Solution Profile

2027-28 DCIG TOP 3

CYBER RESILIENT GPBAs // 10PB+ HYBRID NAS EDITION

Infinidat, a Lenovo Company, InfiniBox G4 F84SH

By Jerome M. Wendt, Principal Analyst

Cyber Resilient GPBAs // 10PB+ Hybrid NAS Edition

Infinidat, a Lenovo Company, InfiniBox G4 F84SH Solution Profile

SOLUTION

InfiniBox F84SH

COMPANY

Infinidat, a Lenovo Company
500 Totten Pond Road
Waltham, MA 02451
Tel: (855) 893-6994
Web: https://www.infinidat.com/en/products-technology/infinibox

DISTINGUISHING FEATURES OF INFINIBOX F84SH

- Creates immutable snapshots with enforced retention policies.
- Guarantees recoverable immutable snapshots in one minute or less.
- Provides fenced forensic environments isolated from production networks.
- Supports local and remote logical air-gapped recovery copies.
- Helps identify trustworthy recovery points following ransomware attacks.
- Integrates InfiniSafe ACP with SIEM, SOAR, and SOC workflows.
- Triggers immutable snapshots automatically following configured security alerts.
- Offers optional AI-powered InfiniSafe Cyber Detection that analyzes over 200 indicators.
- Uses Neural Cache machine learning to optimize hybrid storage performance.
- Combines three active controllers with an InfiniBand interconnect.

Cyber Resilience Becomes a Primary General Purpose Backup Appliance Selection Criterion

Enterprises 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 enterprises 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 enterprises from recovering critical applications and data, despite earlier reports of successful backups.

Consequently, enterprises 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 – 10PB+ Hybrid NAS Edition Inclusion Criteria

To qualify for inclusion in the Cyber Resilient GPBA – 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 and scale to 10PBs or more of usable capacity. 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

Enterprises 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. Enterprises 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.*** Enterprises 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.

Enterprises 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.

Enterprises 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 their 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 10PB+ Hybrid NAS GPBA Selection

Three emerging trends influence how enterprises select GPBAs for cyber resilience and recovery. Enterprises 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. Enterprises 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.

Enterprises 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.

Enterprises 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.

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

© 2026 DCIG, LLC. All rights reserved.

Infinidat, a Lenovo Company, InfiniBox G4 F84SH

DCIG reviewed 29 cyber-resilient GPBAs with nine meeting the criteria for the 10PB+ Hybrid NAS GPBA edition. Among those nine, DCIG recognized the Infinidat InfiniBox G4 F84SH as a 2027-28 DCIG TOP 3 solution. The F84SH specifically earned this recognition in the 10PB+ Hybrid NAS Edition.

InfiniBox F84SH combines immutable snapshots, logical air-gapping, and guaranteed rapid recovery with hybrid enterprise storage.

Infinidat, a Lenovo company, positions its InfiniBox G4 platform for enterprise storage workloads, including backup and recovery. Its hybrid architecture combines SSD performance with HDD capacity and economics. The F84SH particularly distinguishes itself through Infinidat's InfiniSafe cyber resilience technologies that provide end-to-end data validation and instant recovery readiness.

The following capabilities help distinguish the Infinidat InfiniBox F84SH from other GPBAs.

- ***Combines immutable snapshots with logical air-gapping and isolated forensic recovery.*** InfiniSafe creates immutable, point-in-time snapshots whose retention policies prevent modification or deletion, even by administrators with compromised credentials.

  Enterprises can logically isolate these snapshots within the local InfiniBox without deploying separate storage hardware. They can also replicate protected copies to a remote InfiniBox, adding geographic separation and another recovery location.[iii]

  InfiniSafe further supports a fenced forensic environment using dedicated networking resources isolated from production. Administrators activate this private network when they need to inspect, test, or recover protected data.[iv]

  With InfiniSafe Cyber Detection, administrators can investigate possible ransomware contamination and determine a "known good" copy of data to recover from. These copies can identify a trustworthy recovery point before reconnecting recovered data to production, with Infinidat claiming up to 99.99% accuracy.

- ***Guarantees recoverable immutable snapshots in a minute or less.*** Infinidat guarantees InfiniBox immutable snapshot recovery in one minute or less, regardless of dataset size, subject to guarantee terms.[v] Its snapshot-based recovery approach avoids copying entire backup datasets before making recovery points available. This capability can help enterprises reduce recovery time following ransomware attacks or other disruptions.

- ***Automates threat-triggered snapshots and forensic validation.*** InfiniSafe Automated Cyber Protection (ACP) integrates with SIEM, SOAR, and Security Operations Center (SOC) workflows through syslog notifications and APIs.

  Enterprises configure security alerts to trigger immediate immutable snapshots of selected InfiniBox volumes or broader datasets. These event-driven snapshots supplement scheduled protection and receive a default three-day retention period that administrators may extend but cannot shorten.

© 2026 DCIG, LLC. All rights reserved.

The optional InfiniSafe Cyber Detection's scanning engine identifies potential malware, pinpoints compromised data, and helps identify the last known good recovery point.

Enterprises may configure ACP to respond to suspected ransomware activity, abnormal file changes, or other security alerts identified by their monitoring tools. Optional InfiniSafe Cyber Detection then scans protected snapshots using AI and machine learning. Its scanning engine analyzes more than 200 content and metadata indicators to identify potential malware, pinpoint compromised data, and help identify the last known good recovery point.[vi]

- ***Uses machine learning and three storage tiers to deliver high performance at hybrid storage economics.*** InfiniBox F84SH combines three active controllers, an InfiniBand interconnect, and a tiered DRAM, SSD, and HDD architecture. Its patented Neural Cache algorithms continuously learns application I/O patterns and predicts which data applications will access next. They proactively place frequently accessed data in DRAM, minimizing slower SSD and HDD reads.[vii] ■

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. iii. https://www.infinidat.com/en/blog/enterprise-must-have-cyber-resilience. Referenced 10/21/2026.
iv. iv. https://www.infinidat.com/en/blog/enterprise-must-have-cyber-resilience. Referenced 10/21/2026.
v. v. https://www.infinidat.com/en/cyber-resilience. Referenced 10/21/2026.
vi. vi. https://www.infinidat.com/en/blog/infinisafer-automated-cyber-protection-acp-fill-gap-storage-cyberattack-data-protection-and. Referenced 10/21/2026.
vii. vii. https://www.infinidat.com/en/resource-pdfs/infinidat-storage-architecture.pdf. Pg. 5. Referenced 10/21/2026.

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 Infinidat, a Lenovo Company, with unlimited and unrestricted distribution rights through December 2028.