Solution Profile

2025-26 DCIG TOP 5

CYBERSECURE NAS SOLUTIONS SUB-10PB // GLOBAL EDITION

Infinidat InfiniBox G4 Solution Profile

By

Jerome M Wendt, Principal Analyst
Ken Clipperton, Principal Researcher
Todd Dorsey, Sr. Storage Analyst
Joshua Konkle, Consulting Researcher

Infinidat InfiniBox G4 Solution Profile

Table of Contents

Cybersecure NAS Solutions Sub-10PB // Global Edition

Infinidat InfiniBox G4 Solution Profile

SOLUTION

Infinidat InfiniBox G4

COMPANY

Infinidat
500 Totten Pond Road
Waltham, MA 02451
info@infinidat.com

https://www.infinidat.com/en/products-technology/infinibox

DISTINGUISHING FEATURES OF INFINIDAT INFINIBOX G4

- Platform-native architecture with three active controllers.
- Includes SLAs in writing for 100% availablity, performance, and cyber resilience and recovery.
- InfusOS supports block (FC/iSCSI), file (NFS/SMB) and S3 object in 2H25.
- InfiniSafe ACP integrates with most existing cybersecurity software.
- InfiniSafe Cyber Detection utilizes AI & ML to detect cyber incidents.
- InfiniVerse platform monitors, manages, and optimizes storage services.

CATEGORIES OF FEATURES EVALUATED

- Architecture.
- Cyber Resilience.
- Data Protection.
- Deployment
- Efficiency.
- Performance Management.
- Performance Resources.
- Product Management.
- Technical Support and Service.

NAS Solutions Embrace Cybersecurity

NAS solutions' support for NFS and SMB continues to make them practical choices for all size organizations. Simple to set up, configure, and deploy, broadly adopted, and well-understood, the continued use and growth of NAS seems certain. However, these same strengths make NAS solutions targets during ransomware events due to their prevalent use by organizations.

Forecast Use and Growth of NAS

The pace of data growth continues to accelerate in most organizations. More devices and applications generate more data and larger file sizes. Further, organizations increasingly use media files such as high-resolution images and videos.

Recent reports indicate that organizations will continue to expand their use of NAS solutions. For instance, Fortune Business Insights anticipates the global NAS market will more than triple in value over the next seven years. Valued at $40.3 billion in 2024, Forbes forecasts the NAS market could grow to nearly $130 billion by 2032.[1]

While that estimate represents the high end of the forecasts reviewed by DCIG, all forecasts predict NAS usage to increase. More than 80 percent of organizations already use NAS, making its future seemingly secure for now.[2] Further, NAS continues to offer new cybersecurity features that should encourage organizations to expand their use of it.

Network File Protocols Embrace Encryption

Nearly all file systems that organizations use support either the NFS or SMB network file protocols available on NAS solutions. This broad support led to NAS's initial adoption and use in organizations. However, early versions of these network file protocols provided few or no options to encrypt transmitted data.

Leaving transmitted data unencrypted increases the risk of successful man-in-the-middle attacks. Man-in-the-middle attacks monitor data transmitted using network file protocols. These attacks may hijack sessions, collect sensitive data (passwords or personal or banking information), alter transmitted data, or inject malicious payloads.

Recent security enhancements to NFS and SMB have given organizations increased confidence to continue using them. Mutual authentication, message signing and integrity features, and granular security policies represent just some of the improvements. Addi-tionally, organizations can opt to encrypt data they transmit by using the latest NFSv4.x or SMB 3.x protocols.

Cybersecurity Now Core to NAS Solutions

NAS solutions also remain targets during ransomware attacks as bad actors look to exploit their common usage by organizations. Ransomware may attempt to:

- Encrypt data stored on them, including snapshots or backup files.
- Exfiltrate data stored from them.
- Steal credentials to gain administrative privileges to the NAS solution itself.
- All the above.

In response, modern NAS solutions typically offer multiple cybersecurity features to protect data from attacks, including:

- Anomaly detection that monitors for unusual read or write activity.
- At-rest encryption so that bad actors cannot read any data if exfiltrated.
- Cloud integration for backup, replication, and storage tiering.
- Immutable snapshots to facilitate fast, tamper-proof data restore.
- Integrations with Active Directory (AD) to authenticate individual administrators.
- Multi-factor authentication (MFA) to authenticate individual logins.
- Write Once Read Many (WORM) technologies to prevent ransomware from changing data.
- Zero trust integration.

By NAS solutions utilizing more cybersecurity features and NFS and SMB protocols supporting encryption, organizations may continue embracing these technologies. However, they will encounter many cybersecure NAS solutions from which to choose that possess notable differences in their respective architectures.

Infinidat InfiniBox G4 Solution Profile

The State of Cybersecure Sub-10PB NAS Solutions

Organizations deploy cybersecure sub-10PB NAS solutions to meet a growing number of internal use cases. These multiple use cases demand that NAS solutions support increased levels of availability, capacity, and performance. Cybersecure sub-10PB NAS solutions may meet these requirements in the following ways.

High Availability

Delivering a highly available (HA) cybersecure NAS solution has become almost a prerequisite for adoption. Regardless of how organizations use a cybersecure sub-10PB NAS solution internally, they expect it to remain highly available. To meet this expectation, providers generally ship their cybersecure sub-10PB NAS solutions in one of the following seven HA controller configurations:

1. Active-Active
2. Active-Passive
3. Dual Active
4. Federated
5. Hyperconverged
6. Mesh
7. Scale-out

Flash use in cybersecure sub-10PB NAS solutions represents perhaps the biggest contributor to their improved performance.

Each HA configuration provides benefits that align with specific organizational objectives. For instance, organizations with basic HA requirements may find a sub-10PB NAS solution with an Active-Passive configuration sufficient. This configuration represents a baseline HA deployment where one controller does all processing. The other sits idle and only takes over if the first controller goes offline.

The other six HA configurations utilize two or more controllers when processing file requests. Generally, performance improves as more controllers participate in handling file network traffic. Further, architectures such as Active-Active, Hyperconverged, Mesh, and Scale-out minimize or eliminate service interruptions should a controller go offline.

High Capacity

Cybersecure NAS solutions with less than 10 petabytes (PBs) of internal capacity represent about 35 percent of the available NAS solutions today. Further, many of these sub-10PB NAS solutions include options to tier data to object storage located on-premises or with cloud storage providers. Tiering allows a single sub-10PB NAS solution to manage tens or perhaps hundreds of petabytes of data.

Many cybersecure sub-10PB NAS solutions support both hard disk drives (HDDs) and solid-state drives (SSDs). However, the number of sub-10PB NAS solutions supporting only SSDs continues to increase. Aside from their performance boost, SSDs often last longer and consume less power than HDDs.

High Performance

Flash use in cybersecure sub-10PB NAS solutions represents perhaps the biggest contributor to their improved performance. Using SSDs, sub-10PB NAS solutions can significantly reduce read and write times.

File networking protocols have also benefited from improvements in Ethernet networking. Most organizations minimally run 1Gb Ethernet though many now use 10Gb, 25Gb, and even 100Gb Ethernet. This improved throughput, combined with improved file protocol efficiencies, contributes to cybersecure sub-10PB NAS solutions delivering better performance.

Available Cybersecurity Features on Sub-10PB NAS Solutions

All the evaluated sub-10PB NAS solutions offer one or more of the following cyber secure capabilities. Possessing these features has become more critical as ransomware often targets NAS solutions. The availability, breadth, and implementation of these cyber security features on each sub-10PB NAS solution does vary.

Infinidat InfiniBox G4 Solution Profile

DCIG anticipates that the use of AI by NAS solutions will continue to mature to provide even more sophisticated anomaly detection capabilities.

Data Immutability

Data immutability, or storing data in an unchangeable format, represents a feature that many sub-10PB NAS solutions support. NAS solutions may implement data immutability in one or more of the following ways.

- ***WORM file format*** such that after a file gets written, it can only be read but neither changed nor deleted.
- ***Tiers data to object storage*** that supports data in an immutable format.
- ***Creates immutable snapshots.***

When used, this feature negates ransomware's ability to either delete or encrypt data stored on the sub-10PB NAS solution.

Encryption

More organizations want the option to encrypt their files when stored at-rest on-premises. Many ransomware strains attempt to exfiltrate data *(copy data outside of the organization)* as part of their attack. Encrypting files does not prevent ransomware from exfiltrating them outside of the organizations. However, hackers will find it almost impossible to decrypt and read any encrypted files they obtain.

Multi-factor Authentication

Using multi-factor authentication (MFA) to log into a sub-10PB NAS solution represents a significant cyber security enhancement in recent years. Implementing MFA helps ensure only the appropriate individuals can access and manage the sub-10PB NAS solution.

Some sub-10PB NAS solutions even require a second administrator to authenticate before it allows certain configuration changes. These may include tasks such as changing folder permissions or deleting data, among others.

Artificial Intelligence

Artificial intelligence (AI) has begun to make inroads as a cyber secure feature on sub-10PB NAS solutions. A growing number of sub-10PB NAS solutions use AI to monitor reads, writes, and changes in files to detect anomalies. If it detects an anomaly, the sub-10PB NAS solution may take actions ranging from generating alerts to quarantining the affected files. DCIG anticipates that the use of AI will continue to mature and to provide even more sophisticated anomaly detection capabilities.

Infinidat InfiniBox G4

Upon DCIG's completion of reviewing 15 cybersecure sub-10PB NAS solutions, DCIG ranked the Infinidat InfiniBox G4 as a TOP 5 solution. The Infinidat InfiniBox G4 offers a platform-native architecture with three active controllers that can concurrently access all backend storage. Supporting both SSDs and HDDs, the InfiniBox G4 supports all-flash, and hybrid storage configurations. The InfiniBox's three active/active/active controllers with multipoint active interconnects leverage InfiniBand and utilizing remote direct memory access (RDMA) for high throughput. The InfiniBox G4 platform includes several guaranteed Service Level Agreements (SLAs) in writing for 100% availability, performance, and cyber resilience and recovery.[3]

As a unified platform, InfiniBox G4's InfuzeOS™ software-defined operating system simultaneously supports both block (FC/iSCSI) and file (NFS/SMB) protocols. It also plans to offer S3 support in the 2H2025. InfuzeOS implements and distributes file services across all InfiniBox controllers thereby eliminating controller ownership of directories and files.[4] Further, InfuzeOS Cloud Edition (AWS and Azure) gives organizations a means to extend from on-premises storage to leverage object storage in multiple clouds.

Additional features that help distinguish the Infinidat InfiniBox G4 from the other TOP 5 solutions include:

- ***InfiniSafe® Automated Cyber Protection (ACP).*** InfiniBox's InfiniSafe ACP functions as a "listener" that can be integrated into almost any existing cyber security software applications. These applications include simple integrations leveraging syslog, or more

Infinidat includes its cloud-based InfiniVerse platform that helps monitor, manage, and optimize storage services on the InfiniBox G4.

direct API-based integrations to Security Information and Event Management (SIEM), and Security Orchestration and Response (SOAR), among others. If these applications generate a security alert or notification, these events can trigger InfiniBox to take an immutable snapshot, without performance impact to the production environment.

- ***InfiniSafe Cyber Detection.*** Available as an optional service on the InfiniBox, InfiniSafe Cyber Detection utilizes AI and ML technologies to detect cyber incidents. InfiniSafe Cyber Detection works in conjunction with InfiniSafe ACP to automatically queue up immutable snapshots for scanning.

  InfiniSafe Cyber Detection then does a forensic, full-content analysis of these snapshots. It examines them for data corruption, fingerprints of latent data corruption attacks, and other cyber issues. Its analysis helps identify compromised data, good known copies of data, and insights into the origins of any compromised data.

  Should InfiniSafe Cyber Detection find corrupted data, it generates a list of corrupted files and tags them. This can also be fed back to a security operation center. Finally, it creates forensic reports to diagnose and identify the impact of the attack and provides recommendations for recovery.[5]

- ***InfiniVerse cloud-based monitoring and management platform.*** Infinidat includes its cloud-based InfiniVerse platform that helps monitor, manage, and optimize storage services on the InfiniBox. InfiniVerse collects millions of data points across Infinidat's global install base and analyzes this information in real-time. This collected data powers InfiniVerse's AIOps and DevOps capabilities to provide infrastructure-wide predictive analytics, monitoring, and reporting on capacity and performance. Additionally, its performance and capacity widgets (used, unassigned, free and snapshots) help organizations determine costs. For organizations with Green IT initiatives Infinidat added two "green" widgets, Historical Power Consumption (kW) and Historical CO2 Emissions (kg/h).

  InfiniVerse also includes consumption services and the option to future-proof the InfiniBox under its services umbrellas. InfiniVerse's Consumption Services feature offers a consumption-based, storage-as-a-service (STaaS) model for organizations that want a cloud-like operational model. For those organizations continuing to use a CapEx storage model, Infinidat's InfiniVerse Mobius feature provides a non-disruptive controller upgrade option that has no requirement for support uplift or prepayment programs. ■

Sources

1. https://www.fortunebusinessinsights.com/industry-reports/network-attached-storage-market-100505. Published March 10, 2025. Referenced 3/25/2025.
2. https://www.mordorintelligence.com/industry-reports/network-attached-storage-nas-market. Referenced 3/25/2025.
3. https://futurumgroup.com/document/infinidat-infinibox-product-review/. Referenced 4/16/2025.
4. https://www.infinidat.com/en/resource-pdfs/infinidat-infinibox-datasheet-us.pdf. Referenced 4/16/2025.
5. https://www.infinidat.com/en/resource-pdfs/infinisafe-cyber-detection.pdf. Referenced 4/16/2025.