Backup and Cyberstorage with Nutanix Unified Storage

Data is essential for organizations and modern applications, enabling them to make strategic, data-driven decisions about products, services, and overall business direction. Ensuring data availability is crucial to keeping operations and services up and running smoothly.

Did you know that every 11 seconds, an organization is hit with a ransomware attack? Let's apply that to the real world now. Imagine a healthcare organization suddenly unable to access critical patient records or a bank cut off from its customers' financial data.

Despite heavy investments in cyber resilience tools, systems updates, and strict internet controls, organizations of all sizes remain vulnerable. Cybercriminals are becoming more sophisticated and relentless, exploiting even the smallest vulnerabilities. As a result, it's no longer a question of if an attack will happen, but when.

Immutable Storage:
A Foundation for Resilient Data Protection

In today's digital landscape, protecting backup data from cyberattacks, especially ransomware, is essential. Immutable storage, particularly WORM-enabled S3 Object Storage, has become an indispensable technology for organizations aiming to strengthen their backup and recovery strategy.

WORM technology enforces data immutability, meaning that once data is stored, it cannot be modified or deleted for a designated retention period, even by administrators. This immutability ensures data integrity, keeping backup data unaltered and reliable for recovery in case of data loss or corruption.

In the case of a ransomware attack, immutability acts as a safeguard by preventing any unauthorized modification or deletion during the retention period. This fortified security layer gives organizations confidence that their backups remain intact and untouchable by malicious actors, enhancing their resilience against data compromise.

Nutanix offers robust solutions in this space with its WORM-enabled Object Storage, empowering businesses to implement secure, immutable storage for backups. By leveraging Nutanix's solution, organizations can build a resilient backup strategy, mitigating the risks of data tampering and ensuring the integrity of their critical assets.

Key Benefits

- Tamper-proof backups with Nutanix WORM-enabled Object Storage to secure data against threats.

- End-to-end encryption safeguards your data both during transmission and while stored on Nutanix Objects.

- Air-gapped architecture with network segmentation for management and data access reduces ransomware risks.

- Rapid, granular recovery minimizes downtime and allows point-in-time recovery options. Restore data precisely to a specific moment without impacting your production environment.

- Tighter integration with backup apps and granular access control allows for secure task delegation and resource access.

- Nutanix Data Lens provides an additional layer of protection by proactively identifying and mitigating data theft and compromise attempts within Nutanix Objects

Protecting Backup Data Through Isolation

Nutanix Objects, with built-in support for network segmentation to isolate external connections from the internal storage network, provides an ideal platform for implementing isolated backups. By creating a dedicated Nutanix Objects cluster specifically for backups, organizations can effectively air gap their backup data from the production network. This ensures that even if the production environment is compromised, the isolated backup data remains out of reach for malicious actors.

Nutanix Objects also allows granular RBAC, allowing organizations to restrict access to the backup Nutanix Objects cluster to only authorized backup servers and administrators. This minimizes the risk of unauthorized data modification, deletion, or exfiltration.

In addition to network-level isolation, Nutanix Objects can be deployed in physically separate locations from the primary datacenter, adding another layer of protection against physical disasters or targeted attacks. By combining the immutability of WORM-enabled S3 Object Storage with the isolation and access control capabilities of Nutanix Objects, organizations can establish a robust and secure backup and recovery strategy.

Beyond Recovery: Nutanix Data Lens' Proactive Ransomware Defense

Nutanix Data Lens (NDL) is a cloud-based cyber resilience and data insights solution that proactively detects and helps block known and potential threats. NDL offers integrated ransomware resilience by using active defense technology with rapid detection and blocking. It leverages signature-based detection to identify known threats and behavior-based analysis to detect unknown threats exhibiting suspicious behavior. NDL can detect and block known threats within the first 20 minutes of an event, offering faster protection than manual detection and blocking.

NDL offers a ransomware "anti-warranty" that focuses on proactive measures and damage containment within minutes, unlike traditional ransomware warranties. These conventional warranties only guarantee recovery or coverage of eligible recovery expenses without SLAs on detection and mitigation. NDL aims to contain damage from a ransomware attack within 10 minutes – far quicker than recovery warranties, which might take days, weeks, or months to pay out for recovery costs.

In an evolving threat landscape, Nutanix offers comprehensive solutions to protect critical data with WORM-enabled, air-gapped backups and rapid threat detection. Nutanix Objects and NDL combine immutability, access controls, and proactive ransomware defenses to contain threats swiftly. Get started today with Nutanix Unified storage or take it for a spin with a Test Drive.

Learn more https://www.nutanix.com/solutions/unified-storage

NUTANIX