Security in the hybrid cloud begins with a robust infrastructure foundation. This is where the industry leading solution from Nutanix not only provides operational and financial value, but also aids in improving security posture and preventing data breaches by supporting a defense-in-depth approach for hybrid cloud security.
DEFENSE AT EVERY LEVEL

Platform Security: Security is a foundational aspect of product design at Nutanix, starting with security hardening practices (like data-at-rest encryption, comprehensive access controls, etc.) built into the enterprise cloud platform. Industry best practices and government standards are incorporated into an automated configuration monitoring and self-healing process that supports compliance goals. Strict tests for common vulnerabilities and frequent patch releases minimize the risk of data breaches. Inconsistencies are logged and reverted to the baseline ensuring consistency of security configuration.

Application and Network Security: Nutanix Flow delivers advanced network security inside the data center, providing application visibility and protection from the spread of cyber threats like ransomware. Networks and applications can easily be segmented via a software-defined policy without any additional hardware or complex network configurations. Native network microsegmentation functionality provides a discovery, visualization, and policy enforcement model that simplifies and automates the application of granular network policy (microsegmentation) between VMs.

SecOps, Compliance, and Audit: Flow Security Central provides hybrid-cloud security posture visibility, policy management assistance, configuration audits, and compliance validation for Nutanix HCI. Security Central uses a collection of automated security audits to detect and fix infrastructure security vulnerabilities and configuration errors. Security admins can create automated policies to remediate vulnerabilities in real-time. Security Central also helps to validate the level of compliance with regulatory guidelines such as PCI-DSS, HIPAA, NIST, etc., delivering an always-on security compliance solution.

Prevent, Detect, and Recover: There is no single action, software solution, or security control that can completely safeguard your organization from the threats of malware and ransomware. The best solution is a multi-layered approach, commonly called a “defense in depth” strategy. To minimize both your operational and financial costs, your comprehensive plan should include all the Nutanix built-in capabilities working alongside controls and safeguards that may already exist in your datacenter.
TRUST NUTANIX AS PART OF YOUR CYBER DEFENSE STRATEGY

HCI Platform
- Self-healing security configuration baseline
- Storage snapshots and recovery points
- Data protection, replication, and runbook automation
- FIPS 140-2 validated data-at-rest encryption
- Data plane & control plane segmentation
- Native virtualization - built for security

Patching and Upgrades
- “One-click” CVE patching, platform upgrades, and life cycle management
- Firmware and BIOS upgrade management

Management and Automation
- Role-Based Access Control (RBAC)
- Identity and Access Management
- Resource analytics, insights, and anomaly detection
- Codeless automation and event triggers
- Application blueprints and automation to ensure consistent policy application

Networking and Security
- Network and application segmentation
- Application and network visibility
- Deep packet inspection and threat intelligence partner integrations
- Policy and event logging
- Security Compliance and Audit Tools

Storage Services
- File type blocking policies
- File activity anomaly detection
- ICAP support for antivirus integration
- Immutable WORM policy support

Backup, Business Continuity, and Disaster Recovery
- Native replication and data protection
- Archive and backup solution for secondary storage
- Cloud Disaster-Recovery-as-a-Service