SEPTEMBER 2025

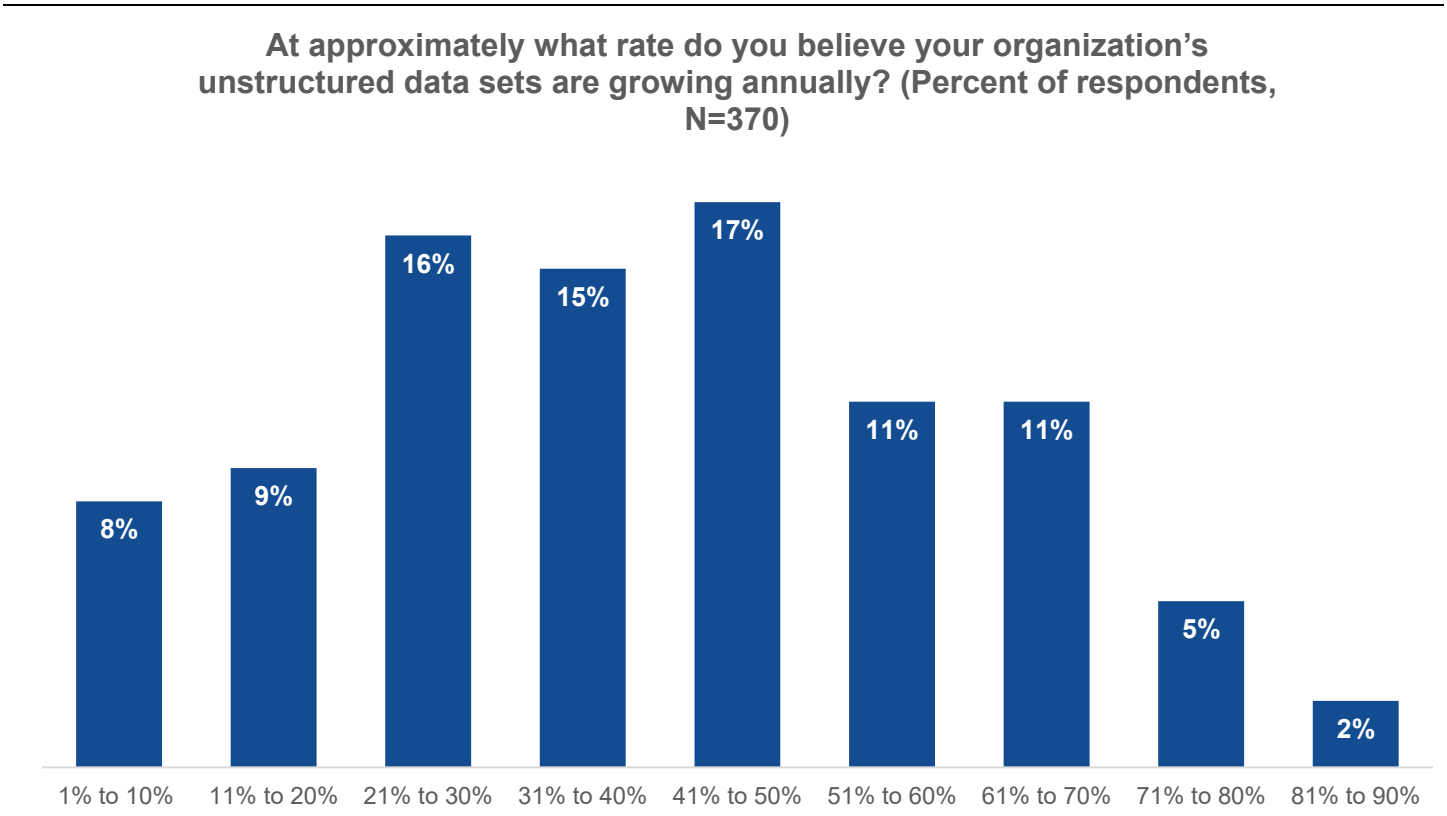
Modernizing Legacy NAS With CTERA

Alex Arcilla, Principal Analyst – Validation Services

Challenges Encountered With Legacy NAS

Network-attached storage (NAS) remains a critical part of an organization's storage strategy, as Enterprise Strategy Group found that 61% of organizations have deployed NAS within their on-premises data centers, while 44% planned to accelerate their NAS spending over the next couple of years.[1] This comes as no surprise, as we found that nearly half of survey respondents stated that their unstructured data will grow at least 40% or more annually.(see Figure 1).[2]

Figure 1. Nearly Half of Organizations Are Facing At Least 40% Growth in Unstructured Data



Source: Enterprise Strategy Group, now part of Omdia

[1] Source: Enterprise Strategy Group Research Report, *Navigating the Cloud and AI Revolution: The State of Enterprise Storage and HCI*, March 2024.
[2] Source: Enterprise Strategy Group Complete Survey Results, *Reinventing Data Loss Prevention: Adapting Data Security to the Generative AI Era*, May 2025.

As with any data growth, whether structured or unstructured, organizations must ensure that:

- Capacity can grow accordingly without needing to overprovision and without running out of space to ensure business continuity.
- End users can access any amount of data with minimal delay.
- Data is constantly protected against cyberattacks and ransomware.
- Data can be recovered with minimal or no loss (translating into minimized RTOs and RPOs).

Addressing these challenges with legacy NAS platforms in highly distributed environments is likely to be difficult.

As data growth continues, scalability and performance remain two top factors to consider with any storage platform. Yet legacy NAS devices in today's highly distributed environments were not built to easily scale; organizations still rely on best-guess forecasts and overprovisioning to deal with unexpected growth spikes. And as end users access more data from NAS devices, performance issues arise, especially when sharing large files or facing heavy network traffic. Addressing these challenges leads to scaling up or scaling out existing NAS and, ultimately, to increased capital costs and more operational complexity.

Highly distributed environments call for collaboration, as end users are not limited to working from a centralized location. However, legacy NAS limits how effectively end users can collaborate. While legacy NAS was ideal for storing data needed only by users at single locations, using NAS in distributed environments can easily lead to data silos. With end users sharing data across locations, multiple data versions emerge, leading to data fragmentation, duplication, and inconsistency. Not only does this cause user confusion, but it also leads to operational problems and ever-increasing storage costs. This cycle will continue to balloon as organizations begin deploying AI products and services and need to uncover the value lying within their unstructured data.

The continued onslaught of cyberattacks and ransomware also leaves legacy NAS in a precarious position. Existing NAS devices can be a weak link in the evolving threat landscape, as organizations might not adhere to the latest security practices consistently across the entire NAS infrastructure. Inconsistent security defenses in place can lead to security gaps.

If the business were disrupted, recovery is paramount to minimize downtime. Unfortunately, local backup and recovery are the norm with NAS deployed in distributed environments. Not only would there be inconsistent backup and recovery procedures in place, but any recovery would lead to further data fragmentation. This process disrupts users and typically introduces additional security threats.

Solution – CTERA Intelligent Data Platform

With a security-first approach, CTERA designed a global file system (GFS) for multi-site collaboration to address scalability, performance, and security challenges organizations face with legacy NAS. Using single namespace file and object storage access, the file system provides a centralized and consistent cloud storage-like experience for managing, scaling, and securing storage of unstructured data, while giving end users the local access experience typical of legacy NAS storage.

The CTERA Intelligent Data Platform is deployed as a hub-and-spoke model running on a hybrid cloud architecture and deployed using:

- The CTERA Portal, which delivers a centralized cloud-like experience, providing a single source of truth and control via "single-pane-of-glass" management. With the portal, organizations can orchestrate and automate services such as new deployments using infrastructure as code and data services to support business operations and continuity.
- CTERA Edge Filers, which enable data access for local and remote physical offices.

- CTERA Drive, which provides remote file access and sharing for user workstations and mobile devices outside office settings.
- Object-native backend storage built on a private or public cloud architecture. (CTERA offers an extensive ecosystem comprised of on-premises storage vendors and IaaS providers, including Amazon Web Services, Microsoft Azure, IBM Cloud, HPE, Hitachi Vantara, and Cloudian.)

To enable the high performance and low latency that end users expect with local NAS, the CTERA platform leverages caching technology in both CTERA Edge Filers and Drives. Used in combination with other technologies (primarily WAN optimization, compression, and deduplication), CTERA enables low-latency times, as frequently accessed (hot) data is kept in cache, removing the need to retrieve the same data repeatedly from a centralized location. The use of caching technology speeds up write operations, as local cache can be updated and synced up in the cloud so that all users can access the same data version. While hot data is easily accessible, end users can view all hot and cold data. End users can automatically recall cold data stored in the cloud when needed.

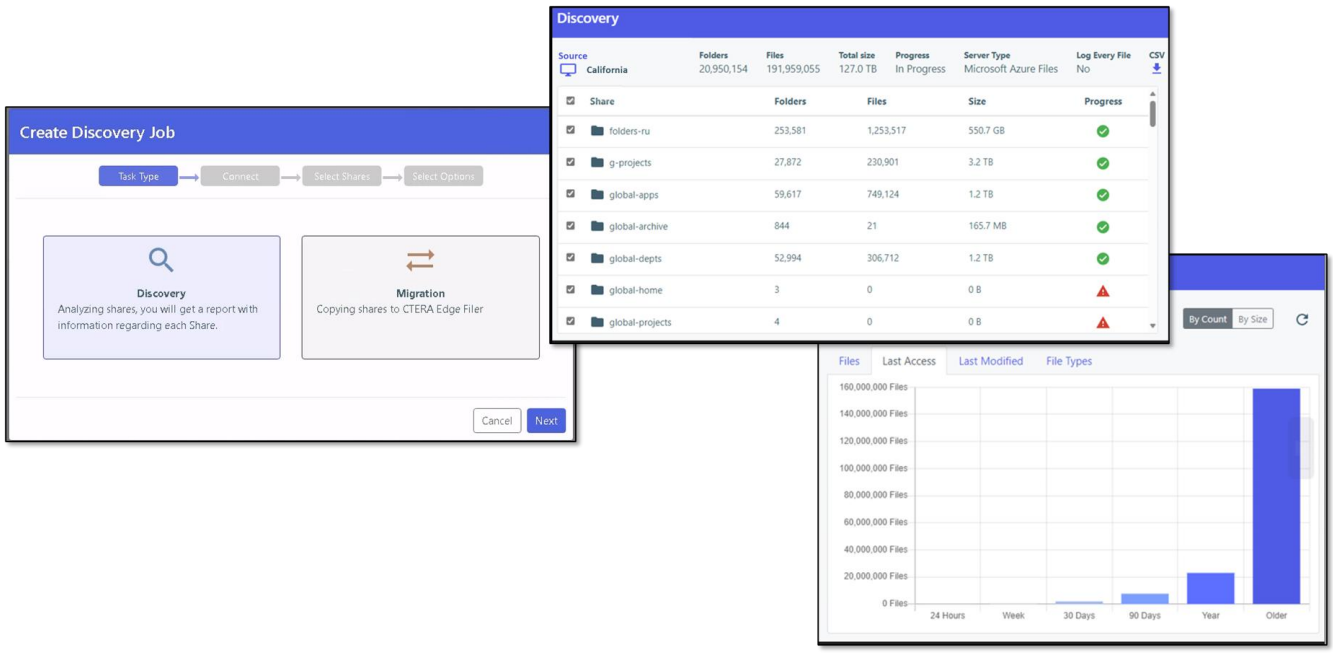
With caching, organizations can streamline data storage, as the CTERA GFS can eliminate the need for remote site backup and disjointed disaster recovery systems and procedures and updates data in the cloud with the latest version when modified in local cache. Deduplication and compression with CTERA Edge Filers and CTERA Portal also streamline data storage by eliminating redundant data copies and minimizing the storage footprint. The reduced amount of storage used helps to increase operational efficiency and reduce capital and operational expenses.

CTERA also leverages multiple technologies for bolstering data security, including AI-powered ransomware and exfiltration detection and prevention, antivirus software both in the cloud and at the edge, WORM immutability for immediate remediation once a threat or attack is detected, zero-trust access, and honeypot defense using tripwire files. CTERA also complies with multiple industry standards and regulations (e.g., DISA, SOC 2 Type II, FIPS140-3) for protecting sensitive data, reducing security risk and establishing trust with both business partners and end users. Organizations can also integrate security controls into third-party security operations tools such as Varonis and Microsoft Sentinel for sending alerts when detecting threats and attacks.

First Look

Enterprise Strategy Group evaluated how organizations can use CTERA to migrate from a legacy NAS architecture, while ensuring data security with its ransomware detection and recovery capabilities. We first reviewed how easily organizations can deploy and manage CTERA. We navigated to the free and built-in discovery and migration tool, CTERA Migrate, to uncover exactly what data currently exists in legacy NAS devices. Given the choice of running a discovery or migration job, we opted for a discovery (see left of Figure 2).

Figure 2. Discovery and Migration Tool for Legacy NAS



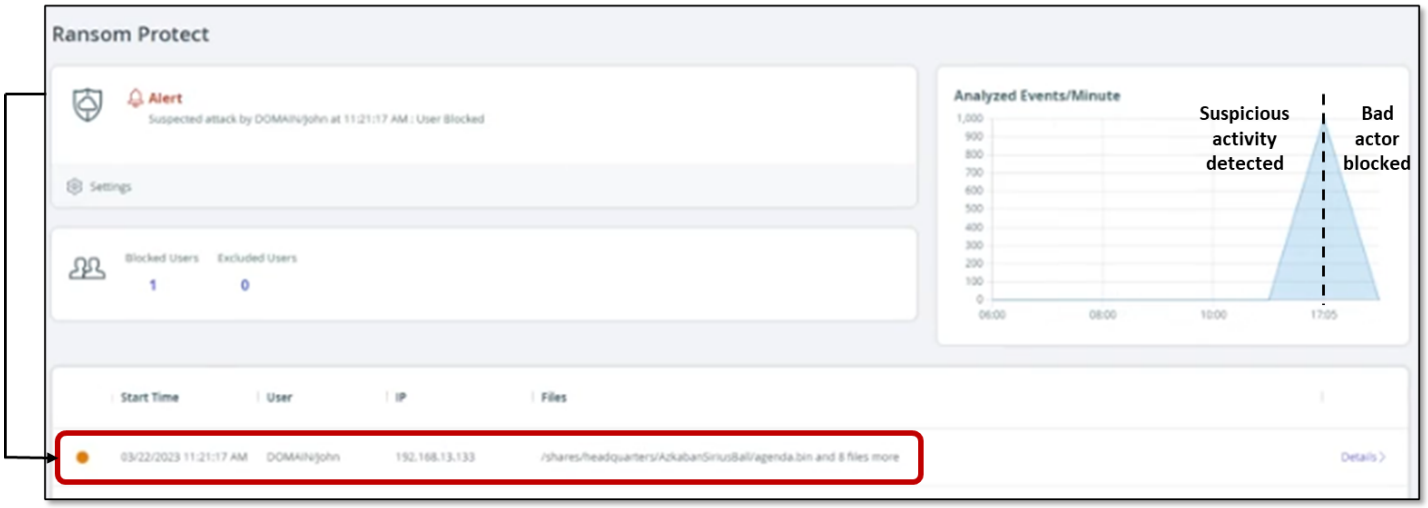
Source: Enterprise Strategy Group, now part of Omdia

Once completing the discovery, we viewed exactly what was found in the existing NAS infrastructure (see right of Figure 2), such as the number of folders and files present, the amount of data they represented, and access patterns (e.g., files that have been accessed more frequently vs. older data). To further simplify migration, not only could organizations select the files to be migrated, but they could also migrate existing access, archiving, and security rules and policies (e.g., ACLs). These rules and policies could also be modified after the data migration. We noted that end users would still have access to their data during any migration, thus minimizing business disruption.

Enterprise Strategy Group also evaluated how organizations can fortify their data security with CTERA Ransom Protect, which uses an AI-powered behavioral engine to reduce the time to detect encryption attacks and remediation. To examine CTERA Ransom Protect in action, we observed the actions taken when simulating a ransomware attack on a CTERA Edge Filer network share. CTERA Ransom Protect was enabled to automatically detect and alert cyberattacks and block bad actors from exfiltration attempts.

Using the CTERA Ransom Protect Dashboard, we monitored the activity that took place when the simulation began. When the attack occurred, a spike in malicious activity was detected, followed by an alert (see Figure 3). Once CTERA Ransom Protect detected a spike in suspicious activity, the bad actor was blocked. Activity immediately decreased to indicate that the issue was automatically remediated.

Figure 3. Ransomware Detection and Protection With CTERA Ransom Protect



Source: Enterprise Strategy Group, now part of Omdia

Conclusion

Unfortunately, according to Enterprise Strategy Group research, 60% of organizations reported that their IT environments are more complex than they were two years ago. Three of the most cited reasons for the increase in complexity were the increasing and changing cybersecurity landscape, new data security and privacy regulations, and higher (structured and unstructured) data volumes.[3] And these are the very same challenges that organizations face when dealing with legacy NAS. Without a path to modernizing NAS infrastructure, organizations face the risk of higher costs when provisioning and managing legacy infrastructure, degraded collaboration and productivity, and higher security and compliance risk. Effectively addressing these challenges requires rethinking if NAS should be deployed and managed. Enter the CTERA Intelligent Data Services Platform.

CTERA has designed its platform to help organizations modernize their legacy NAS infrastructure for handling growing amounts of unstructured data within distributed environments. Using a hybrid cloud architecture, organizations can access all data using edge devices while storing all organizational data centrally within an object backend. With caching technology, end users can access and modify hot data locally. All data stored centrally is updated to the latest version as changes occur locally. Organizations can use the CTERA Portal to centralize storage provisioning and management of all locally deployed (physical and virtual) CTERA Edge Filers, orchestrate and automate workflows, and provide the necessary data services to ensure data security and recovery.

Using the CTERA Intelligent Data Platform, organizations can achieve what was not possible using legacy NAS in distributed environments:

- Lower capital expenses achieved with the platform's caching technology, centralized object backend storage and hybrid cloud architecture.
- Increased operational efficiency via a common and consistent cloud-like management experience.
- Organizational resiliency with a security-first architecture.

[3] Source: Enterprise Strategy Group Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

- Decreased business, security, and compliance risk with adherence to multiple industry standards and regulations applied consistently across the platform.
- Accelerated workforce productivity for achieving business objectives without unnecessary delay while removing impediments to collaboration.

Throughout our First Look, Enterprise Strategy Group validated that the CTERA Intelligent Data Platform can indeed simplify an organization's migration from legacy NAS while preserving existing access and security policies. Enabling simpler migrations removes the friction that organizations face when modernizing their infrastructure. We also verified how CTERA bolsters overall security with automated detection, isolation, and remediation of ransomware attacks. Organizations can then drastically decrease the time and effort spent in protecting valuable data assets.

By addressing the challenges with legacy NAS, organizations can ultimately facilitate better collaboration in achieving business objectives, bolster data security, and lower overall expenses. If these objectives rank high on your list as you consider modernizing your NAS infrastructure, we strongly suggest looking more closely at CTERA.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com