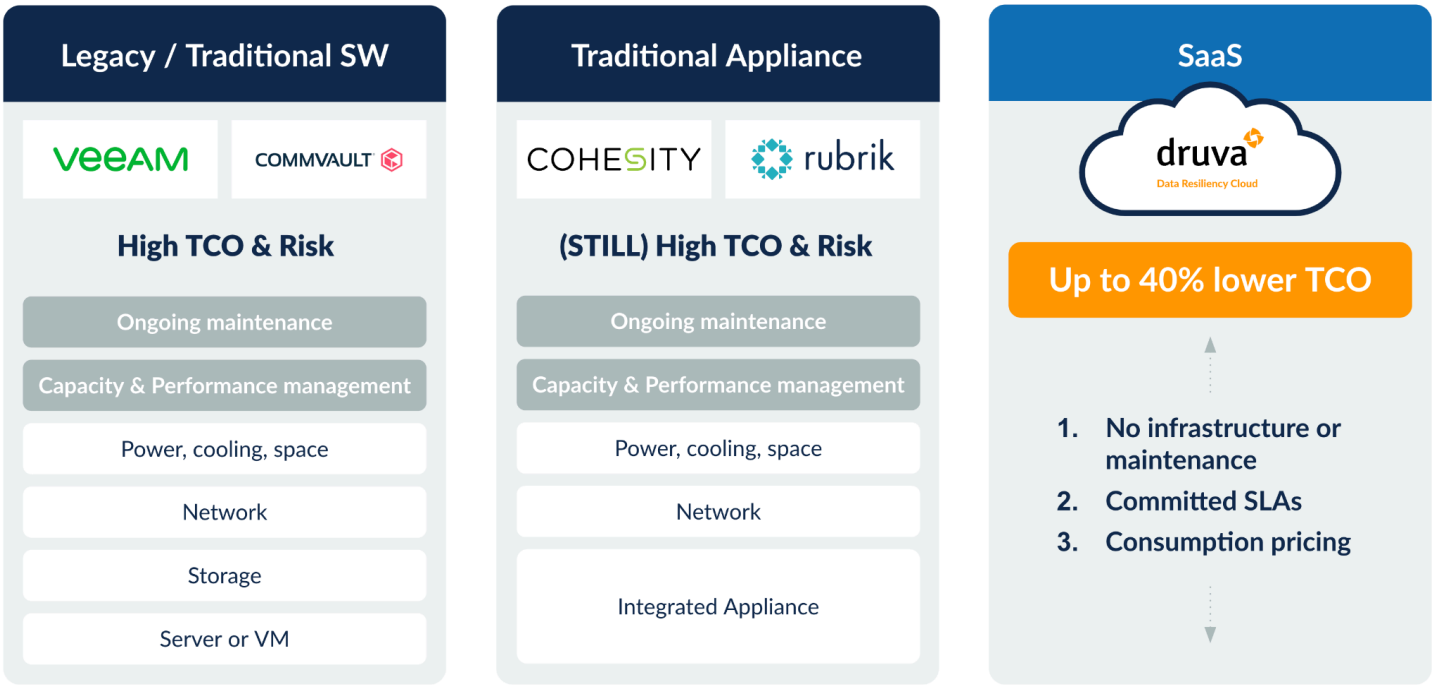
# You Deserve Better Than Legacy

Data Protection Should Work for You, Not the Other Way Around

Over the last decade, customers have experienced a continental shift in their data landscape. Today, customers are protecting more data sources, in more global locations, and face a greater financial impact when data loss occurs than ever before. As a result, customers are looking for solutions to protect their diverse workloads, while also seeking to simplify their overall data protection strategy. Unfortunately, traditional data protection solutions have lagged behind the simplification trend and rely on a customer "Do It Yourself" (DIY) model for infrastructure planning, purchasing, management, maintenance, and hardening. The result? More complexity, not less.

At the same time, in the current economic backdrop, customers are prioritizing reducing total cost of ownership (TCO) as a critical value driver for long-term business viability. And as with production applications, customers understand that price doesn't equal cost when it comes to data protection. Legacy costs include on-premises hardware, software, management, and data center power, cooling, and floorspace, and represent a much larger financial commitment than cloud-native alternatives. Again, legacy solutions trend in the wrong direction — higher TCO, not lower.

Finally, customers are pursuing new data security and protection strategies in the wake of high-profile cyberattacks, especially with sophisticated ransomware groups targeting backup environments. Customers often discover too late that they lack visibility into attacks occurring inside their environment and are not prepared or equipped to execute a recovery. In some cases, legacy's negative publicity on ransomware results from its complex architecture requiring customers to take the same DIY approach to security as they do to infrastructure — source, build, manage, and ensure ongoing vulnerability updates and patching.[1]




[1] Veeam Backup & Replication 12 User Guide

## What Do Customers Get with Legacy Solutions?

### Higher TCO… Every. Time.

The DIY nature of legacy solutions means the cost of data protection is spread across many different categories - most of which go beyond the standard list price (such as maintenance time and effort). In some cases, customers manage over seven different vendor products to satisfy solution requirements, each of which requires their own licensing structures, contract lengths, training and expertise, and future planning. For example, legacy relies on third-party products to fill gaps across workloads - including deduplication, storage tiering, and security.

Additionally, the fragmented nature of the solution requires separate products and deployments to backup on-premises, cloud, and SaaS workloads, leading to further operational complexity. What's worse? Securing all of these components end-to-end across various locations leads to even higher costs and burden of responsibility.

Ultimately, this hands-on approach results in a cost multiplier across workloads, capabilities, locations, and management that can become cost-prohibitive as the environment grows.

### Ransomware Groups' Favorite Target is Legacy Infrastructure

The DIY approach is just one of the security challenges legacy customers face. Additional security issues exist and will persist over time with legacy Windows-based framework — popular among hackers seeking vulnerabilities. Security with legacy is "secure-by-implementation" and is dependent on the user's diligence in knowing, implementing, and continuously maintaining security best practices. This responsibility includes air-gapping the backup infrastructure, ensuring immutability, and continuous monitoring of the environment that relies on third-party involvement.

### DIY = Management Headaches

Focusing on solution management, the DIY approach coupled with legacy architecture can create significant complexity for administrators, starting with the presence of multiple user interfaces tailored for data center, cloud, and SaaS environments. Each of these interfaces operates independently, with distinct consoles, policies, development cycles, and associated learning curves. The separation of Edge and SaaS backups (e.g., end-user data lives on both endpoints and M365) compounds these issues as shown in the lack of consistent federated search, legal hold, or eDiscovery across these distinct realms. The static nature of legacy's license approach places the responsibility of planning for future growth squarely on the user, with the risk of overprovisioning both SW and HW, leading to unexpected costs. All in all, these complexity challenges pose a considerable barrier for organizations seeking a streamlined and efficient data protection experience.

## The Solution

Druva's fully managed, 100% SaaS approach effectively removes the challenges that plague DIY backup solutions. Everything customers need to protect and secure their data is included on day one — storage, compute, software, and security. With just one platform, organizations protect all workloads and rest easy knowing the solution is fully maintained, security-hardened, and ready with the latest features and capabilities. Best of all, SaaS delivers the lowest possible TCO and ongoing cost predictability by a wide margin. Finally, a data protection solution that works for you, and not the other way around.

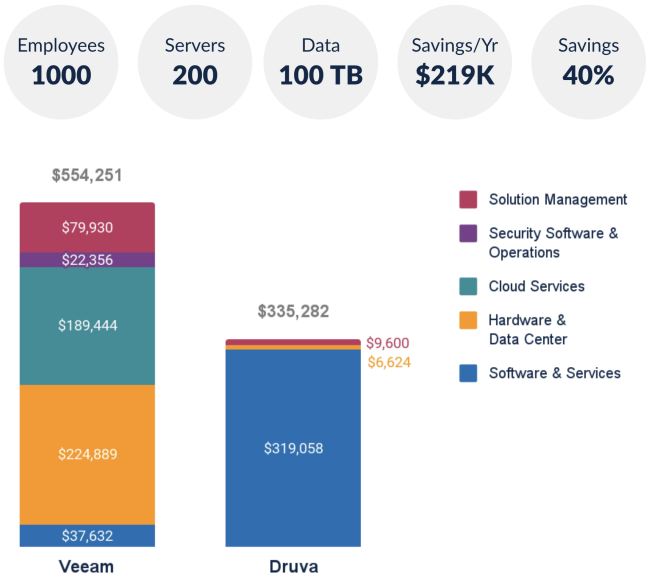
## You Deserve More For Your Data

### With Druva, Save up to 40% or More

The hands-off nature of SaaS sets Druva apart, as it is fully managed, maintained, and monitored to ensure implementation of up-to-date features without any user intervention. A single cloud-native UI seamlessly covers on-premises, cloud, edge, and SaaS environments, eliminating the need for additional deployments and associated costs.

Druva's efficiency shines with built-in global deduplication and storage tiering, optimizing capacity and reducing storage costs. Moreover, its transparent pricing model ensures predictability and flexibility, allowing organizations to pay only for the resources they actually use. In total, Druva's cost-effective, streamlined, and

efficient data protection allows customers to save up to 40% vs. traditional on-prem solutions.




*Example cost comparison for a medium-sized deployment*

## Stay Out of the Ransomware Headlines

Built on robust AWS infrastructure, FedRAMP-certified, and compliant with the strictest regulations, Druva takes a “secure-by-design” approach, fully managing and hardening security with 24/7 continuous monitoring by expert security professionals. Druva is committed to protecting the entire backup infrastructure, not just storage, and employs a fully air-gapped and immutable system with dual-envelope encryption. This proactive stance is evident in the included Managed Detection and Response (MDR) for backup service which offers immediate human alerting at no extra cost.
Always-available backups, backed by guaranteed SLAs for recoverability, and the deployment of three copies of data with separated and air-gapped control and data planes provide a robust defense against potential threats.
Finally, Druva includes important capabilities to assist in recovery: 1) a Sandbox Recovery feature to enable customers to scan their environment and restore to a specific point, and 2) Curated Recovery to reduce data loss by sourcing clean files from numerous snapshots into a single “golden snapshot."

## Break Up With DIY Infrastructure for Good

Druva redefines simplicity in backup and recovery with a seamless and hassle-free experience allowing customers to "set it and forget it." A unified view of both corporate and end-user data features federated search, compliance, and legal hold capabilities for the latter, allowing organizations to manage data confidently from anywhere in the world. The elastic nature of Druva ensures transparent scalability of storage and performance as your environment grows, all without additional costs or surprises. Druva's commitment to a rapid time-to-value is evident through free trials and SaaS simplicity, enabling users to explore protecting any workload on-demand, at no additional cost, and with self-service ease.

## Spotlight on Customer Success

**Pyrotek** — Compared to previous solutions, the team achieved 30% time savings on managing backups, 3X global deduplication savings, and 20% TCO savings — including hardware and software maintenance costs. Learn more in the case study.

**Greater Anglia** — After switching to Druva, the Greater Anglia team reduced the amount of time spent managing backups by 70% over their previous legacy solutions, and found restores now take place 100X faster. Learn more in the case study.

## Learn more

Modernize Your Data Protection with Druva


Demo: Dru AI Remedies Backup Errors

Optimize Your Ransomware Recovery Solution