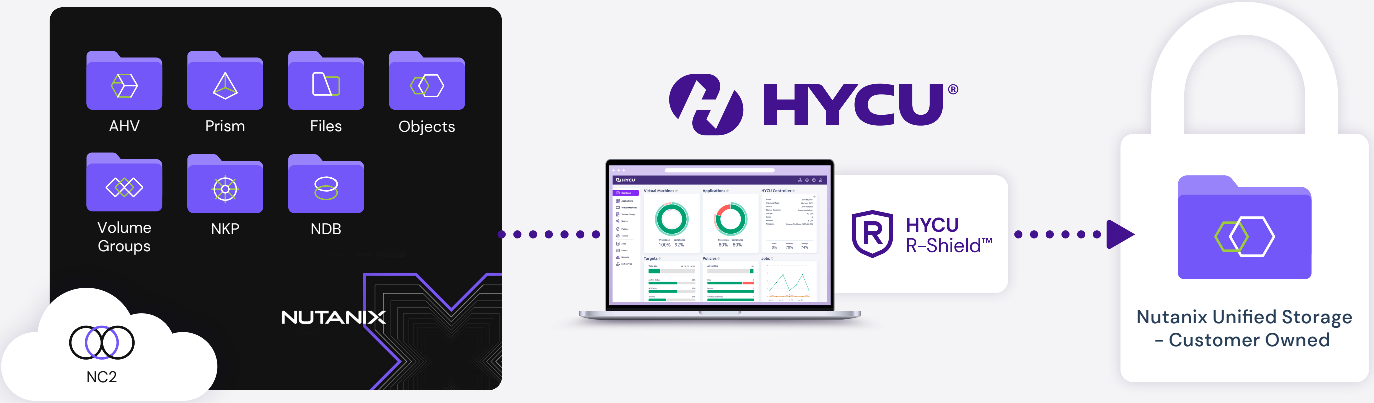
Stay Protected: Achieve Cyber Resilience With HYCU & Nutanix

WHITEPAPER

Always Protected: Achieve Cyber Resilience With HYCU & Nutanix

Cyber resilience starts at the platform. Nutanix and HYCU ensure it extends to every workload.

In a world where ransomware, insider threats, and configuration drift are everyday risks, protecting your environment begins with a secure foundation. Nutanix and HYCU work as one to deliver cyber protection that's embedded from infrastructure to data – so you're protected, by default and by design.



Platform: Built-in Resilience by Design

Nutanix and HYCU share a core principle – resilience must be built in, not bolted on. Nutanix delivers a hardened foundation for every workload with integrated compute, storage, and networking services. HYCU extends that resilience by deploying as a secure, virtual appliance – purpose-built for production environments that can't afford downtime or vulnerability.

Nutanix Platform Highlights:

- Self-healing architecture with native high availability and failover
- Data-at-rest encryption and secure boot enforcement
- Micro-segmentation via Nutanix Flow for workload-level isolation
- Unified Storage (NUS) for block, file, and object services in one platform

HYCU Platform Highlights:

- Delivered as a pre-hardened, locked-down virtual appliance
- The only backup vendor with a published DISA STIG security benchmark
- Runs on production or on a dedicated NUS cluster to isolate the backup plane
- No OS-level access or shell interaction – fully sealed design

Together, Nutanix and HYCU provide a unified, self-defending platform built to withstand modern threats.

Security Controls: Zero-Trust Across Layers

Both platforms apply zero-trust principles to infrastructure, data, and backup workflows.

By combining native platform security with hardened data protection, Nutanix and HYCU help close the gaps that attackers target most – designed so that access is limited, logged, and controlled.

Nutanix Security Controls:

- Role-based access control (RBAC) and multifactor authentication via Prism management console
- Flow virtual networking and micro-segmentation solution for lateral threat prevention
- Secure snapshots and native encryption to preserve workload integrity

HYCU Security Controls:

- Appliance-level hardening and no open services exposed to the network
- RBAC and MFA to limit administrative access
- All data traffic encrypted in-flight and at rest, across all targets
- Continuous permission validation and backup integrity checks
- Secure Multi-tenant isolation and intelligently simple SLA-driven protection policies

Security isn't a feature – it's enforced at every level, automatically.

Workload Coverage: No App Left Behind

HYCU delivers the deepest and most complete native backup for Nutanix environments. Unlike retrofitted backup solutions that miss edge cases or require agents, HYCU is purpose-built for Nutanix – adding protection for every workload, consistently and without complexity.

Nutanix Workload Foundation:

- AHV and VMware hypervisor support
- Native integration with Prism and VM-level snapshot orchestration
- Support for legacy and next-gen apps, including DBs, VMs, containers, and more

HYCU Workload Protection:

- Agentless, app-aware backups with consistency groups
- File-level, VM-level, and app-specific restore workflows
- Support for databases, cloud-native apps, SaaS workloads, and Kubernetes
- Deep level protection across NDB, NC2, NUS, NKP, Volume Groups & More.

With Nutanix and HYCU, protection for all data is the priority – no matter where or how it runs.

Storage & Immutability: Isolated and Untouchable

Together, Nutanix and HYCU give you immutable, air-gapped protection – without adding complexity.

Ransomware recovery starts with making sure your backups can't be modified. Nutanix Unified Storage and HYCU combine to deliver tamper-resistant backups, isolated storage, and protection that's out of view to attackers.

Nutanix Storage and Immutability Features:

- Nutanix Objects Storage with native WORM (write-once-read-many) support
- Nutanix Data Lens for anomaly detection and ransomware pattern alerts
- Secure storage fabric across file, block, and object workloads

HYCU Immutability and Isolation:

- Immutable backups to customer-owned targets such as Nutanix Objects Storage, Amazon S3, Azure Blob Storage, Wasabi Hot Cloud Storage
- Ability to run on a dedicated Nutanix cluster, creating a virtual air gap
- No reliance on proprietary storage – full data control and freedom of movement
- Built-in backup validation to confirm recoverability after every backup

→ Backups are not only immutable – they're isolated and primed for recovery.

→ With Nutanix and HYCU, protection isn't stitched together – it's unified.

→ The entire platform is self-healing and secure.

→ No workloads are left behind, cyber resilience isn't just for VM's.

→ The data is locked down and hidden.

→ The entire solution is hardened, intelligent, and proven in production.

→ **That's what it means to be Always Protected.**

Always Observing

Full-spectrum visibility that detects threats early and enables clean-room investigations – even during active incidents.

In a cyber incident, speed and certainty matter. Nutanix and HYCU give organizations the tools to detect, monitor, and investigate threats in real time – across infrastructure, storage, and data protection. Together, they deliver unified observability, anomaly detection, and isolated forensic investigation – all while keeping operations online.

Platform Observability and Audit Control

Nutanix provides deep visibility and continuous risk posture monitoring – automating security operations from infrastructure to unstructured data.

From system-level telemetry to real-time analytics, Nutanix enables a proactive security stance with tools that identify vulnerabilities, enforce zero-trust policies, and audit interactions.

Nutanix Observability and Compliance Features:

- Unified dashboard for automated cyber operations, supporting Zero Trust Architecture (ZTA) and Defence-in-Depth initiatives
- Continuous risk assessment across workloads to detect vulnerabilities
- Nutanix Prism for real-time health, security, and configuration monitoring
- Data Lens for ransomware detection, permission auditing, and behaviour analytics on unstructured data
- Integrated audit trails for file events and user actions, correlated across clusters
- Continuous compliance monitoring with security baseline enforcement and alerting
- Native logging and SIEM integrations for live threat feeds and forensic traceability

Benefits: Nutanix gives teams the insight and automation they need to reduce risk, help meet compliance requirements, and respond quickly, with no third-party bolt-ons.

HYCU R-Shield: Anomaly Detection and Threat Hunting

HYCU extends observability into the backup layer – turning protection into a proactive security surface.

R-Shield brings intelligent, source-side scanning to every backup job, allowing early identification of malware, corruption, or compliance violations – before restoration even begins.

HYCU Anomaly Detection and Continuous Assurance Features:

- YARA-based threat hunting at the source – without moving or rehydrating data
- Change-rate and entropy analysis to detect hidden threats or silent attacks
- RTO assurance to verify backup recoverability and SLA compliance in real time
- Alerting to customer-owned SIEM systems for full visibility and sovereignty
- Workload discovery across Nutanix, SaaS, and cloud – surfacing unprotected assets
- Backup Posture management ensures continuous checks on backup infrastructure to check that best practices are being met
- Mechanisms in place to prevent the expiration of good backups due to policy definitions in the event of a ransomware/malware detection

Benefits: HYCU ensures backup environments aren't just passive – they're intelligent, self-monitoring, and audit-ready.

Clean-Room Forensics: Joint Isolation and Investigation

Nutanix Flow and HYCU R-Shield enable isolated, forensic-grade environments for secure investigation.

When a breach occurs, Nutanix and HYCU enable joint clean-room recovery and analysis – without exposing production data or networks.

Joint Forensic Capabilities:

- Nutanix Flow uses micro-segmentation to dynamically isolate workloads and investigation traffic
- HYCU enables recovery to a sandboxed zone – preserving clean, tamper-resistant snapshots for analysis
- Together, they provide a safe space for root cause investigation, threat validation, and evidence collection

Benefits: You get clarity without compromise – analyze incidents safely, contain threats quickly, and recover with confidence.

→ With Nutanix and HYCU, you're not just watching data – you're understanding risk, detecting anomalies, and enforcing compliance with zero-trust discipline. Whether it's monitoring infrastructure or scanning backups, every layer of your environment becomes observable, auditable, and protected.

→ **That's what it means to be Always Observing.**

Always Ready

Recovery isn't just about speed – it's about confidence. Nutanix and HYCU make sure you're ready to restore what you need, when you need it.

Modern resilience means knowing you can recover – not just hoping you can. Whether it's a full environment, a single database, or one user's files, Nutanix and HYCU give you the tools to recover quickly, smarter, and with zero guesswork.

Platform Performance and Cloud Mobility

Nutanix delivers high-performance storage and flexible hybrid options – so recovery is never constrained.

Recovery readiness starts with a platform that can respond as fast as the business demands. Nutanix provides a resilient, high-speed foundation with flexible deployment options – on-premises or in the cloud – so you can restore workloads where they make the most sense.

Nutanix Recovery and Performance Highlights:

- High-speed storage performance via Nutanix Unified Storage (NUS) solution, enabling low-latency restore from snapshots and backups
- Native snapshots and replication across Nutanix clusters for rapid local or DR site recovery
- Nutanix Cloud Clusters (NC2) for hybrid resilience – instantly spin up Nutanix environments in AWS or Azure
- Automated DR orchestration with built-in application awareness and replication control

Together, these capabilities provide fast access to the resources needed to bring applications back online – without waiting on infrastructure.

HYCU Recovery: Fast, Granular, and Automated

HYCU accelerates recovery with instant restores, application-aware automation, and full restore flexibility.

HYCU turns recovery from a manual process into a streamlined, policy-driven workflow – so whether you're restoring a single file or a full environment, you can act with precision and speed.

HYCU Recovery Capabilities:

- Instant restore of virtual machines, applications, or file shares directly from backups or native Nutanix snapshots
- Granular recovery of individual files, databases, application components, or user records – no full restores required
- Continuous validation to ensure every backup is production-ready and recoverable before it's needed
- Flexible recovery to Nutanix clusters, NC2 environments, or customer-owned cloud storage
- No agents or bloated, hard to manage proxies – recovery flows securely through HYCU's pre-hardened virtual appliance

With HYCU, there are no bottlenecks, no manual delays – just reliable, application-aware recovery.

Recovery Orchestration and Application-Centric Workflows

Together, Nutanix and HYCU enable intelligent, policy-based recovery that aligns with how your apps and teams operate.

Nutanix simplifies infrastructure recovery with built-in DR and snapshot orchestration. HYCU complements this with application-centric workflows and policy-driven automation.

Joint Orchestration Features:

- Recovery runbooks mapped to application dependencies and SLAs
- Automated, ordered recovery of multi-tier services and critical applications
- SLA-based targeting of the fastest recovery paths
- Fully integrated workflows across on-prem, NC2, and cloud-native environments

Whether recovering from ransomware, system failure, or accidental deletion, Nutanix and HYCU ensure that recovery is not only fast – it's deliberate and dependable.

The Bottom Line

→ With Nutanix and HYCU, recovery is no longer a reactive scramble – it's a tested, ready outcome.

→ The platform is fast.

→ The backups are proven.

→ The workflows are automated.

→ The result is recovery that's under your control.

→ **That's what it means to be Always Ready.**

Always Resilient, Together

Nutanix and HYCU deliver a unified approach to cyber resilience – from infrastructure to backup to recovery.

Today's organizations can't afford fragmented protection strategies. Cyber threats move fast. Recovery windows are shrinking. And operational complexity has become the enemy of security.

That's why Nutanix and HYCU work together to deliver a modern alternative – one that's built for resilience at every layer.

- **Protected** with hardened infrastructure, immutable storage, and agentless backup
- **Observing** with real-time audit trails, anomaly detection, active threat hunting , and clean-room investigation workflows
- **Ready** with instant recovery, flexible restore options, and continuous validation of your recovery plans allows recovery quickly with confidence.

This is not just integration. It's intentional design. Nutanix and HYCU bring together performance, protection, and simplicity – so you can protect what matters most, see issues before they cause problems, and recover the data that matters, where you want it.

**Cyber resilience doesn't have to be complex.
With Nutanix and HYCU, it's built in.**

Stay Protected: Achieve
Cyber Resilience With
HYCU & Nutanix