druva

White paper

The SaaS Advantage for IT Cost Reduction

Don’t get sunk by legacy backup systems

Q223-20387

Introduction

The uncertainty arising from today's macroeconomic conditions is driving many IT departments to take a closer look at their budgets. Data remains the most critical asset for how companies operate and gain competitive advantages and it's growing rapidly, which makes protecting it a top priority. Unfortunately, many organizations are protecting their growing data with a mix of software, hardware, and appliance-based solutions that have excessive hard costs from redundant copies, over-provisioned storage, excessive cloud costs, long-term licenses, as well as under-accounted-for soft costs like capacity management, software and hardware patching and upgrades, cloud management, and performance tuning.

As organizations consider how to save money and do more with less, they're turning to SaaS data protection for help. But for many IT leaders, comparing the cost of SaaS to traditional hardware, software, or appliance-based data protection solutions can be complicated. In fact, just because an organization is using SaaS solutions (who isn't using SaaS somewhere in their organization?) doesn't mean they have experience alleviating all of the hidden hard and soft costs of traditional solutions.

Are hidden costs sinking your transformation plans?

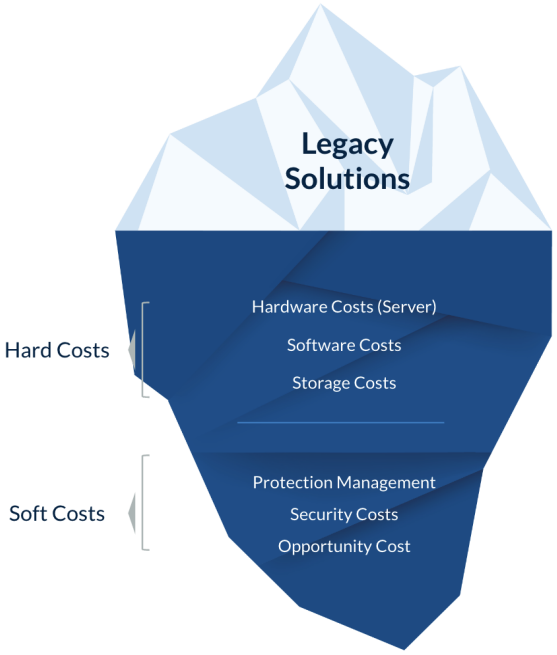
It can be difficult to break out of the traditional software and hardware refresh cycle of legacy backup systems because of hidden costs that have been taken for granted for years. These hidden costs make it difficult to compare traditional data protection solutions with modern SaaS solutions.

Let's dive deep and examine some of the costs that keep you locked in the legacy backup trap.

What costs are hiding below the surface?

When you're thinking about the fixed costs of legacy data protection systems, some costs are obvious. You need to purchase the software, along with the servers and storage to run the backup systems.

Soft costs are the cost of management of your data protection platform. Much of these costs are connected with managing and securing systems that host the backup environment. However, there are even more hidden costs to consider when evaluating the true TCO of legacy backup systems.



Hardware / Software / Storage Costs

- Over-provisioned appliances
- Long-term SW Licenses
- Cloud costs & fees
- Redundant copies

Management Costs

- Capacity Management
- Software upgrades & patches
- Cloud management
- Performance & Cost Tuning

Security Costs

- Air-gapped ransomware copy
- Secure & patch backup infrastructure
- Threat monitoring & alerting
- Incident response

How can you get the full picture of how these costs add up in your organization? Ask yourself the following questions:

Hardware / software / storage costs

- **Over-provisioned appliances —** Are you building out capacity "just in case" you need it? Do you have infrastructure sitting idle because you don't need it yet?
- **Long-term software licenses —** How many different software licenses do you need to manage across your data centers, remote offices, and cloud instances? Are you paying for future licenses before you use them just to get an arbitrary lower amount per TB or instance?
- **Cloud costs and fees —** Do you need to pay cloud fees to run your solution in the cloud? What about recovery fees? If you're hit with ransomware will you be required to pay an egress fee to restore that data to on-premises machines?
- **Costly duplicate copies —** Every copy of data has associated storage, management, and other operational costs. How many copies of your data do you have? Do you have the backup copy, then another for ransomware recovery, and perhaps one more in the cloud?

Management costs

- **Capacity management —** Why spend time managing or worrying about storage capacity and efficiency for your data center, remote offices, cloud instances, and offsite location(s)?
- **Software upgrades and patches —** Are you running the latest version of your current backup solution? If not, it's probably because of the time and risk associated with upgrades.
- **Cloud management —** If you're running cloud workloads or protecting SaaS applications, you're most likely spending time managing one or more instances of a backup solution running in the cloud, not to mention security and user access.
- **Performance and cost tuning —** How many hours do your valuable IT personnel spend keeping the backup infrastructure in working order?

Security costs

- **Air-gapped ransomware copy —** Simply replicating backups to another site will not create an air-gapped, ransomware-protected copy of backup data. What steps do you need to take and how many people do you need to involve to ensure you automatically have an air gapped copy of data and immutable backups when required?
- **Secure and patch backup infrastructure —** Is your entire backup environment secure today? Ensuring every component of your on-premises backup infrastructure is secure, from user roles to servers to storage to the network takes time and different types of expertise. And what's in place must be validated on a regular basis as you upgrade, expand, or change your environment.
- **Security monitoring of backup environments —** Backup environments are often targeted by ransomware, so they must be monitored to stop attacks. Additionally, the entire backup environment must be continuously monitored to be sure it is ready to withstand a cyberattack.
- **Incident response costs —** Time is money during a cyber attack. But when ransomware attacks are discovered, they have usually been infecting systems for days or weeks. Many traditional backup solutions can only recover data, but can't tell you on which day ransomware may have infected a particular snapshot from a particular system. Coordinating from which day to restore data across different systems and snapshots can take days or weeks.

Opportunity costs

If your team is babysitting legacy backup systems, they won't have any bandwidth left over to drive new business initiatives. This impacts future revenue because your team isn't able to support new business requirements. Another consequence of having talent only focused on backup infrastructure management is that it can impact the retention of operations staff. Many people in IT don't view spending all their time building, managing, patching, and securing legacy backup systems as high-value work by most people in IT today.

Traditionally, backups have been a very time consuming task in the data center. Organizations have accepted this cost because it is vital to be able to restore data to meet a range of data loss scenarios from accidental deletions to malicious attacks. Since it is so important and time consuming, senior IT administrators can get consumed managing data protection. By some estimates, 64% of new IT rollouts fail because of a lack of senior IT resources.[1] Isn't it more important to focus these talented leaders on new initiatives?

Break the cycle without rip and replace

1. **Calculate hidden costs.** Make sure you're aware of the hidden costs when using DIY and HCI architectures. Calculate the hidden costs of legacy data protection platforms when you compare them to SaaS platforms.
2. **Don't expand on-premises backup storage.** Legacy on-premises backup is expensive and more vulnerable to attacks. In fact, analyst firm Enterprise Strategy GroupESG says cloud provides 41% better security when compared to on-premises resources.[2]
3. **Adopt a SaaS data resilience architecture.** As your legacy data protection software and hardware licenses age or expire, plan to move to a SaaS data resilience architecture.
4. **Start protecting new workloads with SaaS architecture.** If you're building cloud applications or adopting SaaS applications like Microsoft 365 or OneDrive for Business, retrofitting legacy backup applications isn't going to cut it. Cloud apps require a SaaS-based data protection solution.

5 ways Druva's SaaS-based data protection unlocks your potential

If your legacy backup approach is dragging you underwater, maybe it's time to soar in the clouds with a SaaS-based approach. A modern and mature SaaS solution can lower your costs, reduce complexity, and accelerate time-to-value. The Druva Data Resiliency Cloud is a 100% SaaS-based data protection platform that manages enterprise data assets. It scales to meet the needs of your business without the overhead of infrastructure, maintenance, and support costs. Here are five ways Druva's SaaS data protection delivers major benefits:

Modernize for flexibility and scale

A SaaS-based data protection solution eliminates the need to over-provision resources because it will scale-up and scale-down on demand as your business grows. Your people won't need to tend to growing the environment, and instead can focus on higher-level activities that will grow your business.

Refocus IT on managing data

Instead of tasking system administrators to build and manage a legacy backup infrastructure, SaaS-based data protection frees their time and makes it possible for them to focus on the data. This is because the team won't need to manage the backup hardware or software, patching, or security activities.

Break free with better time-to-value

Organizations see faster time-to-value with SaaS-based data protection solutions whether supporting new offices or new workloads in the cloud. With no hardware or software to install and manage they break the status quo which increases IT agility. SaaS solutions have shorter purchasing cycles, and have fully automated platform updates. They just work. And since they scale up or down automatically, you don't need to worry about storage management. Anyone in IT can use the solution without special training.

[1] https://www.techrepublic.com/article/gartner-talent-shortages-are-behind-lagging-adoption-of-new-technologies/
[2] https://www.esg-global.com/hubfs/ESG-Infographic-From-Data-Backup-to-Data-Intelligence.pdf

Go beyond typical backup and data security

SaaS-based data protection solutions build in security with a logical air gap between the customer environment and the cloud. Backup data is stored in a public cloud on a separate network from the customer environment. Additionally, customers can't directly access a backup file system, but neither can ransomware. The backup data, application, users, and activity are all on one platform enabling advanced security monitoring and coordinated incident response activities from one source of data. The added value of using backup data to enhance security is truly a multiplier effect across workloads and clouds.

Drive savings and reduce TCO

SaaS data protection solutions offer a tremendous amount of savings. Customers no longer need to purchase or manage backup hardware and software, as the SaaS provider handles that. SaaS pricing is transparent and consumption based. Since everything is in one place, your backup data becomes an asset, allowing you to streamline governance, improve cyber resiliency, and gain critical insights for your business.

Customer Story: Suez soars to modernization with Druva

Suez Water Technologies & Solutions solves the toughest water and process challenges where they occur. When the company expanded by acquiring GE Water, their data protection footprint exploded. The acquisition came with 60 on-premises servers (VMs and file servers) that needed a data protection solution.

Suez was already using the public cloud to run its enterprise resource planning (ERP) software. They worked with a managed service provider (MSP) to back up those workloads in AWS. However, they were facing storage cost issues because database administrators (DBAs) took as many snapshots as they needed, not realizing they were driving up costs. And now they were faced with an aggressive acquisition timeline to figure out how to protect an on-premises dataset.

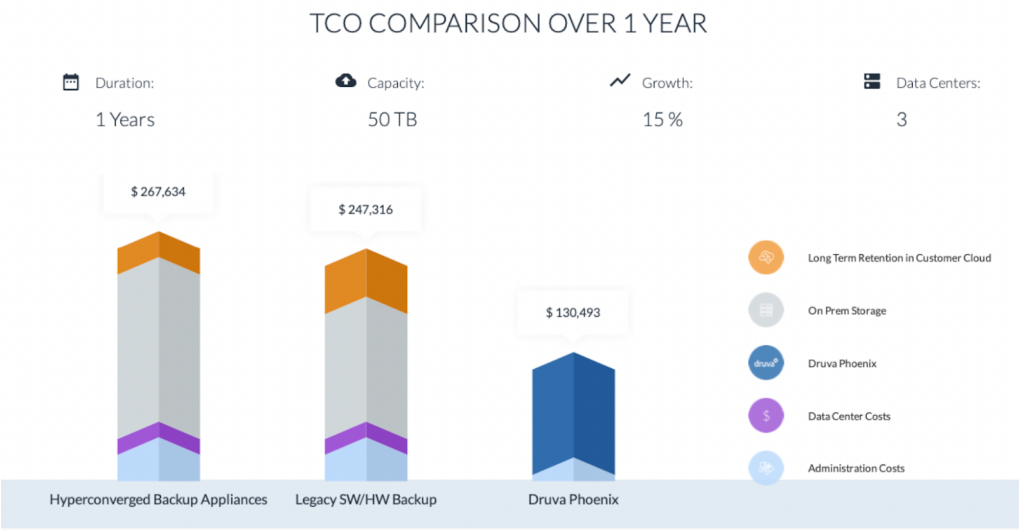
The acquisition caused Suez to consider the total cost of ownership for a data protection solution including critical requirements like time to value. Doing an extensive POC with different hardware infrastructure would take too long and those solution architectures did not align with their cloud focus. They quickly chose Druva to protect and centrally manage their data center and cloud workloads in AWS (e.g., Oracle on EC2). Now they have one tool to protect, store, and recover all of their data on-premises and in AWS.

	Before: Traditional Approach + MSP	After: Druva Data Resiliency Cloud	TCO improvement
Hard costs	• Build legacy solution (hardware, software, storage) • Script-based backups • 600TB EBS database storage	• No hardware or software needed for on-premises solution • One solution for AWS and on-premises • Oracle and SQL Server solution + snapshot visibility reduced EBS storage consumption	**50% TCO** improvement **4x reduction** in Amazon EBS storage
Soft costs	• Administrative costs to manage legacy solution • Missed RPO and RTO times • Snapshot sprawl but no unified tool to gain insight to solve the problem • IT time tied up with backups, not helping with business goals	• Backups cut in half, and users can restore data themselves meaning less admin hours needed tending backup issues	**6x reduction** in backup admin time requirements

Start your own journey to savings and agility

You have read how one customer reduced costs and improved their operational agility. You can begin to get a picture of potential savings and benefits in another TCO comparison below. The most important outcome is to ask the right questions and not discount the savings from soft costs. Your people and data are your most valuable assets.

The figure below compares the TCO of hyperconverged backup appliances, legacy software and hardware backups, and the Druva Data Resiliency Cloud.



Source: https://tco.druva.com

Conclusion

Legacy data protection solutions are complex and too expensive. It is easy to compare solutions based only on the costs provided by different vendors which is only the tip of the iceberg. It's important to consider both hard and soft costs when comparing solutions and building a TCO to help decision making. At a time when companies need to protect their data more completely, quickly, and cost-effectively than ever before, a better approach is needed.

You need the Druva Data Resiliency Cloud.

Discover how much you could lower the total cost of ownership of your data protection solution with the Druva. Learn more about the Druva SaaS advantage, or contact Druva for a TCO workshop.

druva Sales: +1 888-248-4976 | sales@druva.com

Americas: +1 888-248-4976
Europe: +44 (0) 20-3750-9440
India: +91 (0) 20 6726-3300
Japan: japan-sales@druva.com
Singapore: asean-sales@druva.com
Australia: anz-sales@druva.com

Druva enables cyber, data and operational resilience for every organization with the Data Resiliency Cloud, the industry's first and only at-scale SaaS solution. Customers can radically simplify data protection, streamline data governance, and gain data visibility and insights as they accelerate cloud adoption. Druva pioneered a SaaS-based approach to eliminate complex infrastructure and related management costs, and deliver data resilience via a single platform spanning multiple geographies and clouds. Druva is trusted by thousands of enterprises, including 60 of the Fortune 500 to make data more resilient and accelerate their journey to cloud. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.