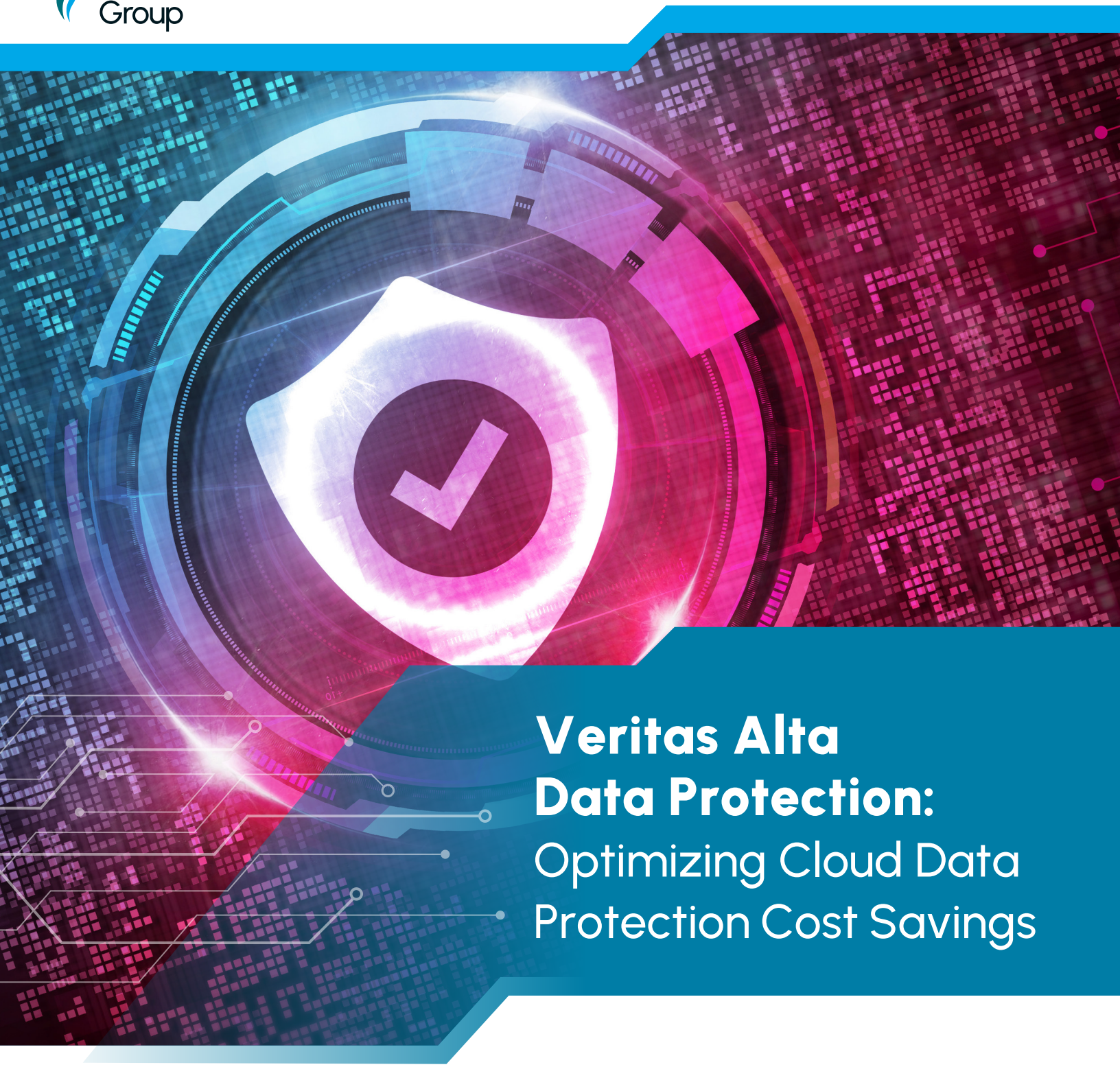
The Futurum Group



Veritas Alta Data Protection: Optimizing Cloud Data Protection Cost Savings

AUTHOR

Krista Macomber
Senior Analyst | The Futurum Group

Randy Kerns
Senior Strategist and Analyst | The Futurum Group

IN PARTNERSHIP WITH

VERITAS™

DECEMBER 2023

Introduction

Organizations continue to integrate public cloud resources into their IT implementations. Data protection is no exception. In fact, one of the earliest use cases for the public cloud was as a storage repository for backup and archive data. In The Futurum Group's *Trends in Enterprise Data Protection 2023* study, approximately 80% of respondents noted using the public cloud in some manner for data protection, and half of respondents indicated that they are using the public cloud as a backup storage target. As public cloud hosting models continue to mature, enterprises are evolving from using the cloud as just a storage target to running their backup software in the cloud, as well, as a part of their efforts to streamline and simplify operations across every aspect of their IT environment. Nearly 30% of respondents in The Futurum Group's study reported that they are using public cloud-hosted backup software.

Turning to the public cloud is helping IT Operations teams to address the three top challenges with their data protection implementations. Specifically, respondents note these as:

At the outset, the public cloud promised a cost-efficient, consumption-based purchasing model paired with greatly streamlined and simplified deployment and day-to-day management for IT Operations teams that are stretched thin.

However, if not managed effectively, public cloud services can quickly and easily become much more expensive than their on-premises counterparts. While consumption-based purchasing and as-a-service delivery offer the potential to save costs, a vast variety of factors impact overall total cost of ownership (TCO). For many organizations, this unfortunately results in unexpected cost increases and incremental costs post-cloud migration. With this in mind, it is advisable that CIOs evaluate purchases strategically with long-term returns in mind.

To help, The Futurum Group has partnered with Veritas to create a financial model for evaluating the TCO of data protection in the public cloud. Specifically, we compared the total cost of the Veritas Alta™ Data Protection offering to that of native AWS and Azure cloud services.

Overall Cloud Data Protection Cost Factors

While the factors influencing the total cost of a cloud-based data protection solution are numerous and varied, they exist in two general categories: hard costs and soft costs.

- Hard costs are expenses that are directly related to procuring and operating the data protection solution. They can be specifically calculated. A prime example is the cost to operate compute and storage infrastructure in the cloud.

- Like hard costs, soft costs relate directly to procuring and operating the data protection solution. However, they cannot be specifically calculated, and they vary from case to case. As a result, they are calculated by using best estimates.

The table below outlines key examples of hard and soft costs, many of which are included in The Futurum Group's **TCO model**.

Hard Costs	Soft Costs
Protection storage capacity	Cyber resiliency requirements – setting up environment and performing recovery when necessary
Protection storage capacity growth (yearly)	Ransomware insurance premium costs
Number of snapshots retained (daily, weekly, monthly)	Risk mitigation costs
Data egress/ingress costs	Additional resiliency costs for recovery
Other base infrastructure costs (e.g., compute)	
Cost for supporting elastic infrastructure (i.e., snapshot management)	
Subscription for the protection software	
Deployment	
Ongoing administration	

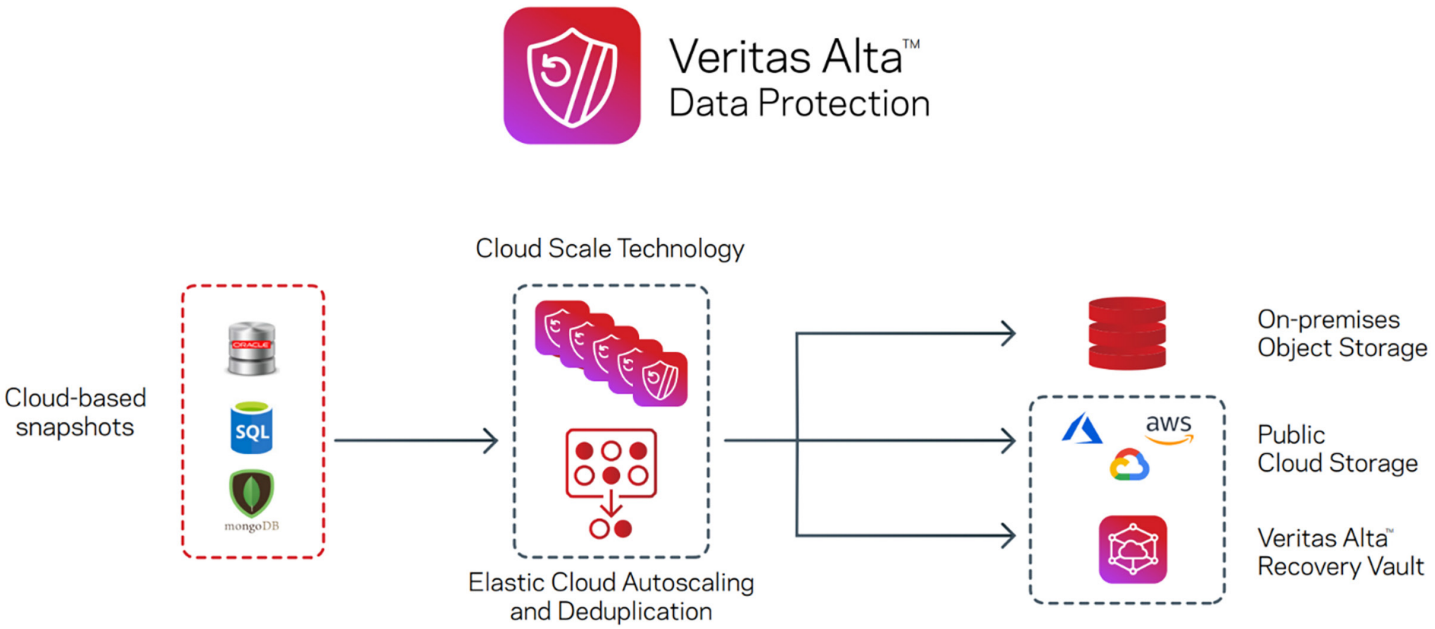
Hard costs, including protection storage capacity, are greatly influenced by the organization's ability to apply data reduction techniques, including compression and deduplication. In addition to reducing the total amount of data stored, compression and deduplication allow retention of more snapshots and for a longer period. Both are important when it comes to guaranteeing recovery points from ransomware — and to meeting regulatory requirements for data retention. The data's percentage change rate, and the ability to back up only the changed data on an incremental basis, also materially influence storage infrastructure costs.

Other notable hard-cost variables include the subscription for the protection software, which generally increases as the resources under protection grow over time. Data-retrieval costs are also highly material, though unfortunately generally unpredictable as they are predicated largely on requirements for disaster and cyber-recovery as well as legal discovery.

Hard costs also factor in predictable and recurring day-to-day administrative efforts, including setting and maintaining automated protection policies. It is possible to materially reduce this effort if one tool can support multiple cloud environments, as opposed to the cumbersome approach of requiring separate tools and their unique and dedicated training and management costs for different cloud environments.

In today's era of cybercrime, soft costs are largely dictated by cyber-resiliency and cyber-recovery requirements. These include lost business and brand damage due to downtime and data loss, ransomware insurance premium costs, and the need to execute a full recovery validation test at least once per year.

Cloud Cost Optimization with Veritas Alta™ Data Protection



Veritas Alta™ Data Protection is a data backup and recovery solution for multi-cloud enterprise environments. Specifically, the solution is built on Veritas Cloud Scale Technology, which is a cloud-native, distributed, and microservices-based architecture that is deployable in AWS and Azure public clouds. Per Veritas, this architecture is scalable to support large numbers of workloads and petabytes of data, without requiring major advance planning and changes to the environment.

Data backup and recovery operations are executed via media servers (also known as data movers) that can be deployed on-premises or in the cloud. The Futurum Group's TCO model assumes a cloud-based deployment. Veritas Alta Data Protection automatically provisions the cloud compute resources to meet surges in performance requirements. And as performance requirements subside, it automatically deprovisions the cloud compute resources.

Veritas Alta™ Data Protection integrates with native public cloud snapshots, as well as the cloud providers' snapshot management functionalities, to back up these cloud snapshots using a containerized deduplication engine that minimizes storage footprint. The solution also supports incremental backup of PaaS workloads to further optimize the data stored and transferred in cloud environments.

All data is encrypted throughout every part of the backup operation, from the client to the media server to the back-end cloud storage service — including all data sent over the network. Customers also have the option to add Veritas Alta Recovery Vault for a fully integrated, cyber resilient cloud storage service. It provides a choice of cloud providers, immutable and isolated storage, no data transfer fees, and a predictable per-TB monthly cost model (see above diagram). Immutability is available by default and irrespective of storage tier.

Included at no additional cost, Veritas Alta View provides centralized, single-pane-of-glass policy-based management, reporting, and general management/oversight across all backup domains (both on-premises and cloud).

The Futurum Group – Key TCO Model Assumptions and Findings

The Futurum Group's TCO model compares Veritas Alta Data Protection to native AWS and Azure backup services. The model is designed to project hard, soft, and overall costs compounded over a total of seven years.

Veritas Alta Data Protection Hard Costs vs. Native Cloud Services

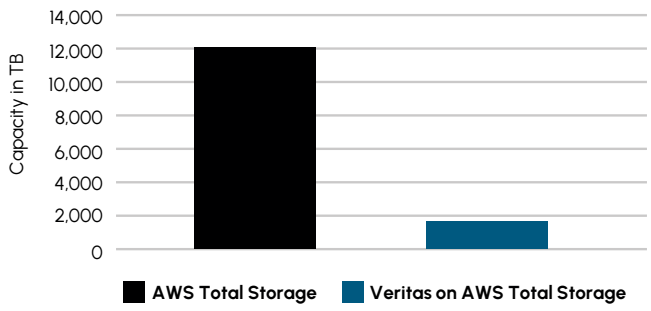
The following are the key assumptions factored into the model for overall storage costs:

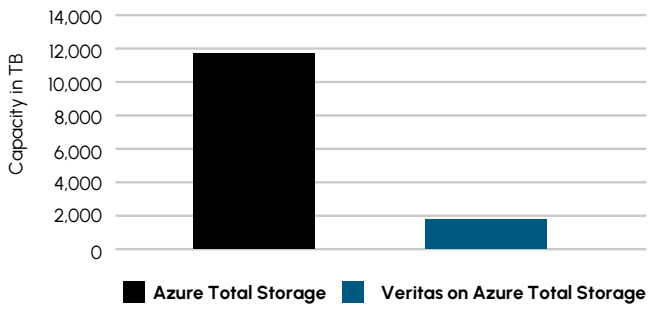
Storage Costs			
	Veritas	AWS	Azure
Protection storage capacity	500 Front-End Terabytes (FETB)		
Protection storage capacity—annual growth	10%		
Daily change rate	3%		
Data reduction—initial/full	75%	0%	0%
Data reduction—incremental	95%	0%	0%
Data egress/retrieval costs	4%	14%	14%

The model factors in the retention of an initial full snapshot, as well as backups of periodic, incremental snapshots on a daily, weekly, and monthly basis. From the standpoint of overall storage costs, the major advantage of Veritas Alta Data Protection compared to native cloud services is its efficient and global data reduction. It is relevant to note that Veritas deduplication engine is containerized and applied elastically through the cloud. In addition to reducing the total storage capacity required, this also lowers the percentage of data that needs to be retrieved in the event of a recovery. The result is substantial data egress cost savings to the tune of an estimated $4,800 versus $16,800 per year.

Also notable is the fact that AWS Backup does not archive backups to a lower-cost storage tier automatically, leaving the backup copies on more expensive storage. All these factors combined result in substantial storage capacity savings that compound during each of the projected seven years. Additional occasional costs may include extended retention for snapshots to enable granular recovery. Veritas Alta Data Protection avoids this by retaining stored images with a feature that Veritas calls Instant Access.

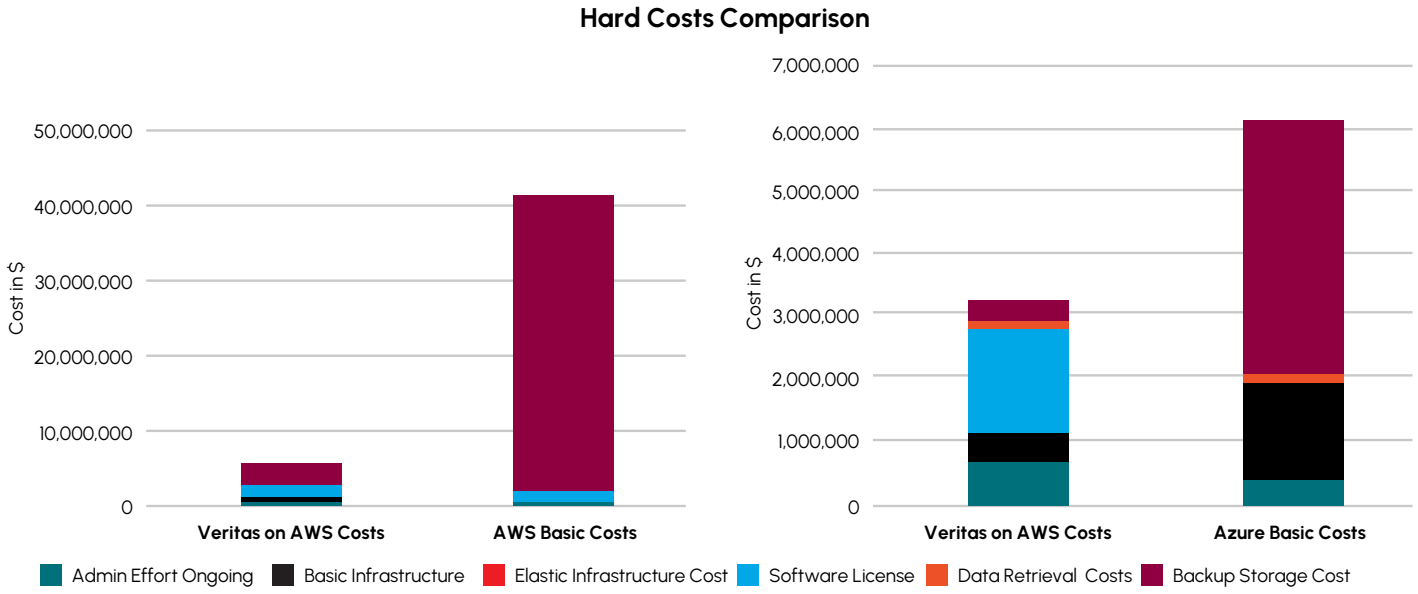
Storage Required at Year 7

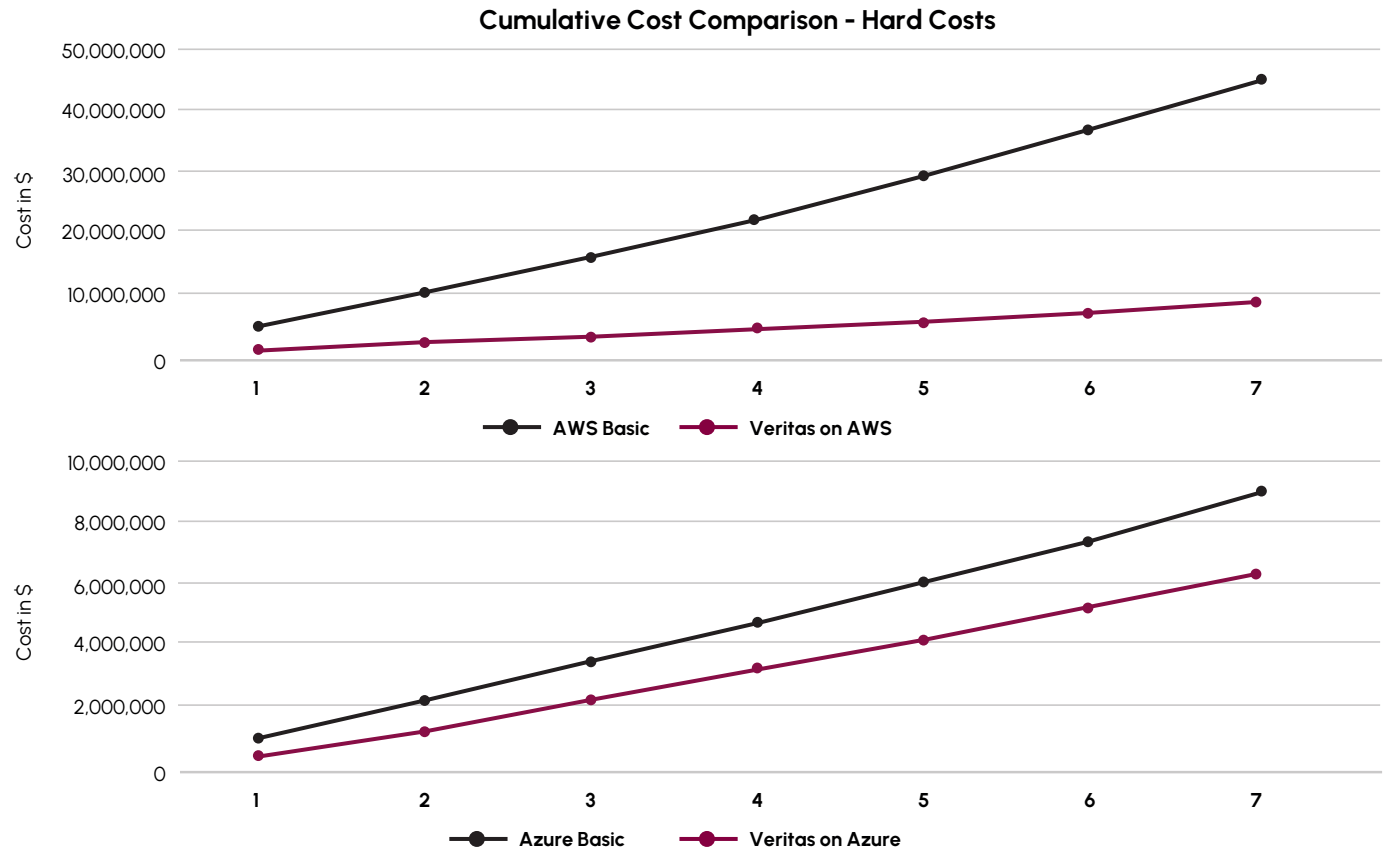




Looking beyond the storage capacity costs, Veritas Alta Data Protection also includes the ability to optimize elastic compute resources. These functions are primarily snapshot management and the ability to scale compute resources up and down dynamically as workload requirements fluctuate. This ensures that the Veritas solution can always meet demands of backup jobs without overprovisioning compute cycles. While it adds a small overhead cost, it substantially lowers overall infrastructure and hard costs. Like the storage capacity savings, these cost efficiencies compound over time.

Other operational costs factored in to The Futurum Group's model include deployment and ongoing administration of both solutions. These are streamlined in hybrid multi-cloud implementations with Veritas Alta Data Protection, due to the solution's ability to support multiple cloud environments.





Veritas Alta Data Protection Soft Costs vs. Native Cloud Services

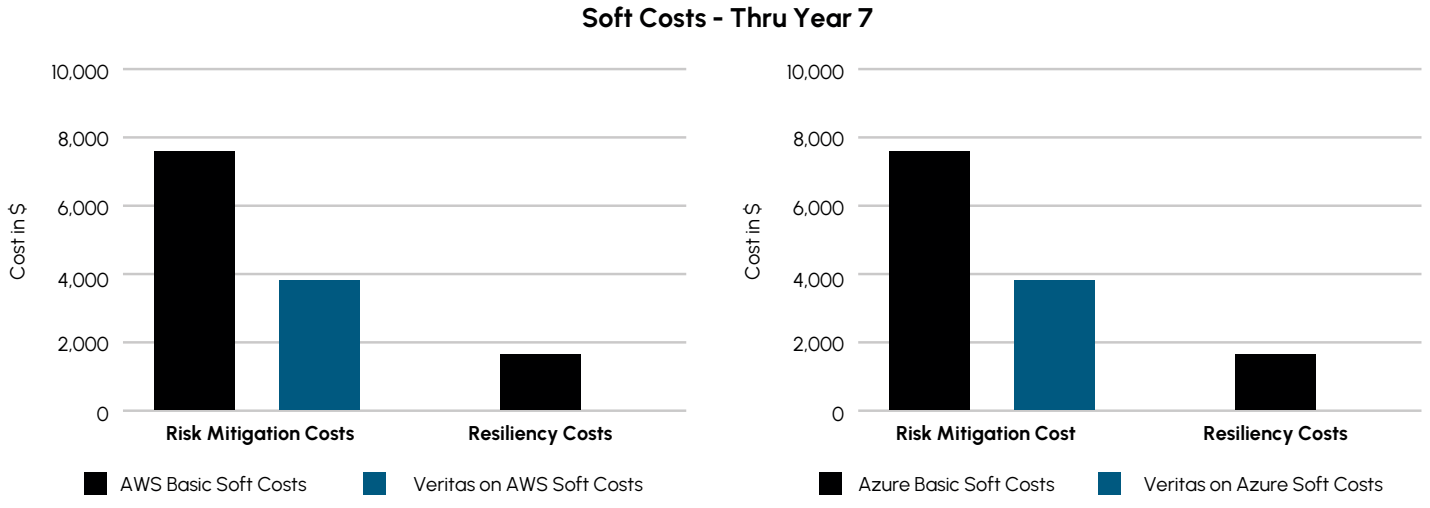
The soft costs factored in to The Futurum Group's model hinge primarily on cyber resiliency and risk mitigation. With ransomware plaguing all industries, these cannot be ignored. These cost factors fit into four key areas for evaluation from a TCO perspective:

- Data loss prevention, which is, over the long term, less expensive than recovering data. This is especially true when factoring in the lost productivity and revenue that are likely to occur during a breach.
- The ability to avoid regulatory compliance fines and legal fees relating to a data breach.
- The ability to avoid detrimental, potentially long-term impact to the organization's reputation and customer confidence that is likely to result from a data breach.
- The ability to avoid increased premiums for cyber insurance due to a data breach.

Specifically factored in to The Futurum Group's model is the fact that basic cloud services require at least twice the recovery time objectives (RTOs), when compared to Veritas Alta Data Protection. Lower RTOs are available from cloud providers but require an additional cost. Achieving equivalent resiliency provided by native cloud services also requires clustering, which is approximately twice the cost of basic infrastructure. As a result, Veritas Alta Data Protection helps to mitigate loss of business due to downtime and avoid increases to ransomware insurance premiums.

Additionally, testing of recovery is increasingly required, both by business leaders and for compliance purposes. Native services require rehydration of the data from the protection storage, which then must be copied to an isolated recovery environment (IRE) and scanned. All of this incurs additional compute and storage costs, as well as licensing fees for the software used to scan the data. With Veritas Alta Data Protection, an IRE can be set up that includes network isolation, inline malware scanning of data, and clean recoveries at scale — all with highly granular recovery point objectives and minimal RTO —at no additional cost.

Finally, it is worth noting that additional, environment-specific costs are likely to come up on a case-by-case basis. The model accounts for these costs using representative numbers from existing customers. Interested customers may contact Veritas sales for more specific information and detailed discussion.

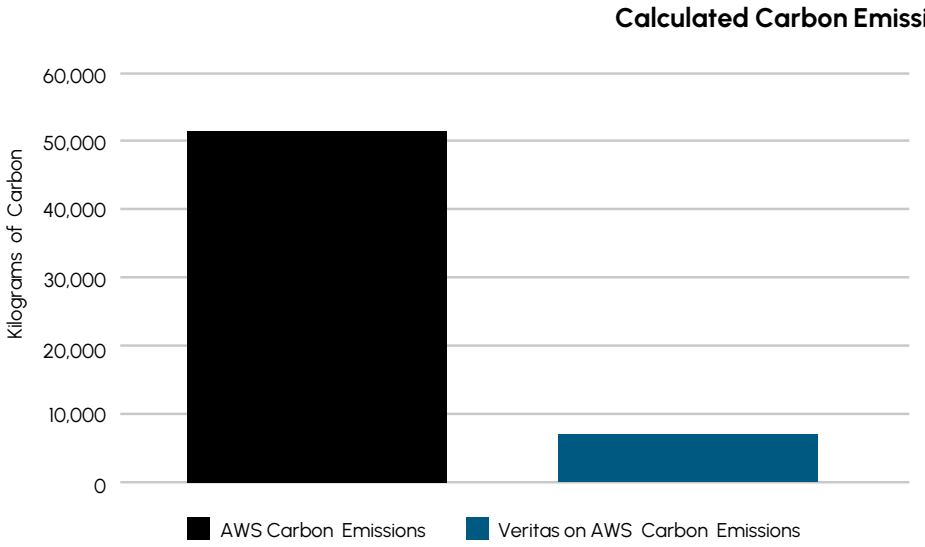


Sustainability and Carbon Emissions

Everything that burns carbon-based fuels or consumes electricity from the power grid leaves a carbon footprint. This is an increasing concern among executives and leaders in every industry. Today, it's estimated that data centers generate 2.5% of all human-induced carbon dioxide emissions, an even bigger carbon footprint than the aviation industry (2.1%). And the data center percentage is growing at an extremely rapid pace.[1]

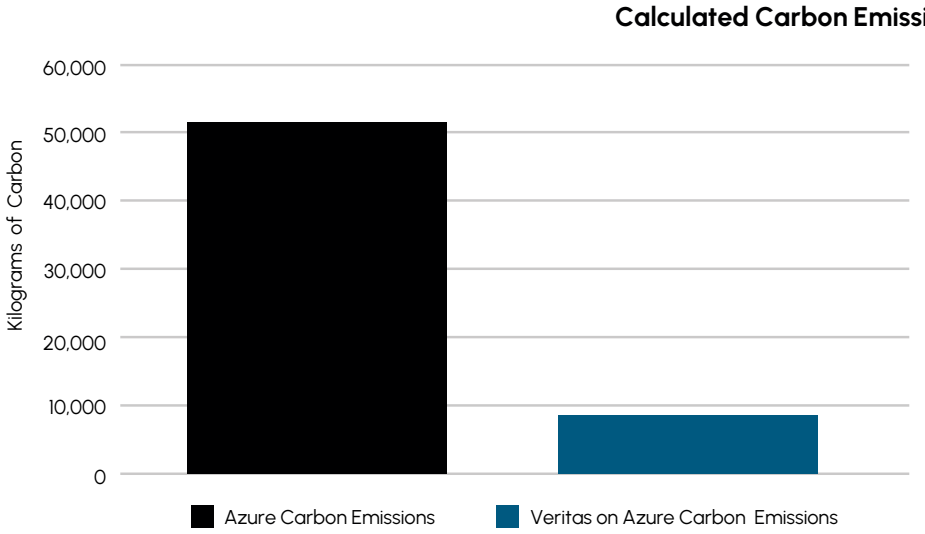
Although estimates vary, a detailed analysis by Gerry McGovern found that every 1 TB of data stored in the cloud generates 4.2 kg of CO2 emissions.[2] Every 1 PB of data stored would then generate 4200 kg, or 4.2 metric tons of CO2 emissions.

With Veritas Alta™ Data Protection, the material reductions in data transferred and stored can also substantially lower carbon emissions by 84% or more. For 1 PB of data, this equals a reduction of approximately 3.5 metric tons of CO2 from our atmosphere.



Energy consumption: 0.015 kWh per GB (15 kWh per TB)

Carbon output: .28kg per kWh



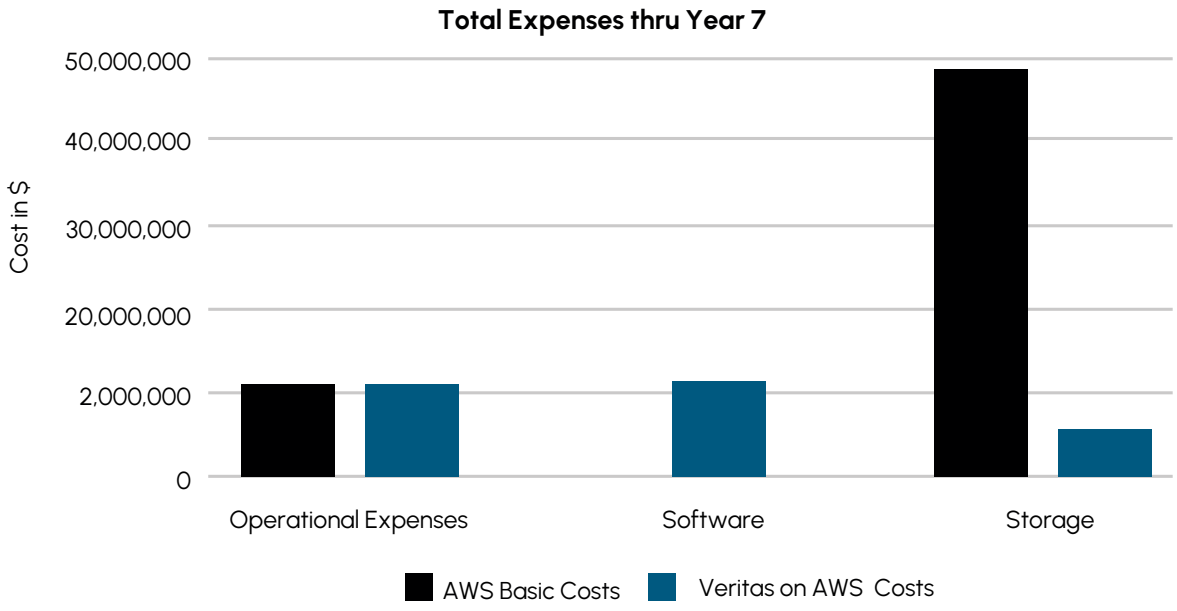
Energy consumption: 0.015 kWh per GB (15 kWh per TB)

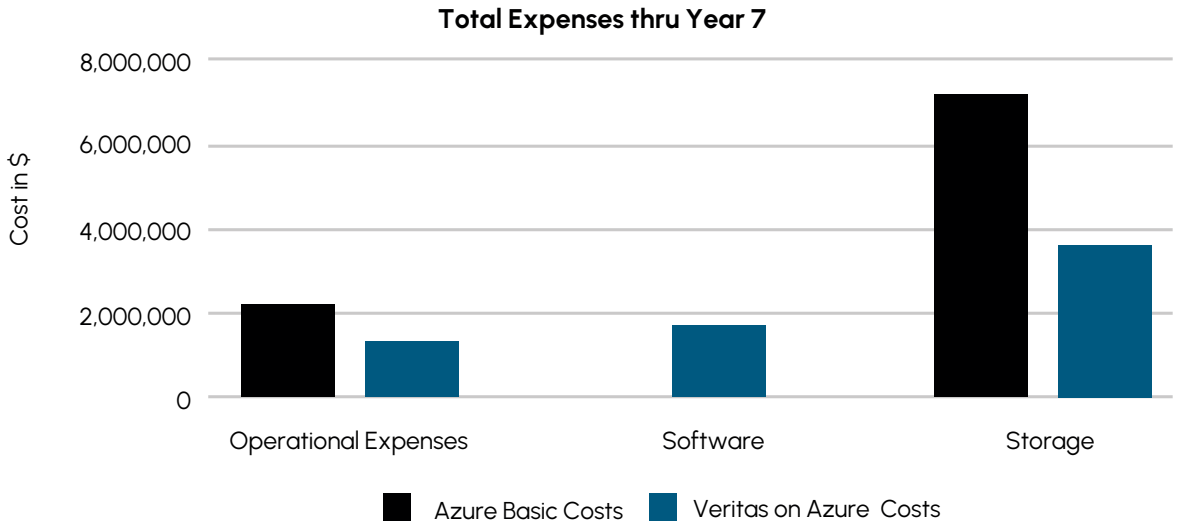
Carbon output: .28kg per kWh

* The energy consumption rate used is an estimation based on an analysis of cloud energy usage and actual energy consumption rates may vary. Carbon emissions were derived from a UK government statistic from 2018. Actual C02 emissions may vary by location and energy sources used. The same carbon emissions calculations were used for Veritas Alta, Azure, and AWS and the resulting carbon emissions savings are a result of lower overall capacity.

Conclusion

In summary, the Futurum Group's model found that Veritas Alta Data Protection stands to save customers 80.8% and 31.3% when compared to AWS and Azure native services, respectively. In total, we estimate net operational savings of more than 42% when comparing to both environments, as well as a significant reduction in risk mitigation costs. Complementing these figures, arguably the most notable area of cost savings lies in storage infrastructure, via the Veritas data reduction technologies as well as the ability to control egress fees. Veritas also provides a more sustainable solution for protecting data – across any cloud, for any workload, and at any scale.





Learn more about **Veritas Alta Data Protection.** Try out the **TCO Model** for your own organization.
To contact Veritas Sales, call (866) 837-4827 in the United States or r**equest a call** from our sales team.

References

1 "'Dark Data' Is Leaving a Huge Carbon Footprint. And We Have to Do Something About It," Science Alert, September 2022.
2 "Calculating the pollution effect of data," Gerry McGovern, March 2020.

Important Information About this Report

CONTRIBUTORS

Randy Kerns
Senior Strategist and Analyst | The Futurum Group

Krista Macomber
Senior Analyst | The Futurum Group

PUBLISHER

Daniel Newman
CEO | The Futurum Group

INQUIRIES

Contact us if you would like to discuss this report and The Futurum Group will respond promptly.

CITATIONS

This paper can be cited by accredited press and analysts, but must be cited in-context, displaying author's name, author's title, and "The Futurum Group." Non-press and non-analysts must receive prior written permission by The Futurum Group for any citations.

LICENSING

DISCLOSURES

The Futurum Group provides research, analysis, advising, and consulting to many high-tech companies, including those mentioned in this paper. No employees at the firm hold any equity positions with any companies cited in this document.

VERITAS™

ABOUT VERITAS

Veritas is uniquely equipped to help organizations of all sizes conquer the complexity of managing and protecting their business-critical data. Through our integrated product portfolio, we provide a unified data management experience that delivers unmatched performance and versatility – edge to core to cloud.. for more information click here.

ABOUT THE FUTURUM GROUP

The Futurum Group is an independent research, analysis, and advisory firm, focused on digital innovation and market-disrupting technologies and trends. Every day our analysts, researchers, and advisors help business leaders from around the world anticipate tectonic shifts in their industries and leverage disruptive innovation to either gain or maintain a competitive advantage in their markets.

CONTACT INFORMATION

The Futurum Group LLC | futurumgroup.com | (833) 722-5337