Lab Insight

Modern Data Protection for Mid-Sized Enterprises & ROBO

Author: Russ Fellows
August 2021

Evaluator Group

arcserve®

Executive Summary

Enterprises of all sizes consider data protection to be one of their top challenges, perennially ranking it as an area for investment and improvement. As information becomes a primary corporate resource, protecting these digital assets becomes increasingly important. Regardless of a company's size, factors such as scalability, ease of use, and cost-effectiveness are key considerations for data protection tools.

Additionally, it is now critical that data protection tools support using multiple targets, including the Cloud, to ensure offsite copies are maintained for regulatory compliance, disaster recovery, and as part of an overall strategy to mitigate hacks and ransomware. While large corporations have tools that often provide these options, these products have often been complex, costly, or not suited for smaller enterprises.

Evaluator Group was engaged to test and analyze Arcserve OneXafe Solo and a leading competitor from the standpoint of their ability to meet mid-sized enterprise data protection requirements. Our testing found that while both products meet the basic requirements of data protection and recovery, Arcserve's OneXafe Solo provided more features and capabilities than its top competitor.

Summary of Arcserve OneXafe Solo benefits vs. a Competitor:

- Significantly more scalable (OneXafe Solo has no specific capacity or system limits)
- Multiple backup target locations, including multiple copies (Competitor: only two targets)
- Agentless for VMs, no deployment required (Competitor: Requires agent per each system)
- Able to protect far more systems (OneXafe Solo: no limits, Competitor: limit of 4 systems)
- Instant VM recovery is significantly faster: (Solo: Seconds, Competitor: up to 1 hour)

Data Protection Requirements

Evaluator Group works with organizations of various sizes across multiple countries and industries to assist with their IT strategy. Additionally, Evaluator Group performs research into new technologies and areas of focus for CIOs and IT professionals. A topic that consistently ranks near the top of firms' interests is improving their data protection methods and tools.

A recent Evaluator Group study on the effects of COVID-19 found that security, data protection, and disaster recovery initiatives have received increased funding due to the pandemic. Additionally, most respondents indicated that many of the changes being made are permanent, with COVID-19 accelerating digital transformation initiatives and heightening the need to preserve and protect corporate digital assets.

In another Evaluator Group research study of data protection trends across more than 120 organizations, more than 50% of respondents indicated being likely to change their data protection tools to lower their costs or improve ease of use. A majority also reported they are currently using cloud technologies for some portion of their data protection while indicating a desire to further increase their use of the Cloud.

This study also indicates the top data protection challenges are the ability to address data growth and to meet desired recovery point and recovery time objectives (RPO/RTO) while lowering solution costs. Nearly all participants indicated that data protection would become increasingly important in the future.

Data protection is a key part of enterprises' digital transformation strategy to affect IT modernization while increasing flexibility and adapting to a changing economy and workforce. There can be significant differences in requirements for small to mid-sized enterprises, with some needing to protect only a few dozen applications with data under protection measured in Terabytes. In contrast, others may have hundreds of systems with data under protection measured in Petabytes. Additionally, many applications have unique service levels requirements.

One common factor is the need to meet protection RTO objectives with a solution that is scalable, easy to use, and cost-effective. Typically, mid-sized companies have multiple locations with data that requires protection; however, managing disparate equipment with limited IT staff is an ongoing challenge for many organizations.

Typical requirements for mid-sized enterprise data protection:

- Ease of use and manageability
  - Easy to deploy and use for IT staff
  - Remote management access for ROBO environments
- Ability to meet a variety of RPO and RTO needs
- Flexible replication options, including on-site and Cloud
- Scalable support for growing applications and data needs
- Ability to provide file recovery and near-instant application recovery

OneXafe Solo Overview

Arcserve offers a portfolio of data protection offerings, including OneXafe Solo, which may be used by small to mid-sized enterprises as their primary protection tool, or used for branch and remote offices as part of a corporate-wide data protection strategy. Arcserve also offers ShadowXafe for larger enterprises using the same core technologies and user interface.

OneXafe Solo's features include:

- Agentless VM technology minimizes administration overhead
- Support for physical and VM protection using traditional OS agents
- Instant restoration of VM's and files from any location to existing infrastructure
- Appliance-based protection for rapid deployment with remote management
- Scalable solution with no limitations on capacity or number of systems protected
- Support for local and direct to cloud backup targets
- Able to replicate backups to multiple locations(iSCSI, NAS, USB) and Cloud (AWS, Azure, Wasabi)

A comparison of Arcserve OneXafe Solo vs. the tested Competitor:

Requirement	Competitor "X"	OneXafe Solo	OneXafe Solo Benefit
Simplified Management	**Simplified Appliance** Remote access UI, agent installation required per protected client	**Simplified Appliance** Remote access UI, agentless for fast deployment of multiple clients	Both offer a simple appliance that may be deployed in datacenters and ROBO locations to protect systems
Limited Application Impact	**Agent Only** Agents impact application, minimize data transfer	**Agent and Agentless** Agentless for no application impact, or agent backups	Choice of agentless for ease of deployment and mgmt., or agents for reduced data transfer
Scalable	**Limited Scale** Limit of 4 systems and 2 TB local capacity per appliance	**Unlimited Scale** Unlimited # of systems, unlimited capacity	Significantly more scale and with no limitations on number of systems protected or capacity
On-site and Cloud Replication	**Cloud Only** Single replication to proprietary cloud is only DR option	**Multiple Options** Replication of backup to multiple on-prem and Cloud locations	More DR options allow multiple copies locally and cloud copies
Instant recovery of Applications	**Cloud Only** Instant VM recovery in proprietary Cloud only	**On-prem & Cloud** Instant VM recovery both on-premises and in the cloud	More instant recovery options, on-premises instant recovery is critical for low RTO
Security	**Minimal** No visible data at rest encryption settings, MFA for cloud portal only	**Multiple Items** Data at rest encrypt for on-premises and cloud with separate key, also MFA for UI access	Separate data at rest encryption for each device and required multi-factor authentication for access to appliance UI

Table 1: Comparison of Data Protection Requirements (source: Evaluator Group)

Evaluation of OneXafe Solo vs. Competitor

Evaluator Group tested OneXafe Solo vs. a leading competitor in our Boulder, Colorado labs, using Evaluator Group personnel and equipment except for the OneXafe Solo and competitor backup appliance products. The testing included initial deployment, setup of backup policies and storage locations, testing backing up systems, and recovering files and entire systems. Details of the testing and the results are provided herein, with additional details in the Appendix.

A depiction of the test environment is shown below.

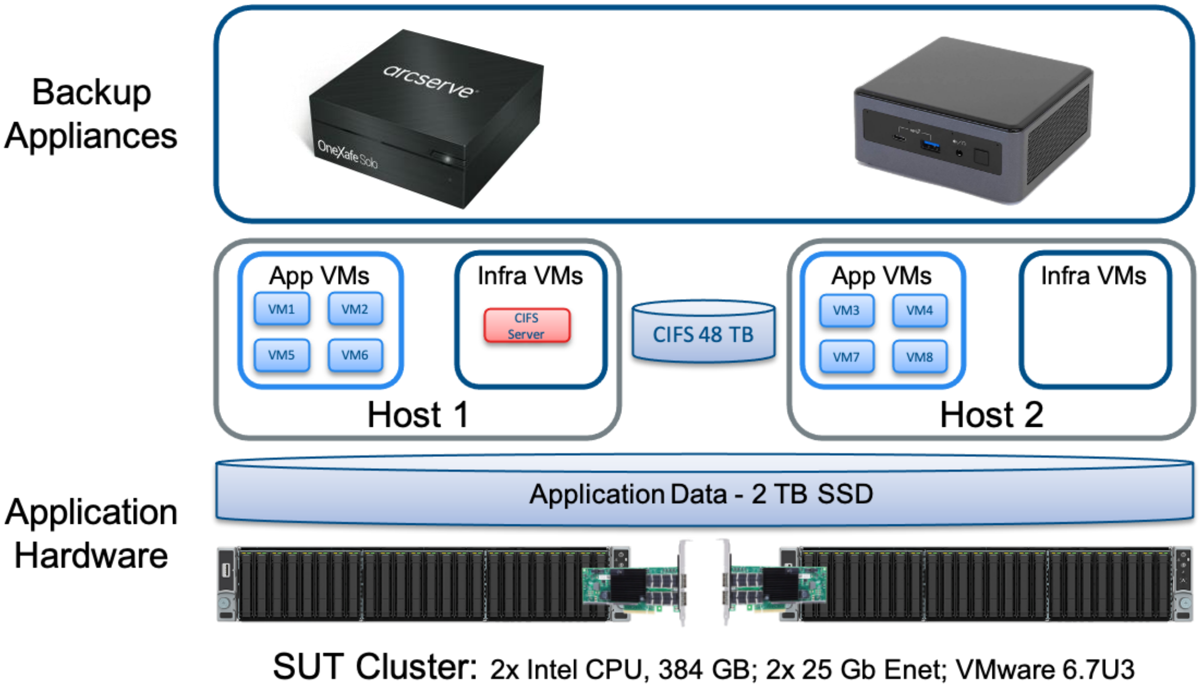

FIGURE 1: TEST ENVIRONMENT (SOURCE: EVALUATOR GROUP)

Test Overview

Testing was designed to include typical use cases and scenarios, including initial deployment, along with a focus on data protection and, in particular, data recovery. Measurements were objective where possible, measuring the number of steps and time required. Subjective assessments included ease of use and other aesthetics. Testing both products entailed a one-time setup, and typical day-one system administration tasks required to protect systems including adding storage targets, identifying systems to protect, and establishing protection policies. Afterward, data protection occurred automatically using the established protection policies.

The majority of testing focused on data protection and recovery operations, along with the available options. The previously identified criteria were used for evaluation, specifically: Ease of use, scalability, amount of administration required, the performance of data protection, and data recovery with a particular focus on the ease and speed of data recovery. For more details on the test environment and testing method, please refer to the Appendix.

Initial Setup Results

OneXafe Solo and the Competitor's product were both designed for remote, low-touch environments. Both are small form factor appliances that require only a DHCP network connection and power. After connecting each appliance, they required registration via a web portal interface and established account credentials and other licensing information.

OneXafe Solo utilizes agentless technology for VM backups while also supporting physical systems using agents. The Competitor requires agents for all data protection, which requires agent installation on each network to be protected. This increased the setup time and complexity for the Competitor's product. For optimal restoration, OneXafe Solo requires a one-time installation of a hypervisor driver onto either a VMware cluster or Hyper-V host to perform instant recovery.

Setup Summary

- Both systems were set up with a minimal IT staff on-site (only power and network connection)
  - Some additional steps (and remote desktop access) were required to install the required agent for the Competitor
  - OneXafe Solo required additional VMware agent installation required for instant recovery
- Total setup time for OneXafe Solo is constant, regardless of the number of VMs (using agentless)
- Total setup time for competitor increases with each additional system or VM protected

Data Protection Testing

As previously identified, the data protection needs for small and mid-sized enterprises differ from larger environments. The most significant difference is around the increased demand for simplicity and a decreased need for high-performance backups. Companies with fewer data to protect, longer windows, or both can tolerate slower backup performance.

Data Protection Summary

- Arcserve OneXafe Solo:
  - Good performance, data limited by 1 Gb/s network bandwidth (appx. 100 MB/s)
  - The effective backup performance was 100 MB/s (data reduction on target OneXafe Solo)
  - Offloaded backup operations to ESXi host, no VM or application impact
  - Policies executed as expected, providing warnings when exceptions occurred
  - Multiple policies may be in place, including the ability to replicate data to additional media/locations, including the Cloud
- Competitor:
  - Good performance, data rate limited to 1 Gb/s network bandwidth (appx. 100 MB/s)
  - Effective backup performance appx. 250 MB/s (data redux occurs at source)
  - Agent backup operations required one vCPU, network, and memory impact
  - Policies executed as expected, providing warnings when exceptions occurred
  - Multiple policies may be in place for a time, no replication or location options available

OneXafe Solo and the Competitor's interfaces and policies were both easy to use. They each had different strengths and weaknesses. The Competitor's agent-based approach resulted in less data being transmitted, thereby reducing the performance limitation of a 1 Gb/s network. However, the use of agents also reduced the available CPU and memory available to the application while backups occur.

Two of the biggest differentiators for OneXafe Solo are the ability to create policies that create multiple copies of data locally, along with a cloud replication option. Thus, it is possible to have multiple local copies of data on premise in addition to cloud copies to enable on site tiering of protected copies or simply having multiple copies for greater reliability. Additionally, OneXafe Solo's ability to perform an instant recovery of a VM enables a very low RTO, by reducing the time to recover to a number of seconds. In contrast the competitor was unable to restore the entire system locally, greatly complicating the process and lengthening the RTO.

For many smaller enterprises, or for ROBO locations, backup speed is only important to ensure backup windows are met. Additional considerations include limiting application impact and the ability to create off-site copies quickly. One of the most significant benefits for OneXafe Solo compared to its competitor was the ability to utilize many more backup target locations and to create multiple replicated copies. These capabilities were not possible with the competitors product, but worked easily with OneXafe Solo.

Restoration Testing

Backing up data is often the focus of testing data protection products because most of an administrator's time and interactions are spent on these aspects. However, data restoration is the critical test of any data protection solution. The speed, ease of use, and the number of restoration options available are often critical in determining whether a momentary loss of data becomes a minor disruption or a major system outage.

We tested both products to see how quickly data could be recovered, including when an entire system or application needs to be restored or scenarios where only a few files or folders need to be restored. Additionally, both products support creating a VM from a backup image in their respective private cloud environment.

***Note**: Private clouds have no inherent connectivity to corporate or public cloud environments.*

Data Recovery Summary

- Arcserve OneXafe Solo:
    - Full System recovery to existing infrastructure
        - Nearly instant recovery of a VM (in as few as 10 seconds)
            - Recovery time dependent upon recovery location and media
    - Full System recovery to Arcserve Private Cloud
        - Recovery and boot of VM in private cloud location
            - Requires separate web portal for cloud recovery in under 5 minutes

        - Note: File recovery may be performed by copying files from VM after boot
    - File Recovery methods
        - Utilize instant recovery, then browse and copy files to desired location
        - Optionally, use instant recovery, then mount virtual disk to existing VM
- Competitor:
    - Full system recovery to existing infrastructure
        - Full recovery on premises was not possible for a VM, only for physical systems
    - Full System recovery to Private Cloud
        - Recover VM in a vendor, private cloud location
            - Utilizes same UI to perform cloud recovery in under 1 minute
        - Note: File recovery may be performed by copying files from VM after boot
    - File Recovery
        - UI provides ability to browse and then copy files or folders locally
            - Sources include local and cloud
            - Fast copy from any location (limited by Internet for Cloud copy)

OneXafe Solo and its Competitor's recovery options appeared similar on a datasheet. However, in practice, they were significantly different. OneXafe Solo was designed to provide rapid, nearly instant recovery of a VM or system locally, from data copies residing on-premises or in the Cloud. Although file and folder recovery is an option, the most efficient method is to perform a system restore and then copy the files to the desired location. In contrast the competitors design seems optimized around providing file and folder recovery, with full system restoration cumbersome or limited.

Arcserve's approach to recovery proved to be more flexible, in that providing nearly instant VM recovery provides superior RTO compared to the competitor for full recovery. Although recovering a file or folder using Arcserve's methodology may prove somewhat slower, the amount of time (RTO) for file recovery is often less critical than recovering an entire system.

Note: For both OneXafe Solo and Competitors products, recovering a VM to the cloud also enables copying files or other system files from the cloud VM. Additionally, application functionality running in a cloud VM may require additional network, DNS and other aspects required for full functionality. These caveats apply to any product that enables moving or recovering a VM into a new, cloud environment.

In summary, when restoring an entire system, minimizing the amount of time (RTO) required to accomplish the task is the primary goal, along with simplicity. When restoring file or folders, RTO is often less critical and having several recovery options provides flexibility. OneXafe Solo excelled at minimizing the RTO for full system recovery while providing several options for file recovery.

Final Thoughts

Data protection is critical for all companies, regardless of their size or the amount of data they need to protect. Ensuring corporate data is safeguarded from accidents, disasters, malware, and ransomware attacks is a key part of every companies' IT strategy. Choosing the right set of tools is an essential part of this overall protection strategy.

As our research indicated, cost and complexity are often two of the primary factors that motivate a company to search for alternative products, along with other considerations such as features and performance. In some ways, complexity and performance are related to cost in that complexity increases operational costs while simplicity can lower costs. Cost is also related to performance, as dictates the number of systems required to meet service objectives, each of which require capital resources along with some incremental management.

In comparing Arcserve OneXafe Solo to a typical competitor, we evaluated these products for their intended deployments, namely, small to mid-sized enterprises. For most criteria, we found that the OneXafe Solo outperformed its competitor by providing significantly more capacity scalability, more backup target, and replication options while having fewer limitations in general.

While backing up data is essential, restorations are often critical, particularly the simplicity, reliability, and speed of these operations. Our testing found that restoring a full VM was nearly instantaneous with OneXafe Solo, while the same procedure was never successfully completed using the competitor's product. The design and optimization of recovery differed for Arcserve Solo compared to their competitor. OneXafe Solo was optimized for fast recovery of a full VM, which also enables browsing of files in order to copy and restore files or folder if desired. In contrast, the competitor appeared to optimize file restoration, but critically was unable to provide full system recovery locally for VMs.

Overall, we found that the Arcserve OneXafe Solo appliance provided a reliable data protection tool designed with scalability and ease of management for small and growing environments. By offering additional backup products using the same user interface, adding larger or additional appliances to address larger environments is a non-disruptive operation.

Companies looking to improve their existing data protection methods or enhance their toolset with additional products should consider Arcserve's portfolio. Its appliance-based deployments, agentless technology, and variety of protection targets enable IT administrators to implement multiple data protection and retention options to meet various RTO, and RPO needs cost-effectively.

Appendix

Test Environment Details

The test environment utilized the following hardware, infrastructure, software, and application data.

Hardware and Infrastructure

- Two, Intel E5-2699v4 servers with 256 GB DRAM and 2 x 25 Gb Ethernet
- VMware vSphere 6.7U3 (ESXi on each node with vCenter server)
- 4 x 1.6 TB Intel NVMe media used as a local datastores for VMs
- Multiple VMs, each utilizing approximately 300 GB of capacity (from local datastores)
- External SAN storage (attached via FC to a Windows VM) for SMB backup target option
- Local storage (connected to OneXafe Solo appliance) for local backup target option
- Cloud storage (proprietary connection to each appliance)

Application / VM Environment

- Each virtual machine ran Windows Server 2019 with 4 CPUs and 32 GB of RAM
- Each VM had a boot "C:" drive of 40 GB and a data drive "F:" sized at 250 GB
- File Data on 250 GB "F:" drive
    - Directories: 3,905; files: 46,860; bytes: 243.114 GB
    - Lognormal file sizes: 4K – 256 MB
    - Data was 2:1 de-duplicatable and 2:1 compressible
- Between "incremental" backups, 10% of data on "F:" drive was modified (appx. 24 GB)

Test Overview

- Deployment (measure time, steps, and ease of use):
    - Setup of appliances, portal registration, and initial configuration
    - Setup and deployment of agents and plugins (where required)
- Continued operations (measure ease of use)
    - Setup and monitoring of VM's being protected
    - Use of 'self-service' portal, as used by a shared tenant of an MSP
- Data Protection: Backup all application instances, full and incremental
    - Measure load on VMs, (CPU, Disk, Network) while backup occurs
    - Measure time to complete full and incremental
    - Measure agentless based performance using VirtualBoot using vSphere 6.7 and similar capability with Veeam, and the performance hit on the environment.

- Restore:
  - — VM Restore: Recover a single VM
  - — Measure time to become operational from backup storage
    - Note use of Instant Restore and ability to be 'instantly operational' versus requiring vMotion to recover
  - — File Restore: Measure time to recover a few files on one VM
- DR in the Cloud: Recover a single VM from the Cloud

Test Steps

- Backup Steps:
  - — Full backup, appx. 250 GB of data on 4 VMs, (1.3 TB total)
  - — Allowed the policy for both Arcserve and Competitor to operate as planned
- Arcserve OneXafe Solo Full Backup:
  - — All VM's were backed up using agentless, VADP process to ShadowXafe VM
  - — CPU usage was negligible, with all data movement offloaded to the hypervisor
- Competitor's Full Backup:
  - — All VMs were backed up using a local agent
  - — CPU usage was about 25%, with local dedupe and compression
  - — Higher performance, due to local dedupe and compression (less network bottleneck)

About Evaluator Group

Evaluator Group Inc. is dedicated to helping ***IT professionals*** *and vendors create and implement strategies that make the most value of their storage and digital information. Evaluator Group services deliver* ***in-depth, unbiased analysis*** *on storage architectures, infrastructures, and management for IT professionals. Since 1997 Evaluator Group has provided services for thousands of end-users and vendor professionals through product and market evaluations, competitive analysis, and* ***education. www.evaluatorgroup.com*** *Follow us on Twitter @evaluator_group*

This document was developed with StorageCraft funding. Although the document may utilize publicly available material from various vendors, including StorageCraft and others, it does not necessarily reflect such vendors' positions on the issues addressed in this document.