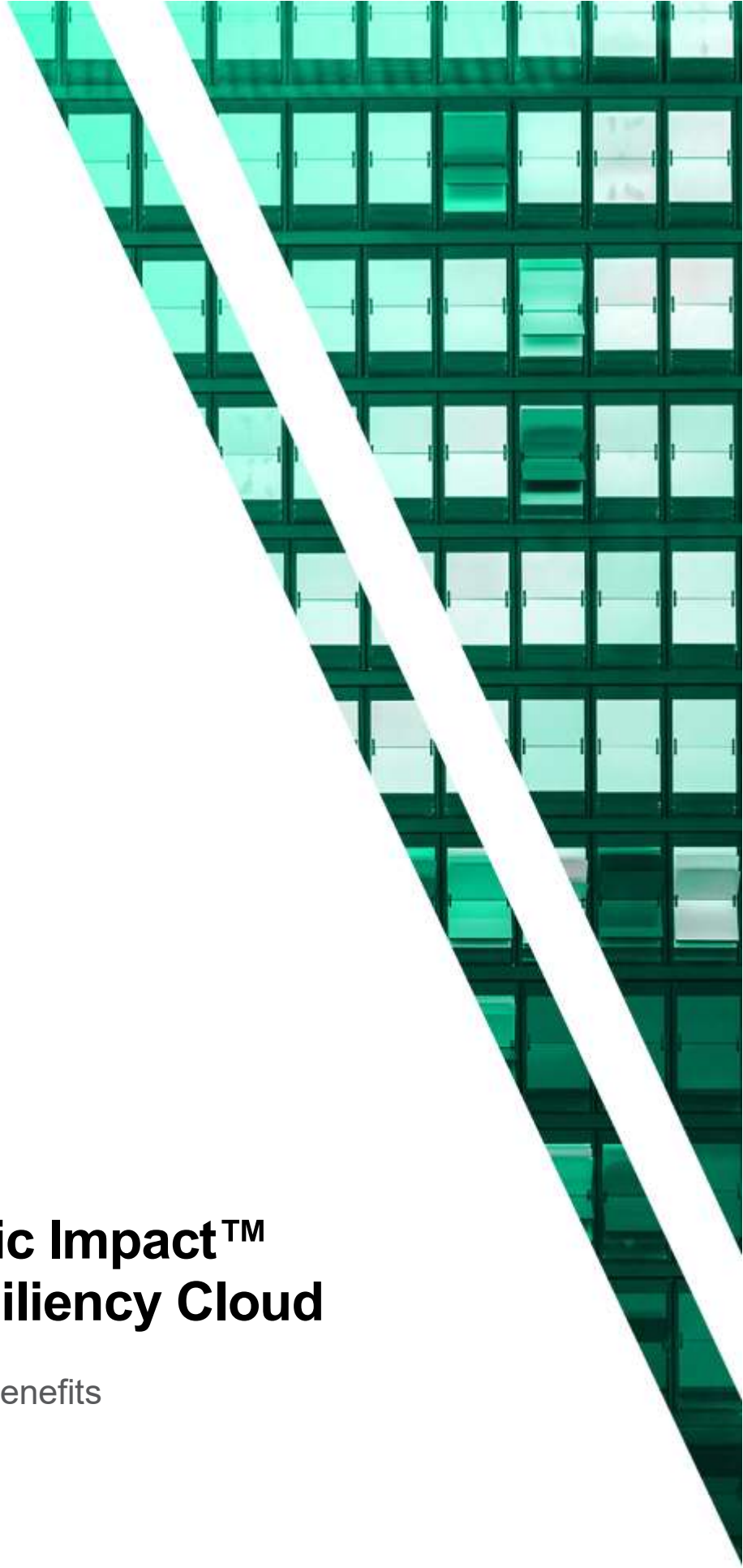
FORRESTER®



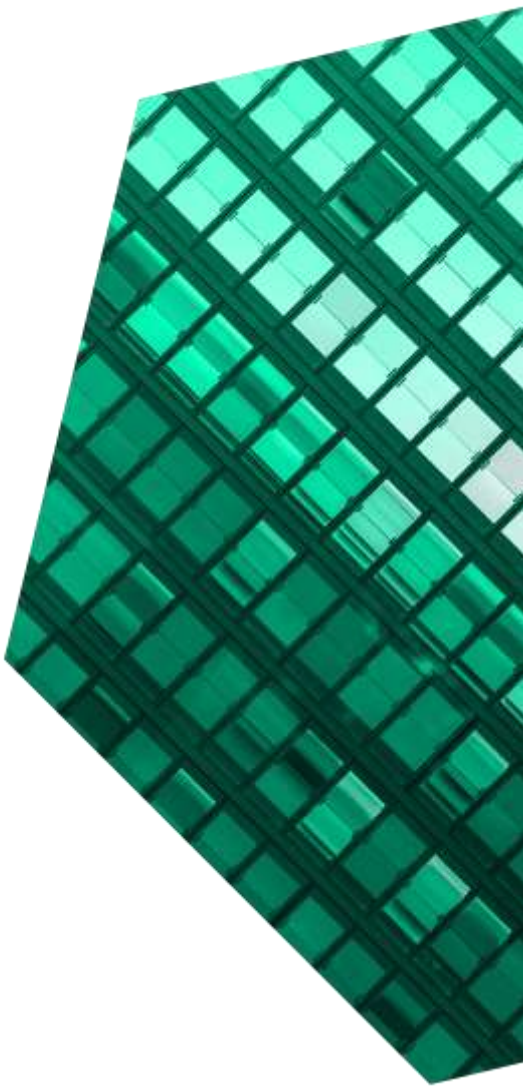
The Total Economic Impact™ Of Druva Data Resiliency Cloud

Cost Savings And Business Benefits Enabled By Druva

February 2022

Table Of Contents

Consulting Team: Courtenay O'Connor
Sean Owens



Executive Summary

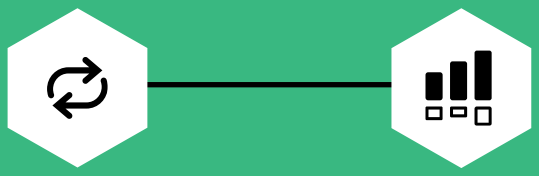
Data integrity poses the top high-impact systemic risk of this decade.[1] Firms struggle to protect complete and accurate copies of critical datasets and continually monitor complex, distributed technology infrastructures. Facing massive growth in data and the specter of ransomware and other breaches, firms must expand and shield their backup and recovery environments. In this context, the cloud poses a potential refuge and opportunity for new capabilities in data resiliency and integrity.

The Druva Data Resiliency Cloud offers a secure, cloud-native backup-as-a-service platform built on Amazon Web Services (AWS). It provides a consolidated data repository for all backup data from data centers, cloud workloads, and endpoints. Druva's hybrid workload service supports data center infrastructure and applications while also offering data protection for public, cloud-native workloads. Druva offers coverage for traditional data centers, virtualized infrastructure, public cloud hosted services, and software as a service (SaaS).

Druva commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Druva.[2] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Druva on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four decision-makers with experience using Druva. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. Resembling the interviewees' experience, the composite organization is a global manufacturing and logistics organization; it backs up 150 terabytes (TB) of source data in Druva, with a 15% annual data growth rate.

KEY STATISTICS



Return on investment (ROI)
253%

Net present value (NPV)
$1.20M

Prior to using Druva, the interviewed decision-makers noted how their organizations had difficulty responding to the shifting data landscape, with changes in business applications and needs, regulatory data requirements, and attack vectors. Their production sites and remote offices were hindered by siloed business units backing up their disparate environments without centralized standards or tools.

Legacy solutions left interviewees' organizations with legal and compliance challenges; they lacked visibility and control of highly vulnerable data integrity. Mission-critical backup and recovery data sets were at risk of infection when a breach occurred. This level of threat penetration renders them unusable, as in one of the unsuccessful recovery efforts experienced by the interviewed decision-maker for a chemicals manufacturer.

These limitations led to siloed and complex data backup and recovery practices which limit data visibility. A further lack of integration between data protection and disaster recovery strategies meant that interviewees ran the risk that data lost may never be fully recovered.[3] After the investment in Druva, interviewees gained a centralized version of truth, allowing them to deliver more consistent and expedient backup and recovery services across their organizations. Druva's single pane of glass helped them manage the entire corporate environment from the cloud on behalf of the interviewees and their teams.

All interviewees reported similar results in key cost optimizations related to the Druva investment:

- Flexible backup scheduling and retention policies.
- Significant storage reductions from global deduplication and compression technologies.
- Convenient, public cloud-hosted platform.

The interviewee from the chemicals industry further appreciated the billing efficiencies from the investment in Druva, saying: "We only have one contract with Druva. No need to talk with any cloud provider — just with Druva and that's all." As an early entrant into the cloud-native backup and recovery space, interviewed decision-makers described how Druva added to their team and toolset.

Druva's intrinsic and cloud-native cyber-resiliency and daily backup monitoring services freed up interviewees' lean and savvy IT teams. Rather than rote process monitoring and triage, resources were able to further capitalize on the additional insights afforded by Druva's comprehensive analytical dashboard.

All interviewees further noted Druva's attractive storage pricing. With incremental backups, it saves only what has changed since the last backup. Deduplication, compression, and flexible retention options translate to significant cost savings when faced with long-term retention requirements. Customers paid only for what they consumed and did not need to buy additional storage to allow for growth, performance, and surge capacity.

ANATOMY OF A RANSOMWARE ATTACK [3]

According to Forrester Research, ransomware attacks often put the backup infrastructure itself under siege. It's not about just recovering from a backup. The resulting nexus requires infrastructure and operations pros to work closely with their security and risk peers to ensure that they are recovering from an uninfected copy.

The chief information officer in the logistics industry described how their organization implemented Druva to protect the organization's mission-critical backup sets:

"From a ransomware perspective, we've implemented a multifaceted approach. On the proactive side, we have a third-party prevention product; on the reactive side, Druva is the solution if [an attack] does in fact happen. At least we know we can do a backup and a recovery, so we do have some reactive components there if we do get a ransomware attack."

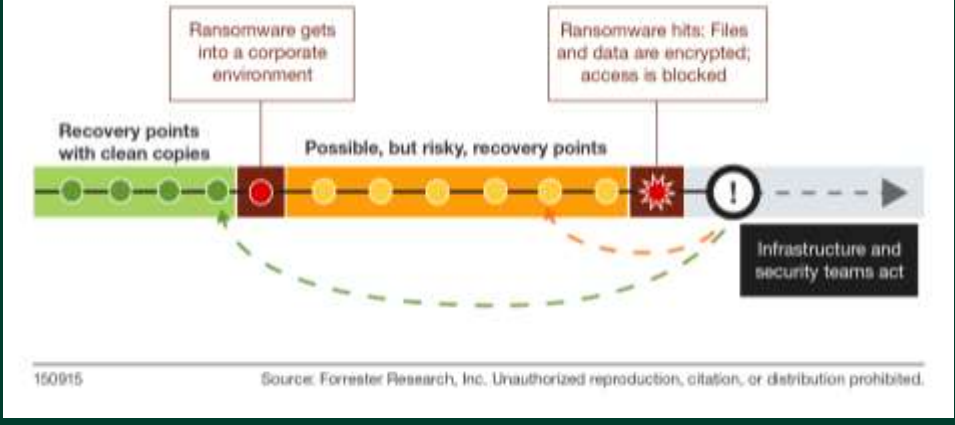


Figure 1: Backup infrastructure is the last and best line of ransomware defense

KEY FINDINGS

Quantified benefits. Risk-adjusted present value (PV) quantified benefits include:

- **Decreased legacy solution and cloud service costs by more than $635,000 over three years.** In addition to the significant cost savings, the shift towards Druva helped to reduce the complexity and vulnerability of their technology stacks, billing and procurement, and physical plant footprint.
- **Permitted a 100% data restore in a fraction of the time when compared to previous solutions.** The flexible scheduling of incremental backups means there is always a full copy of mission-critical data cordoned off from ransomware and other threat events. The system administrator from the chemicals industry reported that previous environments could never achieve 100% like Druva can. For the composite organization, the time savings is noteworthy, decreasing the number of hours required to manage backup and restore from over 2,000 hours to approximately 200 hours.
- **Avoided hours of ransomware remediation by in-house experts.** Ransomware events are top of mind for every IT leader. The ambiguous nature and variable probability of such an event, however, makes them exceedingly difficult to predict. In previous backup and restore environments, the prevailing chaos in the day-to-day backup and restore activities greatly strained IT teams' ability to remediate extraordinary events. Although the total number of hours needed for remediation was hard to measure, interviewees indicated Druva conferred much more simplicity across the entire environment. When applied to the composite organization, these efficiencies translate to savings of approximately 800 remediation hours from more costly technical resources.
- **Averted ransomware and other threat penetration, avoiding untold business losses.** For some interviewees, Druva was implemented as a solution to protect critical backups in the event of a ransomware attack or other breach. Backups can more successfully be restored in the event of ransomware, ensuring the recovery of critical business data.

"The product is very easy to use, which is the real key when you're implementing. If senior management wants to get a file back, they don't want someone struggling to recover that file."

— Chief information officer, logistics services

Unquantified benefits. Benefits that are not quantified for this study include:

- **Agility and compliance.** Druva offered the interviewed decision-makers' organizations the ability to restore backup instances quickly and flexibly to different environments across varying geographies. This supported entry into new markets and ensured that data retention and privacy policies were aligned with country-level limitations on data storage and transfer.
- **Remote, virtualized management of data environment.** At the onset of the COVID-19 global pandemic in 2020, interviewees were relieved to have a data security solution that could also ensure the health and safety of IT staff while preventing significant business disruptions. Interviewees with physical data environments were grateful to conduct their essential backup and recovery processes from anywhere while their staff remained safe from COVID-19.
- **Cloud-native, cyber-resilient architecture.** By design, Druva's cloud-native infrastructure provided a more secure data environment than interviewee's prior solutions; however, it was not a security cure-all for organizations. While it was a part of a broader cyber-resiliency strategy for all interviewees, Druva specifically served them as a reactive solution that keeps threat events from destabilizing critical back-up infrastructure and overall integrity and viability. Furthermore, it has several security features built into the already fortified environment.

Costs. Risk-adjusted PV costs include:

- **Backup service subscription fees.** Over three years, the composite organization pays $406,000 for Druva's subscription fee for their backup and recovery-as-a-service solution. This fee is primarily based on storage consumed after deduplication; dedupe rates can vary based on the type of data and the daily change rate.[4]
- **Implementation costs.** The composite organization's implementation costs were derived from the number of IT resource hours required to navigate the data onboarding and tagging process. Typically, these will be experienced resources like cloud architects and managers. The composite organization spends $30,000 of internal resource hours to deploy Druva.
- **Management and administrative costs.** Management of Druva costs the composite organization $39,000 of internal resource hours to administer the solution on an annual basis. This internal cost encompasses the number of resources needed to ensure regular backup is properly administered and ongoing management and monitoring of the system.

The decision-maker interviews and financial analysis found that a composite organization experiences benefits of $1.68 million over three years versus costs of $475,000, adding up to a net present value (NPV) of $1.20 million and an ROI of 253%.

DRUVA'S INTRINSIC CLOUD RESILIENCY AND DATA INTEGRITY

Protects SaaS applications previously outside of the main data environment.

Secure, single sign-on mode of entry, noted by the cloud systems administrator at the utility company as safer than environments with legacy sign-in methods.

Full backups stored offline and in the cloud with continuous incremental backups

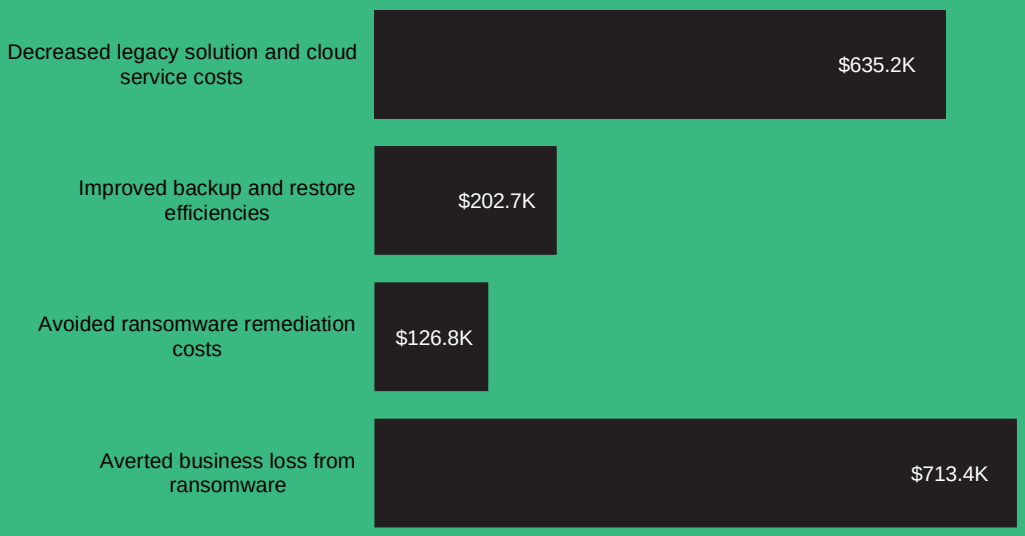
Third-party validations, credentials, and certifications ensure broad-ranging data compliance and integrity

ROI
253%

BENEFITS PV
$1.68M

NPV
$1.20M

Benefits (Three-Year)



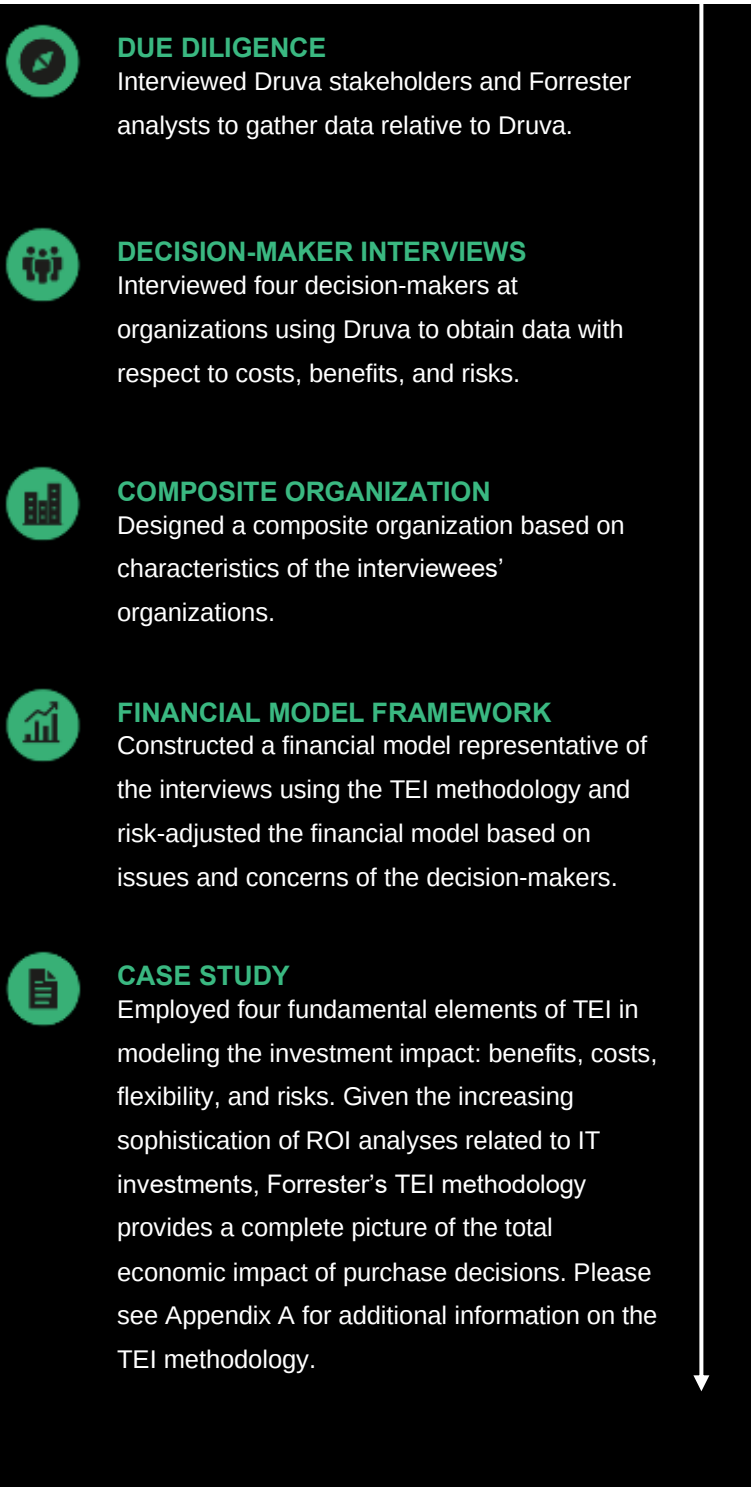
“We are much more protected now with Druva. We are fully protected from ransomware attacks, crypto viruses, and infection, which can totally destroy backup sets in our local data centers.”

— System administrator, Chemical manufacturer

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Druva.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that Druva can have on an organization.



The Druva Customer Journey

Drivers leading to the Druva investment

Interviewed Decision-Makers

Interviewee	Industry	Region	Revenue	Data in Druva
Technical architect	Industrial goods manufacturer	Global, with Europe and United States headquarters	US$300 billion	100 to 300 TB
Cloud infrastructure services leader	Utility	Northeast United States utility division of global organization	US$1.1 billion	100 to 300 TB
System administrator	Chemical manufacturer	MEA and Europe division of global organization with Europe headquarters	€20 billion	100 to 300 TB
Chief information officer	Logistics services	Australia	A$100 million	Less than 100 TB

KEY CHALLENGES

Like most enterprises today, interviewees came from distributed organizations with their business applications — and by extension, their data — spread across multiple data centers that were on-premises, at managed data centers, and in the cloud. Although interviewees' data environments and industries varied broadly, they discussed many common challenges characteristic to their backup and recovery processes. IT environments were internally heterogeneous, with:

- Up to dozens of globally distributed remote offices or business units.
- Manual on-premises and hyperconverged cloud data storage processes.
- A variety of backup software solutions.

The shifting data landscape has introduced changes in regulatory data requirements and attack vectors, resulting in a lack of data visibility that can make management, governance, and recovery more difficult, if not impossible. Interviewees noted how their organizations struggled with common challenges, including:

- **Sprawling, opaque, expensive legacy architecture.** Before implementing Druva as their backup-as-a-service solution, the organizations had developed a sprawling and disparate backup architecture over time that caused a lack of clarity and visibility. This rendered it impossible to even develop a single version of truth, let alone coordinate around it. Visibility, however, is an essential precondition for both cost optimization and for safeguarding a resilient backup and recovery process from threat events.
- **Expensive and inefficient data storage options.** Interviewees also needed additional server hardware and storage space to accommodate expected periods of high activity and anticipated growth. As a result, this forced organizations to stake out more data storage than they immediately needed.
  Additionally, with their distributed backup environments, many departments overlapped with what data they backed up, meaning more backup time and storage used than needed. Central operations teams had little visibility into this.

Customer Pain Points

The technical architect for the industrial goods manufacturer said that departmental backups led to a **"Shadow IT,"** with staff hiding data to stop corporate IT from maintaining control and applying a few rules.

The cloud infrastructure services leader for the utility highlighted **disparities in backups**. No centrally managed retention policy, tooling, or guidelines were being followed. They lacked visibility into backup status, and superfluous backups created extra costs.

The system administrator for the chemical manufacturer reported **their organization had suffered from crypto viruses** as on-prem backup storage was not protected. All backup sets were infected, and because backups may have failed or had not been scheduled yet, recovery was never 100%.

A **third-party vendor** for the logistics services company had been hit by a ransomware attack, resulting in a three-week business stoppage with sales delayed until reopening. The logistics services company (and many other businesses using the same vendor) was offline for three weeks and spent 15 developer days (including weekends) to remediate.

- **Many versions of truth**. When individual departments or divisions managed their own backups, organizations lacked a single, complete version of truth related to their backups. Those companies ended up duplicating entire backup systems, complete with extra servers, storage, and personnel. This duplication of cost was doubly dangerous at the point of recovery where it was not clear which group was responsible for data being backed up in multiple systems, and which version of the data is best to restore. Furthermore, representatives at interviewed organizations highlighted how inefficient and vulnerable their backup and recovery infrastructure and processes were. Traditional tape backups had high failure rates with long turnaround times to get tapes to secure backup locations or back to the IT team for recovery. Individual department backup policies did not follow consistent standards, leaving some departments more exposed to mistakes and phishing or ransomware attacks.
- **Unnecessary vulnerabilities**. While the decision-makers' organizations might have considered their hyperconverged cloud-protected data more secure than their on-premises physical backups, this actually led to more exposure. Existing cloud-based backup and recovery options were offered by traditional or hyperconverged vendors and service providers. This meant they were required to add additional equipment and processes to conduct backups, store physical backup media (usually tape), and recover data from storage when needed. Every step of this approach opened an organization up to further vulnerability from threat actors due to the various staging servers, production servers, and network connections.

SOLUTION REQUIREMENTS

All interviewees shared the same, primary solution requirement: a cloud-native system built for, and on, an accessible and resilient public cloud. As demonstrated in Figure 2, Forrester identifies five sources of data that can be protected via one or a combination of four key backup use cases. At the time of investment, Druva was the only back-up-as-a-service solution built for the cloud. Interviewees understood this positioning, which would allow them to optimize multiple objectives to harvest maximum protection and efficiency from Druva at a minimum cost.

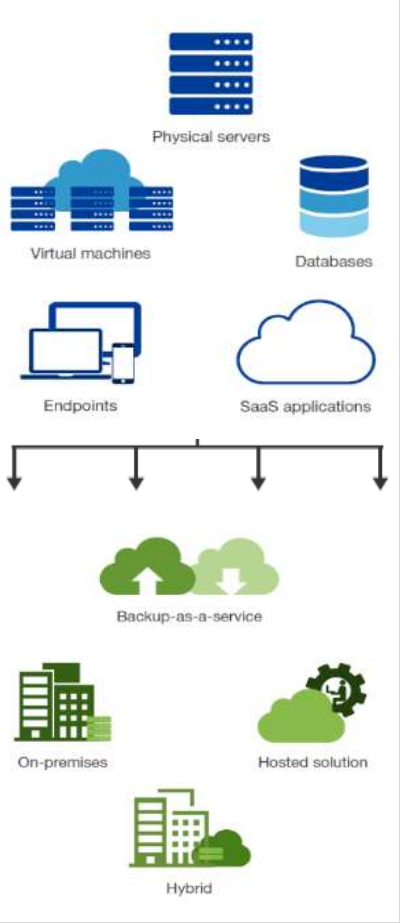
Additional investment objectives included gaining the ability to:

- **Centralize data in the cloud**. All interviewees cited moving their backup infrastructure to the cloud as their main business objective. Their already-lean teams were thinly distributed for constant coverage of their global remit. Interviewees wanted the ability to bring backup management control into central IT operations and monitor their data all from the cloud.
- **Respond to their organization's specific and granular needs**. Interviewees were drawn to Druva's first-to-market, cloud-native data resiliency solution for several reasons. Multiple interviewees discussed the excellent customer service they would have missed with prior vendors. Druva's responsive product development processes helped them shape the Druva roadmap to align with their specific use cases and allowed the customer to have greater influence on Druva's product strategy.

Customer Resiliency Goals

As part of its organization-wide security and retention updates and best practices, interviewees had varying data resiliency goals, ranging from moving completely to the cloud and eliminating all data centers, to moving from fully on-premises to a hybrid SaaS model.

Figure 2. Sources and Backup options for enterprises span technologies and locations



COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four decision-makers that Forrester interviewed and is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The global commodities manufacturing and logistics organization is headquartered in the United States with global operations. With annual revenue of $1.5 billion, it is enmeshed in a global goods chain with multiple vendor and ecosystem partners. Due to the sensitive nature of its product, it is deemed as an essential service. It must continue operations at production sites during the global COVID-19 pandemic and is sensitive to geopolitical factors which may limit in-country networking abilities.

Deployment characteristics. The composite organization has multiple country-level productions and operational sites, business units, and remote offices (ROBOs) serving 5,000 total employees. It wants to transition from a fully on-premises backup and recovery configuration to a hybrid infrastructure model. Its deployment of Druva includes protection solutions for hybrid workloads, SaaS applications, as well as physical and virtual servers, databases (on premises and in the cloud), and NAS storage; this analysis does not include endpoint protection. The composite has an IT team of seven, with three resources spending a portion of their day on regular backup and recovery administration. Druva stores 150 TB of the composite's critical source data. The majority is stored in VM snapshots but includes unstructured data (files/NAS) and databases as well.

Key assumptions

- **$1.5B revenue**
- **5,000 total employees**
- **15% data growth rate**

Customer Voices

"Four years ago, not many of the main players were doing a cloned backup technology the way Druva [did when it] went cloud native. At that moment, other providers were pivoting to replicate their existing physical technologies in bits and pieces to take the whole thing to the cloud.

The other offerings available were not managed services. They felt heavy and would require a lot more user direction from us to manage it. [Competitors] were just offering a cloud location that we could backup to; we would still have had to manage all our data in the cloud ourselves with those other offerings.

It was too early for most people, no one was anywhere near ready to do what we wanted to do with Druva."

Technical architect, industrial goods manufacturer

Analysis Of Benefits

Quantified benefit data as applied to the composite

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Decreased legacy solution and cloud service costs	$204,250	$258,875	$313,500	$776,625	$635,165
Btr	Improved backup and restore efficiencies	$71,440	$81,486	$93,765	$246,691	$202,736
Ctr	Avoided ransomware remediation costs	$51,000	$51,000	$51,000	$153,000	$126,829
Dtr	Averted business loss from ransomware	$286,875	$286,875	$286,875	$860,625	$713,416
	Total benefits (risk-adjusted)	$613,565	$678,236	$745,140	$2,036,941	$1,678,146

DECREASED LEGACY SOLUTION AND CLOUD SERVICE COSTS

Evidence and data. Interviewed decision-makers reported that legacy costs naturally tended to run high because of the chaotic prior environment with significant redundancy and inefficiency. Their experiences with classic on-premises and hybrid storage and backup environments came with myriad expenses. These expenses included data center costs, hardware costs, management, and license fees for purpose-built software. They could also include assorted costs like bandwidth, extra storage held to improve performance, ongoing maintenance, cyber insurance, electricity, and equipment replacement.

Interviewees were also sensitive to the rapidly changing nature of data policies for privacy, retention, and other concerns. They faced significant challenges meeting the current data retention mandates. In addition, the anticipated exponential growth in data meant that interviewees were going to have to back up, replicate, and have the capability to recover ever larger volumes of data. However, given the sheer volume of data generated and stored by organizations today, it's impossible to apply the same degree of protection to all data.[5]

Upon implementing Druva, interviewees experienced significant reductions in their capex and opex line items, which offered interviewees a range of business value.

No longer needing the hardware, the system administrator at the chemical manufacturer was able to decommission an entire data center and the physical hardware it contained. In addition to these legacy savings, Druva's compression and deduplication capabilities further decreased the total amount and cost of data storage.

The interviewee from the chemical manufacturer elaborated, "In the end Druva charged us only for what we used, which was 50% less than with prior solutions where we had to pay for all the data we submitted to them before deduplication and compression."

The chief information officer in the logistics services industry anticipated the closure of his organization's only data center as a result of the shift to Druva's service platform. Several interviewees were decommissioning their prior solutions due to switching to Druva. For some, this translated into significant cost savings.

The system administrator from the chemical manufacturer explained their calculations: “With the other options, we still would have needed a local server. We still would have had to pay a license, and also have our own cloud account. We would have needed a contract with the prior backup service provider as well as a contract with the cloud providers.”

Modeling and assumptions. Avoided legacy solution and cloud service benefits relate to cost savings associated with reducing or retiring on-premises backup hardware, software, and facilities, reduced backup requirements, and optimized cloud service consumption.

Before Druva, the composite organization shouldered costs such as:

- Maintaining, upgrading, and replacing legacy hardware such as manual tape drives and other hardware expenditures.
- Paying for costs related to utilities and other physical plant expenses for data centers and off-site storage sites.
- Purchasing upgrades and ensuring maintenance of software other platform service costs.
- Paying for legacy cloud platform service provider backup services.
- Paying for additional cloud consumption when backing up uncompressed data to cloud services.
- Addressing additional hidden costs related to performance, growth, and resiliency.

By switching to Druva, the composite organization saves capex and opex costs from legacy or decommissioned hardware, software, and/or services expenses. Decoupled from the legacy environment, costs related to ongoing incremental backup instances are drastically reduced.

Risks. Forrester recognizes that these results may not be representative of all experiences and the cost will vary depending on very specific needs of an organization.

Organizations must examine which architecture suits their data backup needs, how much data center space backups are using; how mature their previous processes were; and whether their business case will even permit a full digital transformation. To rationalize their tech stack, they should further examine how much data center space, hardware, etc. they can decommission.

For example, some may not be able to fully transition to the cloud if retention of data or recovery time objective (RTO) exceeds capabilities of Druva’s local cache feature (CloudCache).

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of over $635,000.

Decreased Legacy Solution And Cloud Service Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Avoided legacy hardware, data center, and offsite storage costs	Research	$100,000	$125,000	$150,000
A2	Decreased software, maintenance, and other services costs	Interviews	$75,000	$100,000	$125,000
A3	Savings from cloud backup services	Interviews	$15,000	$17,500	$20,000
A4	Savings from optimized cloud consumption	Interviews	$25,000	$30,000	$35,000
At	Decreased legacy solution and cloud service costs	A1+A2+A3+A4	$215,000	$272,500	$330,000
	Risk adjustment	↓5%			
Atr	Decreased legacy solution and cloud service costs (risk-adjusted)		$204,250	$258,875	$313,500
	Three-year total: $776,625		**Three-year present value: $635,165**		

IMPROVED BACKUP AND RESTORE EFFICIENCIES

Evidence and data. Recognizing that no single data protection solution will meet all enterprise data security needs, organizations deployed Druva's backup-as-a-service solution as part of a broader security and resilience strategy.

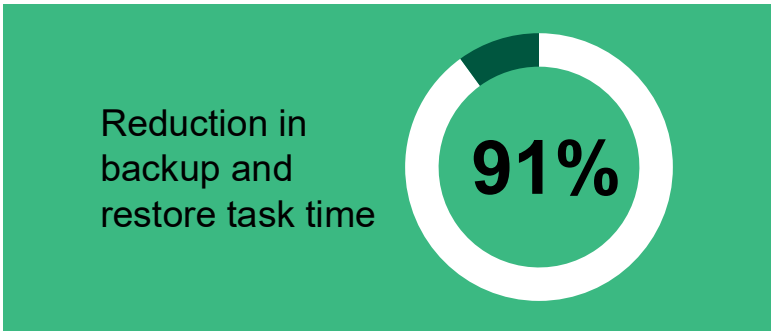
Backup processes included administration and maintenance of backup servers.

Restore processes were more labor-intensive and required security teams to:

- Find the correct backup locations. These might have been offsite and would then require even more time to request and wait for the media to arrive.
- Diagnose the extent of the breach, including checking on the viability of recovery datasets.
- Scan and sanitize the data the environment.
- Work through restore and recovery confusion from multiple copies of data. This caused delays in restores and sometimes reinitiating a restore upon client verification of the data.
- Reestablish a Zero Trust data integrity model.

After Druva, interviewees reported significant efficiencies for both regular backup processes and high-pressure restores following a disaster or threat event. It allowed them to expeditiously react and resolve recovery events at a greatly enhanced level of service and consistency. Having a single view of all backup data meant that it was easier to locate data to be restored and ensure that it was the most relevant copy of the data for the client. This was true for both the day-to-day management of backups and occasional restore requests, as well as recovery from threat and breach events. It offered a greatly enhanced level of service and consistency.

This translated to a commensurate, drastic reduction in hours required to troubleshoot and resolve errors, which were cited as a frequent occurrence prior to Druva. Although there is a significant decrease in the time spent on backup and recovery, the staff involved in executing these tasks was never a large team for any of our interviewees. Therefore, interviewees indicated that, while Druva did not impact headcount overall, it did help improve the quality of work and reduce errors.



This backup-as-a-service approach had a significant impact on IT teams, freeing them to address greater challenges. Interviewees described unwieldly prior IT environments and growing pressure on data storage and protection resources. They sought a solution that would actively manage their cloud consumption, check and report on issues with regular backup schedules, and provide flexible and granular retention.

"With Druva, and comparing to the old traditional local backup, we expected to have slow restore performance due to bandwidth and Internet traffic limitations. But in reality the restore was very fast and helped us to quickly recover."
System administrator, chemical manufacturer

Modeling and assumptions. The modeling is calculated as follows:

- A large portion of the composite organization's data stored in Druva aligns with its flexible longer-term data management and retention capabilities. Less critical data that nevertheless must be retained can be pushed to cold storage, whereby recovery will take longer (up to three days) but at significant cost reductions. Although data can still take up to three days to recover (and recovery of more recent data held in warmer storage is much faster), IT staff are able to do so with the push of a button, saving a lot of time dealing with former inadequate policies.
- The composite's prior backup environment required three resources each to spend about 11 hours per week, for a combined total of approximately 1,750 total hours in the first year on backup and recovery tasks.
- Following Druva implementation, the number of hours spent on backup and recovery is drastically reduced to just under 3 hours per week for only two resources in the first year.
- Backup and recovery responsibilities were not dedicated to specialized roles; rather, they were folded into the day-to-day responsibilities of the global IT team of seven. The average fully burdened hourly salary of these resources is $47.

Risks. Forrester recognizes that these results may not be representative of all experiences and the cost will vary depending on the following:

- The overall number of company sites may have an impact on this benefit.
- Long-term data retention requirements can permit cost savings if organizations have a sizeable portion of less-critical data to be retained. Organizations that have more immediate recovery needs for larger or more complex backup sets may experience different cost savings related to those of the composite organization.
- A large portion of the composite organization's data stored in Druva aligns with its flexible long-term data management and retention capabilities. Less critical data that nevertheless must be retained and can be pushed to cold storage, whereby recovery will take longer (up to three days) but at significant cost reductions.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of almost $203,000.

Improved Backup And Restore Efficiencies

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Hours spent before Druva on backup and restore tasks	Interviews	1,750	2,000	2,300
B2	Hours spent today on backup and restore tasks after Druva	Interviews	150	175	200
B3	Fully burdened hourly salary	TEI standard	$47	$47	$47
Bt	Improved backup and restore efficiencies	(B1-B2)*B3	$75,200	$85,775	$98,700
	Risk adjustment	↓5%			
Btr	Improved backup and restore efficiencies (risk-adjusted)		$71,440	$81,486	$93,765
	Three-year total: $246,691			**Three-year present value: $202,736**	

AVOIDED RANSOMWARE REMEDIATION COSTS

Evidence and data. When it comes to backups of mission- or business-critical data, anything less than all data available at any time is unacceptable. A robust data resiliency strategy considers the full spectrum of disasters and threat events.

To proactively address threats, decision-makers' organizations maintained or deployed a combination of various third-party solutions that provided data storage and governance structures for data located in varied compliance markets. This included out-of-the-box protection plans apps and workloads, such as for email and file clients and other best practices.

Even with heightened security, ransomware attacks were still a risk. The decision-makers' organizations were better able to handle a successful ransomware attack with Druva cloud backups that could be segregated for special ransomware protection. Without this step, a ransomware attack could put all data at risk, including backed up data. Remediating a ransomware attack before Druva was much more likely to require additional time on backup recovery steps and recreating unrecoverable data.

Modeling and assumptions. This ransomware scenario investigates the impact of Druva on the composite organization in the event of a ransomware attack. In particular, the event involves a remediation and disaster recovery incident whereby data was recoverable, but, in the prior environment, was costly and labor-intensive to remediate. Assumptions include:

- Before Druva, a successful ransomware attack would require significant remediation time from the composite organization.
- With Druva's secure cloud infrastructure that safely stores regular backups to protect from ransomware, remediation of a successful ransomware attack would take less time, as backups are more likely to be free of ransomware, and recovery is much quicker.
- Forrester estimates that with Druva the composite organization reduces the IT resource time to remediate a successful ransomware attack by an average of 800 hours per year.

Customer Perspective:

For the system administrator in the chemicals industry, Druva offered their organization agility and efficiency in new and distinctive markets. It reduced costly infrastructure in scarcity-driven geographies. Further, Druva helped circumvent geopolitical tensions to preserve data integrity and business continuity.

- "With the old traditional backup, we avoided several costs, including those related to buying a new, physical server, which is really expensive — especially in Middle Eastern and North African countries."
- "The recovery solution even applies to situations of political instability. We work in North Africa and just in recent weeks we had some political issues that triggered networking limitations in-country. Our Druva instance for Tunisia, however, is the same for Egypt, so we took the server from Tunisia and restored it via Druva to an alternate location in Egypt. By doing this, we ensured business continuity despite the surrounding political situation there, as it allowed the users in Tunisia to work with the application that's hosted in Egypt. We were able to get through this while allowing the business to keep working."

- Because of the sensitive, urgent, and high-level nature of major attack events, the composite organization sends higher-skilled resources to lead remediation efforts. They have a fully burdened hourly salary of $75.

Risks. Forrester recognizes that these results may not be representative of all experiences and the cost will vary depending on:

- **Industry targets**. Attacks can vary based on industry targets. Larger and more sensitive industries, such as healthcare and critical infrastructure, will have drastically different threat likelihoods and fallout.
- **Types of data sources**. Some organizations may choose to keep some data in legacy systems, which can limit backups and disaster recovery capabilities.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of almost $127,000.

Avoided Ransomware Remediation Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Annual average reduction in hours spent on ransomware recovery with Druva	Interviews	800	800	800
C2	Fully burdened hourly salary of senior IT employees	TEI standard	$75	$75	$75
Ct	Avoided ransomware remediation costs	C1*C2	$60,000	$60,000	$60,000
	Risk adjustment	↓15%			
Ctr	Avoided ransomware remediation costs (risk-adjusted)		$51,000	$51,000	$51,000
	Three-year total: $153,000		**Three-year present value: $126,829**		

AVERTED BUSINESS LOSS FROM RANSOMWARE

Evidence and data. If an organization suffers a successful ransomware attack, the importance of backups is mission critical. If ransomware spreads to backups, or poor backup processes result in missed backups, data loss as a result of either issue could be drastic. In addition to the avoided ransomware recovery remediation measured in the previous benefit, several of these ransomware consequences can be avoided with proper preparation:

- Needing short-term loans or missing business opportunities.
- Impact on consumer trust and brand.
- Third party audit or investigation costs.
- Other business risks.

Modeling and assumptions. The composite organization is protection from ransomware-related business loss with Druva. The benefit is calculated with the following considerations:

- Research by the Ponemon Institute estimates a 3% overall likelihood of a successful ransomware attack. For the purposes of this analysis, Forrester has conservatively downgraded to 1.5% to reflect the narrower probability of a successful ransomware attack that also results in unrecoverable backups.[6]
- At-risk revenue estimates are derived from both the extrapolated, real-world implications of market disruption as well as the inferred avoided costs of disruptions to business continuity. The interviewee from the logistics company informed this metric, having experienced similar loss when a software partner was compromised.

“We’re a team of engineers, network folks — this isn’t our full focus in our jobs. This is just a piece of it, and we’re able to experience these wins using a tool like Druva ”

— Cloud infrastructure services leader, utility

- Based the Ponemon Institute's research, Forrester assumed that the average business loss at risk from a ransomware attack is $30 million for the composite organization.
- Druva is one part of the composite organization's broader data resiliency and remediation strategy, making remediation much easier once the threat has been stopped and cleaned. This results in a 75% total attribution of avoided business loss to Druva.

Risks. Forrester recognizes that these results may not be representative of all experiences. The results may vary depending on the overall number of company sites.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of over $713,000.

Averted Business Loss From Ransomware

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Risk of loss from a ransomware attack	Ponemon	$30,000,000	$30,000,000	$30,000,000
D2	Average percent likelihood of a successful ransomware attack that also results in unrecoverable backups	Ponemon	1.5%	1.5%	1.5%
D3	Percent of loss from these ransomware attacks avoided with Druva	Composite	75%	75%	75%
Dt	Averted business loss from ransomware	D1*D2*D3	$337,500	$337,500	$337,500
	Risk adjustment	↓15%			
Dtr	Averted business loss from ransomware (risk-adjusted)		$286,875	$286,875	$286,875
	Three-year total: $860,625			**Three-year present value: $713,416**	

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Cloud architecture supported entry into new markets.** Compliance institutions around the world are taking a more active role in shaping the data landscape. Limitations on where data can be stored require multitenant solutions that are interoperable with data regulations within and across global markets. The system administrator for the chemical manufacturer indicated: "Africa is a perfect example of a new market we can enter now that we have Druva. There were some laws regarding critical data — it had to be stored locally and could not get outside the country. After checking with our lawyers, we were able to provide a certification that Druva's AWS data centers in Europe are working according to the GDPR regulations. In the end, we could save data there. It was a help to both the African countries and to the European countries in our organization."
- **Remote management permitted health and safety and business continuity.** The recent years of the COVID-19 pandemic upended the traditional backup structures that interviewees would have had in place if they had not switched to Druva. The system administrator at the chemical manufacturer stressed: "During COVID, Druva really helped us to stay at home and protected. With the old backup, you would need to go into the office. With Druva, those manual steps are eliminated so physical attendance at the office isn't needed anymore."
- **Layers of cyber resiliency offered unprecedented methods of data protection**. Druva's cloud-native infrastructure convers many added levels of resiliency to an organization's overall threat strategy.

Interviewees shared myriad ways Druva's inherently secure platform assuaged their data security concerns should their critical infrastructure ever be hit with a successful ransomware attack.

Its single sign-on mode of entry was more secure than the traditional approach, noted the system administrator at the chemical manufacturer. Further, Druva supports best practices that allow organizations to secure remote backups in separate locations. Interviewees provided additional insights into their redoubled ability to protect the integrity of their organization's data:

- The cloud infrastructure services leader at the utility said, "There's also the ability to copy our databases across accounts and across regions for a little bit more resiliency, all within a single pane of glass."
- The system administrator in chemical manufacturing said: "Druva helped us set up a penetration test, and our team did not find any vulnerability or risk in the Druva environment. I've never seen an application where our cyber team couldn't find any vulnerability."

"We are now centralized, essentially managed and governed through our Druva environment."
Cloud infrastructure services leader, utility

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement Druva and later realize additional uses and business opportunities, including:

- **Cloud disaster recovery**. While similar to ransomware recovery in that it is a major event and data loss is possible, a disaster event is an act of God and much harder to estimate. The reader can use the same benefit calculations as the ransomware remediation and business impact benefits outlined above, but the chance of an event and amount of revenue demanded or recovered will likely be different for each organization.
- **Decommissioning data centers and other hardware.** The divestment of hardware and infrastructure was mentioned by several interviewees as a major benefit. [7]

Flexibility would also be quantified when evaluated as part of a specific project (described in more detail in Appendix A).

Druva: Optimization And Sustainability In Data Centers

Forrester research highlights how sustainability can improve infrastructure optimization: "Across the infrastructure stack, sustainability is synonymous with optimization, and optimization leads to efficiency." [10]

Interviewees reported they have prioritized efforts around tech stack rationalization or backup and recovery tools.

Traditional data storage was tied to data gravity, which mandates that the backup technology be in close physical proximity to the mission-critical data being backed up. As data shifts out of data centers and organizations seek to secure resilient cloud data environments, they may unlock many sustainability-related advantages in the future.

Information technology is already under scrutiny for its growing carbon footprint; it's also becoming the backbone of every industry, and firms are taking notice. Forrester analysis shows a recent 30% to 40% rise in sustainability-related RFP questions from our clients across various industries, with top four as:

1. Scope 1, 2, and 3 emissions and carbon capture.
2. Roadmap and carbon goals.
3. Data center efficiency — power usage effectiveness and water usage effectiveness.
4. Infrastructure operations-specific initiatives.

According to the International Energy Agency (IEA), global data center electricity demand in 2019 was about 200 terawatt-hours (TWh), or around 0.8% of global final electricity demand.

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Backup service subscription fees	$0	$137,500	$165,000	$192,500	$495,000	$405,992
Ftr	Implementation costs	$29,700	$0	$0	$0	$29,700	$29,700
Gtr	Management and administrative costs	$0	$15,840	$15,840	$15,840	$47,520	$39,392
	Total costs (risk-adjusted)	$29,700	$153,340	$180,840	$208,340	$572,220	$475,084

BACKUP SERVICE SUBSCRIPTION FEES

Evidence and data. Interviewees deployed various configurations of the Druva cloud platform's hybrid workload (Phoenix) and native-cloud workload support (CloudRanger).

Interviewees cited two components as the main factors determining the overall subscription fee:

- The number of remote offices or business units with critical data in need of resilient and secure backup.
- The average growth rate across all types of protected data.

"We found Druva to be the best solution — it totally fits our needs, from the financial to the technical side."
System administrator, chemical manufacturer

Modeling and assumptions. Implementation fees are calculated based on the size and composition of the implementation team:

- The composite organization has a mix of data types protected, but most of it is in the form of virtual machines.
- The composite organization is backing up mission-critical data from its headquarters' central data centers as well as several edge devices distributed around the global production environment.
- With Druva, the composite organization pays one flat subscription fee based on the data use cases and forecasts tied to the organizations' data growth rate.
- With an investment objective to simplify the management of their backup and restore processes, interviewees sought a straightforward solution with minimal ongoing maintenance or attention required for it to operate effectively. As such, the composite does not incorporate any additional configurations.
- The composite organization predicts an average year-over-year backup data growth rate of 15%.

Based on the amount of data, data workloads, retention needs, and expected growth, Forrester made Druva licensing assumptions for the composite organization. This includes the use of less expensive long-term storage options for a majority of stored non-critical data. The Druva backup service subscription fees reflect estimates for the composite organization based on those assumptions. Any individual organization should have a full Druva cost configuration discussion while building their own business case.

Risks. Druva's subscription model offers tailored storage solutions for organizations. As such, key drivers for cost assumptions should consider:

- Clear, measurable governance and backup goals.
- Accurate scoping of data aggregation across data center, ROBOs and cloud data sources.
- Maturity of data governance policies.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of about $406,000.

Backup Service Subscription Fees

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Subscription fees	Interviews	$0	$125,000	$150,000	$175,000
Et	Backup service subscription fees	E1	$0	$125,000	$150,000	$175,000
	Risk adjustment	↑10%				
Etr	Backup service subscription fees (risk-adjusted)		$0	$137,500	$165,000	$192,500
	Three-year total: $495,000			**Three-year present value: $405,992**		

IMPLEMENTATION COSTS

Evidence and data. As with the subscription fees, implementation costs are also reliant on the number of data silos integrated under Druva. Furthermore, the configuration of services will have more of an impact on implementation than it will on the ongoing maintenance.

All interviewees described a simple implementation process once their data had been aggregated and governance policies were developed and applied. As the cloud infrastructure services leader in the utility industry said: "Today's implementation is just set it and forget it. It's me and two other people. As we onboard new assets, they are tagged and then picked up by the proscribed backup retention policy."

Once they started deployment, most interviewees took a land-and-expand implementation approach. All interviewees included mission-critical data from headquarters and remote productions sites, with several citing the cost optimization advantages of Druva's Long-Term Retention offering. This allowed them to store data they needed to keep but that wasn't critical to daily operations and could therefore be stored in the further reaches of the cloud.

Modeling and assumptions. The interviewed decision-makers' organizations' before states were often described as the Wild West. For the composite organization's modeling assumptions, Forrester assumed a high level of aggregation and standardization required to consolidate data in the Druva environment.

Implementation is estimated at three months for three FTE working full time.

To support configuration, Forrester included staffing costs at a higher hourly rate, reflecting the higher level of expertise needed at the outset of the Druva engagement.

Risks. The migration process from prior environments into Druva revealed a high level of variability of visibility into existing data. Interviewees were often incorrect by orders of magnitude when estimating the number of remote offices or business units with critical data in need of resilient and secure backup.

Results. To account for these risks, Forrester included staffing costs as a higher hourly rate. To account for the variability in data visibility, this cost upward by 10%, yielding a three-year, risk-adjusted total PV of almost $30,000.

Implementation Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Months for implementation	Interviews	3	0	0	0
F2	Number of people	Interviews	3	0	0	0
F3	Hourly salary (fully burdened)	Composite	$75	$0	$0	$0
F4	Number of hours devoted to implementation	Interviews	40	0	0	0
Ft	Implementation costs	F1*F2*F3*F4	$27,000	$0	$0	$0
	Risk adjustment	↑10%				
Ftr	Implementation costs (risk-adjusted)		$29,700	$0	$0	$0
	Three-year total: $29,700		**Three-year present value: $29,700**			

MANAGEMENT AND ADMINISTRATIVE COSTS

Evidence and data. Interviewees came from technology environments that embraced an early shift to the cloud. As such, their teams generally were made up of tier-one administrators with a growing number of cloud architects involved in the strategic visioning and ongoing management of backup and disaster recovery processes.

Unlike the implementation phase, once calibrated, ongoing maintenance and administration of an organization's Druva subscription needed minimal ongoing management time. It was often deployed in a set-it-and-forget-it approach.

As such, the major lift in structuring the backup and restore environment is far offset by the ease in which it can be maintained on a day-to-day basis.

Modeling and assumptions. Ongoing management and administration costs are calculated based on the size and composition of the implementation team. With Druva, two resources at the composite organization dedicated some time for backup and recovery processes. This amounted to about 8 hours per month per person.

Risks. Forrester recognizes that these results may not be representative of all experiences and the cost will vary depending on the number of ROBOs. Although the total IT team size does not seem significant, the total number of remote offices and distributed staff is a powerful lever in this model calculation.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of over $39,000.

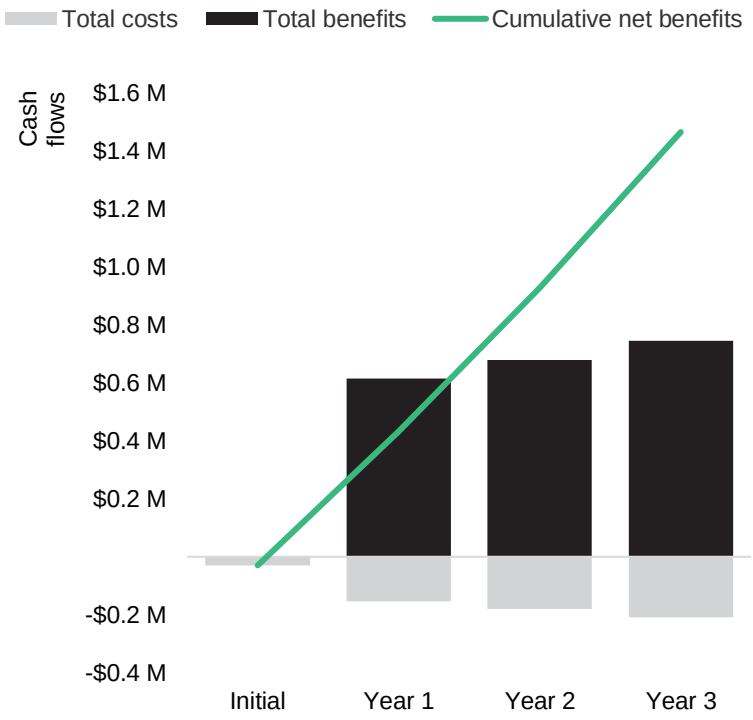
Management And Administrative Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of people working on backup administration	Interviews	0	2	2	2
G2	Fully burdened hourly salary	TEI standard	$0	$75	$75	$75
G3	Hours per month per backup administrators	Interviews	0	8	8	8
Gt	Management and administrative costs	G1*G2*G3*12	$0	$14,400	$14,400	$14,400
	Risk adjustment	↑10%				
Gtr	Management and administrative costs (risk-adjusted)		$0	$15,840	$15,840	$15,840
	Three-year total: $47,520			**Three-year present value: $39,392**		

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



The financial results calculated in the Benefits and Costs sections can be used to determine the ROI and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

These risk-adjusted ROI and NPV values are determined by applying risk-adjustment factors to the unadjusted results in each Benefit and Cost section.

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($29,700)	($153,340)	($180,840)	($208,340)	($572,220)	($475,084)
Total benefits	$0	$613,565	$678,236	$745,140	$2,036,941	$1,678,146
Net benefits	($29,700)	$460,225	$497,396	$536,800	$1,464,721	$1,203,062
ROI						253%

Appendix A: Total Economic Impact

Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

The initial investment column contains costs incurred at "time 0" or at the beginning of Year 1 that are not discounted. All other cash flows are discounted using the discount rate at the end of the year. PV calculations are calculated for each total cost and benefit estimate. NPV calculations in the summary tables are the sum of the initial investment and the discounted cash flows in each year. Sums and present value calculations of the Total Benefits, Total Costs, and Cash Flow tables may not exactly add up, as some rounding may occur.

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made, unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix B: Endnotes

[1] Source: The Top Systemic Risks, 2021," Forrester Research, Inc., February 9, 2021.

[2] Total Economic Impact is a methodology developed by Forrester Research that enhances a company's technology decision-making processes and assists vendors in communicating the value proposition of their products and services to clients. The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

[3] Source: "Addressing Data Management Risks For The Public Cloud Era Leverage Public Cloud To Future-Proof Your Data Protection And Governance," a commissioned Thought Leadership Paper conducted by Forrester Consulting on behalf of Druva, March 2018.

[4] The structure of the data to be backed up (e.g., VMs vs. database) will have different growth and decompression rates.

[5] Source: "Addressing Data Management Risks For The Public Cloud Era Leverage Public Cloud To Future-Proof Your Data Protection And Governance," a commissioned Thought Leadership Paper conducted by Forrester Consulting on behalf of Druva, March 2018.

[6] Source: "The 2021 Cost of Phishing Study," Ponemon Institute, June 2021.

[7] Source: "Factors Driving The ROI Of Sustainability," Forrester Research, Inc., April 22, 2021.


FORRESTER®