HYCU® NUTANIX

Why Nutanix Requires a New Approach to Data Protection

How to reduce cost, complexity, and risk when developing a backup strategy for your Nutanix environment

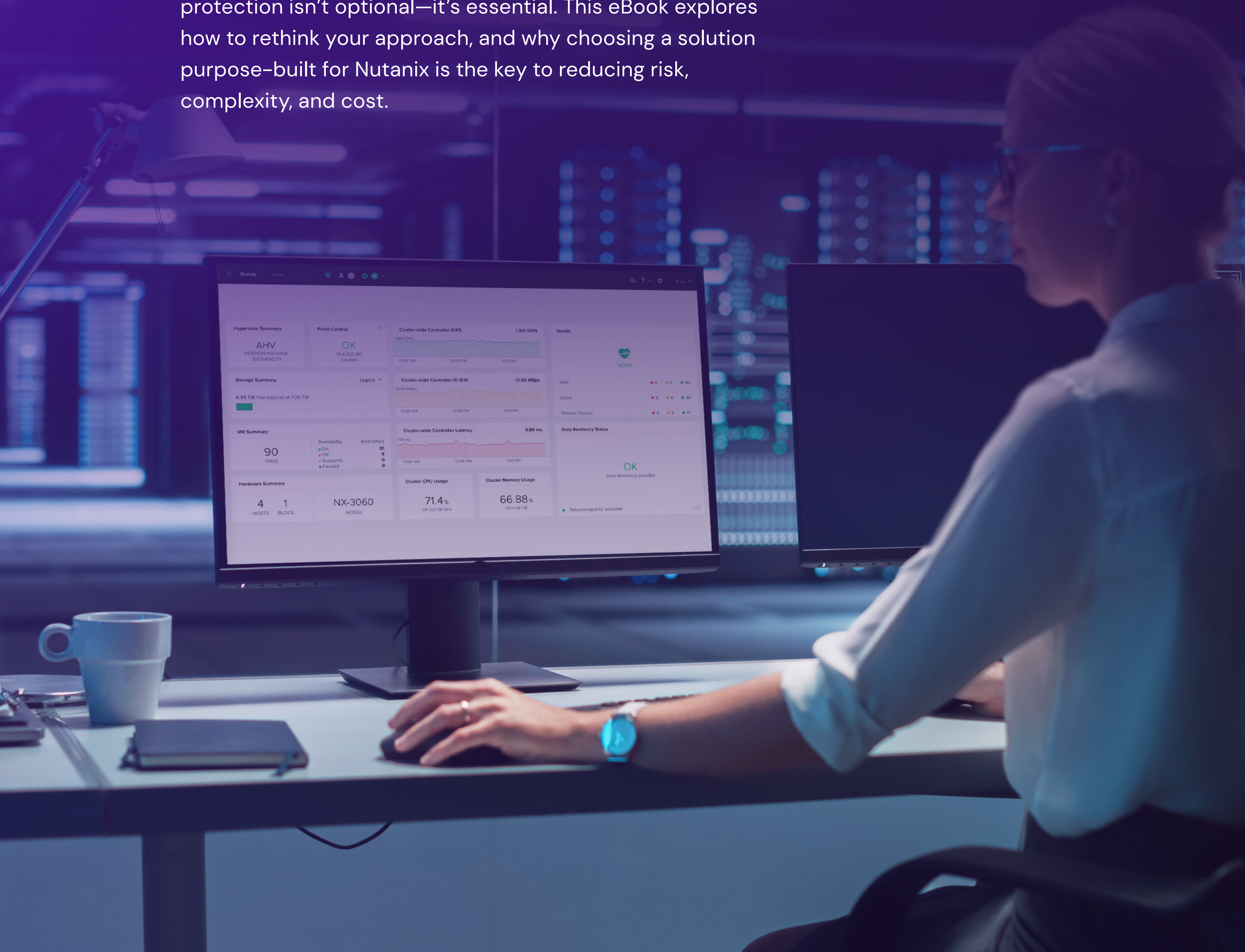
EBOOK

Introduction

As IT teams look to modernize their infrastructure, more organizations are moving away from legacy hypervisors and embracing Nutanix AHV. It's easy to see why: Nutanix delivers the simplicity, scalability, and lower TCO that businesses need to stay agile.

Yet making the shift to Nutanix isn't just a hypervisor change—it's a mindset shift. Traditional data protection solutions weren't built with Nutanix in mind. Attempting to retrofit them onto a modern HCI environment often leads to added complexity, poor performance, and gaps in protection.

With ransomware threats growing more aggressive and downtime more costly than ever, reliable, built-in data protection isn't optional—it's essential. This eBook explores how to rethink your approach, and why choosing a solution purpose-built for Nutanix is the key to reducing risk, complexity, and cost.



Why Legacy Backup Tools Fall Short for Nutanix

Many organizations try to carry their existing backup solutions into Nutanix environments—and quickly run into limitations. These tools were designed for legacy infrastructure, and they struggle to keep up with Nutanix's scale-out architecture and application-centric design.

Key shortcomings:

Inflexible architectures
Traditional backup platforms rely on static, hardware-centric deployments that don't align with Nutanix's elastic, software-defined model. This mismatch creates bottlenecks and hinders scalability.

Complex deployment and management
Legacy tools often require agents, proxies, or dedicated backup infrastructure—all of which add overhead and slow things down.

Limited workload visibility
Nutanix spans more than just virtual machines. Legacy solutions often lack full visibility or protection for Nutanix Files, Objects, NDB, and containers.

Slow recovery times
When every second counts, outdated recovery processes delay RTOs and put business continuity at risk.

Hidden costs
Licensing fees, infrastructure bloat, cloud egress charges—the true TCO of legacy tools is often far higher than expected.

Legacy approaches simply weren't designed for the speed and simplicity of Nutanix. Modern environments call for a modern solution.

Understanding Nutanix Workloads

Nutanix offers exceptional flexibility across a wide range of workloads and services:

- ✓ VMs on AHV or ESXi
- ✓ Nutanix Files and Objects
- ✓ Nutanix Database (NDB) and third-party databases
- ✓ Nutanix Cloud Clusters (NC2) on AWS and Azure
- ✓ Containerized apps on Nutanix Kubernetes Platform (NKP)

Each has unique protection needs. Legacy solutions may handle one or two of these well, but rarely all. It's essential to choose a data protection platform built for the full Nutanix ecosystem—not just VMs.

Mine
NC2
Metro
ROBO
NKP
Object
Frame
Calm
Prism
AHV
NDB
Files
Volume Groups
NUS

Backup Strategies for Nutanix Environments

There are two common paths for protecting Nutanix workloads:

Third-Party Integration

While some third-party solutions offer partial Nutanix support, they often introduce:

- **Added complexity:** Multiple tools to manage, maintain, and secure.
- **Limited flexibility:** Scaling backup with your Nutanix growth becomes inefficient and costly.
- **Hidden costs:** Proprietary hardware, agents, cloud compute, and storage overheads inflate TCO.
- **High operational burden:** Resources diverted from mission-critical applications.

Native Nutanix-Optimized Protection

The better approach is to adopt a purpose-built solution designed for Nutanix. Benefits include:

- **Simplified management:** One platform protects all Nutanix workloads with auto-discovery and one-click policies.
- **Lower TCO:** No agents, proxies, or complex integration. Just native, streamlined efficiency.
- **Elastic scale:** Grows with your Nutanix environment—automatically.
- **Stronger security:** Minimized attack surface with built-in immutability and compliance controls.

With the right solution, you can unlock the full value of Nutanix—securely, efficiently, and confidently.

Disaster Recovery for Nutanix

Outages happen. Whether it's human error or a regional disaster, you need to bounce back fast. A strong disaster recovery strategy should address:

→ **RTO (Recovery Time Objective):** How quickly can you resume operations?

→ **RPO (Recovery Point Objective):** How much data are you willing to lose?

→ **Failover strategy:** Can you switch to a backup system without data loss?

Leverage Nutanix-native snapshots and seamless DR replication to minimize both RTO and RPO. A backup platform designed for Nutanix can automate these processes and ensure continuous protection.

Protecting Against Ransomware

Ransomware is the leading cause of downtime and data loss worldwide. Nutanix environments are no exception. Your data protection solution must be prepared.

Key best practices:

- **Immutable backups:** Air-gapped, tamper-proof data copies ensure recovery even if attackers gain access.
- **Hidden snapshots:** Prevent visibility and deletion by unauthorized users.
- **Rapid recovery:** Restore systems within minutes to minimize business disruption.
- **End-to-end security:** Compliance-ready protection with military-grade controls.
- **Diversified restores:** Restore to any cloud or hypervisor—ideal for clean-room recovery.

Ransomware isn't going away. Proactive, Nutanix-optimized protection ensures you're ready.

Hybrid and Multi-Cloud Data Protection

Today's enterprises run across multiple clouds and platforms. Your backup strategy should, too.

A strong data protection solution for Nutanix should:

- **Enable seamless backups to public cloud:** Support AWS, Azure, and GCP with native optimization.
- **Simplify hybrid DR:** Eliminate vendor sprawl and integrate easily with Nutanix NC2.
- **Reduce cloud TCO:** Optimize cloud storage, automate policy management, and avoid waste.

With unified protection across environments, you gain agility without complexity.

Key Questions to Ask

As you evaluate options for protecting your Nutanix environment, ask:

- ? Is it purpose-built for Nutanix?
- ? Can it restore VMs, databases, and files in one click?
- ? Does it deliver full ransomware resilience?
- ? Can it support automated DR to any location?
- ? Is it built to help meet compliance and data privacy goals?

→ If the answer isn't a clear "yes" across the board, it might be time to rethink your solution.

The Solution for Nutanix: HYCU

HYCU is the only data protection platform built specifically for Nutanix. Here's what sets it apart:

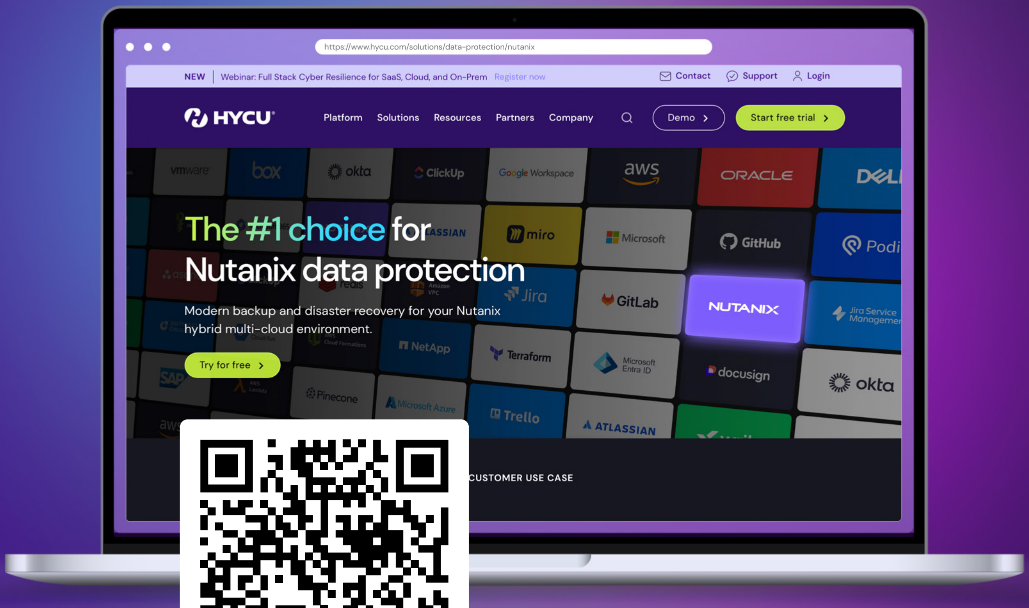
- ✓ **Zero-impact protection:** No agents, no proxies, no extra hardware.
- ✓ **Broadest Nutanix coverage:** From VMs and files to databases and containers.
- ✓ **Fastest recovery:** Restore directly to your Nutanix environment in minutes.
- ✓ **Lowest TCO:** Eliminate complexity and reduce infrastructure waste.
- ✓ **Familiar interface:** Prism-like experience makes backup feel native.

Save time.
Cut costs.
Protect everything.

All with one platform, designed with Nutanix in mind.

Experience effortless data protection for Nutanix

Request a demo or free trial today



https://www.hycu.com/solutions/data-protection/nutanix

NEW | Webinar: Full Stack Cyber Resilience for SaaS, Cloud, and On-Prem Register now

The #1 choice for Nutanix data protection

Modern backup and disaster recovery for your Nutanix hybrid multi-cloud environment.

Get Started