druva

Switch from Veeam to Druva, Reduce TCO by up to 40%

Veeam's Legacy Approach To Data Protection Will Cost You More, Everytime.

Summary

When considering the best backup solution for workloads in data centers and remote offices[1] organizations need to carefully evaluate their decision criteria and cost models to achieve the best outcomes for their business. A dependable cost model takes into consideration not just hard costs like hardware, software, and cloud capacity, but also supporting costs such as current data center investment, administration time, networking requirements, security, and long-term growth footprint.

Is Veeam right for your environment today? It's important to look deep into the numbers to truly understand if you're getting the best bang for your buck. What was great about Veeam 10-15 years ago, a server-based approach for emerging VMware usage, has now become a model of the past. At the same time, SaaS has continued to make huge technology advancements, making it the de facto standard for data protection in modernized IT environments. Organizations today can and should look at a leading SaaS backup provider, like Druva as part of any IT modernization and cost reduction effort.

There are three market factors that have shifted the traditional cost model dramatically in recent years.

- **Evolving Security Risks:**
  Data breaches and ransomware attacks continue to make daily headlines, and unfortunately continue to evolve and outsmart some of the most robust on-premises security setups. The escalating costs of protection and potential loss are well documented.

- **SaaS Modernization:**
  SaaS has set a new standard in time-to-value, and increased access to enterprise technologies that many businesses previously couldn't afford (e.g., for data durability, resilience, security, analytics, …). SaaS delivers a fully managed, financially favorable opex-based model, and only in unique cases, where an organization already has sunk data center costs, unprovisioned hardware and storage, and trained staff, or, very complex, extremely tight RPO/RTO requirements does considering on-premises still make financial sense.
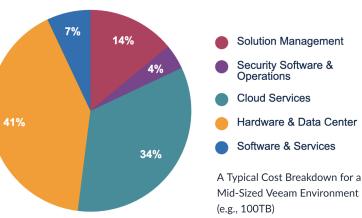
- **Data Sprawl:**
  Life was easier when data was all on local machines, but that's no longer the case. There has been a dramatic increase of complexity in managing backup environments; servers, laptops, cloud services (SFDC, Microsoft 365, …), and even IoT devices. On-premises solutions often struggle with this type of expansion, creating a fragmented and complex management experience, where SaaS solutions are able to deliver a fully integrated front-end environment.

These factors lead to a significant Total Cost of Ownership (TCO) advantage for Druva of up to 40% when compared directly to Veeam. In the following sections we'll dive deeper into these factors, as well as show a series of sizing models for common implementations of Druva vs. Veeam and the associated costs. Should organizations consider switching from Veeam to Druva, especially with the overwhelming shift to SaaS? Read on, the conclusion is straightforward that for nearly all use cases the better option is Druva's SaaS-based approach.

Implementing Veeam: A Complete Cost Picture

When evaluating a Veeam backup environment, there are multiple cost components involved for a typical mid-sized organization. To assess Veeam's TCO, current infrastructure investments, size of your data footprint, number of sites, existing security investments, and staffing all are important factors to consider. The pie chart to the right represents the typical cost allocations for a 100TB environment, 200 VMs, and using a backup cadence of 30 dailies, 4 weeklies, 12 monthlies, 3 yearlies for retention (*see the cost comparisons later in this document for a more detailed breakdown*).

Veeam Costs Breakdown

- Solution Management — 14%
- Security Software & Operations — 4%
- Cloud Services — 34%
- Hardware & Data Center — 41%
- Software & Services — 7%

A Typical Cost Breakdown for a Mid-Sized Veeam Environment (e.g., 100TB)

---

[1] E.G., files, network attached storage, and virtual machines such as VMware, Microsoft or Nutanix.

Software, Hardware, and Data Center (48% of Total Cost):

This category represents the largest of the costs, which will vary from one organization to the next based on existing infrastructure, size of VMs, and if a single-site or multiple sites are involved. The diagram to the right is an example architecture, following best practices, for a standard 3-2-1 type backup deployment.

An Example On-Premises Backup Architecture for Med. Environments (100TB)

Data Center Infrastructure Components for Veeam	
Local Storage	On-premises storage represents the largest cost item. Veeam does NOT recommend using cloud storage as a primary backup repository[2]. Cloud storage is relegated to secondary or tertiary copies.
Server Hardware and Networking	Complexity is a function of the number of Veeam services. An environment for 50-100TB that follows security best practices requires at least 9 servers[3] and scales depending on secondary, offsite/cloud storage, etc.
Software Licenses	Veeam requires a Microsoft Windows Server environment — cost scales by number of servers.
Data Center Space Allocation	On-site vs co-location factors are nominal and represent a small percentage of the total costs. However, space allocation needs to be considered given the 9 server recommendation for this deployment.

Third-Party Cloud Storage (34% of Total Cost):

Organizations that want to use cloud (AWS S3, Azure Storage, …) have a few options available:

- Use their own contracted cloud storage, or
- Use Veeam's Cloud Connect capabilities via one of their providers.

In this case, you'll want to take a hard look at ingress and egress fees, API costs, and also be aware that deduplication inefficiencies will be passed onto the cloud storage, increasing storage footprint/cost. Keep in mind that when we talk about cloud in this case we're not talking about SaaS services, but predominantly object storage, like AWS S3, Azure and similar. Customers need to manage this storage including access controls and proper security configurations, as well as negotiate their own contracts with their chosen cloud provider.

A note on deduplication and its impact on storage costs:

The most significant cost impact to storage efficiency is how deduplication is optimized for backups. In the Veeam world, best practice standard is per VM type storage which means deduplication is local to each server backed up, this narrow scope of deduplication equates to storage inefficiencies that get amplified downstream into secondary storage. If secondary storage is cloud this equates to much higher cloud costs over time, especially for organizations with long retention schedules[4].

---

[2] Veeam Backup Repository Design, Veeam Documentation.
[3] Based on architecture design proposed by a Veeam certified solutions architect.
[4] Veeam Backup and Replication 12, Veeam Documentation.

Solutions Management (14% of Total Cost):

For midsize organizations as scoped in the evaluation, this is an area that can't be trivialized. Depending on available personnel resources and training, administering an on-prem backup solution like Veeam needs to be factored into the overall cost model. Multiple administrative duties must be undertaken, including:

Solutions Management	
Initial, and ongoing setup and configuration	This includes secondary-site configuration, infrastructure modifications, networking, storage setup, and ongoing adaptation/expansion of environment/services.
Management of Multiple Backup Services	No unified management console spanning all services. Requires hardware and setup configuration, as well as regular independent service management.

Storage Management	You're fully in control of storage provisioning, access, security, and ongoing administration on-premises and in the cloud. However, this could easily become untenable and result in unnecessary storage costs and security issues. Organizations need to consider:
	
	• **On-premises capacity management:**
	  Ensure proper sizing of storage, provisioning, and maintenance.
	• **Cloud storage:**
	  Managing capacity, utilization, access controls, and security of the data.

Software updating, patches, and hotfix administration	Organizations need to ensure they stay on top of updates and patches. Depending on environment size and resources, this could be a small or extensive burden.

Security Cost Considerations (4% of Total Cost):

Backups are the last stronghold of the company jewels of information; financial data, IP, legal documents, and more, all in one place. That data being compromised, or deleted in the case of advanced ransomware attacks, poses a significant security risk to businesses – often costing millions, or the business entirely. For example, one construction company learned the hard way with their Veeam environment.

To properly secure a backup environment, at a minimum, anti-malware/virus, and security operations management must be included. Customers must also include the time and effort required to manage these components, as part of a complete cost picture. As well, other elements to consider in total cost include:

- **Air-gapped backup copies:**
  Veeam is dependent on 3rd party storage to provide immutability, which is a requirement to address today's constantly under siege environments from security risks. Usually cloud-based, organizations need to take extra precautions to ensure a secure data environment that delivers an air-gapped and immutable configuration.

- **Vulnerability assessments and recovery testing:**
  Ensuring on-prem backup environments are well insulated from threats goes beyond just the security software, it's recommended that regular security audits and testing are conducted as well.

- **Continuous monitoring:**
  Given that backup environments are often targeted by ransomware, backup environment monitoring plays an important role to ensure fast response in case of a cyber attack.

Why Druva SaaS Data Protection Leads the Way in Cost Effectiveness

SaaS data protection for VMware and server-based workloads have had a unique advantage in the last decade. Specifically, the ability to take advantage of continuous technology advancements and deployments: serverless, object storage, security hardening and monitoring, networking, multi-region protection, and more have out-paced mostly 'frozen' on-premises environments. Druva was the first native SaaS data protection solution to come to market, enabling customers to receive the benefits of these technology advances, both in cost and

utility, without having to update their infrastructure. These types of service benefits are reflected by the number of organizations that have already deployed SaaS applications.

- Among the top drivers of overall cloud adoption are security and data protection (37%), data modernization (22%), and the cost and performance of IT operations (15%).[5]

The Druva SaaS Advantage

The Druva Data Resiliency Cloud is a 100% SaaS-based data protection platform to manage enterprise data. It scales seamlessly to meet the needs of your business without infrastructure, maintenance, or support costs. Here are five ways Druva's SaaS data protection delivers major benefits:

Modernize for flexibility and scale
Druva eliminates the need to provision resources as it will scale up or down as your business needs evolve.

Refocus IT on managing data
Instead of tasking IT to build and manage legacy backup hardware or software, patching, or security activities, SaaS data protection frees their time and makes it possible for them to focus on higher-value initiatives.

Break free with better time-to-value
Organizations see faster time-to-value with Druva, whether supporting new offices or workloads in the cloud. Better still, anyone in IT can use the solution without special training.

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. 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 anomaly detection across backup data and coordinated incident response activities from one source of data.

Drive savings and reduce costs
In addition to removing hardware and software costs, SaaS pricing is transparent and consumption-based. Since everything is in one place, backup data becomes an asset, allowing you to streamline governance, improve cyber resiliency, and gain critical insights for your business.

"Of course, managing backups for IT in the old days was a significant portion of what you did. That is no longer the case with Druva. All of that hassle is gone, and with it, most of the risk."
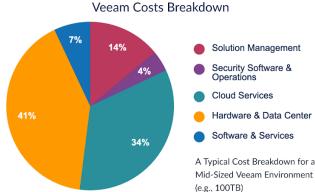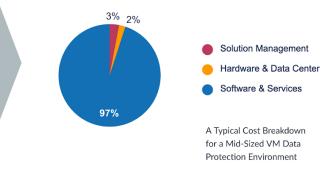
— Gabe DiSarro, CIO

COLDWELL BANKER
PRIME PROPERTIES

---

[5] S. Bennett, "SaaS Backup Statistics 2024 – Everything You Need to Know," Jan. 9, 2024.

The Cost Model When Comparing Druva to Veeam

When evaluating a SaaS backup solution for VM environments, the overall cost model is simpler as there are only two primary cost categories: the monthly expense for the SaaS service and administration costs of the service. The following pie chart represents the same cost allocations for a 100TB environment with 200 VMs, and a standard retention policy (*see the medium environment sizing comparison for a more detailed breakdown*).

Veeam Costs Breakdown

- 14% Solution Management
- 4% Security Software & Operations
- 34% Cloud Services
- 41% Hardware & Data Center
- 7% Software & Services

A Typical Cost Breakdown for a Mid-Sized Veeam Environment (e.g., 100TB)

Druva Costs Breakdown

- 3% Solution Management
- 2% Hardware & Data Center
- 97% Software & Services

A Typical Cost Breakdown for a Mid-Sized VM Data Protection Environment

The table to the right illustrates both hard and soft costs to consider for TCO with an emphasis on the components that you will have to manage (soft costs). Keep in mind the following:

- Data protection solution costs today are typically based on storage consumption required to protect your source data.

- Validate that you're using the same assumption for growth and the backup storage required in all locations (including long-term retention) when evaluating TCO.

- Don't underestimate the soft costs and benefits of one solution versus another. Who is managing the backup servers, storage, and security across locations?

Hard and soft costs	Veeam (Traditional)	Druva (SaaS)
Backup policies	You manage	You manage
Backup SW+server	You manage	Druva manages
Backup storage & deduplication	You manage	Druva manages
Secure, offsite storage	You manage	Druva manages
Long-term retention storage	You manage	Druva manages
Backup security monitoring	You manage	Druva manages
Space, power, cooling	You manage	Druva manages
Direct backup infra. support	You manage	Druva manages
Indirect backup infra. support	You manage	Druva manages

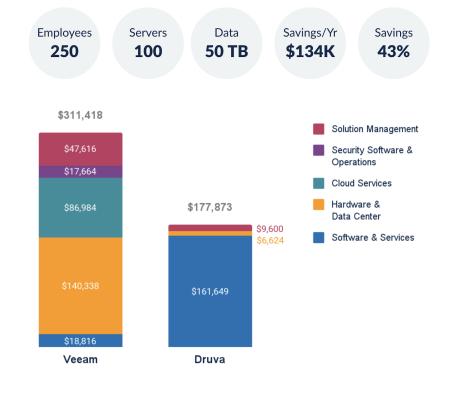## A Close-up View of Veeam (Legacy) vs. Druva (SaaS) Costs

Based on what we covered above, and a clearer understanding of how the cost models differ, we can now dive a level deeper and review comparison tables. The cost comparisons include small (100 VMs, 50TB) and medium (200 VMs, 100TB) backup environments. These environments are derived from hundreds of real-world engagements with mid-sized organizations. Each model also includes an overview of key assumptions that have been used to derive costs. As with all comparisons, an organization's own nuanced environment may have varying cost differences from the models used in the comparisons. That said, one can derive that the cost delta between Druva and Veeam is large enough to subsume those differences.

Cost Comparison Simulations — Snapshot at Year 2 of 3-Year Deployment
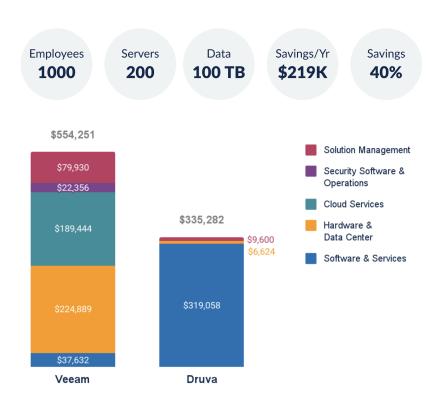
Small environment sizing

50TBs of VMs and Files

Our first example is ABC Company. They employ 250 employees and utilize 100 virtual machines and 50TB of source storage in their primary data center.[6]

Employees	Servers	Data	Savings/Yr	Savings
250	**100**	**50 TB**	**$134K**	**43%**

Veeam — $311,418
- $47,616 (Solution Management)
- $17,664 (Security Software & Operations)
- $86,984 (Cloud Services)
- $140,338 (Hardware & Data Center)
- $18,816 (Software & Services)

Druva — $177,873
- $9,600
- $6,624
- $161,649 (Software & Services)

Legend:
- Solution Management
- Security Software & Operations
- Cloud Services
- Hardware & Data Center
- Software & Services

Medium environment sizing

100TBs of VMs and Files

Our second example is DFE Council. They employ 1000 employees and utilize 200 virtual machines and 100TB of source storage in their primary data center.[7]

Employees	Servers	Data	Savings/Yr	Savings
1000	**200**	**100 TB**	**$219K**	**40%**

Veeam — $554,251
- $79,930 (Solution Management)
- $22,356 (Security Software & Operations)
- $189,444 (Cloud Services)
- $224,889 (Hardware & Data Center)
- $37,632 (Software & Services)

Druva — $335,282
- $9,600
- $6,624
- $319,058 (Software & Services)

Legend:
- Solution Management
- Security Software & Operations
- Cloud Services
- Hardware & Data Center
- Software & Services

---

[6] Druva Cost Comparison Simulations.
[7] Druva Cost Comparison Simulations.

Cost Comparison Assumptions

We have created two example calculations to demonstrate the Total Cost of Ownership (TCO) of a legacy backup solution done to best practice vs. a best-in-class, true SaaS platform.

To ensure an apples-to-apples evaluation of Veeam and SaaS costs, we use the following assumptions:

- Industry **3-2-1 best practice guidelines,** which provide a template for the required infrastructure, deployment, and ongoing management costs:

    - 3 copies of your data, stored on 2 different media types, and 1 copy off-site
    - At least one copy air-gapped and immutable
    - End-to-end encryption

- Security best practice elements as recommended by industry experts, governments, and other agencies that address the challenges and risks posed by threats such as ransomware to protect backup environments.

- Environment sizings that match up to common mid-sized business;

    - Small 100 VMs @ 50TB total data footprint
    - Medium 200 VMs @ 100TB total data footprint

- A standard retention policy is followed for nightly backups

    - 30 dailies
    - 4 weeklies
    - 12 monthlies
    - 3 yearlies

- An expected Recovery Point Objective (RPO) of 24 hours and Recovery Time Objective (RTO) of 4 hours for non-cyber related incidents.

- Assumed hardware/software cost model over a 3-year term.

Conclusion: Look at all the costs

As can be seen from reviewing this paper and the cost comparisons, Druva's SaaS backup clearly comes out the winner, not only in the enterprise-scale breadth of capabilities it provides, but also at attractive price points for mid-sized businesses. In each of these models, SaaS has an overwhelming cost advantage, especially for organizations assessing their first backup deployment or looking to reduce their data center footprint.

Another great advantage of Druva is it's easy to get started and try out for free to see if it aligns with your needs.

To learn more, get a free trial of the Druva platform and see for yourself.

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 is the industry's leading SaaS platform for data resiliency, and the only vendor to ensure data protection across the most common data risks backed by a $10 million guarantee. Druva's innovative approach to backup and recovery has transformed how data is secured, protected and utilized by thousands of enterprises. The Druva Data Resiliency Cloud eliminates the need for costly hardware, software, and services through a simple, and agile cloud-native architecture that delivers unmatched security, availability and scale. Visit druva.com and follow us on LinkedIn, Twitter, and Facebook.