Solution Profile

2025-26 DCIG TOP 5

CYBERSECURE NAS SOLUTIONS 10PB+ // US EDITION

Hitachi Vantara VSP One File Solution Profile

By

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

Hitachi Vantara VSP One File Solution Profile

Table of Contents

Cybersecure NAS Solutions 10PB+ // US Edition

Hitachi Vantara VSP One File Solution Profile

SOLUTION

Hitachi Vantara VSP One File

COMPANY

Hitachi Vantara, LLC.
2535 Augustine Drive
Santa Clara, CA 95054-3003
(678)403-3035

https://www.hitachivantara.com/en-us/products/storage-platforms/file-storage

DISTINGUISHING FEATURES OF HITACHI VANTARA VSP ONE FILE

- 100% Data Availability guarantee.
- At-rest (FIPS 140-2) and in-flight encryption, hardened immutable snapshots, MFA, RBAC, and WORM.
- Cohasset validation to meet stringent regulatory compliance requirements.
- Independently scale capacity and performance.
- Integrates hybrid cloud tiering directly into its file system layer to support tiering to Alibaba, AWS S3, Azure Blob, Google Cloud Storage, and VSP One Object.
- No-Questions-Asked 4:1 Effective Capacity guarantee.
- Scale-out, scale-up architecture.

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 susceptible to 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 nearly 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 fore¬casts 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 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 bank-ing information), alter transmitted data, or inject malicious payloads.

Recent security enhancements to NFS and SMB have given organizations increased confi-dence 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 susceptible to 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.

By NAS solutions utilizing more cybersecurity features and NFS and SMB protocols supporting encryption, organizations may continue embracing these technologies.

The State of Cybersecure NAS Solutions

Organizations deploy cybersecure 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 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 NAS solution internally, they expect it to remain highly available. To meet this expectation, providers generally ship their cybersecure 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

Each HA configuration provides benefits that align with specific organizational objectives. For instance, organizations with basic HA requirements may find a 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 all available 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 that scale over 10 petabytes (PBs) of internal capacity represent the bulk of available NAS solutions today. Further, many of these NAS solutions include options to tier data to object storage located on-premises or with cloud storage providers. Tiering allows a single NAS solution to manage tens or perhaps hundreds of petabytes of data.

Most cybersecure NAS solutions support both hard disk drives (HDDs) and solid-state drives (SSDs). However, the number of 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 NAS solutions represents perhaps the biggest contributor to their improved performance. Using SSDs, 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 NAS solutions delivering better performance.

Available Cybersecurity Features on NAS Solutions

All the evaluated 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 NAS solution does vary.

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 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 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 NAS solution represents a significant cyber security enhancement in recent years. Implementing MFA helps ensure only the appropriate individuals can access and manage the NAS solutions.

Some 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 NAS solutions. A growing number of NAS solutions use AI to monitor reads, writes, and changes in files to detect anomalies. If it detects an anomaly, the 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.

Hitachi Vantara VSP One File

Upon DCIG's completion of reviewing 23 cybersecure 10PB+ NAS solutions, DCIG ranked the Hitachi Vantara VSP One File as a TOP 5 solution. Hitachi Vantara makes its Virtual Storge Platform (VSP) One File NAS solution available in a scale-out, scale-up architecture. The VSP One File solution consists of two components, VSP One File controllers and VSP One Block appliances.

Continued

Cybersecure NAS Solutions 10PB+ // US Edition

Hitachi Vantara VSP One File Solution Profile

VSP One File offers a 100% Data Availability guarantee that ensures uninterrupted access during cyber threats or operational failures.

VSP One File controllers present file services to clients and deliver performance resources. Hitachi Vantara offers VSP One File in the up to 4-node File 34, and up to 8-node File 38.

These clustered controllers connect via Fibre Channel (FC) to the VSP One Block storage appliances on the backend to provide the storage capacity. This FC connectivity offers VSP One File access to local, high-performance TLC and QLC flash storage. This architecture affords VSP One File the flexibility to independently scale capacity and performance.

Additional features that help distinguish the Hitachi Vantara VSP One File from the other TOP 5 solutions include:

- ***Secures data against multiple types of cybersecurity events.*** NAS solutions are prime targets during cybersecurity events due to their broad accessibility, large-scale data storage, and critical business importance. VSP One File enhances protection with at-rest (FIPS 140-2) and in-flight encryption, hardened immutable snapshots, MFA, RBAC, and WORM features.

  VSP One File also integrates with multiple security solutions for identity and access management (IAM) and threat detection. For privileged access control it integrates with CyberArk. It also integrates with security platforms from Broadcom, Varonis, Splunk, and TrendMicro for advanced threat monitoring and rapid response. Additionally, VSP One File safeguards unstructured data with replication, active/active clustering, automated failover, and failback. These features minimize data loss and maintain operational continuity even during major disruptions.

  It backs these capabilities with Cohasset validation to ensure VSP One File meets stringent regulatory compliance requirements. These include SEC 17a-4(f), SEC 18a-6(e), FINRA 4511(c), CFTC 1.31(c)-(d), and MiFID II Delegated Regulation (72)(1). An independent assessment confirms VSP One File maintains records in a non-rewriteable, non-erasable format, support audit trails, and provide redundancy.

- ***Guarantees 100% Data Availability and 4:1 Effective Capacity.*** Downtime and escalating storage costs can prompt organizations to compromise on data protection, leaving critical assets vulnerable. VSP One File eliminates these concerns with a 100% Data Availability guarantee that ensures uninterrupted access during cyber threats or operational failures.

  The No-Questions-Asked 4:1 Effective Capacity guarantee further strengthens its cyber resilience position. This permits cost-effective data retention to allow organizations to store more immutable snapshots and protected copies of data.

- ***Cloud tiering core to VSP One File's architecture.*** Corporate file servers often store vast amounts of data. This contributes to making it difficult to classify critical data while increasing exposure to cyber threats.

  To address this challenge, VSP One File integrates hybrid cloud tiering directly into its file system layer. It intelligently moves data to secure cloud object storage while maintaining full visibility and control. It supports tiering to its VSP One Object, as well as to Alibaba, AWS S3, Azure Blob, and Google Cloud Storage.

  It also integrates with file services such as snapshots, replication, and data reduction to ensure tiered data remains protected. This limits the impact from ransomware attacks while preserving rapid recoverability. Additionally, it supports smart tiering policies to help organizations avoid egress fees and minimize costs. ■

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.