

# 2025-26 DCIG TOP 5

# CYBERSECURE NAS SOLUTIONS 10PB+ // GLOBAL EDITION



By

Jerome M Wendt, Principal Analyst

Ken Clipperton, Principal Researcher

Todd Dorsey, Sr. Storage Analyst

Joshua Konkle, Consulting Researcher

### Table of Contents

<b>3</b>	NAS Solutions Embrace Cybersecurity
3	Forecast Use and Growth of NAS
3	Network File Protocols Embrace Encryption
3	Cybersecurity Now Core to NAS Solutions
<b>4</b>	The State of Cybersecure NAS Solutions
4	High Availability
4	High Capacity
5	High Performance
<b>5</b>	Five Common Cybersecure NAS Solution Use Cases
<b>6</b>	Available Cybersecurity Features on NAS Solutions
6	Data Immutability
6	Encryption
6	Multi-factor Authentication
6	Artificial Intelligence
<b>7</b>	Features Common Across All Cybersecure NAS Solutions
<b>8</b>	Distinguishing Features of the TOP 5 Cybersecure NAS Solutions
<b>9</b>	Differences Between the TOP 5 Cybersecure NAS Solutions
<b>10</b>	TOP 5 Cybersecure NAS Solution Profiles
11	Tintri VMstore T7080
12	Arcitecta Mediaflux Appliances
13	Huawei OceanStor Dorado 6000
14	NetApp AFF A50
15	Nutanix Unified Storage
<b>16</b>	Cybersecure NAS Solution Inclusion Criteria
<b>16</b>	DCIG Disclosures

## Cybersecure NAS Solutions 10PB+ // Global Edition



Tintri VMstore T7080

Arcitecta Mediaflux

Huawei OceanStor Dorado 6000

NetApp AFF A50

Nutanix Unified Storage

*\*Products are listed with the licensee's product on top, followed by the other TOP 5 award recipients in alphabetical order.*

### EVALUATED CYBERSECURE NAS SOLUTIONS 10PB+

1. 45Drives Storinator XL60
2. 45Drives Stornado F2
3. Arcitecta Mediaflux
4. Cloudian HyperStore 4400
5. Cloudian HyperStore File 1100
6. Cloudian HyperStore Flash 2000
7. Dell PowerFlex File Services
8. Dell PowerScale F910
9. Dell PowerScale H700
10. Dell Unity XT 880F
11. Hitachi Vantara VSP One File
12. HPE GreenLake for File Storage MP
13. Huawei OceanStor Dorado 6000
14. IBM Storage Scale System 3500
15. IBM Storage Scale System 6000
16. Lenovo DSS-G280
17. NetApp AFF A50
18. Nexsan Unity NV10000
19. Nutanix Unified Storage
20. Oracle ZFS Storage Appliance ZS9-2
21. Pure Storage FlashBlade//E
22. Tintri VMstore T7080
23. Tintri VMstore T7040
24. VDURA Data Platform/ActiveStor Ultra Edge 100

### CATEGORIES OF EVALUATED FEATURES:

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

## 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 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.<sup>1</sup>

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.<sup>2</sup> 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 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. Additionally, 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.

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

- 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.

### 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.

***Flash use in cybersecure NAS solutions represents perhaps the biggest contributor to their improved performance.***

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.

### **Five Common Cybersecure NAS Solution Use Cases**

Organizations now utilize NAS solutions for many roles beyond simply delivering corporate file shares. As DCIG uncovered in its recent research into NAS solutions, organizations now routinely use them in the following five roles.

#### **Enterprise File Services**

Providing file services to users remains its principal use case and perhaps the primary context in which organizations view NAS solutions. Supporting both the network file service (NFS) and server message block (SMB) file networking protocols, they can centrally service Linux and Windows users alike. The introduction of more cybersecurity features into both file protocols and NAS solutions further ensures NAS retains its primary role in delivering file services.

NAS solutions have also taken steps to handle today's workloads that demand more capacity. To facilitate storing large amounts of data (tens or hundreds of petabytes), many internally support high-capacity HDDs or SSDs. Further, many connect to external object storage (*on-premises, in the cloud, or both*) to enable storing large amounts of data.

#### **Hosting Performance-sensitive Workloads**

Many organizations once viewed hosting performance-sensitive workloads such as databases on NAS solutions as problematic at best. This viewpoint has changed as Ethernet networking and NAS solutions have both improved to offer better performance and lower latency.

Application and database providers have recognized these improvements in Ethernet networks and the availability of SSDs in NAS solutions. These advances provide millisecond response times that applications need to run well on NAS-based architectures. This has led providers to certify hosting their applications on NAS solutions.

#### **Hosting Hypervisors**

Using NAS solutions as backend storage for server virtualization now represents a common production workload use case. Many organizations already host VMware vSphere datastores on NAS solutions, though other hypervisors also support backend NAS solutions. These include Microsoft Windows Hyper-V and Linux KVM implementations, such as from Red Hat Enterprise Linux. Further, organizations may potentially use the same NAS solution to host datastores for multiple hypervisors.

#### **Backup Target**

Deploying NAS solutions as a backup target represents yet another frequent use case for NAS solutions. Using NAS solutions in this role makes sense for at least two reasons.

First, all enterprise backup solutions recognize and support NAS solutions as backup targets. This expedites setting up backup processes while using NAS' easily understood architecture.

Second, should organizations need to restore files or perform a recovery, they often can directly access the NAS solution. They can navigate directly to the folder on the NAS solution hosting the

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

backups and restore the file or files. They may even use the NAS solution as backend storage when recovering and running a restored VM. While the NAS solution may not perform as well as production storage (though it might), it expedites organizations getting up and operational.

### **Edge/Remote**

Many organizations of all sizes operate edge and remote offices that also face rapidly growing storage requirements. Here again, many cybersecure NAS solutions offer models with lower maximum capacity limits to meet the needs of these offices. Using these NAS solutions enables organizations to centrally monitor, manage, and secure data at these distributed sites.

Most NAS solutions also support replication that serves a two-fold purpose. They can replicate data back to the central office, or alternatively, replicate data to edge and remote sites.

## **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.

### **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

**25Gb Ethernet represented the more commonly supported Ethernet interface on cybersecure NAS solutions that scale over 10PB.**

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.

## Features Common Across All Cybersecure NAS Solutions

DCIG evaluated about 40 different cybersecure NAS solutions, of which 24 met DCIG's criteria for this 10PB+ global edition. Across these 24 cybersecure NAS solutions, DCIG evaluated over 300 features on each one. Due to the relative maturity of all these products, all cybersecure NAS solutions share support for multiple features. DCIG found that the following features (*listed in alphabetical order*) were supported by 90 percent or more of these 24 solutions:

1. **25Gb Ethernet.** While all cybersecure NAS solutions support Ethernet, 25 Gigabit (Gb) Ethernet represented the more commonly supported Ethernet interface. Over 90 percent of evaluated solutions supported 25Gb Ethernet interfaces with 10Gb and 100Gb being the next most supported interfaces (83 percent each).
2. **3- and 5-year hardware maintenance contracts.** The availability of both three and five-year hardware maintenance contracts from all NAS providers suggests today's cybersecure NAS solutions offer improved durability and reliability.
3. **AD and LDAP integration.** Ransomware and insider threats have prompted cybersecure NAS solution providers to implement better forms of identity management. All the evaluated solutions integrate with and support Active Directory (AD) while over 90 percent support the lightweight directory access protocol (LDAP).
4. **Asynchronous replication.** Using asynchronous replication represents a feature that organizations often use on their NAS solutions. They may use it for business continuity, centralizing data from remote sites, content distribution to remote sites, or disaster recovery. Over 90 percent of the cybersecure NAS solutions support periodic asynchronous replication, with all solutions supporting some form of replication.
5. **AWS S3 storage target.** Amazon Web Services Simple Storage Service (S3) APIs has resulted in these APIs becoming a default industry standard for object storage. It also has resulted in all cybersecure NAS solutions supporting the AWS S3 APIs as a storage tier. However, products differ in which S3 operations they may perform on AWS S3 objects.
6. **Compression.** Over 90 percent of cybersecure NAS solutions offer compression to minimize data growth and control storage costs. However, NAS solutions may vary in how they implement compression (inline or post-process, or both). Further, they may offer the option to turn compression off or on systemwide or granularly (specific folders.)
7. **Encrypt data at-rest.** Using the cybersecure NAS solution to perform encryption still represents a common way that organizations encrypt their data. By encrypting files, even if a hacker obtains a copy of them, the hacker cannot read the data. Over 90 percent of the cybersecure NAS solutions support encryption of data at-rest.
8. **Multi-tenancy** permits multiple departments or organizations to use the same physical cybersecurity NAS solution. The NAS solution will then maintain logical isolation and instances of the departments or organizations using it. All evaluated cybersecure NAS solutions support this feature.
9. **Multiple options to contact technical support with 4-hour response times and 24x7x365 availability.** Over 90 percent of cybersecure NAS solution providers

**Organizations should expect to pay for a support contract to obtain higher levels of technical support.**

offer email, phone, an online knowledge base, and the web to contact support. Once contacted, all offer technical support 24x7x365, with over 90 percent offering onsite support, remote technical support logins, and response times in under four (4) hours. However, organizations should expect to pay for a support contract to obtain these higher levels of technical support.

**10. NFSv3 and SMB 3.0.** Organizations that want to fully utilize cybersecurity functionality on these NAS solutions should note how each one supports NFS and SMB. While all cybersecure NAS solutions support these two file networking protocols, they do not support all versions of them equally. All NAS solutions universally support NFSv3 and SMB 3.0, with 95 percent supporting NFSv4. However, under 60 percent support SMB 3.1.1, and only two-thirds of the evaluated solutions support both these protocols concurrently.

**11. Web-based GUI and CLI management interfaces.** Over 90 percent of cybersecure NAS solutions offer either a command line interface (CLI), a web-based graphical user interface (GUI), or both that organizations may use to manage it.

Additional features that over 90 percent of cybersecure NAS solutions support include the following:

- **Access control policies** to implement and enforce an organization's internally-defined data security and governance policies.
- **Email alerting** to notify organizations of alerts generated by the cybersecure NAS solution.
- **At least 256GB of RAM** per cybersecure NAS solution in its largest configuration.
- **At least 40 CPU cores** per cybersecure NAS solution in its largest configuration.
- **Multi-factor authentication** for secure logins.

## Distinguishing Features of the TOP 5 Cybersecure NAS Solutions

Each of the TOP 5 products supports all the features listed above. The TOP 5 cybersecure NAS solutions further distinguish themselves by supporting all the following features. The large number of additional supported features highlights the overall maturity of cybersecure NAS solutions. These, in alphabetical order, include:

- 1. All-flash configurations.** To accommodate workloads that demand high performance and low latency, each TOP 5 NAS solution offers an all-flash configuration.
- 2. Auto-tiering leveraging DRAM, flash, or SCM.** In addition to offering an all-flash configuration, each TOP 5 solution offers tiering. This permits the NAS solution to utilize higher performing tiers of flash such as DRAM or storage class memory (SCM) for improved read and write performance. They may then use QLC or TLC SSDs for more cost-effective, long-term storage.
- 3. Multiple fast Ethernet options.** In addition to supporting 25Gb Ethernet, all TOP 5 solutions support 10, 40, and 100Gb Ethernet. These give organizations the option to use the most appropriate form of Ethernet connectivity for their environment and workloads.
- 4. Deduplication.** Each TOP 5 solution offers additional means for organizations to reduce the size of their data stores using deduplication. Further, each one supports both inline and post-processing deduplication to better manage deduplication's performance overhead.
- 5. Encryption—array controller-based and self-encrypting drives.** Encryption represents another feature that can incur a performance hit when enabled. To help

***Each TOP 5 solution gives organizations the flexibility to scale-out or scale-up capacity and performance as-needed and on-demand.***

organizations control and manage encryption performance overhead, all TOP 5 solutions support encryption using the array controller and self-encrypting drives. These two give organizations more flexibility to choose the best form of encryption for their environment.

6. **More replication options.** All TOP 5 solutions support multiple forms for replication in addition to periodic asynchronous replication. Each one provides support for continuous asynchronous replication, synchronous replication, and synchronous replication in metro clusters. These give organizations the flexibility to choose specific types of replication for specific workloads or business needs.
7. **REST APIs.** Each cybersecure NAS solution offers its own set of REST APIs. The REST APIs offered by each cybersecure NAS solution differ from the more well-known AWS S3 APIs. The REST APIs permit activities such as third-party applications managing or monitoring the cybersecure NAS solution.
8. **Retention policies.** Each TOP 5 solution permits implementing retention policies. These policies manage a data's lifecycle, including how long it gets retained, if it gets archived, and eventually deleted. Using this feature permits organizations to retain the right data for the right amount of time to comply with legal, regulatory, and business requirements.
9. **Scale-out and scale-up.** Each solution gives organizations the flexibility to scale-out or scale-up capacity and performance as needed and on-demand. These two options have become more critical for organizations due to the dynamics of today's NAS environments. While each solution scales to over 10PBs of storage capacity, they also scale out to support at least 24 controllers. In so doing, organizations can more granularly add storage capacity, performance, or both as their environment demands.
10. **WAN optimization—bandwidth throttling and compression.** Moving large amounts of data between different NAS solutions locally or remotely can take a significant amount of time. To help move and manage this data movement more effectively, each TOP 5 solution offers bandwidth throttling and compression to optimize WAN traffic.
11. **WORM file format.** Storing data in a write once, read only (WORM) format helps eliminate the possibility that ransomware may alter, delete, or encrypt stored data. Each of these TOP 5 solutions supports a WORM file format to prevent any changes to files once stored.

## Differences Between the TOP 5 Cybersecure NAS Solutions

While the TOP 5 cybersecure NAS solutions possess many similarities, they also differ in their implementation of multiple features. These differences primarily appear in how organizations may deploy them, their HA controller configurations, support for other general-purpose and purpose-built cloud object storage targets, and how they support snapshots. While each TOP 5 cybersecure NAS solution supports more than one of these features, they do implement them differently. Consider:

- **Deployment options.** All TOP 5 cybersecure NAS solutions give organizations multiple ways in which to deploy them. While the NAS solution must ship as a preconfigured physical appliance to be included in this report, each provider offers other deployment and support options.

Four offer software-defined storage (SDS) deployments with two options. One allows deploying the NAS solution on other provider's hardware, though the choice of hardware will vary. The other option permits deploying the NAS solution as an instance in various public clouds. Here again, public cloud support will vary by NAS provider.

***The TOP 5 cybersecure NAS solutions vary in supporting public cloud storage targets other than AWS S3.***

Organizations may also elect to deploy the NAS solution as a storage-as-a-service (STaaS). In this deployment model, the vendor provides most or all support services. Four vendors offer STaaS as both an on-premises configuration and managing their NAS solution in a colocation facility. Three also deliver their NAS solution via STaaS in a provider-managed cloud with another three offering their NAS solution using STaaS in a public cloud.

- **HA controller configurations.** All TOP 5 solutions ship with HA controller configurations. However, they use different controller configurations to provide high availability. Two offer Active-Active configurations that permit the two controllers to access all backend LUNs equally and concurrently. Three providers use Active-Standby controller configurations that assign all LUNs to one controller, which then fail over to the other controller should the primary one go offline.

Since each TOP 5 solution supports scale-out, each new appliance gets added to the cluster in a two-controller configuration. Four NAS solutions then manage the appliances in the scale-out cluster using a federated architecture.

- **Other general-purpose and purpose-built cloud object storage targets.** Most organizations now utilize multiple clouds. Further, utilizing multiple cloud object storage providers for storage tiering represents a common first way that organizations adopt multiple clouds.

Despite organizations adopting multiple cloud storage targets, cybersecure NAS solutions vary in supporting cloud storage other than AWS S3. Four support Microsoft Azure Blob, three support Alibaba and Wasabi Hot Cloud Storage, and two support Google Cloud Storage.

- **Snapshots.** More organizations look to create regular backups of their files and folders in the form of snapshots for multiple reasons. While protecting against ransomware events represents a common motivation, snapshots also facilitate shorter recovery time objectives (RTOs) and recovery point objectives (RPOs).

All TOP 5 NAS solutions support snapshot functionality but implement it differently. For example, four offer the option to:

- Automatically and continuously take snapshots.
- Create VM-level snapshots that only capture data associated with a VM.
- Take immutable snapshots that cannot be altered once created.
- Take space-efficient snapshots by using various data reduction techniques, such as only storing changes since the last snapshot, compressing and deduplicating snapshots, or using thin provisioning.

## TOP 5 Cybersecure NAS Solution Profiles

Each of the following TOP 5 cybersecure NAS solution profiles highlights at least three ways each one differentiates itself. These differentiators represent some of the best methods that cybersecure NAS solutions offer to store and/or secure data using network file protocols. Within each solution, organizations may find specific features that better meet their needs.

***VMstore's TxOS makes each snapshot both immutable and "invisible" by storing each one on internally reserved storage space that no applications can access.***

### **Tintri VMstore T7080**

Tintri by DDN makes its VMstore T7080 solution available in a scale-out architecture. Deployed as a dual controller appliance, VMstore scales from one to 64 nodes in a federated cluster. VMstore can scale by drive, controller, or frame and supports combining disparate models within the management cluster.

Each VMstore runs the Tintri Operating System (TxOS) that Tintri has optimized to host containerized applications, databases, and VMs. For instance, VMstore's TxOS gives each persistent volume, database, or VM its own path or "lane" to storage. This technique balances performance across VMs, and applications hosted on VMstore while mitigating the noisy neighbor problem.<sup>19</sup>

Additional features that help distinguish the Tintri VMstore T7080 from the other TOP 5 solutions include:

- **Optimizes VM performance for multiple different hypervisors.** Broadcom's recent VMware software licensing changes have prompted more organizations to consider adopting VMware vSphere hypervisor alternatives. VMstore well positions any organization considering such a change. A single VMstore may concurrently support Citrix Hypervisor, Microsoft Hyper-V, RedHat Enterprise Virtualization, and VMware vSphere.<sup>20</sup>

- **Secure VM snapshots and fast recoveries.** VMstore protects and secures data against cybersecurity events while offering fast, granular recovery options. In addition to MFA and RBAC, the VMstore T7080 offers a sophisticated, immutable, "invisible" snapshots feature.

VMstore can take more than 100 per-VM snapshots. VMstore's TxOS makes each snapshot both immutable and "invisible" by storing each one on internally reserved storage space that no applications can access.<sup>21</sup> Its SyncVM function then gives organizations the flexibility to store snapshot copies either locally or in the cloud.<sup>22</sup>

SyncVM further helps identify the best snapshot for recovery by preserving each VM's associated snapshot and performance history. Organizations can analyze these snapshots for any inconsistencies or anomalies to find the best one for recovery. They may then recover either an entire VM or recover specific files or folders.

- **Workload-aware enabling VMstore to identify break/fix and performance issues.** The Tintri Global Center software, included with VMstore TxOS, monitors the full application stack down through the storage layer. This visibility into the application stack enables it to perform multiple functions such as:
  - Quickly detecting and reporting on hardware issues and failures.
  - Troubleshooting latency issues across the host, network, and storage layers.
  - Drilling into performance metrics of individual VMstores or individual applications.

Using Tintri Global Center Advanced introduces additional management features for large VMstore deployments. It treats all VMstores as a single, federated pool of resources and automatically optimizes application placement across them.<sup>23</sup>

***Arcitecta Mediaflux enables organizations to initiate searches across petabytes to exabytes of data and get results in under a minute rather than hours or even never.***

### **Arcitecta Mediaflux Appliances**

Arcitecta got its start as a data management software provider before making its Mediaflux software available as a pre-integrated appliance. Arcitecta now offers three Mediaflux appliance models in highly available configurations: the Burst, the Edge, and the Multi-site.

The Burst model utilizes data stored locally but leverages cloud computing resources, or another location with available resources, when local deployments have limited computing resources. The Edge model primarily serves as a cache for centrally stored data that edge applications and users frequently access. The Multi-Site model creates a unified view of the data through a global namespace and manages large datasets across multiple locations.

Additional features that help distinguish the Arcitecta Mediaflux Appliances from the other TOP 5 solutions include:

- ***Space efficient metadata database facilitates data management at scale.*** Multiple NAS solutions scale to host and manage tens or hundreds of petabytes of data. However, managing and searching all that data to locate needed data may become inefficient at best and impossible at worst.

Arcitecta created its own XML Object Database, XODB, to overcome this challenge. XODB's compact size facilitates Mediaflux's ability to manage large-scale file stores across globally distributed environments. It enables organizations to initiate searches across petabytes to exabytes of data and get results in under a minute rather than hours or even never.

- ***Offers near-zero RPOs and RTOs for large amounts of data.*** Storing large amounts of data on a NAS solution creates challenges on two fronts. It makes completing either fast backups or recoveries of all this data very difficult to achieve.

Mediaflux's Point in Time recovery capability addresses these two challenges. It provides continuous, real-time data protection and rapid recoveries for data managed by Mediaflux. However, Point in Time differentiates itself from NAS snapshot features in an important way. It leverages XODB's capture of every structural and data change to permit near-instantaneous recovery to any previous point in time.

- ***Manages data across multiple backend storage systems and media types.*** Arcitecta optimizes Mediaflux to store and manage large amounts of distributed data that can scale to exabytes. To cost-effectively store all this data, it supports multiple types of backend storage media. In addition to supporting HDDs and SSDs, it supports block, cloud object storage, NAS, and tape.
- ***Licenses Mediaflux software by appliance.*** NAS providers often license their solutions based on the total amount of capacity or data stored. Arcitecta licenses its software by Mediaflux appliance based on the number of concurrent users accessing it. This allows organizations to store large amounts of data on a Mediaflux appliance without incurring additional software licensing costs.

***The OceanStor Dorado's HyperDetect data protection technology offers three options to detect ransomware in files.***

### **Huawei OceanStor Dorado 6000**

The Huawei OceanStor Dorado 6000 mesh architecture enables organizations to start small and scale the Dorado 6000 out if needed. The OceanStor Dorado 6000 can start with one dual-controller node and scale out to sixteen dual-controller nodes. Its controllers then communicate with one another over a 25Gb or 100Gb RDMA mesh to deliver high performance.<sup>3</sup>

The Dorado 6000 includes both block (FC/iSCSI) and file (NFS/SMB) protocols as part of its scale-out OceanStor operating system. Huawei notably implements file protocols using an active-active distributed file system, which is made possible by Dorado's mesh architecture.

The Dorado 6000 OceanFS distributed file system eliminates controller ownership of the file system. It evenly distributes directories and files across all controllers using a balancing algorithm. Each Dorado 6000 controller then processes the read and write I/Os of the directories and files that reside on it. The Dorado 6000 may then utilize all available resources across its storage controllers to deliver file services.<sup>4</sup>

Additional features that help distinguish the Huawei Oceanstor Dorado 6000 from the other TOP 5 solutions include:

- **Multiple ransomware detection options.** The OceanStor Dorado's HyperDetect data protection technology offers three options to detect ransomware in files.
  - **Ransomware file interception** monitors for ransomware strains that generate encrypted files with specific file name extensions. It identifies them and intercepts any writes to files with those file name extensions.
  - **Real-time ransomware detection** analyzes file I/O behavior characteristics. It monitors the file system by constantly performing content analysis on files. It then filters out files it classifies as "abnormal," creates a secure snapshot of that file system, and generates alerts.
  - **Intelligent ransomware detection** builds on the real-time ransomware detection feature. In addition to constantly monitoring the file system, it analyzes and compares changes in file system snapshots. It then uses machine learning algorithms to check changes in snapshots for the presence of ransomware.<sup>5</sup>
- **Offers its own backup application.** The Dorado 6000 offers its own CloudBackup that builds on its file system snapshot functionality. CloudBackup uses file system snapshots to then back up files to object storage located either on-premises or in the cloud without the need for extra backup servers. CloudBackup supports periodic incremental and periodic synthetic full backups along with full file system recoveries or recoveries of specific files.<sup>6</sup>
- **Utilizes containers to deploy its services.** The overhead associated with running backups, ransomware detection, and other services can potentially degrade file services. To mitigate any possibility of degradation or disruption of file services, the Dorado 6000 utilizes containers to host these services. This technique helps the Dorado 6000 control the impact of these services on performance for production workloads.<sup>7</sup>

***NetApp includes AI-powered ransomware detection that could successfully and accurately identify 99 percent of ransomware occurrences.***

### **NetApp AFF A50**

The NetApp AFF A50 exclusively uses SSDs and comes as a dual-controller appliance in an active-active configuration. An AFF A50 deployment may begin with a single appliance and scale out to twelve A50 appliances in a cluster. AFF A50 appliances in a cluster communicate with one another using either a 40Gb or 100Gb Ethernet connections.<sup>8</sup>

The AFF A50 utilizes NetApp's latest ONTAP 9 multiprotocol software to provide data management, file, and storage services. To provide file services, NetApp uses its own Write-Anywhere-File-Layout (WAFL) file system. NetApp specifically designs WAFL to manage file activity and deliver prompt responses to write requests while optimizing backend data storage.<sup>9</sup>

Additional features that help distinguish the NetApp AFF A50 from the other TOP 5 solutions include:

- ***Includes AI-powered ransomware detection in ONTAP.*** Detecting the presence of ransomware has increasingly become more difficult due to more sophisticated means of attacks. To more quickly and effectively detect ransomware, NetApp includes AI-powered ransomware detection with ONTAP (v9.15 or later.) Once enabled, it was found by a third-party lab to successfully and accurately identify 99 percent of ransomware occurrences. This includes successfully identifying patterns and anomalies now often associated with ransomware attacks.<sup>10</sup>
- ***Offers a ransomware recovery guarantee.*** Every organization possesses legitimate concerns about successfully restoring data compromised during a ransomware event. To alleviate these concerns, NetApp offers its Ransomware Recovery Guarantee that extends to AFF A50 systems. To enable this guarantee, organizations must contact NetApp Professional Services. It must then complete and successfully validate a SnapLock Compliance Volume on the organization's AFF A50.<sup>11</sup>
- ***NetApp BlueXP to monitor and manage IT resources across hybrid cloud environments.*** The hybrid environment in which many organizations operate already makes understanding them challenging. To diagnose any issues that arise adds yet another level of complexity.

To address this common concern of organizations, NetApp introduced BlueXP. BlueXP offers a single control plane for organizations to build, protect, and govern their on-premises and cloud deployments. It specifically gives organizations the tools to better store, move, protect, and analyze data across their hybrid.

Organizations may use BlueXP to first discover the AFF A50 and then manage file services and storage resources on it. They may also use it to perform data mobility functions such as moving data between NetApp systems or implementing storage tiering. They may even use it to perform backups as well as analyze and classify data stored on the AFF A50.<sup>12</sup>

***NUS offers multiple storage optimization technologies that minimize capacity requirements while considering performance demands.***

### **Nutanix Unified Storage**

Nutanix delivers Unified Storage as software-defined storage (SDS) based on a hyper-converged architecture with scale-out and scale-up options. In addition to its own configured-to-order Nutanix NX nodes, Nutanix makes its SDS available on server hardware platforms. It offers them from seven original equipment manufacturers (OEMs) and eleven third-party providers.<sup>13</sup>

Nutanix Unified Storage (NUS) provides features not routinely available in NAS solutions. For example, NUS may host virtual machines on its platform. Organizations may also “right-size” NUS to accommodate their different size IT environments with varying requirements. NUS supports single-node deployments as well as two to 32-node cluster configurations.

Additional features that help distinguish the Nutanix Unified Storage from the other TOP 5 solutions include:

- ***Proactively identifies and resolves technical issues.*** NAS solutions often support core business processes that have few, if any, tolerances for degradations in service or outages. To prevent these scenarios, Nutanix offers Nutanix Insights which includes its Pulse and Alert support services to provide context-aware support.

The Pulse support service regularly captures diagnostic data that gets anonymized and transmitted back to Nutanix. Nutanix then monitors and analyzes this data to proactively identify issues and make recommendations on how to resolve them.

In contrast, events drive how the Alert support service functions. Should a hardware or software issue occur, NUS generates an alert and notifies Nutanix. Nutanix then proactively troubleshoots and diagnoses the cause of the alert and, if needed, creates a support case to resolve it.<sup>14</sup>

- ***Constantly assesses its security posture.*** Enabled by default, NUS leverages the Security Configuration Management Automation (SCMA) framework to inspect all its running services. Running on a schedule set by an organization, SCMA assesses over 800 NUS settings to ensure they meet or exceed regulatory requirements. Nutanix logs any inconsistencies, and it enables NUS to self-heal from any deviations from preset security baseline configurations.<sup>15</sup>
- ***Employs multiple data optimization and placement features.*** NUS offers multiple storage optimization technologies that minimize capacity requirements while considering performance demands. For example, NUS supports both inline and post-process data reduction technologies and gives organizations a choice in how to implement them.<sup>16</sup> Also, as file data ages or goes “cold”, NUS Smart Tiering can tier “cold” data off to other storage on-premises or in the cloud.<sup>17</sup>

When some VMs write more data than others or when cluster configurations change, the per-node capacity utilization can become skewed. Nutanix disk balancing runs both as a scheduled process and when a node breaches a set capacity threshold. The automated disk balancing process restores balance by moving the coldest data on the overused node to other cluster nodes.<sup>18</sup>

### Cybersecure NAS Solution Inclusion Criteria

The inclusion criteria for each cybersecure NAS solution are as follows:

1. Available globally as a preconfigured physical appliance.
2. Supports either the network file system (NFS) or server message block (SMB) network file protocol.
3. Scaled to support at least ten (10) petabytes of usable physical storage capacity.
4. Be commercially available on or by February 1, 2025.
5. DCIG can publicly evaluate the solution.
6. Achieved a sufficiently high score on DCIG's internal evaluation
7. Sufficient information is available to DCIG for DCIG to make an informed, defensible decision on the product's capabilities.

### DCIG Disclosures

Providers of some cybersecure NAS solutions covered in this DCIG TOP 5 report are or have been DCIG clients. In that vein, consider the following when evaluating the information contained in this TOP 5 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 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a TOP 5 designation.
- DCIG based its research and reached conclusions using publicly available information, information shared by the provider, and the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate if features worked as described.
- No negative inferences should be made against any provider or solution not covered in this TOP 5 report.
- It is a misuse of this TOP 5 report to compare solutions included in this report against those not included.

No provider was privy to how DCIG weighted individual features. In every case, the provider only found out the rankings of its solution after DCIG had completed its analysis. To arrive at the TOP 5 solutions included in this report, DCIG went through a seven-step process to reach an objective conclusion.

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

### 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://e.huawei.com/en/material/storage/all-flash-storage/17f29b2a779a4948bce56161a31eef97>. Pg. 36. Referenced 3/23/2025.
4. Ibid. Pg 43. Referenced 3/23/2025.
5. <https://support.huawei.com/enterprise/en/doc/EDOC1100278583/d8db409b/overview>. Referenced 3/23/2025.
6. <https://support.huawei.com/enterprise/en/doc/EDOC1100233763/6bae019d/overview>. Referenced 3/23/2025.
7. [https://support.huawei.com/enterprise/en/doc/EDOC1100233763/6053cf9d/concepts-related-to-the-container-service#EN-US\\_TOPIC\\_000001552739041](https://support.huawei.com/enterprise/en/doc/EDOC1100233763/6053cf9d/concepts-related-to-the-container-service#EN-US_TOPIC_000001552739041). Referenced 3/23/2025.
8. <https://docs.netapp.com/us-en/ontap-systems/a20-30-50/install-cable.html#step-1-cable-the-clusterha-connections>. Referenced 4/1/2025.
9. <https://www.netapp.com/media/23892-sw-WAFL.pdf>. Page 2. Referenced 4/1/2025.
10. <https://community.netapp.com/t5/Tech-ONTAP-Blogs/NetApp-s-AI-based-real-time-ransomware-detection-solution-achieves-AAA-rating/ba-p/453379>. Referenced 4/1/2025.
11. <https://www.netapp.com/how-to-buy/sales-terms-and-conditions/additional-terms/ransomware-recovery-guarantee/>. Referenced 4/1/2025.
12. <https://bluexp.netapp.com/blog/netapp-bluexp-unifying-the-data-estate>. Referenced 4/1/2025.
13. <https://portal.nutanix.com/page/documents/list?type=compatibilityList>. Referenced 3/21/2025/
14. <https://www.nutanix.com/content/dam/nutanix/en/resources/datasheets/ds-nutanix-support-services-pulse-alerts.pdf>. Referenced 3/22/2025.
15. [https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v5\\_17:sec-security-nutanix-security-infrastructure-wc-c.html](https://portal.nutanix.com/page/documents/details?targetId=Nutanix-Security-Guide-v5_17:sec-security-nutanix-security-infrastructure-wc-c.html). Referenced 3/22/2025.
16. <https://download.nutanix.com/solutionsDocs/TN-2032-Data-Efficiency.pdf>. Pg. 9. Referenced 3/22/2025.
17. [https://download.nutanix.com/documentation/files\\_v51/Files-v5\\_1.pdf](https://download.nutanix.com/documentation/files_v51/Files-v5_1.pdf). Pg. 138. Referenced 3/22/2025.
18. <https://download.nutanix.com/solutionsDocs/RA-2019-Virtualizing-Splunk-on-Nutanix.pdf>. Pg. 25. Referenced 3/22/2025.
19. <https://tintri.com/wp-content/uploads/2022/12/tech-brief-011-tintri-OS-3.pdf>. Referenced 3/19/2025.
20. <https://tintri.com/wp-content/uploads/2023/11/data-sheet-009-vmstore-t7000.pdf>. Referenced 3/19/2025.
21. <https://tintri.com/wp-content/uploads/2023/01/211207-DCIG-Tintri-VMStore-Ransomware-Recovery-Tech-Report.pdf>. Pg. 3. Referenced 3/19/2025.
22. <https://tintri.com/blog/dont-let-your-data-become-a-hostage/>. Referenced 3/19/2025.
23. <https://www.tintri.com/wp-content/uploads/2023/01/tech-brief-009-tintri-global-center.pdf>. Referenced 3/18/2025.

### 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](http://www.dcig.com).



DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552

[dcig.com](http://dcig.com)

© 2025 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.