

# HYCU's Cyber Resilience Kit for Nutanix





#### **Step 1: Map Out Your Data Estate Beyond Nutanix**

# Identify your on-premises footprint, inside and complementary to Nutanix:

- Nutanix AHV
- · Nutanix Files
- · Nutanix Object Storage
- Nutanix NDB
- Nutanix Cloud Clusters (NC2)
- Nutanix Data Services for Kubernetes (NKP)

Why?

Ensuring each workload in Nutanix has immutable protection and rapid, consistent recovery is critical. Make sure you view the checklist below from the perspective of protecting all Nutanix services, not just AHV.

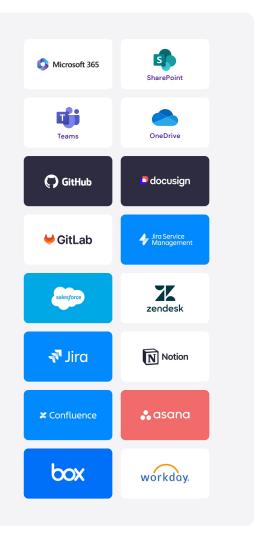


## Identify third-party applications and services used in and out of IT:

- Collaboration (Email, Chat, Conference, etc.)
- File Storage & Management
- CRM
- ERP Solutions
- Git Repositories
- Bug Tracking
- · Service Desk and Ticketing
- Knowledge Base
- Web Management (CMS)
- E-Signature & Document Signing
- Business Intelligence & Analytics
- HR (HCM/HRIS core suite)
- · Learning Management
- · Marketing Automation
- Billing, Invoicing, and Subscription Management
- · And many more

Why?

Attackers know many SaaS apps fly under IT's radar. That's why they target overlooked platforms first—not just Microsoft 365, but every service storing customer, employee, or financial data. Complete visibility and protection are non-negotiable.



Prism Security Central

### **Nutanix Data Protection & Resilience** Checklist

Identity, API & Privilege	<b>Ensuring Recovery</b>
Enable MFA for all Prism Central SSO providers.	Reduce Backup Attack Surface
Implement least privilege RBAC roles.	Run backup appliances on an up to date, security hardened Linux OS.
Use security certificate authentication for backup services.	Eliminate Windows servers from backup infrastructure.
Cluster & Hypervisor Hardening	Eliminate agents and cloud gateways wherever the backup product supports Nutanix APIs transport.
Apply all settings in the Nutanix Security Guide v6.7 (AHV & CVM hardening, STIG alignment).	Backup service must be DISA-STIG compliant.
Patch to an AOS/AHV build not listed in an active security advisory (check NXSA bulletins & CVEs).	Isolated network segmentation with encrypted data in transit/at-rest.
Enable Secure Boot, TPM 2.0, and data at rest encryption (software or SED) on every node.	Prevent backups from being deleted through the backup solution or directly on backup target.
Run NCC security-health checks weekly; export JSON to SIEM for trend analysis.	Prevent unauthorized access.
Anomaly Detection & Ransomware Scanning	Test and Validate Application- Centric Recovery
Implement anomaly detection and real-time alerting to SIEM/SOAR systems.	Use application-consistent snapshots for VMs.
Scan real data (not just metadata) for threats. Scan at the source and avoid delayed scans in a third-party cloud service.	Maintain at least one off platform, off site immutable copy (cloud S3, DR cluster, tape) with retention ≥ 14 days.
Restore and forensically analyze backups in a safe environment without impacting production or backups.	Ensure the use of Nutanix snapshots for fast recovery option.
Key Cyber Resilience Resources for Nutanix Admins  Nutanix Security Guide v7.0	Document and test <b>four recovery modes</b> each quarter:  1) High speed instant recovery (run VM from backup)  2) Clean room restore to isolated VLAN  3) Cross-hypervisor restore (AHV → other hypervisor)
NXSA Security Advisories Portal	4) Cloud restore (AHV → Azure/AWS)

#### **Recovering SaaS Data from Cyber Threats** Checklist

Gove	nance & Policy
	Publish a SaaS security standard that maps CIS Benchmarks / CSA CCM controls to each SaaS used.
	Maintain a live SaaS service inventory (owner, data category, residency, RTO/RPO, last BCP test).
Identity, API & Privilege	
	Single Sign On + Multi-Factor Authentication for every human and machine user.
	Enforce Just-in-time admin elevation.
	Rotate API tokens and OAuth app secrets.
Monitoring, Detection and Insider Threat Controls	
	Stream SaaS audit logs & CASB alerts (login, sharing, API, DLP) to SIEM within 5 minutes.
	Build a correlation rule: detect privilege escalation combined with data exfiltration within 24 hours, then automatically isolate the user and disable associated tokens.
	Spot anomalies at the application-level (bulk deletion, access management changes, etc.
Backup & Recovery	
	Schedule daily backups for each SaaS application in your environment (Define a minimum backup frequency based on the application).
	Store backups offsite in S3-compatible storage, independent of the primary SaaS applications. (ex. Nutanix Object Storage)
	Ensure backup copies are accessible in the event of an outage or cyber threat via offline exports.
	Ensure the backup system is running outside and detached from the primary SaaS applications.
	Enable immutability on the backup storage target in case of a cyber event. Backup storage site must meet residency requirements (if applicable).
	Backup requirements Incident response & recovery Develop and regularly update disaster recovery plans that include templates for different incident scenarios.
	Ensure these plans are comprehensive and tailored to organizational needs.



**Start Protecting** Your Entire Data **Estate Today** 

Try HYCU for Free

