Solution Profile



2027-28 DCIG TOP 3

CYBER RESILIENT GPBAs // UP TO 10PB HYBRID NAS EDITION

Nexsan® Unity™ NV6000™

By Jerome M. Wendt, Principal Analyst

2027-28 DCIG TOP 3

Cyber Resilient GPBAs // Up To 10PB Hybrid NAS Edition
Nexsan® Unity™ NV6000™ Solution Profile



SOLUTION

Nexsan® Unity™ NV6000™

COMPANY

Nexsan, Inc.
1287 Anvilwood Avenue
Sunnyvale, CA 94089
408.724.9809
https://www.nexsan.com/products/unified-block-and-file-storage/unity/

DISTINGUISHING FEATURES OF NEXSAN® UNITY™ NV6000™

- Active-Active dual-controller architecture provides high availability with no single point of failure.
- All-inclusive software licensing.
- FASTier® SSD caching accelerates underlying HDD performance by up to 10X.
- Immutable snapshots protect volumes and file systems from modification or deletion.
- Includes HA, inline compression, replication, data integrity, and nondisruptive upgrades.
- Integrates with Nexsan Assureon® to create a separate immutable WORM backup tier.
- Natively supports NFS, SMB, S3, iSCSI, and Fibre Channel storage protocols.
- S3 Object Lock provides WORM immutability for object-based backup data.
- Supports hybrid and all-SSD configurations.
- Supports Arcserve, Commvault, Veeam, Bacula, and other enterprise backup applications.

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 technolo-gies help organizations preserve trustworthy recovery points despite malicious or accidental administrative actions.

Cyber Resilient GPBA – Up to 10PB Hybrid NAS Edition Inclusion Criteria

To qualify for inclusion in the Cyber Resilient GPBA – Up to 10PB Hybrid NAS Edition analysis, GPBAs had to demonstrate meaningful cyber resilience capabilities. Each GPBA must offer and support at least two of the following four key cyber resilience features:

- Detects anomalies or ransomware in backup data.
- Offers data immutability or data preservation capabilities.
- Offers Identity and access management (IAM)
- Performs data encryption.

These capabilities help organizations strengthen backup security, reduce ransomware risk, and improve recovery confidence.

Beyond cyber resilience functionality, qualifying solutions must also support a hybrid storage configuration (both HDDs and SSDs) for storing data. Additionally, the appliance must provide a network-attached storage (NAS) interface supporting the CIFS and/or NFS file storage networking protocols. Supporting these NAS protocols ensures compatibility with a wide range of backup applications and environments.

DCIG further limited consideration to GPBAs that ship as physical appliances, were specifically positioned for the backup use case, and generally available no later than September 1, 2026. Providers also needed to provide sufficient publicly available and verifiable technical information for DCIG to conduct a thorough evaluation. These requirements ensured GPBAs meet baseline enterprise deployment expectations and allowed DCIG to make informed, objective, and defensible inclusion decisions.

© 2026 DCIG, LLC. All rights reserved.

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 modifi cation 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 suffi ciently 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 effi ciency, 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.

Providers that explicitly position their NAS appliances as backup targets may better address today's modern backup requirements.

Regarding the 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 fi le 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.

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.

© 2026 DCIG, LLC. All rights reserved.

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 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 protocols. 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] 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.

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.

© 2026 DCIG, LLC. All rights reserved.

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.

GPBAs can offer multiple forms of immutability to protect backup data against unauthorized modification or deletion, to include immutable snapshots, WORM file retention, and S3 Object Lock.

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.

Nexsan® Unity™ NV6000™ Solution Profile

DCIG reviewed 29 cyber-resilient GPBAs with seven meeting the criteria for the Up to 10PB Hybrid NAS GPBA edition. Among those seven, DCIG recognized the Nexsan® Unity™ NV6000™ as a 2027-28 DCIG TOP 3 solution. The NV6000 specifically earned this recognition in the Up to 10PB Hybrid NAS Edition.

Unity and Assureon combine rapid operational restores with a separate, policy-controlled immutable WORM backup tier.

Each member of the Nexsan Unity NV-Series™ family, the NV10000™, NV6000™, and NV4000™, offers the same core functionality. They each combine the capacity and economics of HDDs with the flash acceleration of SSDs. They all support file, block, and S3 storage protocols so organizations can use them as backup targets across multiple protocols. Their architecture also gives organizations the flexibility to utilize them to support other enterprise application workloads.

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

The following capabilities help distinguish the Nexsan Unity NV-Series systems from other general-purpose NAS backup appliances.

- ***Accelerates backup and restore performance.*** Nexsan's FASTier technology uses SSDs to cache reads and writes to the Nexsan Unity'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.*** All Unity NV-Series systems natively support 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 Nexsan Unity NV-Series systems if they choose.[iv]

- ***Offers multiple immutable technologies to make backup data more cyber resilient.*** The 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 integrate any Unity NV-Series system with Nexsan Assureon® to create Nexsan's Unbreakable Backup architecture. Assureon provides a separate, policy-controlled WORM tier with fingerprinting, verification, self-healing, redundant copies, and restricted access. These controls prevent even administrators from modifying protected data before its retention policy expires.[vi]

  This integration also supports tiered backups. Organizations can keep backups on the higher-performance Unity tier for rapid operational restores and store immutable copies on Assureon. They can offload older backups from Unity while shortcuts preserve access, freeing capacity without sacrificing protected data.[vii]

© 2026 DCIG, LLC. All rights reserved.

The NV4000, NV6000, and NV10000 deliver common Unity functionality at different capacity and performance points.

- ***Proven support for multiple enterprise backup applications.*** Nexsan documents every Unity NV-Series system as an immutable backup target for Commvault,Veeam, Bacula, and Arcserve. Each system can also serve most backup software through any supported storage networking interface.[viii]

- ***Obtain these same core Unity capabilities at different capacity and performance points.*** The Unity NV-Series currently includes the NV4000, NV6000, and NV10000. Nexsan positions the NV4000 for smaller, edge, backup, and surveillance deployments.

  At the other end of the family, the NV10000 extends Unity into substantially larger and higher-performance environments. Nexsan equips the NV10000 with NVMe all-flash technology. It also supports configurations designed for different performance and capacity requirements. Nexsan publishes transfer rates of up to 20GB/s for the NV10000 and positions it for core enterprise deployments.[ix]

  The NV6000 occupies the middle of this portfolio and provides a balance of capacity, performance, and hybrid-storage economics. The three-model approach also gives organizations options for deploying a common Unity architecture across different locations and workloads. They then have access to the same software features without requiring every environment to use the same hardware configuration. ■

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/. Referenced 10/19/2026.
vii. https://www.nexsan.com/products/immutable-storage/. Referenced 10/6/2026.
viii. https://www.nexsan.com/resources/unity-nv6000-enterprise-class-unified-storage-with-immutable-snapshots/. Referenced 10/6/2026.
ix. https://www.nexsan.com/resources/unity-nv10000-datasheet/. 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 and TOP 3 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.