NEXSAN

Beyond Traditional Backups

White Paper

Exploring Advanced Data Protection and Recovery Techniques

Introduction

Unity™ Unified Storage

NV10000

NV6000

In today's digital economy, data is the lifeblood of your business and must be protected. The escalating sophistication of cyber threats, particularly ransomware, underscores the imperative for robust data protection measures on multiple levels. The Nexsan Unity™ NV-Series emerges as a cutting edge solution, offering a comprehensive suite of advanced data protection features designed to protect enterprises from data loss, corruption, unauthorized access, and cyber-attacks. This document delves into the strategic importance of data protection for backups, leveraging the Unity NV-Series' innovative capabilities, such as immutable snapshots, S3 object-locking, and the Unbreakable Backup with Assureon® technology.

The digital threat landscape is evolving with alarming velocity, evidenced by the staggering statistic from Sophos' "The State of Ransomware 2023" report[1], which indicates that 66% of organizations were impacted by ransomware in 2023 alone. The vulnerability of backup systems is particularly concerning, as highlighted by the attack on CloudNordic, where ransomware encryption incapacitated both primary and secondary backup systems, leading to a total loss of data accessibility[2]. Many attacks target the backups to undermine an organization's ability to recover without surrendering to ransom demands. This strategic targeting of backups and cyber insurance's prohibitive costs and limitations amplify the urgency for impenetrable backup solutions.

Within this context, this document will explore the options with the Unity NV-Series in fortifying backup infrastructures against these pervasive threats. By examining the capabilities of formative options for backup protection, this paper aims to outline immutable backup options and provide information for those considering their data protection strategies in the face of the growing threat of ransomware, cyber-attacks, and other digital dangers.

The Critical Role of Data Protection in Today's Businesses

In the current digital landscape, the impact of data breaches and losses can be devastating, leading to significant financial impact, damage to reputation, legal repercussions, and even the complete dissolution of the enterprise. It's essential for businesses to place a strong emphasis on sophisticated data protection strategies to avoid these dire outcomes.

No enterprise is immune to threats or attacks. The reality is that data, regardless of company size, is of the utmost importance and cannot be compromised. More importantly, the firm with fewer resources is often the target of an attack because these digital bandits know they have limited resources to respond and may, in fact, choose to pay a ransom.

With the market flooded with various add-on security solutions, it's worth considering integrating data protection directly into the foundational storage solutions your business relies on daily. This approach ensures a more seamless and robust defense mechanism and can provide greater protection than software solutions alone.

A comprehensive toolkit for safeguarding your data is non-negotiable. Remember, your backup system is often your last line of defense in the fight against data breaches. It's crucial to have a failsafe-tested backup strategy in place. Many firms who have not hardened their backup protection wind up paying much more in ransomware than they would have insuring their ability to recover from the attack.

Challenges in Data Security and Protection

The challenge of ensuring data security is universal, yet it manifests differently across enterprises of varying sizes. Both large corporations and small to medium-sized enterprises (SMEs) grapple with the escalating complexity of cyber threats, the maze of regulatory compliance requirements, and the rapid expansion of data volumes, all adding additional challenges to consider.

Large enterprises face numerous challenges. The sheer volume of data spread across diverse departments and geographic locations introduces data management and security complexity. The valuable data these organizations hold makes them a constant target for sophisticated cyber threats. Legacy systems pose additional challenges, as integrating and updating them requires significant effort and resources. Moreover, with a larger employee base, the risk of insider threats, whether intentional or accidental, increases, necessitating stringent access controls and vigilant monitoring.

Conversely, SMEs face their own unique set of challenges, primarily rooted in limited resources. Budget constraints often lead to underinvestment in cutting-edge cybersecurity tools and skilled personnel. Many SMEs rely on IT generalists or external vendors for their data protection needs, which might not always offer the level of specialized security required. Additionally, limited funds mean that training on cybersecurity awareness and user-targeted threats is often insufficient, leaving employees more vulnerable to attacks. Furthermore, SMEs typically have less robust disaster recovery and business continuity plans, making it harder to bounce back from data breaches or losses.

The market's response to these challenges has been an overwhelming array of add-on security products. However, a more integrated approach, embedding data protection directly into the essential storage solutions that businesses rely on daily, can offer a more effective defense. A robust, comprehensive set of data protection tools is indispensable, with backup systems serving as the critical last line of defense.

This backdrop of diverse challenges across different business scales underscores the need for a resilient and adaptable approach to data protection. It also highlights the critical role of solutions like those offered by the Nexsan Unity NV-Series in safeguarding the digital assets of modern enterprises.

Overview of
Nexsan Unity NV-Series

The Unity NV-Series is a multifaceted storage solution that expertly blends high-performance, scalability, and cutting-edge data protection features. This makes it ideal for a wide range of enterprise environments, catering to the varying needs of different organizations.

Unity NV6000: Designed with Small and Medium-sized Enterprises (SMEs) in mind, the NV6000 is perfect for efficiently handling scaling applications and mixed workloads. It's the go-to choice for businesses seeking efficient, unified storage capabilities without compromising performance or security.

Unity NV10000: The NV10000 is for medium to large enterprises, leveraging All-Flash NVMe technology to deliver exceptional performance. With data transfer speeds reaching up to 20GB/s and 500K IOPs, alongside a massive storage capacity of up to 9.6PB, it's engineered for businesses that demand the utmost speed and volume.

What sets the Unity NV-Series apart is its comprehensive software licensing. Features integral to Unity include object store capabilities, immutable snapshots, in-line compression, data integrity checks, and FASTier™ Caching, an industry-leading caching process.

The Unity NV-Series provides data protection options so organizations can choose what works best for their needs. Each solution plays a crucial role in ensuring data security and compliance, offering an additional and final layer of defense against the ever-present threat of cyberattacks and unauthorized access. Unity is also positioned as a formidable protection against malware and accidental data loss.

Immutable Snapshots: The Backbone of Data Recovery

Immutable snapshots are essentially point-in-time copies of data set in digital stone; they cannot be changed or deleted. This feature turns snapshots into reliable recovery points, safeguarding against data corruption or loss.

Understanding Immutable Snapshots **Instant Data Protection**: These snapshots offer immediate protection by capturing data at specific moments, creating a "freeze-frame" of your information that remains untouchable.

- **Locked and Secure:** Once set, immutable snapshots are locked down, immune to changes or deletion for a predetermined duration, ensuring the data snapshot and its pool are protected.
- **User Control:** Whether through Unity's graphical user interface (GUI) or command-line interface (CLI), users have the power to create or convert existing snapshots to immutable status, offering flexibility and control over data protection.

Why Immutable Snapshots Are Essential

- Shield Against Tampering: In an age where ransomware seeks to undermine data integrity by targeting and deleting snapshots, immutable snapshots stand indestructible, offering a robust defense against both intentional and accidental data destruction.
- Rapid Restoration: Whether it's making data immediately accessible to applications or rolling back to a preferred snapshot, immutable snapshots enable quick data recovery, minimizing downtime.

How Immutable Snapshots Function

- **Snapshot Creation:** Users can initiate snapshots either automatically or manually, capturing the exact state of data at a precise moment.
- **Efficient Snapshot Management:** Through setting comprehensive policies for their creation, retention, and eventual deletion, snapshots are managed efficiently to optimize storage utilization.

Practical Applications of Immutable Snapshots

- **Data Recovery:** They enable swift data restoration to a known-good state, invaluable in accidental deletions or data corruption scenarios.
- **Version Control:** By maintaining multiple data versions, immutable snapshots facilitate easy rollback to previous states whenever necessary.
- This allows for rapid recovery and getting back to business in minutes. Downtime can exceed the cost of a robust solution in hard dollars and cause a loss of customer confidence.

Advantages of Unity Immutable Snapshots

Utilizing immutable snapshots on Unity simplifies data recovery through rollbacks or making snapshots accessible to applications but also minimizes downtime, ensuring business continuity. Integrating automated data integrity checks via pool scrub mechanisms further enhances reliability by detecting and correcting checksum errors.

Ransomware Recovery with Immutable Snapshots

Ransomware recovery using immutable snapshots centers on leveraging these snapshots' inherent resilience and tamper-proof nature to restore data to its pre-attack state. The strategy begins with preemptive measures, ensuring that immutable snapshots are regularly created and maintained as part of a comprehensive data protection plan. This setup creates a series of unalterable data points that serve as a failsafe in the event of an attack.

Upon identifying a ransomware incursion, the immediate steps involve isolating affected systems to halt the spread of the malware and conducting a thorough assessment to determine the extent of the impact. Following the removal of the ransomware threat from the systems, the recovery phase taps into the immutable snapshots, which are immune to encryption or alteration by ransomware, enabling the reinstatement of uncompromised backup data.

S3 Object-Locking: Enhancing Data Security in the Unity NV-Series

Introduction to S3 Object-Locking

S3 Object-locking is a powerful feature designed to enhance data protection by preventing the deletion or alteration of object versions for a specified period. This capability, integral to the Unity NV-Series, ensures data remains immutable, Write-Once Read-Many (WORM), safeguarding against ransomware and accidental changes. Unity's implementation of S3 object-locking stands out for its scalability, catering to clients of all sizes from smaller deployments upwards.

Implementation in Unity NV-Series

- **Configuration Settings:** Users can define object-locking policies within the Unity NV-Series, including retention periods and legal holds, to ensure data remains secure and unaltered.
- **Enabling Object-Lock on Data:** Specific datasets can be protected with object-locking, shielding them from unauthorized alterations. Unity NV-Series leverage Object Locking, enforcing WORM immutability to protect versioned objects from being deleted. Duration-based and indefinite legal hold retentions are also supported by object locking.
- **Immutable Data Integrity:** With S3 object-locking enabled, not even the root user can modify or delete a protected object version, ensuring the data's integrity throughout its retention period and protecting backups from any form of tampering.

Use Cases for S3 Object-Locking

- **Compliance and Legal Holds:** Essential for maintaining data in an unchangeable state to meet stringent legal and regulatory standards.
- **Ransomware Protection:** Provides a solid defense against ransomware by rendering critical data immutable and invulnerable to encryption or deletion.
- **Data Retention Enforcement:** Allows organizations to enforce data retention policies by locking data for predetermined periods, ensuring compliance and data preservation.

Benefits of S3 Object-Locking

The inclusion of S3 object-locking in the Unity NV-Series adds a crucial layer of security, ensuring data remains protected from cyber threats and compliant with regulatory requirements. This feature is particularly beneficial for enterprises looking for a versatile storage solution capable of managing a range of workloads, combining the efficiency of SSDs for performance and HDDs for capacity within a cost-effective framework.

Challenges and Best Practices

While S3 object-locking significantly enhances data security, its implementation requires meticulous planning to ensure data remains accessible when needed without compromising on protection and compliance. Unity's versatile approach to storage, combining traditional and object storage capabilities within a single system, makes it an ideal solution for organizations seeking a balanced, cost-effective storage solution.

Why Unity Stands Out for S3 Object Locking

Unity's NV-Series is uniquely positioned to offer S3 object-locking due to its unified storage platform, which can accommodate file, block, and S3 object store needs without requiring separate systems. This flexibility, combined with the series' cost-effective entry point, makes Unity an attractive solution for businesses needing a small to medium-sized S3 object-store.

Ransomware Recovery with Object Locking

Ransomware recovery with object locking involves a proactive and reactive strategy to safeguard and restore data. Initially, the focus is on prevention through best practices like enabling versioning and object lock for data immutability, coupled with regular backup verification. Upon detecting a ransomware attack, immediate action is taken to isolate the threat and assess the damage, followed by the eradication of the ransomware from the system to prevent further spread.

The core of the recovery process leverages the immutable backups and versioned objects, allowing for the restoration of data to a pre-attack state without succumbing to ransom demands. A post-recovery analysis complements this to identify security gaps and strengthen defenses against future attacks. Effective communication with stakeholders throughout the process ensures a coordinated and informed approach to navigating the challenges of ransomware recovery.

Unity + Assureon
Delivering Unbreakable Backup Solutions

Introduction to Unbreakable Backup

The combination of Unity and Assureon offers the pinnacle of data protection with its Unbreakable Backup solution. Assureon, when integrated with Unity, provides immutable storage, ensuring that data remains unchanged and secure from tampering. This powerful duo is essential for preserving vital information and adhering to regulatory compliance standards, offering an unmatched level of protection.

How it Works

- **Immutable WORM Storage:** Assureon offers immutable Write-Once Read-Many (WORM) storage, complete with stringent data integrity checks, file locking, and restricted access controls. It keeps at least two copies of your data, ensuring redundancy and security.
- **Rigorous Security Measures:** Assureon creates a secure, impenetrable backup layer with its self-healing capabilities and policy-based governance. Data is locked down and made immutable, with no access paths available, not even for administrators, until the policy's expiration.
- **Flexible Backup Solutions:** Assureon allows for a tiered backup approach, maintaining backups on both the fast-access Unity and secure Assureon tiers. This setup facilitates quick restores and efficient capacity management, ensuring immutable backups are always accessible, especially in disaster recovery scenarios.
- **Assureon's Lockdown Mechanism:** At the core of Assureon's prowess is the OS lockdown, rendering the system impenetrable to external modifications and programs. With read-only access governed by NTFS permissions and firewall protection, this system ensures that end-users interact with data without altering its fundamental state.
- **Tamper-Resistant Design:** Constructed with multiple layers of defense, Assureon is a strong defense against illicit attempts at file modification. Even in rare instances of data corruption, its redundant setup seamlessly replaces compromised files, preserving data integrity without interrupting business operations.
- **Dual-Hashing Immutability:** The innovative dual-hashing process involving a 128-bit MD5 and a 160-bit SHA-1 hash for each file, coupled with serialization, ensures that every data asset managed by Assureon is unalterable, authenticated, and easily retrievable, marked by a globally unique identifier only Assureon can provide.

Key Features of Unbreakable Backup

- **Data Integrity and Authenticity:** Assureon ensures data immutability with features like file fingerprinting, time/date stamps, serialization, and extensive auditing capabilities.
- **Enhanced Data Security:** With multiple secure copies and tightly controlled access, Assureon provides robust protection against data loss and unauthorized access and offers strong defenses against ransomware..
- **Compliance and Recovery:** The solution supports compliance with various regulatory standards and enables rapid data recovery, minimizing downtime and ensuring business continuity.
- **WORM Emulation and Metadata Binding:** Assets are shielded under WORM emulation, guaranteeing their state until the prescribed backup expiration date. This, combined with the secure attachment of metadata to digital assets, fortifies data against any unauthorized deletions or changes, safeguarding its integrity.
- **Human-Operated Deletion Control:** Assureon elevates data lifecycle governance by mandating human confirmation for file deletion at the end of retention periods, putting critical checks in place against automated misdeeds, and ensuring conscious data management.

Use Cases for Unbreakable Backup

- **Critical Infrastructure Security:** The immutable and restrictive nature of the Unity and Assureon combination serves as a robust foundation for infrastructure demanding uncompromised security and data integrity, such as governmental and financial institutions.
- **Advanced Compliance Readiness:** With features designed to uphold stringent regulatory standards, organizations find Unbreakable Backup an ally for compliance without compromising data accessibility and flexibility.
- **Long-Term Data Archival:** Ideal for the long-term preservation of critical data, maintaining its integrity over extended periods.

Advantages of Unbreakable Backup

With Assureon paired with Unity, Unbreakable Backup sets the gold standard in data protection, providing data integrity, robust security, and comprehensive compliance across all levels of enterprise data. Assureon's immutable Write-Once Read-Many (WORM) storage, coupled with stringent security measures like file locking and restricted access controls, guarantees data remains unchanged and resistant to tampering. Assureon's patented lockdown mechanisms and tamper-resistant design, including dual-hashing immutability and human-operated deletion control, further fortify data against unauthorized modifications or deletions. This comprehensive approach ensures compliance with regulatory standards and enhances data security, making it an indispensable asset for critical infrastructure security, ultimate backup protection, advanced compliance readiness, and long-term data archival needs.

Implementation Considerations

Deploying Assureon alongside Unity requires a thorough understanding of the organization's specific security and compliance requirements, ensuring seamless integration into the existing data protection framework. Whether implemented on-premises, in the cloud, or as a hybrid, the flexibility of the Assureon Software Edition ensures that enterprise data remains untouchable yet fully accessible under all circumstances.

Ransomware Recovery from Unbreakable Backup

In the event of a ransomware attack, the Unbreakable Backup solution offers a streamlined ransomware recovery process. First and foremost, the locked-down nature of Assureon® ensures that backup data is safeguarded from unauthorized modifications, even with administrator-level access. Additionally, the solution utilizes advanced techniques such as immutable file fingerprinting and serialization, guaranteeing the authenticity and integrity of backup data. This means that even if ransomware manages to encrypt or tamper with files, the original, unaltered versions remain securely preserved within the backup repository.

To expedite recovery efforts, the Unbreakable Backup solution offers various recovery options tailored to the specific needs of the organization. For instance, organizations can utilize shortcut restoration, which allows for the rapid restoration of data pointers, enabling immediate access to critical files without the need for lengthy data transfer processes. Alternatively, the solution's patented technology can provide a virtual representation of the original file structure, enabling users to access data as though it were on a local volume, thereby minimizing downtime and ensuring business continuity.

Comparative Analysis

In data protection, the Nexsan Unity NV-Series stands out with its multifaceted approach, offering solutions like immutable snapshots, S3 object-locking, and the Unbreakable Backup with the combination of Unity and Assureon. Each method is foundational in protecting data against ever-changing ransomware and cyber-attack threats. Yet, they differ in application and functionality, making a comparative analysis essential for organizations tailoring their data protection strategies.

Immutable snapshots, for instance, provide a point-in-time, unalterable record of data, serving as a robust defense mechanism against data tampering and loss. These snapshots are particularly valuable for rapid data recovery, enabling organizations to revert to a secure state in the event of corruption or malicious attacks. The inherent immutability of these snapshots ensures that critical data remains intact, even in the face of sophisticated ransomware that targets backup data for encryption.

On the other hand, S3 object-locking offers a layer of protection that complements immutable snapshots by preventing the deletion or alteration of data objects for a specified period. This feature is instrumental in enforcing compliance and legal holds, ensuring that data remains unchangeable and accessible, adhering to stringent regulatory standards. S3 object-locking protects against ransomware, securing data in a Write-Once Read-Many (WORM) format that renders critical information invulnerable to unauthorized changes.

The synergy of Unity and Assureon creates the Unbreakable Backup, elevating data protection to new heights. This combination harnesses Assureon's immutable WORM storage capabilities with Unity's advanced storage solutions, providing a comprehensive backup system that is not only resistant to tampering but also equipped with self-healing and policy-based governance features. The Unbreakable Backup solution ensures data integrity, enhances security, and supports rapid recovery. It is an indispensable asset for sectors with high security demands, compliance regulations, and organizations prioritizing the preservation of critical data and assets for the long term.

In summary, while immutable snapshots offer immediate and efficient data recovery options, S3 object-locking provides an additional security layer by ensuring data immutability over time. By combining the strengths of Unity and Assureon, the Unbreakable Backup emerges as the safest option available. It offers unparalleled protection to ensure data security, compliance, integrity, and swift recovery, making it the optimal choice for organizations seeking the highest level of defense in their data protection strategies against evolving threats in the digital realm.

Limitations and Considerations

While the immutable data storage options we have discussed are a cornerstone of data recovery within the Unity NV-Series, it's crucial to recognize that they are not standalone solutions for comprehensive cybersecurity strategies. Instead, they are integral components of a broader, more holistic approach to ensuring complete data protection and recovery readiness in the face of potential emergencies.

Summary

Amid escalating cyber threats, particularly ransomware, the critical need for robust data protection strategies in today's digital economy is evident. The Nexsan Unity NV-Series emerges as a leading solution with its suite of advanced features, including immutable snapshots, S3 object-locking, and Unbreakable Backup with Assureon technology, all designed to shield enterprises from data loss, corruption, unauthorized access, and ransomware attacks. The importance of securing backup systems is underscored by incidents like the ransomware attack on CloudNordic1, which rendered both primary and secondary backups inaccessible.

Regardless of size, enterprises face significant challenges in securing their data amidst the growing complexity of cyber threats, regulatory demands, and increasing data volumes. Integrating data protection directly into foundational storage solutions is proposed as a more practical approach than relying on standalone security products. The Unity NV-Series is a versatile and resilient solution, providing flexibility and options. Should the need arise, a comprehensive, failproof backup strategy is recommended as a vital defense against potential data loss and ransomware recovery.

1 Sophos. (2023, May). The State of Ransomware 2023. *Sophos.com*.

2 Lyons, J. (2023, August 23). Criminals go full Viking on CloudNordic, wipe all servers and customer data. The Register. https://www.theregister.com/2023/08/23/ransomware_wipes_cloudnordic/