2025-26 DCIG TOP 5 MIDMARKET SDS OBJECT-BASED BACKUP TARGETS

By

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

Midmarket SDS Object-based Backup Targets

Table of Contents

3 Two Corporate Priorities Driving SDS Object-based Backup Target Adoption

3 The Incentive for Hackers to Attack Backup Targets

4 The State of Midmarket SDS Object-based Backup Targets

- 4 Level 1 and Level 2 Hybrid Cloud Implementations

4 Two Characteristics of Midmarket SDS Object-based Backup Targets

- 5 Enterprise Backup Software Support

5 Available Cyber Security Features on SDS Object-based Backup Targets

7 Common Features across All Midmarket SDS Object-based Backup Targets

8 Six Distinguishing Features of the TOP 5 Midmarket SDS Object-based Backup Targets

8 Differences between the TOP 5 Midmarket SDS Object-based Backup Targets

9 TOP 5 Midmarket SDS Object-based Backup Target Solution Profiles

- 10 Zadara Object Storage
- 11 Quest QoreStor
- 12 Qumulo Scale AnyWhere
- 13 Scality ARTESCA
- 14 StoneFly StoneFusion

15 Midmarket SDS Object-based Backup Target Inclusion Criteria

15 DCIG Disclosures

Midmarket SDS Object-based Backup Targets

MIDMARKET SDS OBJECT-BASED BACKUP TARGETS

1. DataCore Swarm
2. NetApp StorageGRID
3. Nutanix Objects Storage
4. Open-E JovianDSS
5. Quest QoreStor
6. Qumulo Scale Anywhere™
7. Scality ARTESCA
8. StoneFly StoneFusion
9. StorONE S1:Backup
10. Veritas NetBackup Access Appliance
11. Zadara Object Storage

MIDMARKET SDS OBJECT-BASED BACKUP TARGET FEATURES EVALUATED

- API/Network Protocol Support.
- Cyber Security and Data Protection.
- Management.
- Software Architecture.
- Technical Support.

Two Corporate Priorities Driving SDS Object-based Backup Target Adoption

Twenty years ago, organizations started adopting disk in lieu of tape as their primary backup target. Now organizations have started to make another change in their choice of backup targets. These new backup targets still use disk as their underlying storage media. However, more providers deliver backup targets as software-defined storage (SDS) with a simple storage service (S3) object-based interface.

Two corporate operational priorities currently drive this trend of organizations seeking out SDS object-based backup targets.

- ***First, all size organizations now embrace a hybrid cloud strategy.*** While hybrid cloud usage among organizations varies, adoption rate estimates generally range from 80 to over 90 percent. When pursuing this strategy, organizations often continue to perform backups and recovery. Indeed, backup and recovery may represent the primary way that organizations implement their hybrid cloud strategy.

  However, few if any cloud providers make provisions for organizations to host physical backup targets in their cloud environments. Instead, to obtain backup functionality like they have on-premises, organizations must deploy a backup target in the cloud. This requirement has prompted organizations to seek out SDS backup targets in general, and SDS object-based backup targets specifically.
- ***Second, every organization must deal with the threat of ransomware.*** Object-based backup targets better position organizations to deal with ransomware's threat as they can withstand a common ransomware attack method.

  Most ransomware begins its attack by seeking out backup targets and attempting to delete or encrypt backups on them. SDS object-based backup targets guard against these attacks by storing backups in an immutable format. Further, they help organizations restore and recover their data more quickly and economically.

SDS object-based backup targets also put organizations in control of how much they spend on achieving these two corporate priorities.

Using SDS object-based backup targets, they can potentially re-use storage hardware they already own. SDS object-based backup targets can virtualize and then manage multiple storage types. These types range from high-performance solid-state drives (SSDs) to cost-effective, high-capacity hard disk drives (HDDs) or even cloud object storage.

In so doing, organizations may implement SDS object-based based targets to achieve these competing corporate priorities without breaking their budget.

The Incentive for Hackers to Attack Backup Targets

Ransomware that compromises a backup target or data stored on it hinders an organization's ability to recover from such an attack. Successfully compromising a backup target or its data leaves organizations with little or no recourse for performing restorations or recoveries.

Further adding to the danger of ransomware attacks, 90 percent of these attacks exfiltrate data.[1] Hackers may use exfiltrated data as another means to extract a ransom. Unless organizations pay the ransom, hackers may threaten to sell the data to third parties, release it publicly, or take all these actions. Adding insult to injury, organizations may lack clarity into how hackers initially accessed their IT infrastructure and stole their data.[2]

Bad actors may also attempt to obtain a backup target's administrative logins and passwords. If they access the backup target with administrative permissions, they may perform any number of nefarious activities. These can range from deleting backups to copying backups offsite to changing file permissions and backup retention periods. Any of these activities could make the backups or the backup target unusable during a recovery.

Midmarket SDS Object-based Backup Targets

All evaluated SDS object-based backup targets support hybrid cloud implementations at two levels.

Two Characteristics of Midmarket SDS Object-based Backup Targets

SDS object-based backup targets that specifically target midmarket organizations generally possess the following two characteristics.

- ***They scale to no less than 500 terabytes (TBs) in storage capacity.*** To achieve 500 TBs in storage capacity, these solutions may offer a scale-out architecture, a scale-up architecture, or both.
- ***They may be available in a single controller configuration option.*** Midsized organizations may have less demanding backup availability and performance requirements. They may also face budget constraints. Midmarket SDS object-based backup target providers better satisfy these constraints by making their solution available in single controller configurations.

The State of Midmarket SDS Object-based Backup Targets

Only a relatively few storage providers (11) currently offer an SDS object-based backup target optimized for use by midmarket organizations. This partly stems from the still emerging demand by midsized organizations for SDS object-based backup targets. Despite the limited number of providers, most midsized organizations will find these solutions possess the core features they need.

Level 1 and Level 2 Hybrid Cloud Implementations

All evaluated SDS object-based backup targets support hybrid cloud implementations at two levels.

Level 1: Tier data to a general-purpose cloud, purpose-built storage cloud, or private storage cloud.

Level 2: Deployment options that include the SDS object-based backup target operating both on-premises and in the cloud.

While they support both these levels, differences exist between how they support each hybrid cloud level.

Level 1

For Level 1 hybrid cloud support, each SDS object-based backup targets can tier data to other clouds. They offer this cloud tiering both for disaster recovery purposes and to create air-gapped copies of backups. The differences between the SDS object-based backup targets emerge in the clouds they support and how they implement cloud tiering.

While each SDS object-based backup target supports tiering to other cloud storage, no one product supports tiering to all available cloud storage options. Further, they may differ in the options they offer organizations to tier backups to other cloud storage.

For example, some may only offer options to tier data that satisfies certain policies or reach a certain age. Others may offer sophisticated algorithms or use artificial intelligence that tracks all data access and usage. It then only moves data that meets specific criteria or, when moving data, places it more intelligently in the cloud.

Level 2

To deliver Level 2 hybrid cloud functionality, providers make their solution available in the three configurations that midsized organizations most often need. They may minimally obtain them as:

- Pre-integrated physical appliances.
- Virtual appliances supported by major cloud and hypervisor providers.
- Software installable on bare metal servers.

To deliver Level 2 hybrid cloud functionality, providers make their solution available in the three configurations that midsized organizations most often need.

Few midmarket SDS object-based backup targets support all three of these deployment options. However, organizations will find each product supports at least two of them. Providers usually make one deployment option optimized for on-premises and the other optimized for the cloud.

Enterprise Backup Software Support

Organizations will also find that most enterprise backup software natively supports these SDS object-based backup targets. Minimally, enterprise backup software recognizes the S3 API interface that each SDS object-based backup target presents. This recognition permits backup software to store and retrieve backups from any midmarket SDS object-based backup target.

However, the S3 APIs perform multiple operations. These include multi-part upload, object lock with different data immutability options, replication, and server-side and storage-side encryption, among others.

These differing levels of support for S3 API operations introduce at least two levels of complexity into the decision-making process. First, no midmarket SDS object-based backup target supports every S3 operation. If an organization needs to perform a specific operation, such as object lock, it should verify the backup target supports it. Further, organizations must also verify the backup target implements the operation in the way they intend to use them.

Second, an SDS object-based backup target supporting an S3 API operation does not equate to backup software supporting it. Each enterprise backup software supports different S3 API operations. Further, it may not support the nuances of every S3 API operation. For instance, backup software supporting S3 object lock does not automatically mean it supports how a backup target implements it.

Organizations can take steps to minimize some of these issues. For instance, they can prioritize choosing backup targets that offer certified solutions or reference architectures with their preferred backup software.

Available Cyber Security Features on SDS Object-based Backup Targets

All the evaluated SDS object-based backup targets offer one or more of the following cyber secure capabilities. Possessing these features has become more critical as ransomware often first attacks backup targets. The availability, breadth, and implementation of these cyber security features on each SDS object-based backup target does vary.

Data Immutability

Data immutability, or storing data in an unchangeable format, represents a feature that every SDS object-based backup target supports. A product may support data immutability in compliance mode (data cannot be overwritten or deleted until the data is expired,)

Midmarket SDS Object-based Backup Targets

governance mode (administrators can still delete data,) or both. When enabled, this feature largely negates ransomware's ability to either delete or encrypt backups stored on the backup target.

Encryption

More organizations prefer to encrypt their backups 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 backups does not prevent ransomware from exfiltrating them outside of the enterprise. However, hackers will find it almost impossible to decrypt and read any encrypted backups they obtain.

High availablity has increased relevance due to the role that SDS object-based backup targets play in helping organizations recover from a ransomware attack.

Multi-factor Authentication

Using multi-factor authentication (MFA) to log into an SDS object-based backup target represents perhaps the most significant enhancement in recent years. Implementing MFA helps ensure only the appropriate individuals can access and manage the SDS object-based backup target.

Some backup targets 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.

High Availability

Organizations may not view high availability (HA) in the context of cyber security. However, HA has increased relevance due to the role that SDS object-based backup targets play in helping organizations recover from a ransomware attack.

During restores and recoveries, SDS object-based backup targets may have to perform multiple tasks, which include:

- Scanning backups for the presence of ransomware.
- Providing fast response times for instant restores.
- Hosting recovered applications and/or data.
- Continuing to serve as a backup target for those parts of the enterprise unaffected by ransomware and still operating normally.
- Retrieving backups from the cloud or offsite locations.

In addition to being available to perform these tasks, SDS object-based backup targets possess the resources to perform these tasks. They offer organizations the extra raw resources (computing, memory, networking, and storage) that they need at these times.

Artificial Intelligence

Artificial intelligence (AI) has yet to make significant inroads as a cyber secure feature on most backup targets. This slow adoption of AI in midmarket SDS object-based backup targets somewhat stems from other trends already in play.

For instance, enterprise backup software has begun to implement AI to detect ransomware in backups. This development has contributed to backup targets being slower to include AI that detects ransomware.

If organizations do find AI in backup targets, it likely shows up in AI's first iteration, machine learning (ML). Currently backup targets may use ML for improved technical support and performing proactive maintenance on their systems. DCIG anticipates through their use of ML to perform these tasks that backup targets will mature to soon offer more sophisticated AI functionality.

Midmarket SDS Object-based Backup Targets

All the evaluated SDS object-based backup targets scale to support at least 500 TBs of usable storage capacity.

Common Features across All Midmarket SDS Object-based Backup Targets

DCIG evaluated over 20 different SDS object-based backup targets of which 11 met DCIG's criteria for a midmarket SDS object-based backup target. Across these 11 backup targets, DCIG evaluated over 180 features on each one. Due to the maturing nature of these products and their respective features, organizations may only safely assume that at least 90 percent of the products evaluated possess the following features:

1. ***Active Directory (AD) and Lightweight Directory Access Protocol (LDAP) integration.*** Storage systems of any type (physical or software-defined) integrating with and supporting AD and LDAP were once more the exception than the rule. No more. The threat of ransomware has led to more providers implementing better forms of identity management on their solutions. As it pertains to these SDS object-based backup targets, all support AD and 90 percent support LDAP.
2. ***Encrypt data at-rest on-premises.*** 90 percent of the evaluated midmarket SDS object-based backup targets support encrypting data at-rest on-premises. Though organizations may store backups on an object-based backup target in an immutable state, organizations often also want to encrypt the backups. By encrypting them, even should a hacker obtain a copy of the backup, the hacker cannot read the backup's data.
3. ***REST APIs.*** Each midmarket SDS object-based backup target offers its own set of REST APIs. The REST APIs offered by each backup target differs from the more well-known AWS S3 APIs. The REST APIs permit activities such as another application retrieving data from the backup target. These REST APIs most often get used by other applications that manage or monitor the SDS object-based backup target.
4. ***S3 APIs.*** Amazon Web Services' introduction of its published Simple Storage Service (S3) APIs has resulted in these APIs becoming a de facto industry standard. This has prompted most enterprise backup software and all the evaluated SDS object-based backup targets to support these AWS S3 APIs. The backup software products may then utilize the same S3 APIs to interface with either the SDS object-based backup targets or AWS cloud object storage.
5. ***Scale to at least 500 TBs of usable storage capacity.*** Though their feature set makes these evaluated SDS object-based backup targets more well suited for midsized organizations, they still scale to high storage capacity thresholds. All the evaluated solutions scale to support at least 500 TBs of usable storage capacity. Further, approximately half of the evaluated solutions scale to over 10PBs of usable storage capacity.
6. ***Technical support is provided by email, phone, and online knowledge base with 4-hour response times.*** Each evaluated midmarket SDS object-based backup target offers email as a means for organizations to obtain technical support. Once contacted, each provider offers response times in under four (4) hours. However, organizations may need to subscribe to a support contract to obtain that level of technical support. Organizations may also contact technical support for 90 percent of these providers via phone or obtain technical support through an online knowledge base.
7. ***Web-based GUI.*** Each SDS object-based backup target offers a web-based graphical user interface (GUI) that organizations may use to manage it.

Six Distinguishing Features of the TOP 5 Midmarket SDS Object-based Backup Targets

Each of the TOP 5 products support all the features listed above. The TOP 5 midmarket SDS object-based backup targets additionally distinguish themselves by also all supporting the following six features. These include:

Organizations may deploy any TOP 5 SDS object-based backup target as a VM on VMware vSphere.

1. ***All-inclusive software licensing.*** Each of the TOP 5 midmarket SDS object-based backup targets includes all its software features as part of its software license. This licensing option gives organizations the flexibility to access any of the software features without paying extra for them.
2. ***Encrypt data in-flight and stored at-rest in the cloud.*** Organizations can never know for sure exactly where ransomware may lurk or what data it might try to copy offsite. Encrypting all backups, whether at-rest on-premises, in the cloud, or in-flight mitigates the possibility of ransomware copying readable data. Each of the TOP 5 SDS object-based backup targets offer the option to encrypt backups in these three states.
3. ***May be deployed as software on bare metal server hardware.*** Installing the SDS object-based backup target software on a physical appliance remains a popular option for organizations. Due to the storage capacity and performance demands of backup and recovery workloads, dedicating a physical appliance to this task often makes sense. Organizations may use any server hardware that meets the TOP 5 SDS object-based backup target solutions' hardware specifications.
4. ***May be deployed as a VMware vSphere virtual machine.*** Not every location into which an organization deploys an SDS object-based backup target necessarily needs a physical backup target. In many circumstances it makes more sense to deploy the SDS object-based backup target as a virtual machine (VM). To meet this demand, organizations may deploy any TOP 5 SDS object-based backup target as a VM on VMware vSphere.
5. ***Multi-factor Authentication (MFA).*** Authenticating users attempting to access the SDS object-based backup target has taken on heightened importance as ransomware attacks increase. Some ransomware attacks begin with either the ransomware or individuals within organizations attempting to compromise the backup target. MFA helps to ensure that only authorized entities or individuals can access and administer the backup target. Each TOP 5 SDS object-based backup target supports MFA.
6. ***Versioning.*** Organizations have multiple legitimate reasons to access and use backups and make changes to them. SDS object-based backup targets permit these types of actions. However, ransomware can capitalize on this available functionality to potentially compromise backups. Enabling versioning ensures that every time a backup gets changed, original and prior versions of the backup exist. In this way, organizations can identify a backup version that was not modified by ransomware. Each of the TOP 5 SDS object-based backup targets support versioning.

Differences between the TOP 5 Midmarket SDS Object-based Backup Targets

While the TOP 5 SDS object-based backup targets have similarities, they also differ in their implementation of multiple features. These differences primarily appear in their deployment into clouds and virtualized environments, their implementation of advanced S3 API operations, and their different supported types of replication and snapshots. While organizations can expect these SDS object-based backup targets to support these features, they implement and support each one differently. Consider:

The general-purpose clouds and hypervisors supported by each TOP 5 SDS object-based backup target do vary.

- ***Deployment into general-purpose clouds and virtualized environments.*** Each TOP 5 SDS object-based backup target supports being deployed into multiple general-purpose clouds and hypervisors as a virtual machine. However, the general-purpose clouds and hypervisors supported by each TOP 5 backup target do vary.

  An organization should not expect to deploy any TOP 5 solution into any general-purpose cloud or on any hypervisor. VMware vSphere represents the only exception to this rule. Amazon Web Services and Microsoft Azure represent the two general-purpose clouds most supported with four products supporting deployments into these two clouds. Three products support deployments on the Google Cloud Platform and two support deployments on other cloud platforms.

  Deployment choices become more limited on the hypervisor side. Three products may be deployed on Microsoft Hyper-V and two offer deployment options for the KVM hypervisor.

- ***Support of advanced S3 API operations.*** All TOP 5 SDS object-based backup targets support backup software using standard S3 API operations and commands. These include using standard S3 API operations such as DELETE, GET, POST, and PUT.

  However, some organizations will need or want their backup software to perform more advanced S3 API operations. These may include the backup software using an S3 operator to request the SDS object-based backup target to perform encryption, multi-part uploads, or object locks, among others.

  The TOP 5 SDS object-based backup targets support each of these and other advanced S3 API operations at different levels. Among the advanced S3 API operations evaluated, four of the five TOP 5 SDS object-based backup targets support multi-part upload, storage tiering, and replication operations. Three support enable the compliance mode of an object lock operation while two support the server-side encryption operation.

- ***Snapshots and replication.*** More organizations look to have their SDS object-based backup target make snapshots of their backups and replicate them. They perform snapshots, in part, to do anything from doing malware scans on the snapshots to using the snapshots for instant restores and recoveries. Organizations also may call upon backup targets to replicate backups to another location or to the cloud.

  Here again, each of the TOP 5 SDS object-based backup targets supports either snapshot or replication functionality, or both, with each one offering different options.

  For instance, DCIG evaluated SDS object-based backup targets for their ability to perform continuous, immutable, and space-efficient backups. Four could create immutable snapshots, three could create space-efficient snapshots, and two could perform continuous snapshots.

  On the replication side, DCIG evaluated what type of asynchronous replication each one could do. Three support continuous asynchronous replication which replicates data to a second location as soon as a write completes on the SDS object-based backup target. Two support periodic asynchronous replication which replicates data to a secondary location on a predetermined interval, usually every 15 to 60 minutes.

TOP 5 Midmarket SDS Object-based Backup Target Solution Profiles

Each of the following TOP 5 midmarket SDS object-based backup target solution profiles highlights at least three ways each one differentiates itself. These differentiators represent some of the best methods that midmarket SDS object-based backup targets offer to back up, restore, and/or secure data stored on them. Within each solution, organizations may find specific features that may better meet their specific needs.

Zadara's Object Storage offers complete privacy through tenant separation and dedicated resources, ensuring that each organization or department operates in an isolated environment.

Zadara Object Storage

Founded in 2011, Zadara delivers its Object Storage as a scale-out cluster consisting of two Virtual Controller (VC) layers. The first, upper layer consists of performance Proxy VCs possessing compute and memory to process REST API traffic. The second, lower layer consists of Storage Controllers that manage the underlying storage and store and retrieve data. Each of these two VC layers can then independently scale their respective performance and capacity attributes up and down.

Zadara also embeds an internal load-balancer in the Object Storage Proxy VC performance layer. This load-balancer distributes the REST API traffic across the Proxy VCs before they send the requests to the Storage Controllers.[5]

Additional features that distinguish Zadara Object Storage and helped it earn a DCIG TOP 5 award include:

- ***Offers two options for protecting data residing on its VCs.*** Different organizations have different capacity and performance requirements for their backups. Zadara accommodates these different requirements by providing organizations with two ways to configure data protection in Object Storage. It offers 2-way mirroring policy protection between its VC nodes for those organizations that need greater performance. It offers Erasure Code 4+2 for those organizations that need higher levels of usable capability and durability. Zadara recommends organizations with 1PB or less of capacity deploy 2-way mirroring while 1PB+ environments utilize its Erasure Code option.
- ***Data privacy.*** Zadara's Object Storage offers complete privacy through tenant separation and dedicated resources, ensuring that each organization or department operates in an isolated environment. Zadara Object Storage provides each tenant with dedicated computing, storage, and network resources. This eliminates resource sharing and potential data leakage.

  Zadara guarantees secure, private, and performance-consistent operations. Organizations that require strict data security and regulatory compliance while benefiting from Object Storage's scalability will find this architecture appealing.
- ***Partners with multiple backup software providers to offer additional cybersecurity functionality.*** More organizations want to do more than store backups on immutable object storage and quickly recover data from them. They also want to scan their backups for anomalies, malware, and ransomware. To help organizations meet these emerging objectives, Zadara integrates its object storage with backup software from Acronis, Commvault, and Veeam. Depending on the backup software selected, organizations may scan backups for malware, create air-gapped storage, or set up offsite replication.

Midmarket SDS Object-based Backup Targets

QoreStor compresses and deduplicates data without compromising on restore times. By creating and using a Performance Tier, QoreStor can restore compressed, deduplicated data as fast as raw data stored on disk.

Quest QoreStor

Quest QoreStor represents one of the few midmarket SDS object-based backup targets that concurrently presents both file and object interfaces. Supporting both protocols gives organizations the flexibility to choose the interface that best meets a specific application's backup or recovery needs.

Quest Software's focus on flexibility also shows up in QoreStor's licensing options. As an SDS backup target, organizations may deploy QoreStor on platforms from many hardware, cloud, and hypervisor providers. Then, once licensed, organizations may move QoreStor from one environment to another if their support is up to date. Further, QoreStor comes with all software features included.

Additional features that distinguish Quest QoreStor and helped it earn a DCIG TOP 5 award include:

- ***Offers sophisticated anomaly detection.*** Backup targets that offer anomaly detection may sound appealing on the surface. However, anomaly detection algorithms are not created equally. To identify anomaly that indicates the presence of ransomware, an anomaly detection algorithm must possess some level of sophistication.

  QoreStor addresses this challenge by using more sophisticated algorithms that rely upon machine learning (ML) and artificial intelligence (AI). It examines multiple variables before starting to interpret an anomaly as ransomware. It looks for excessive data retirements, unusual deletions, decreases in compression savings, and successive failed login attempts, among other factors. These contribute to when it makes an assessment if an anomaly represents a ransomware event.
- ***Compresses and deduplicates backups without compromising restore times.*** In securing and storing backups in an immutable format, organizations may forget their backups consume large amounts of storage capacity. QoreStor addresses this concern by compressing and deduplicating backups stored on it, achieving up to 20:1 data reduction ratio.

  More notably, QoreStor compresses and deduplicates data without compromising on restore times. By creating and using a Performance Tier, QoreStor can restore compressed, deduplicated data as fast as raw data stored on disk.
- ***Archive Tier for cost-effective, long term data storage in the cloud.*** Storing backups in the cloud may only make financial sense if organizations can place it on low-cost cloud storage tiers. Quest provides organizations with this option with QoreStor's archive tier feature.

  Organizations may use use data management applications, which includes backup software, or QoreStor's policy engine to create archiving policies. Once set, backups only get moved based after they meet specified file age and on-premises retention criteria. QoreStor can then move these backups to low-cost cloud storage such as Amazon S3 Glacier and S3 Glacier Deep Archive.
- ***Cloud lock technology.*** Direct-to-object storage backups that utilize S3-compatible storage can be safeguarded through object locking and versioning control. Using QoreStor Cloud Lock technology, it can extend its immutability functionality into cloud storage.

Scale AnyWhere gives organizations the flexibility to implement object locking at either the object or bucket levels.

Qumulo Scale AnyWhere

Founded in 2012, Qumulo designed Scale Anywhere™ to address the challenges associated with scale-out solutions deployed in today's IT environments. Scale Anywhere's ability to scale over an exabyte and support multiple hardware platforms and public clouds illustrate Qumulo's design philosophy.

Its support of these different platforms and clouds coupled with its all-inclusive software licensing positions organizations to accomplish multiple business objectives. They can replicate backups to the cloud while also maintaining a secondary on-premises Qumulo cluster. They may do cloud-based backup and restore or even cloud-based DR testing and validation.

Additional features that distinguish Qumulo Scale Anywhere and helped it earn a DCIG TOP 5 award include:

- ***AI-enabled search feature for an expedited premium online support experience.*** Providers often make their product documentation and knowledgeable online and available to search. However, online and searchable product documentation does not automatically equate to it being usable and consumable when needed.

  Qumulo addresses this common support deficiency by incorporating artificial intelligence (AI) into its online search engine. When searching Qumulo's online product documentation and knowledgebase, its AI-powered search summarizes the results. This helps organizations more quickly identify a solution most germane to a specific challenge they face and resolve it.
- ***Automatically encrypts all data stored at-rest on-premises.*** Organizations have justifiable concerns about hackers stealing backup copies and then asking for ransoms to keep them from being released. Qumulo address this concern by automatically encrypting all backups and storing them in an immutable format. Once a backup completes, Qumulo takes a snapshot of the backup, encrypts the snapshot, and then stores encrypted backup in an immutable format. Stored in this format makes the snapshots both unchangeable and, if copied by a hacker, unreadable and unusable to them. Organizations may also optionally set up Scale Anywhere to encrypt data at-rest in the cloud.
- ***Performs object locking at either the object or bucket levels.*** Flexibility in object locking may emerge as a challenge on some object-based backup targets when storing backups on them. Some implementations of object-based storage require objects (i.e., backups) stored in a bucket to inherit that bucket's object locking policy.

  Qumulo gives organizations the flexibility to implement object locking at either the object or bucket levels. This permits organizations to assign specific object locking attributes to each backup. In this way, organizations may store backups with different object lock attributes in the same bucket. Qumulo also offers object versioning so if an object does change, Qumulo can retain prior versions of it.

Midmarket SDS Object-based Backup Targets

Scality incorporates five levels of cyber resilience functionality into ARTESCA that range from its APIs to its architecture.

Scality ARTESCA

Scality as a company focuses on and develops storage software that organizations may use to store their data indefinitely. Scality specifically develops its software to scale, maintain performance, store data securely over time, and support multiple storage media.

ARTESCA represents Scality's midmarket SDS object-based backup target that targets organizations needing 50TBs or more of storage capacity. Available in multiple form factors, ARTESCA scales to over 8PBs of storage capacity in its largest configuration.

Additional features that distinguish Scality ARTESCA and help it earn a DCIG TOP 5 award include:

- ***Offers three on-premises deployment options.*** Multiple factors influence the deployment requirements of a backup target. These can vary depending upon the amount of data an organization needs to back up, backup target uptime requirements, available budget, and more.

  Scality accommodates these varying requirements by offering ARTESCA in three appliance form factors:

  - ***Turnkey hardware appliance*** ships with pre-configured hardware and ARTESCA software. Appliance sizes range from 73 to 377TB of usable capacity.
  - ***The software appliance*** comes in one, three, or six-server configurations and scales from 50 TBs to 8.5PB of usable capacity. Organizations may deploy it on various industry-standard servers.
  - ***The virtual appliance*** gets packaged as an open virtual appliance (OVA) ready for deployment in VMware environments. Deployed as a single virtual machine (VM), it supports up to 106 TBs of usable capacity.

- ***Provides five levels of cyber resilience.*** Like other object-based backup targets, ARTESA offers data immutability. However, Scality incorporates five levels of cyber resilience functionality into ARTESCA that range from its APIs to its architecture. These five levels are:

  1. ***API-level resilience:*** Uses S3 Object Locking APIs to make backups immutable upon creation.
  2. ***Data-level resilience:*** Encrypts data-at-rest and secures user logins with MFA to keep stored backups safe from would-be attackers.
  3. ***Storage-level resilience:*** Uses distributed erasure code technology to encode and spread data across a cluster. This makes data difficult to access at the physical drive level and, if accessed, impractical to decipher.
  4. ***Geographic-level resilience:*** Employs replication to mirror data to ARTESCA instances at other data sites.
  5. ***Architecture-level resilience:*** Offers a security-hardened Linux OS that precludes root access to it to mitigate the impact of common vulnerabilities and exposures.

- ***Validated design configurations with multiple backup partners.*** Due to the different ways that object-based backup target providers implement S3, their deployments are neither always easy nor successful. Scality took steps to alleviate these concerns. Scality provides validated design configuratons with multiple enterprise backup software providers. These include Veeam, Commvault, HYCU, Rubrik, Veritas, and Zerto along with system provider tools.[3]

Midmarket SDS Object-based Backup Targets

StoneFly offers organizations three options to air-gap backups depending on their IT environment and requirements.

StoneFly StoneFusion

Founded in 2000, StoneFly™ has developed its StoneFusion™ and SCVM™ software to support the most used back- and front-end storage protocols. These include the FC, iSCSI, NFS, and CIFS/SMB storage networking protocols with StoneFly adding support for the S3 APIs in 2019.[4] This S3 support specifically positioned StoneFusion to serve as an object-based backup target for multiple backup software solutions.

Additional features that distinguish StoneFly StoneFusion S3 object storage and helped it earn a DCIG TOP 5 award include:

- ***Offers three S3 object storage deployment options.*** Every SDS object-based backup target provider often optimizes its solution for deployment in specific IT environments. StoneFly follows this pattern as it optimizes StoneFusion S3 object storage for deployment in three specific IT environments:
  1. ***Storage as a Service (STaaS)***. Organizations may deploy StoneFly in AWS, Azure, or any cloud with S3-compatible storage.
  2. ***Physical turnkey appliances.*** StoneFly offers a line of turnkey purpose-built S3 object storage appliances. These configurations include single node HA appliances, scale out appliances, and cloud-scale data center, among others.
  3. ***Virtual machine.*** Organizations may deploy StoneFusion S3 object storage as a virtual machine on Hyper-V, KVM, Proxmox, vSphere, and XenServer hypervisors. It can then provide S3 object storage volumes using storage available on or connected to the physical host.

- ***Offers air-gapping***. Air-gapping offsite backups protect them in the event a ransomware attack compromises both an organization's online production and offsite environments. StoneFly offers organizations three options to air-gap backups depending on their IT environment and requirements.
  1. ***Air-gapped repositories.*** Air-gapped repositories consist of a single controller connected to two target storage repositories. One target storage repository remains network-facing, always accessible, and available for use. The second storage repository gets air-gapped by being detached and isolated.
  2. ***Air-gapped controllers.*** Air-gapped controllers resemble the air-gapped repository design except that each repository has its own controller. In this use case, one controller and its target storage repository remains network-facing, always accessible, and available for use. The second controller and its storage repository get air-gapped by being detached and isolated.
  3. ***Air-gapped nodes.*** Air-gapped nodes come as purpose-built appliances with network and power controllers. These nodes only attach and become visible when reading or writing backups. When the backup read or write jobs conclude, the controllers automatically detach isolating the appliances

  In these use cases, organizations may define policies that automatically attach/connect one repository, controller, or node and detach/disconnect the other.

- ***Volume Deletion Protection.*** When enabled, this feature protects volumes from deletion by rogue administrators. Any individual or organization seeking to delete a volume, or volumes must first contact StoneFly support. StoneFly support then responds by contacting two authorized personnel at the organization. Only after StoneFly verifies with these two individuals the deletion is permissible does StoneFly issue a code permitting the organization to delete the volume(s).

Midmarket SDS Object-based Backup Targets

Midmarket SDS Object-based Backup Target Inclusion Criteria

1. A software-defined storage (SDS) solution that the provider specifically markets and positions it for use as a backup target.
2. May be hosted and run on more than one provider's hardware or in one or more general purpose clouds (AWS, Azure, Google Cloud, etc.)
3. The SDS backup target can serve as an SDS backup target for two or more enterprise backup software solutions.
4. Must scale to at least 50 terabytes (TBs) of storage capacity.
5. Commercially available on or by September 1, 2024.
6. Sufficient information is available to DCIG to make an informed decision.

DCIG Disclosures

Providers of some of the midmarket SDS object-based secure backup targets covered in this DCIG TOP 5 report are or have been DCIG clients. In that vein, there are some important facts to keep in mind when considering 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.
- All research is based upon publicly available information, information shared by the provider, and the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the 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 solutions not included in it.

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 completed its analysis. To arrive at the TOP 5 solutions included in this report, DCIG went through a seven-step process to come to the most objective conclusions possible.

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

Midmarket SDS Object-based Backup Targets

Sources

1. https://www.blackfog.com/the-state-of-ransomware-in-2023/. Referenced 1/8/2024.
2. Ibid.
3. https://www.artesca.scality.com/wp-content/uploads/2024/08/ARTESCA-Validated-Partner-Application.pdf. Referenced 10/4/2024.
4. https://stonefly.com/press-release/stonefly-introduces-cloud-gateway-for-file-block-s3-storage/. Referenced 10/5/2024.
5. https://guides.zadarastorage.com/ngos-guide/latest/introduction.html. Referenced 10/6/2024.

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.**