

A Comparison of How Arcserve UDP and Veritas NetBackup Address Backup Costs and Complexity in Midsize Enterprises

by DCIG President & Founder, Jerome Wendt

PRODUCTS

Arcserve UDP 7.0

URL ► <https://www.arcserve.com/>

Arcserve (USA), LLC
8555 Columbine Road, Suite 150
Eden Prairie, MN 55347
(844) 765-7043

Veritas NetBackup 8.2

URL ► <https://www.veritas.com/protection/netbackup>

Veritas Technologies, LLC.
2625 Augustine Drive
Santa Clara, CA 95054
(866) 837-4827

USE CASE

Lowering backup costs and complexity in midsize enterprises.

Complexity Abounds

Anyone involved with enterprise IT in any meaningful capacity intuitively understands the complexities associated with supporting it. Inside the data center one finds multiple types of applications, backup targets, hypervisors, operating systems, and storage systems. Outside the data center, one encounters multiple types of clouds (hyperscale, service provider, private) along with edge devices and PCs.

On top of these variables, enterprise IT must also account for next generation requirements that span the gamut. These may include automated disaster recovery, protecting endpoint devices and Office 365, integrated appliances, ransomware detection and prevention, among others.

All these variables contribute to an enterprise needing a sophisticated solution that protects its data and equips it for future requirements. However, an enterprise may assume a “sophisticated” solution that delivers on these requirements translates into one that is “complex” and “costly”.

Sophistication Minus the Complexity and Cost

One should not immediately conclude “sophisticated” equates to “costly and complex.” This conclusion especially holds true when evaluating data protection solutions that a midsize enterprise plans to use.

A midsize enterprise clearly needs a sophisticated data protection solution to protect its data and equip it to recover. To do so, the solution must possess a comprehensive set of features to deliver on this requirement.

Simultaneously the solution must account for the limitations of a midsize enterprise. It typically relies upon IT staff that perform a wide variety of tasks. These individuals need to deploy and manage the solution’s available features as quickly, economically, and painlessly as possible.

Arcserve UDP and Veritas NetBackup

In response to these requirements, many midsize enterprises frequently consider Arcserve UDP and Veritas NetBackup as solutions to protect their data. Both these products target enterprises though they approach them differently.

Arcserve specifically targets and develops its UDP software for use by midsize enterprises with 250 – 5000 employees. In contrast, a recent analysis of over 2,000 companies that use Veritas NetBackup found these companies range in employee size. 38 percent were midsize (200 – 5,000 employees) and 30 percent were large enterprises (5,000+ employees).¹

This analysis helps illustrate that Veritas NetBackup provides the breadth of features that enterprises need. Few, if any, dispute that conclusion. The larger question becomes whether a midsize enterprise can easily and cost-effectively utilize NetBackup’s features. That’s where the importance of selecting a solution optimized for a midsize enterprise emerges. To answer this question, one should examine the following elements of Arcserve UDP and Veritas NetBackup:

- Breadth of features each solution offers versus midsize enterprise needs
- Configuration of platform needed to host the solution
- Professional services engagement
- IT skill set needed to manage the solution
- Licensing costs

Baseline Requirements for Midsize Enterprises

A midsize enterprise must first verify any solution under consideration meets its baseline data protection and recovery requirements. These needs break down into five areas:

- Operating systems (OSes)
- Applications
- Hypervisors
- Cloud
- Next-gen requirements

Common Core Requirements

In these five categories, midsize enterprises share a great deal of commonality. All primarily, if not exclusively, use Linux, Mac OS, and Windows OSes on their desktops and servers. They also all use Microsoft Hyper-V, VMware vSphere, Linux KVM, or Nutanix AHV as their preferred hypervisors. As such, any data protection solution that a midsize enterprise considers must support these OSes and hypervisors.

1. <https://enlyft.com/tech/products/veritas-netbackup>. Referenced 1/30/2020.

Midsized enterprises diverge somewhat on their data protection needs for applications and databases though they share more similarities than differences. On the application side, most run the standard Microsoft applications, such as Active Directory and Exchange. They do vary in their use of databases though most use DB2, Oracle Database, SQL Server or MySQL.

In their use of cloud resources, midsized enterprises largely turn to Amazon Web Services (AWS) and Microsoft Azure. Currently, midsized enterprises primarily leverage these cloud providers as a backup target and for long term data retention. Here again, any data protection solution under consideration must minimally support these two cloud providers for these two use cases.

That said, most midsized enterprises anticipate doing much more with and in the cloud in the coming years. This necessitates they select a data protection solution that positions them to capitalize on the cloud. For example, many already use or plan to use Microsoft's cloud-based Office 365. They also anticipate performing disaster recoveries in the cloud as well as using integrated backup appliances to simplify on-premises backup.

Similarities Abound, Differences Notable

As Figure #1 illustrates, both Arcserve UDP and Veritas NetBackup deliver the features core to midsized enterprise requirements. Each solution supports the primary applications, databases, operating systems, and hypervisors that a midsized enterprise commonly uses. Granted, the timing and support of specific versions of each one of these items will vary. However, a midsized enterprise can feel confident about each provider's commitment to delivering protection for these core components.

Arcserve's heightened focus on delivering a solution optimized for a midsized enterprise shows up in a few ways. For instance, both Arcserve UDP and Veritas NetBackup recognize and use public cloud storage as a cloud backup target. Enterprises may use either UDP or NetBackup to backup data to public clouds and perform self-service or vendor-assisted recoveries in the cloud or on-premises.

Arcserve differs by bringing its own cloud offering to the table. Arcserve offers this service to address legitimate concerns about the cost and complexity of performing recoveries in public clouds. A midsized enterprise may lack the necessary internal staff and expertise to successfully conduct its own recovery. Using Arcserve's all-in-one disaster recovery service, Arcserve can host backup data and perform recoveries in its cloud on the behalf of the midsized enterprise.

Arcserve's focus on midsized enterprises also shows up in its protection of Office 365 data. As a midsized enterprise adopts Office 365, it recognizes it must protect the data it stores there.

Currently, a midsized enterprise cannot turn to NetBackup to address this need. Veritas Support [states](#) that using NetBackup to protect Office 365 data is **"not possible."** Instead Veritas Support recommends that an organization use Veritas' separate software-as-a-service (SaaS) backup offering to protect its Office 365 data.⁴ In contrast, Arcserve UDP natively includes Office 365 data protection as a core product feature.

Key questions to ask:

- What applications, databases, hypervisors, and OSES does your enterprise need to protect?
- How do you protect Office 365?
- How do you interact with public cloud providers now? Do you anticipate your growth of them expanding?
- How do you currently manage and test disaster recoveries?
- Do you want a roadmap or ideally a solution that provides turnkey disaster recoveries that the enterprise can regularly test, validate, and employ, if needed?

FIGURE 1

Midsize Enterprise Core Requirements

	Arcserve UDP 7.0	Veritas NetBackup 8.2
Applications	Microsoft Apps, Informix, MySQL, Oracle, Sybase SAP R/3, SAP HANA	Microsoft Apps, DB2, MySQL, Oracle, + others
Clouds	Arcserve Private Cloud Multiple Public Clouds	Multiple Public Clouds
Protected Desktop OSES	Mac OS, Windows	Mac OS, Windows
Protected Server OSES	Linux, Windows, UNIX	Linux, UNIX, Windows
Disaster Recovery	Arcserve-managed Hybrid Self-service	Hybrid Self-service
Hypervisors	AHV, ESXi, Hyper-V, KVM, RHEV, vSphere	AHV, ESXi, Hyper-V, KVM, RHEV, vSphere
Integrated Appliances	9000 Series	5200 & 5300 Series
Appliances (Price Range)²	~\$12,000 - \$129,000	~\$12,000 - \$1,609,000+ ³
Office 365 Backup	Native to UDP	Veritas SaaS Backup

Endpoint Data Protection & Ransomware

Factors that influence a midsized enterprise's choice of a backup solution go well beyond the systems residing in their data center. Protecting data at the edge represents a growing priority for all size enterprises.

Enterprises increasingly rely upon data generated by edge devices such as laptops, PCs, and mobile devices to make critical business decisions. While these devices only generate and process about ten percent of enterprise data now, that could grow to 75 percent by 2025.⁵ As this percentage increases, enterprises must put in place solutions to protect this data.

Backups: A Secondary Perimeter Against Ransomware

Ransomware often surfaces as one of the primary reasons that enterprises must prioritize protection of this data. Aside from the business disruption that a ransomware attack causes, a midsized enterprise may pay a small fortune to recover its data. In 2018 alone, ransomware payments cost organizations an [estimated](#) \$1 billion with that amount only forecast to grow in coming years.⁶

End point devices represent a specific point of weakness in enterprise defenses against ransomware. Ransomware uses multiple techniques to enter organizations defenses with end point devices often being the most susceptible. While enterprises use cybersecurity software to detect and prevent ransomware attacks, backup software serves an important role.

2. Source: CDW. Referenced 1/15/2020.
 3. <https://www.cdw.com/search/?key=veritas%20netbackup%20appliance&searchscope=all&sr=1>. Referenced 1/23/2020
 4. <https://vox.veritas.com/t5/NetBackup/Office-365-and-Netbackup/td-p/868984>. Referenced 2/3/2020.
 5. <https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders/>. Referenced 2/3/2020.
 6. <https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/>. Referenced 2/4/2020.

Backup software equips enterprises to recover from a ransomware attack. While cybersecurity software detects many ransomware attacks, it does not catch all strains of it. In the event a ransomware attack succeeds and it encrypts data, backup software provides a means to recover.

Backup Software: A Secondary Ransomware Defense Mechanism

Both Arcserve and Veritas share some traits in common in how their respective solutions help a midsize enterprise protect against ransomware. Both solutions leverage Microsoft Active Directory's (AD) identity and access management (IAM) framework to grant users access to their software. This helps ensure only authorized users can access backup data and controls which data they can access.

They also each recommend that a midsize enterprise follows the same best practices when managing their backup environments. These include:

- Hardening the backup servers from ransomware attacks
- Regularly performing backups and testing restores
- Keeping backup software updated with the latest firmware patches and fixes

Arcserve and Veritas do, however, currently differ in their respective strategies for detecting and preventing ransomware on end point devices. Veritas recommends that a midsize enterprise separately deploy Carbonite EndPoint to secure its endpoint devices from ransomware.⁷ This recommendation places the responsibility on a midsize enterprise to create a cohesive, end-to-end anti-ransomware strategy.

In contrast, Arcserve offers its own backup agents to backup endpoint devices. It also partners with Sophos to detect and protect Windows, Linux, and UNIX clients from ransomware.

Arcserve makes [Sophos Intercept X](#) software available on its integrated backup appliances. Intercept X uses Sophos anti-exploit technology to stop ransomware from executing on endpoint devices by detecting signature-based and signatureless malware. Sophos utilizes artificial intelligence and

machine learning capabilities to monitor for and detect new strains of software. Making these two technologies available on an Arcserve appliance equips a midsize enterprise to quickly and easily deploy one as a secondary defense against ransomware. (Figure 2.)

Key questions to ask:

- Are you currently responsible or being called upon to handle endpoint data protection?
- Have you considered using backup software as a secondary perimeter in the detection of ransomware in your environment?
- Have you been called upon to help recover files infected by ransomware? If so, were you able to successfully recover?

Installation and Management

Every enterprise, regardless of size, wants any solution it acquires to deliver all the benefits it wants without any drawbacks. A backup solution intended for use in a midsize enterprise will ideally want it to:

- Install easily
- Provide the breadth of functions needed
- Centralize feature management through one interface
- Leverage the enterprise's existing skill sets with minimal or no extra training

A Practical Perspective

A midsize enterprise may desire its backup solution to deliver on such ideals. Backup solutions provider such as Arcserve and Veritas may even aspire to deliver on these ideals. However, a midsize enterprise must view Arcserve UDP and Veritas NetBackup more practically.

Each of these solutions address enterprise data protection needs. Enterprise requirements rarely, if ever, translate into a plug-n-play or point-and-click deployment. Their two solutions, like all enterprise solutions, require planning and forethought to successfully deploy and manage.

In that vein, both Arcserve and Veritas offer integrated backup appliances to accelerate and simplify deployment and management of their respective solutions. Using these appliances, a midsize enterprise may save weeks, even months, in set up time. An appliance also serves to significantly reduce the time and cost a midsize enterprise spends managing it.

A Divergence in Software Configuration and Costs

The simplicity of an integrated appliance does not, however, directly translate into simple software configuration and management. To configure NetBackup, best practices call for deploying a minimum of two servers in midsize or large environments: a NetBackup master server and one or more media servers. A midsize enterprise must also acquire and assign the appropriate software license keys to the NetBackup master and media servers.

Having obtained the servers and license keys, a midsize enterprise will typically pay for a professional services engagement and employee training. Due to the number of features NetBackup offers and the specific tuning required, best practices again call for a NetBackup professional to configure it. The midsize enterprise should also plan to train its IT staff on how to use the NetBackup management interface.

A midsize enterprise should find Arcserve UDP provides a more straightforward software configuration and licensing framework. An enterprise may only need to acquire a single Arcserve server that can host all necessary UDP software and associated license keys. This single server approach may also mitigate the need for a professional services engagement. One may configure and manage all features on that server through Arcserve's web-based management console. (Figure 3.)

FIGURE 2

Endpoint Protection & Ransomware Feature Comparison

	Arcserve UDP 7.0	Veritas NetBackup 8.2
Backup Appliance	UDP and Intercept X	NetBackup only
IAM Integration	LDAP, Microsoft AD	LDAP, Microsoft AD
Security Partner	Sophos	Carbonite
Endpoint Data Protection	UDP: Linux, Mac OS, UNIX, Windows Sophos: Anti-exploit Technology Sophos: Intercept-X for Mobile	Carbonite Endpoint for Android, iOS, Mac OS, Windows
AI/ML	Sophos Neural Network	●
Malware Detection	Signature-based Signatureless	●

7. <https://www.veritas.com/protection/hetbackup/ransomware-protection>. Referenced 2/4/2020.

FIGURE 3

Installation and Management Feature Summary Overview

	Arcserve UDP 7.0	Veritas NetBackup 8.2
On-premises Server Installation (Minimum Install)	1	1 - Small 2 - Midsize & Large
License Keys	All keys applied to single server	Separate keys for master & media servers
Professional Services	Optional	Recommended
Training & Certification	Optional	Recommended
Central Mgmt Console	All UDP Features	Select NetBackup Features

Key questions to ask:

- Do your IT staff members generally share administrative responsibilities for the applications they manage?
- Can you dedicate one or more people to manage your backup environment?
- Do you have staff who can manage and track software licensing?
- Can you afford to pay for a professional services engagement?
- Do you want to manage all backup features through a single console?

Backup Solution Costs

There are three costs that every midsize enterprise should minimally examine and quantify when evaluating these two backup solutions.

- Software licensing
- Hardware costs
- Support and renewal costs

Software Licensing Similarities

As backup solutions intended for enterprise use, both Arcserve UDP and Veritas NetBackup offer multiple software licensing options to better meet enterprise needs. Two software licensing options they deliver in a very similar way include their respective appliance-based and instance-based options.

These two options both follow a traditional software licensing model. Each provider licenses its software based on servers and clients protected and agents and options deployed. As a midsize enterprise protects more applications, clients, and/or servers, it must upgrade its software license accordingly.

Both Arcserve and Veritas also offer capacity-based licensing. They each calculate the total amount of front-end terabytes (FETB) of protected data and license their software accordingly. However, the similarities in how they respectively deliver capacity-based pricing end there.

Veritas NetBackup currently offers a midsize enterprise at least seven different tiers of capacity-based licensing. NetBackup’s “Complete” capacity-based licensing option represents its most comprehensive, all-inclusive option of the seven it offers. This option most closely matches Arcserve UDP’s single capacity-based software licensing option.

Distinct Software Licensing Offerings

Both Arcserve and Veritas offer additional software licensing options that may appeal to a midsize enterprise.

Among Veritas NetBackup’s additional software licensing options, two stand out. Its Starter Pack provides data protection for 5, 20, or 40 clients and starts at about \$3,250. However, a midsize enterprise needs to exercise caution in licensing this version of NetBackup. While more affordable, a midsize enterprise cannot upgrade this version to NetBackup Enterprise Server.

The Enterprise Virtual Client licensing option merits consideration for a fully virtualized midsize enterprise. This licensing option uses the CPU count as the sole metric when calculating the licensing fee. Note that this licensing option only protects virtual environments and does not extend to physical machines or UNIX clients.

Arcserve UDP breaks its licensing out in distinct ways that a midsize enterprise may more easily grasp and implement. First, a midsize enterprise may choose from four different editions of Arcserve UDP. Each edition ships with its own feature set and includes progressively more features.

Once a midsize enterprise identifies the edition that best matches its requirements, it selects the most optimal software licensing option for its environment. Arcserve makes capacity-, instance-, and socket-based licensing options available for UDP’s Standard and Advanced editions. Arcserve offers capacity- and socket-based licensing for its Premium edition.

Hardware and Annual Support Costs

A midsize enterprise’s hardware costs for each solution will vary according to its backup requirements. Most if not all deployments of Veritas NetBackup into midsize or large environments will minimally need two servers to host the NetBackup master and media server software. Arcserve UDP may only need one server to host its UDP software.

The annual, ongoing support costs for each solution will come in about the same— 20 – 25 percent of its upfront cost. However, Arcserve UDP’s upfront software cost will likely come in at about half or one quarter of NetBackup’s upfront cost. This will translate into Arcserve’s annual support costs coming in at a similarly large discount as compared to Veritas. (Figure 4.)

FIGURE 4

Backup Solution Cost and Licensing Overview

	Arcserve UDP 7.0	Veritas NetBackup 8.2
Software Licensing Options	Editions 1. Workstation 2. Standard 3. Advanced 4. Premium 5. Appliance Licensing 1. Appliance (per target appliance) 2. Capacity-based (FETB) 3. Instance-based (per OS) 4. Socket-based (per CPU socket)	1. Enterprise Virtual Client 2. Platform Capacity-based (FETB) a. Application & Database Add-on b. Big Data Workloads c. Complete d. Complete (Flexible licensing) e. Limited f. NDMP g. Windows & Linux 3. Starter Packs (Not upgradable) 4. Traditional (clients, agents, etc.)
Lowest Starting Software Cost (Approximate)	\$680*	\$3,250**
Install HW Cost Considerations	Only 1 Server Required Professional Services Optional	Multiple Servers Usually Required Professional Services Required
Renewal Costs	20-25% of Upfront Price	20-25% of Upfront Price
Support Staff	Managed by General IT Staff	Dedicated IT Staff Likely Required

* Arcserve UDP 7.0 Standard Edition 1 Socket. Referenced Insight.com on 2/4/2020.

** NetBackup software 5-client starter pack (not upgradable). Referenced CDW.com on 2/4/2020.

Key questions to ask:

- Do you understand and explain how your current software licensing works?
- What is your budget for a new backup solution?
- If you could obtain a viable new backup solution for the same or less money than the annual renewal cost of your current solution, would you consider it?
- Is managing the backup solution the best way to derive value from your current IT staff?
- Are you trying to reduce your annual spend on software maintenance and renewals?

Arcserve UDP Tuned to Midsize Enterprise Needs

Every midsize enterprise needs a sophisticated backup solution that delivers the breadth of features to backup and recover its environment. Simultaneously, a midsize enterprise also needs these features delivered in a manner that aligns with its IT budget and staffing limitations.

Both Arcserve UDP and Veritas NetBackup provide the range of the features that merit consideration by a midsize enterprise. However, Arcserve specifically tunes its UDP software to match a midsize enterprise's needs.

On top of delivering the core features a midsize enterprise requires, Arcserve prioritizes delivering the next generation of features that it needs now. Arcserve already natively supports Office 365 and endpoint data protection and delivers all-in-one disaster recoveries both on-premises and in the cloud. Further, it provides a turnkey integrated backup that immediately equips a midsize enterprise to create a secondary line of defense against ransomware.

Arcserve delivers these features using a robust, yet simple to understand software version and licensing model. These equip a midsize enterprise to quickly understand them and arrive at a licensing decision that it can financially and technically justify. Further, none of these licensing options place a midsize enterprise in a position where it cannot upgrade them.

A midsize enterprise has very specific backup and recovery needs that require a sophisticated solution to address. These demand the right software with the right features delivered in such a way that a midsize enterprise can economically and easily use them. Arcserve tunes its UDP software specifically for midsize enterprises to give them access to such a solution. ■

About DCIG

DCIG empowers the IT industry with actionable analysis that equips individuals within organizations to conduct technology assessments. DCIG delivers informed, insightful, third party analysis and commentary on IT technology. DCIG independently develops and licenses access to DCIG Buyer's Guides and Top 5 Reports. It also develops custom content in the form of executive white papers, podcasts, competitive intelligence reports, webinars, white papers, and videos. More information is available at www.dcig.com.



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

dcig.com

© 2020 DCIG, LLC. All rights reserved. The DCIG Competitive Intelligence Report Executive Edition 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 attempts 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. No negative inferences should be drawn against any product or vendor not included in this report. DCIG cannot be held responsible for any errors that may appear. No negative inferences should be drawn against any vendor or product not included in this publication. This report was commissioned by Arcserve (USA), LLC.

Licensed to Arcserve (USA), LLC., with unlimited and unrestricted global distribution rights.