

2027-28 DCIG TOP 3 CYBER RESILIENT GPBAS

UP TO 10PB HYBRID NAS EDITION

By

Jerome M. Wendt, Principal Analyst

Table of Contents

3 Cyber Resilience Becomes a Primary General Purpose Backup Appliance Selection Criterion

3 Five Considerations for Selecting Cyber Resilient GPBAs as Backup Targets

4 Differentiating between GPBAs and PBBAs

4 Three Technology Trends Shaping Hybrid NAS GPBA Selection

- 4 Trend #1: Hybrid NAS GPBAs Balance Cost and Performance
- 5 Trend #2: Multiple Forms of Immutability Becoming Increasingly Important
- 5 Trend #3: Air-Gapping and Isolation Extend Backup Protection

6 Common Features Across the Seven Evaluated Cyber Resilient Up to 10PB Hybrid NAS GPBAs

- 7 Table #1: Common Features Across Seven Evaluated Hybrid NAS Backup Appliances

8 Similarities and Differentiators between the 2027-28 DCIG TOP 3 Cyber Resilient Up to 10PB Hybrid NAS GPBAs

- 8 Multiple Immutability Technologies Strengthen Backup Protection
- 9 Cyber-Resilience Controls Extend Beyond Immutability
- 9 Storage Architectures Offer Different Performance and Capacity Options
- 9 Backup Application Interoperability Influences Appliance Selection
- 9 Replication Options Support Different Recovery Strategies
- 9 Enterprise Management and Support Simplify Backup Operation

10 2027-28 DCIG TOP Cyber Resilient 3 Up to 10PB Hybrid NAS GPBAs

- 10 Nexsan Unity NV6000
- 11 StoneFly USO XD-Series
- 12 TrueNAS H30

12 Cyber Resilient GPBAs — Up to 10PB Hybrid NAS Edition Inclusion Criteria

13 DCIG Disclosures

© 2026 DCIG, LLC. All rights reserved.

Cyber Resilient GPBAs // Up to 10PB Hybrid NAS Edition



SOLUTIONS EVALUATED:

1. Nexsan Unity NV4000
2. Nexsan Unity NV6000
3. QNAP ES1686dc R2
4. StoneFly USO XD-Series
5. Synology SA6400
6. Synology HD6500
7. TrueNAS H30

CYBER RESILIENT GPBA FEATURES EVALUATED:

- APIs/network protocols
- Cyber & data resilience
- Hardware configuration
- Management
- Storage optimization
- Technical support

Cyber Resilience Becomes a Primary General Purpose Backup Appliance Selection Criterion

Organizations have historically evaluated network-attached storage (NAS) appliances used as general purpose backup appliances (GPBAs) based on four criteria. These include capacity, performance, price, and ease of deployment and management. These criteria remain important, but the growing threat of ransomware has changed how organizations evaluate backup storage. They must now consider whether their backup appliances can protect recovery data when attackers compromise their IT infrastructure.

Ransomware attackers increasingly target backup environments before encrypting or deleting production data. They compromise backup administrator credentials, change retention policies, delete backup copies, or disable replication. These actions can prevent organizations from recovering critical applications and data, despite earlier reports of successful backups.

Consequently, organizations must evaluate NAS backup appliances based on their ability to preserve recoverable data, not simply store it. This shift places greater emphasis on cyber-resilience capabilities such as immutable snapshots, write-once-read-many (WORM) retention, air-gapped storage, access controls, and replication. These technologies help organizations preserve trustworthy recovery points despite malicious or accidental administrative actions.

Five Considerations for Selecting Cyber Resilient GPBAs

Organizations should now evaluate GPBAs against five primary considerations:

1. ***Cyber resilience and recoverability.*** Appliances should protect backup data against unauthorized modification or deletion while preserving recovery points organizations can use following a ransomware attack.
2. ***Backup and restore performance.*** Appliances must support sustained backup ingest rates, multiple concurrent backup streams, and sufficiently fast restores to meet organizational recovery objectives.
3. ***Capacity and storage economics.*** Appliances should accommodate growing backup volumes and retention requirements. Organizations must balance these requirements against acquisition costs, storage efficiency, expansion options, and ongoing operating expenses.
4. ***Management simplicity and backup application compatibility.*** Appliances should integrate with existing backup applications and support required NAS protocols. They should also offer deployment wizards or web GUIs that simplify routine storage administration, monitoring, and recovery operations.
5. ***Explicit provider positioning and support for backup and recovery workloads.*** Organizations should consider whether providers actively market, configure, document, and support their NAS appliances for enterprise backup and recovery use cases.

Regarding this fifth point, a storage provider explicitly positioning its NAS appliance for the backup use case may seem trivial. All enterprise NAS appliances support NFS and SMB file protocols and organizations can use any of them as backup targets.

However, supporting these protocols does not necessarily mean an appliance has been optimized or tested for sustained backup workloads. Backup environments impose distinct requirements involving concurrent data streams, prolonged write activity, retention management, data integrity, and large-scale recovery operations.

© 2026 DCIG, LLC. All rights reserved.

Providers that explicitly position their NAS appliances as backup targets may better address these requirements. They may document supported backup applications, publish recommended configurations, and provide technical guidance specific to backup and recovery. Their support staff may also possess greater familiarity with troubleshooting backup ingest, restore performance, and application integration issues.

Organizations cannot automatically assume that backup-target positioning guarantees these capabilities. However, it does increase the likelihood they support backup applications, available certifications, recommended configurations, and will provide technical support commitments.

Organizations increasingly prioritize hybrid storage architectures, multiple immutability technologies, and air-gapping capabilities when evaluating GPBAs.

Differentiating between GPBAs and PPBAs

DCIG elected to create two separate sets of research in its evaluation of appliances that support networked attached storage (NAS) interfaces. In this research, DCIG only evaluated those NAS appliances that do not offer its own data protection optimized protocol.

Purpose-built backup appliances (PBBAs) historically differentiated themselves from GPBAs by compressing and deduplicating data. However, many GPBAs now also compress and deduplicate data. As such, this feature no longer serves as a meaningful differentiator between GPBAs and PBBAs.

Support for data protection optimized protocols do, however, provide a meaningful differentiator between PBBAs and GPBAs. Installed on the backup client or media server, data protection optimized protocols compress and/or deduplicate backup data before transferring it.

Both enterprise data protection software and PBBA providers offer data protection optimized proto¬cols. The data protection optimized protocols offered by enterprise data protection software providers often work PBBAs and may work with GPBAs.

When deploying them, these data protection optimized protocols typically recognize and interact with the PBBAs and GPBAs they support. Data protection optimized protocols offered by the PBBA providers only work with their PBBAs. None of the GPBA models examined in this research support a data protection optimized protocol offered by the storage provider. However, some evaluated GPBA models support data protection optimized protocols offered by data protection software providers.

Three Technology Trends Shaping Hybrid NAS GPBA Selection

Three emerging trends influence how organizations select GPBAs for cyber resilience and recovery. Organizations must balance storage performance and cost while strengthening protection against ransomware and unauthorized data deletion. They increasingly prioritize hybrid storage architectures, multiple immutability technologies, and air-gapping capabilities when evaluating GPBAs.

Trend #1: Hybrid NAS GPBAs Balance Cost and Performance

Hybrid GPBAs combine solid-state drives (SSDs) with hard disk drives (HDDs) to balance performance, capacity, and cost. SSDs can accelerate frequently accessed data and storage operations, while HDDs provide economical capacity for retaining backup data.

Hybrid GPBAs have become a practical choice as SSD supply constraints and costs may persist well beyond 2026. Micron's FQ4 2026 earnings projected that DRAM and NAND flash supply-demand conditions would remain constrained through 2027 and 2028.[i]

© 2026 DCIG, LLC. All rights reserved.

Other forecasts call for continuing price increases for server DRAM, NAND flash, and enterprise SSDs of ten percent or more.[ii]

These outlooks reinforce the economic appeal of hybrid NAS architectures. Organizations can use SSDs to accelerate backup and recovery operations while relying on lower-cost HDDs for bulk backup storage. Hybrid NAS architectures offer one option by concentrating flash resources where they provide the greatest performance benefits.

The forecasts for constrained DRAM and NAND flash supply coupled with continuing price increases for flash and SSDs reinforce the economic appeal of hybrid NAS architectures.

Hybrid architecture uses flash caching, automated tiering, and SSD-based metadata acceleration to improve storage responsiveness. These technologies can accelerate backup ingest and restore operations by reducing HDD bottlenecks. Their effectiveness depends on workload characteristics and implementation.

Organizations must balance backup ingest speeds, recovery objectives, and expanding retention requirements against storage economics. Hybrid GPBAs offer flexibility to accommodate changing demands without relying exclusively on costly flash storage. This approach can help control costs while maintaining recovery performance.

Trend #2: Multiple Forms of Immutability Become Increasingly Important

GPBAs can offer multiple forms of immutability to protect backup data against unauthorized modification or deletion. Immutable snapshots preserve point-in-time recovery copies, while WORM file retention prevents changes during specified retention periods. S3 Object Lock protects objects, while deletion protection restricts administrative removal.

These technologies differ in how effectively they withstand compromised administrator credentials. Some enforce retention periods that even privileged administrators cannot shorten. Others permit authorized administrators to change retention settings or delete protected data. In this case, ransomware that obtains compromised administrative credentials can potentially change or delete backups.

Organizations should therefore evaluate how each appliance enforces immutability rather than simply checking whether it offers the feature. They should also examine its retention controls, administrative privileges, deletion restrictions, and recovery procedures. The GPBA's implementation of these features can help determine whether protected backups remain recoverable following an attack.

Trend #3: Air-Gapping and Isolation Extend Backup Protection

Air-gapping strengthens backup protection by isolating recovery data from production environments. Physical air gaps disconnect backup storage from networks, while logical air gaps restrict connectivity through software-defined controls. Both approaches seek to prevent attackers from reaching protected backup copies.

Organizations can establish isolated repositories and use network disconnection or policy-controlled access windows to limit exposure. Replication can transfer backup copies to isolated targets during authorized intervals. These measures reduce opportunities for ransomware to compromise multiple backup copies.

However, organizations must distinguish genuine isolation from ordinary access controls. Authentication, permissions, and network segmentation alone may not prevent attackers with privileged credentials from accessing backups. Organizations should verify isolation mechanisms, connection policies, and administrative safeguards before relying on air-gapped protection.

© 2026 DCIG, LLC. All rights reserved.

Common Features across the Seven Evaluated Cyber Resilient Hybrid NAS GPBAs

DCIG evaluated about 30 different NAS appliances of which seven (7) met DCIG's criteria for an up to 10PB hybrid NAS cyber resilient GPBA. Across these seven GPBAs, DCIG evaluated about 300 features on each one. Enterprises may safely assume that each one minimally possesses or supports the following fourteen capabilities or features:

DCIG evaluated about 300 features across the seven evaluated GPBAs with each one minimally possessing or supportings the same fourteen capabilities or features.

1. ***All-Inclusive Software Licensing*** bundles supported storage software capabilities into a single licensing package. This approach simplifies purchasing and reduces the need to license individual features separately. Organizations can more easily anticipate software costs as their backup environments grow.
2. ***Asynchronous Replication*** copies data between storage systems without requiring simultaneous writes at both locations. It enables organizations to maintain backup copies at geographically separate sites. These additional copies support disaster recovery and reduce dependence on a single backup location.
3. ***Audit Logging*** records administrative activities, configuration changes, and other monitored events within the storage environment. These records help administrators investigate suspicious activities and identify unauthorized changes. Audit trails also support security reviews, troubleshooting, and regulatory compliance efforts.
4. ***Capacity, Performance, and Security Reporting*** capabilities provide information about storage consumption, system performance, and security-related activities. Administrators use these reports to identify capacity trends, performance bottlenecks, and potential security concerns. These insights support backup capacity planning, operational troubleshooting, and security oversight.
5. ***Centralized Storage Management and Reporting*** provides administrators with interfaces for configuring, monitoring, and maintaining storage resources. These interfaces consolidate routine administrative tasks and system information. Centralized administration helps organizations simplify GPBA operations and respond more quickly to storage issues.
6. ***Data Protection Against Media Failures*** in the form of RAID and erasure coding distribute redundant data or parity information across multiple storage devices. These technologies enable appliances to reconstruct data following supported drive failures. They help maintain backup availability and reduce the risk of data loss from hardware failures.
7. ***Directory Service Integration*** connects storage access controls with centralized identity services such as Microsoft Active Directory (AD). Administrators can use existing directory identities to manage access to backup storage. This integration simplifies account administration and supports consistent access policies across IT environments.
8. ***Encryption at Rest*** protects stored backup data by converting it into an unreadable format without authorized decryption keys. This capability helps prevent unauthorized disclosure when someone accesses storage media. Organizations can use encryption to strengthen backup confidentiality and address data protection requirements.
9. ***Installation Services*** provide professional assistance with deploying and configuring NAS backup appliances. Provider personnel or authorized partners help organizations establish supported storage configurations. These services can reduce deployment complexity and help organizations prepare appliances for production backup workloads.

© 2026 DCIG, LLC. All rights reserved.

Snapshot locking helps preserve recovery points against unauthorized or accidental administrative actions.

10. ***Multifactor Authentication (MFA)*** requires administrators to verify their identities using more than one authentication factor. This additional verification helps prevent attackers from accessing backup storage with stolen passwords alone. Organizations can strengthen administrative security and reduce exposure to credential-based attacks.
11. ***Non-Disruptive Capacity Expansion*** allows organizations to increase available storage without taking supported storage services offline. Administrators can add compatible storage resources as backup volumes grow. This capability helps organizations accommodate expanding retention requirements while minimizing planned downtime.
12. ***Snapshot Creation and Management.*** Snapshots preserve point-in-time representations of stored data that administrators can manage through defined schedules or manual operations. These recovery points help organizations restore data following accidental changes or corruption. Space-efficient snapshots can also reduce the capacity required to maintain multiple recovery points.
13. ***Snapshot Locking and Deletion Protection.*** Snapshot locking restricts changes or deletion of protected snapshots according to the appliance's implementation. These restrictions help preserve recovery points against unauthorized or accidental administrative actions. Organizations should verify whether privileged administrators can override locks or shorten retention periods as these settings will impact the immutability guarantees offered by each GPBA.
14. ***Thin Provisioning and Online File-System Expansion.*** Thin provisioning allocates physical storage capacity as applications consume it rather than reserving all provisioned capacity immediately. Online file-system expansion increases available file-system capacity without requiring supported services to stop. Together, these capabilities improve storage utilization and accommodate growing backup repositories.

Table 1

Common Features Across Seven Evaluated Hybrid NAS Backup Appliances

Feature Name	Definition	Value proposition
1. All-inclusive software licensing	Bundles supported storage software capabilities into one licensing package.	Simplifies purchasing and improves software cost predictability.
2. Asynchronous replication	Copies data to another storage system without requiring simultaneous writes.	Supports offsite backup copies and disaster recovery.
3. Audit logging	Records administrative activities, configuration changes, and monitored events.	Supports security investigations, accountability, and compliance reviews.
4. Capacity, performance, and security reporting	Reports storage utilization, performance metrics, and security-related information.	Helps identify capacity trends, bottlenecks, and potential security concerns.
5. Centralized storage management and reporting	Consolidates storage configuration, administration, monitoring, and reporting interfaces.	Simplifies operations and accelerates troubleshooting.

Continued

© 2026 DCIG, LLC. All rights reserved.

The DCIG TOP 3 solutions distinguish themselves through different combinations of cyber resilience, backup interoperability, storage architecture, and enterprise management capabilities.

Feature Name	Definition	Value proposition
6. Data protection against media failures	Uses RAID or erasure coding to reconstruct data following supported drive failures.	Maintains backup availability and reduces hardware-related data loss.
7. Directory service integration	Integrates storage access controls with centralized identity services.	Simplifies identity administration and supports consistent access policies.
8. Encryption at rest	Encrypts stored data and requires authorized keys for decryption.	Protects backup confidentiality against unauthorized media access.
9. Installation services	Provides professional assistance with appliance deployment and configuration.	Reduces deployment complexity and supports production readiness.
10. Multifactor authentication	Requires multiple authentication factors to verify administrator identities.	Reduces exposure to stolen passwords and credential-based attacks.
11. Non-disruptive capacity expansion	Adds storage capacity while maintaining supported storage services.	Accommodates backup growth with minimal planned downtime.
12. Snapshot creation and management	Creates and manages point-in-time representations of stored data.	Provides additional recovery points and supports efficient data recovery.
13. Snapshot locking and deletion protection	Restricts modification or deletion of protected snapshots.	Helps preserve recovery points against unauthorized changes or deletion.
14. Thin provisioning and online file-system expansion	Allocates physical capacity as needed and expands file systems online.	Improves storage utilization and simplifies backup repository growth.

Source: XXXXXXX

While all seven evaluated hybrid NAS backup appliances share numerous capabilities, their implementations and additional features vary considerably. The DCIG TOP 3 solutions distinguish themselves through different combinations of cyber resilience, backup interoperability, storage architecture, and enterprise management capabilities. The following section examines these differences and their implications for organizations selecting NAS backup targets.

Similarities and Differentiators between the 2027-28 DCIG TOP 3 Cyber-Resilient Up to 10PB Hybrid NAS GPBAs

The DCIG TOP 3 distinguish themselves in at least six areas. They offer different combinations of cyber resilience, storage architecture, backup interoperability, and enterprise services. Each offers capabilities that organizations should consider when selecting storage for protecting and recovering critical backup data.

1. Multiple Immutability Technologies Strengthen Backup Protection

The TOP 3 appliances offer different approaches to protecting backup data against unauthorized modification or deletion. These include immutable snapshots, WORM file-system protection, immutable file shares, and S3 Object Lock.

© 2026 DCIG, LLC. All rights reserved.

StoneFly reports additional file-system governance and compliance locks alongside ransomware anomaly detection. Nexsan NV6000 combines snapshot locking with WORM file-system protection and immutable file shares. TrueNAS H30 offers immutable snapshots and S3 Object Lock, giving organizations another means of protecting retained recovery data.

Hybrid NAS architecture combines SSD and HDD resources, but their performance and expansion capabilities can vary considerably.

2. Cyber-Resilience Controls Extend Beyond Immutability

Cyber resilience also depends on detecting storage problems, preserving data integrity, and maintaining access to recovery points. The TOP 3 products approach these requirements differently.

TrueNAS H30 reports extensive data integrity features, including end-to-end checksum validation, scrubbing, automatic repair, and self-healing. StoneFly reports ransomware anomaly detection and several file-system protection mechanisms. Nexsan NV6000 reports background media scrubbing and silent data corruption detection. These capabilities help organizations address different threats to backup data integrity and recoverability.

3. Storage Architectures Offer Different Performance and Capacity Options

Hybrid NAS architecture combines SSD and HDD resources, but their performance and expansion capabilities can vary considerably. StoneFly reports particularly large processor and memory configurations alongside distributed metadata management. Nexsan NV6000 reports substantial HDD and SSD capacity, multiple Ethernet speeds, and nondisruptive hardware expansion. TrueNAS H30 reports workload prioritization, quality-of-service controls, and dynamic client path balancing.

4. Backup Application Interoperability Influences Appliance Selection

All three TOP 3 products identify certifications for one or more enterprise backup applications. These integrations may simplify deployment and provide clearer support paths when organizations encounter backup or recovery problems. TrueNAS H30 identifies Cohesity NetBackup and Veeam. StoneFly identifies Cohesity NetBackup, Rubrik, and Veeam. Nexsan NV6000 identifies Commvault and Veeam.

5. Replication Options Support Different Recovery Strategies

All three appliances support asynchronous replication, but their additional capabilities differ. StoneFly also reports synchronous replication, while TrueNAS H30 supports multiple asynchronous replication topologies.

These options allow organizations to consider different approaches to maintaining geographically separated recovery copies. However, replication alone does not guarantee ransomware isolation. Organizations should evaluate whether replicated recovery points remain protected against compromised credentials, unauthorized deletion, and changes propagated from production environments.

6. Enterprise Management and Support Simplify Backup Operations

The TOP 3 products report enterprise-oriented management and support capabilities, including monitoring, onsite service, and proactive assistance. TrueNAS H30 reports multi-tenancy, SIEM integration, and fleet management. StoneFly reports fleet management, predictive analytics, and managed service options. Nexsan NV6000 reports proactive support, remote monitoring, and rapid-response service options.

© 2026 DCIG, LLC. All rights reserved.

These capabilities help organizations operate backup storage, investigate problems, and maintain recoverability as their IT environment grows.

2027-28 DCIG TOP 3 Cyber Resilient Up to 10PB Hybrid NAS GPBAs

Each of the following TOP 3 Up to 10PB Hybrid NAS Cyber Resilient GPBA profiles highlights at least three ways each one differentiates itself. These differentiators represent some of the best methods that hybrid NAS cyber resilient GPBAs offer to back up, restore, and/or secure data stored on them. Within each GPBA, organizations may find specific features that may better meet their specific needs.

© 2026 DCIG, LLC. All rights reserved.

Nexsan® Unity™ NV6000™

The NV6000 combines the capacity and economics of HDDs with the flash acceleration of SSDs. By supporting file, block, and S3 storage protocols, organizations can use it as a backup target across multiple protocols. This architecture also gives organizations the flexibility to utilize the NV6000 to support other enterprise application workloads.

The NV6000 delivers high availability, nondisruptive operations, data integrity, replication, and inline compression. Hybrid storage and FASTier® acceleration improve performance and flexibility. Further, organizations can access all these options as Nexsan includes them without separate per-feature software licensing.

These capabilities help distinguish the NV6000 from other GPBAs:

- ***Accelerates backup and restore performance.*** Nexsan's FASTier technology uses SSDs to cache reads and writes to the NV6000's underlying HDD storage. Using this technique, organizations obtain many of SSD's performance benefits without needing to deploy an all-SSD system.

  Nexsan finds that FASTier can accelerate HDD performance by up to 10X. This design gives organizations an option to obtain flash-assisted performance while retaining the capacity and economics associated with HDD storage.[iii]

- ***Unified storage gives organizations multiple ways to present backup storage.*** NV6000 natively supports block (iSCSI and Fibre Channel), file (NFS and SMB), and object (S3) protocols. Supporting all these storage networking protocols can eliminate the need to dedicate storage systems that only use specific ones. These protocols position organizations to consolidate backup and other application workloads on the NV6000 if they choose.[iv]

- ***Offers multiple immutable technologies to make backup data more cyber resilient.*** The NV6000's immutable snapshots protect file systems and volumes from modification or deletion during defined retention periods. S3 Object Lock similarly provides WORM protection for objects.[v]

  Organizations may also integrate the NV6000 with Nexsan Assureon® to create a policy-controlled immutable WORM backup tier. Assureon adds capabilities such as file fingerprinting, data verification, self-healing, and restricted access. These features prevent even administrators from altering protected data until the backup's retention policy expires.[vi]

- ***Proven support for multiple enterprise backup applications.*** Nexsan documents the NV6000 as an immutable backup target for Commvault, Veeam, Bacula, and Arcserve. Further, the Nexsan NV6000 can serve as a backup target for most, if not all, backup software using any of its storage networking interfaces.[vii]

"Nexsan combines NV6000 immutable snapshots and NexObject™ S3 Object Lock with Assureon to provide multiple layers of immutable protection for backups."

© 2026 DCIG, LLC. All rights reserved.

StoneFly USO XD-Series

The USO XD-Series represents StoneFly's enterprise-grade, dual-processor storage configuration. Organizations can configure it with enterprise SSDs and HDDs to balance backup performance, capacity, and economics. StoneFly's USO platform also provides unified NAS, SAN, and S3 object storage services.

StoneFly's StoneFusion operating system (OS) gives the USO XD-Series distinctive cyber-resilience capabilities. It combines immutability, isolation, access controls, threat detection, and replication to protect backup data and recovery point.

"The StoneFly USO XD-Series Air-Gapped Vault capability limits backup exposure by automatically connecting and disconnecting protected storage from production environments."

The following capabilities help distinguish the StoneFly USO XD-Series from other GPBAs.

- ***Preserves recoverable backup copies even when ransomware or compromised credentials threaten primary backup data.*** StoneFly provides File-Level WORM that makes designated files immutable according to policy-defined retention periods. It also offers immutable snapshots that preserve point-in-time recovery copies. Volume Deletion Protection adds yet another safeguard by requiring additional authorization before administrators can delete protected volumes.
- ***Automates the isolation of backup data from production networks.*** StoneFly's Air-Gapped Vault supports logical and physical air-gapping. Its logical implementation uses policies to automatically connect and disconnect protected repositories or controllers from production environments.

  StoneFly also offers physically isolated nodes that use network and power controls to disconnect protected backup storage. These options help organizations limit how long backup data remains accessible to ransomware or compromised production systems.

- ***Provides multiple additional layers of cyber resilience.*** StoneFusion supplements immutability and air-gapping with multifactor authentication, administrative access controls, encryption, auditing, replication, and integrated threat detection. StoneFly can monitor I/O activity for anomalous behavior and take actions such as isolating affected volumes when it detects suspicious activity.
- ***Combines flash performance with HDD capacity and economics.*** Organizations can configure hybrid StoneFly storage with NVMe flash and capacity-oriented HDDs. Flash caching and automated tiering place frequently accessed data on faster storage while retaining colder data on HDDs. This architecture gives organizations options to improve backup and restore performance without deploying an all-flash system.
- ***Supports multiple storage protocols and backup workloads.*** USO provides unified NAS, SAN, and S3 object storage. This architecture enables organizations to present storage through file, block, or object interfaces while managing them through the StoneFusion platform.

© 2026 DCIG, LLC. All rights reserved.

"The TrueNAS H30 offers multiple immutability options to protect backup data and recovery points from unauthorized deletion."

TrueNAS H30

The TrueNAS H30 combines NVMe SSD and HDD storage in a compact 2U appliance. Its architecture gives organizations options to balance flash performance with HDD capacity and economics. Organizations may also expand its HDD capacity by adding a shelf with 24-, 60-, or 102-drive options available.

The H30 particularly distinguishes itself through the cyber-resilience capabilities available through TrueNAS Enterprise and OpenZFS. Together, these technologies provide multiple layers of protection for backup data and its recovery points.

The following capabilities help distinguish the TrueNAS H30 from other general-purpose NAS backup appliances.

- ***Offers multiple immutability technologies to make backup data more cyber resilient.*** The H30 can use ZFS snapshots to preserve point-in-time copies of backup data. ZFS copy-on-write prevents snapshot contents from being overwritten as production data changes. TrueNAS also provides Snapshot Hold that administrators can apply to specific snapshots to prevent their deletion.

  TrueNAS further supports Time-Locked SMB Shares that make files read-only after a configurable grace period. This capability provides WORM-like protection for backup applications writing to SMB shares, though TrueNAS cautions that it may not satisfy regulatory write-once requirements.

  TrueNAS Enterprise systems provide S3-compatible Object Storage with S3 Object Lock. Its Compliance mode prevents users, including S3 administrators from deleting protected objects until their retention periods expire.

- ***Preserves the integrity of backup data.*** OpenZFS creates checksums as TrueNAS writes data and validates them when reading it. If OpenZFS detects corruption, it can use mirrored copies or RAIDZ redundancy to reconstruct and repair the corrupted data automatically. Scheduled ZFS scrubs extend this protection to infrequently accessed backup data by periodically checking stored data for silent corruption.
- ***Provides multiple additional layers of cyber resilience.*** TrueNAS Enterprise complements its immutability technologies with encryption, restricted administrator roles, auditing, multifactor authentication, and replication. These capabilities protect backup data against unauthorized access and administrative actions, record potentially malicious activity, and preserve additional recovery copies.
- ***One dataset accessible to backup applications using different file protocols.*** The H30 can simultaneously provide file, block, and object storage services. For NAS backup, TrueNAS can more notably configure the same dataset for concurrent SMB and NFS access. This flexibility permits organizations to use one H30 with multiple backup applications that require different storage interfaces.

© 2026 DCIG, LLC. All rights reserved.

Cyber Resilient GPBAs — Up to 10PB Hybrid NAS Edition Inclusion Criteria

- Must offer and support at least two of the following four cyber resilience features:
  - Detects anomalies and/or ransomware in backup data
  - Offers data immutability and/or data preservation capabilities
  - Offers Identify and Access Management (IAM)
  - Performs data encryption
- Offers a networked attached storage (NAS) interface with support for the CIFS and/or NFS file protocol.
- Ships as a physical appliance.
- Must support a hybrid storage configuration (both HDDs and SSDs) for storing data.
- Total configurable, usable storage capacity does not exceed 10PB.
- Storage provider positions the NAS appliance for the backup use case.
- Shipping and available by September 1, 2026.
- Sufficient information is available for DCIG to make an informed, defensible decision.

DCIG Disclosures

Providers of some of the Up to 10PB Hybrid NAS Cyber Resilient GPBAs covered in this DCIG TOP 3 report are or have been DCIG clients. In that vein, DCIG encourages readers to consider the following when evaluating the information contained in this TOP 3 report:

- No provider paid DCIG a fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any provider that its solution would be included in this TOP 3 report.
- DCIG did not imply or guarantee that a specific solution would receive a TOP 3 designation.
- All research is based upon publicly available information, information shared by the provider, and the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the features worked as described.
- No negative inferences should be made against any provider or solution not covered in this TOP 3 report.
- It is a misuse of this TOP 3 report to compare solutions included in this report against solutions not included in it.

© 2026 DCIG, LLC. All rights reserved.

No provider was privy to how DCIG weighted individual features. In every case the provider only found out the rankings of its PBBA after the analysis was complete. To arrive at the TOP 5 solutions included in this report, DCIG went through a seven-step process to come to the most objective conclusions possible.

1. DCIG established which features would be evaluated.
2. The features were grouped into six general categories.
3. DCIG weighted each feature to establish a scoring rubric.
4. DCIG identified solutions that met DCIG's definition for an up to 10PB hybrid NAS cyber resilient GPBA.
5. A survey was completed for a model of each evaluated GPBA.
6. DCIG evaluated and ranked each PBBA based on information gathered in its survey.
7. Solutions were ranked using standard scoring techniques. ■

Sources

i. https://s25.q4cdn.com/621799436/files/doc_financials/2026/q4/Q4-26-Earnings-Deck.pdf. Pg. 16. Referenced 10/12/26.
ii. https://www.trendforce.com/presscenter/news/20260930-13258.html. Referenced 10/12/2026.
iii. https://www.nexsan.com/wp-content/uploads/2023/12/Unity-NV6000-Datasheet.pdf/. Pg. 2. Referenced 10/5/2026.
iv. https://www.nexsan.com/wp-content/uploads/2025/05/Nexsan-Unity-NV-Series-Unified-Storage-Data-Sheet.pdf. Referenced 10/6/2026.
v. https://www.nexsan.com/resources/unity-nv6000-enterprise-class-unified-storage-with-immutable-snapshots/. Referenced 10/5/2026.
vi. https://www.nexsan.com/products/immutable-storage/assureon/. Referenced 10/6/2026.
vii. https://www.nexsan.com/resources/unity-nv6000-enterprise-class-unified-storage-with-immutable-snapshots/. Referenced 10/5/2026.
viii. https://stonefly.com/storage/uso-appliance/. Referenced 10/7/2026.
ix. https://stonefly.com/storage/nas-storage/. Referenced 10/7/2026.
x. https://stonefly.com/storage/nas-storage/. Referenced 10/7/2026.
xi. https://stonefly.com/resources/what-are-air-gapped-backups/. Referenced 10/7/2026.
xii. https://stonefly.com/storage/nas-storage/. Referenced 10/7/2026.
xiii. https://stonefly.com/storage/nas-storage/. Referenced 10/7/2026.
xiv. https://stonefly.com/storage/uso-appliance/. Referenced 10/7/2026.
xv. https://www.truenas.com/h-series/. Referenced 10/6/2026.
xvi. https://www.truenas.com/blog/truenas-immutable-backup-data-protection/. Referenced 10/6/2026.
xvii. https://www.truenas.com/docs/scale/26/shares/smb/smbsharesscreens/. Referenced 10/6/2026.
xviii. https://www.truenas.com/docs/scale/shares/s3/configurings3/. Referenced 10/6/2026.
xix. https://www.truenas.com/docs/references/zfsprimer/. Referenced 10/6/2026.
xx. https://www.truenas.com/blog/truenas-immutable-backup-data-protection/. Referenced 10/6/2026.
xxi. https://www.truenas.com/docs/scale/26/shares/mixedmodeshares/. Referenced 10/6/2026.

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of DCIG TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**

© 2026 DCIG, LLC. All rights reserved. Other trademarks appearing in this document are the property of their respective owners. This DCIG report is a product of DCIG, LLC. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. Product information was compiled from both publicly available and vendor-provided resources. While DCIG has attempted to verify that product information is correct and complete, feature support can change and is subject to interpretation. All features represent the opinion of DCIG. DCIG cannot be held responsible for any errors that may appear.

Licensed to Nexsan, Inc., with unlimited and unrestricted distribution rights through December 2028.