: 3:30-4:40	W183c
Network and Security Nuggets: I wear My Sunglasses at Dark Sites	Thur: 10:00-10:20	Expo, Innovation Theater



Thank You
