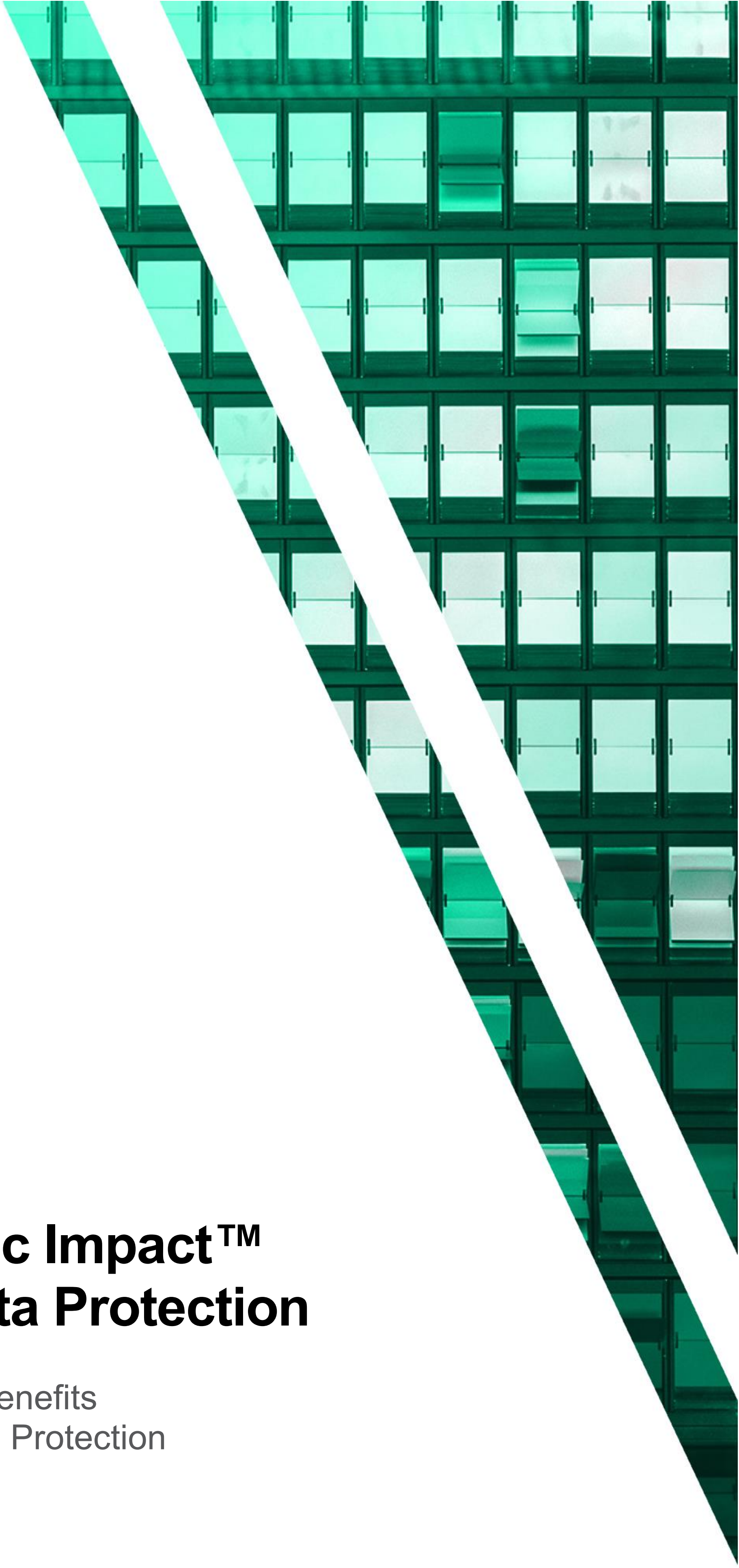
FORRESTER®



The Total Economic Impact™ Of Keepit SaaS Data Protection

Cost Savings And Business Benefits
Enabled By Keepit SaaS Data Protection

JANUARY 2024

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY KEEPIT

Table Of Contents

Consulting Team: *Elia Gollini*
Jan Sythoff

Executive Summary 1

The Keepit SaaS Data Proection Customer Journey 6

Key Challenges 6

Solution Requirements 7

Composite Organization..7

Analysis Of Benefits 8

Faster And More Accurate Recovery From A Ransomware Attack 8

Reduced SaaS Licensing Costs...........................11

On-Premises Backup Cost Avoidance 12

SaaS User Productivity Impact 14

Unquantified Benefits 15

Flexibility..15

Analysis Of Costs 16

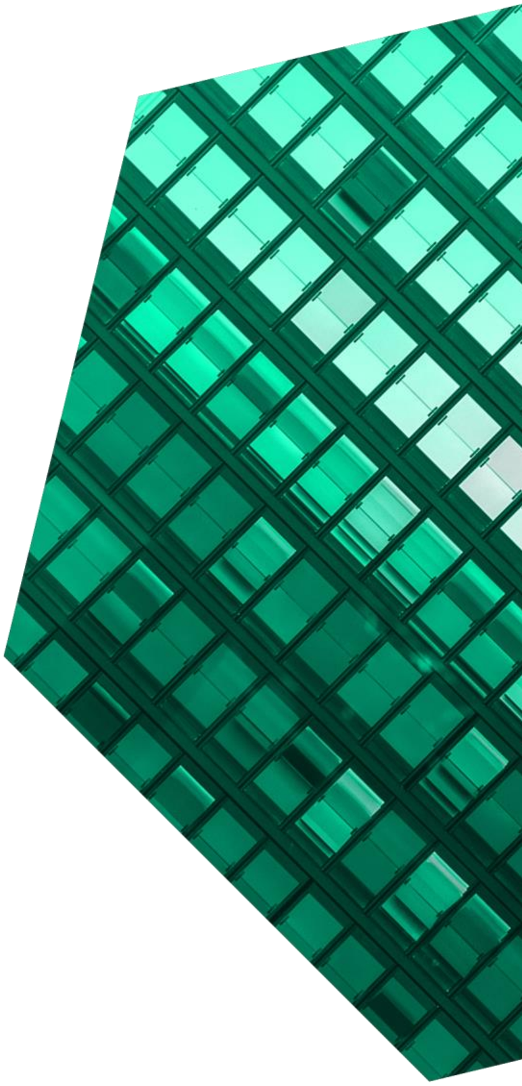
Software subscription cost 16

Other Costs 17

Financial Summary 18

Appendix A: Total Economic Impact 19

Appendix B: Endnotes 20



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute their specific priorities using a unique engagement model that ensures lasting impact. For more information, visit forrester.com/consulting.

© Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

Organizations are increasingly worried about ransomware attacks and losing valuable data. Keepit acts as a safeguard for organizations to recover user data in case of loss, such as in a malicious attack. With Keepit, IT administrators can quickly find, restore, and archive data. This analysis found that the potential negative impact of a ransomware attack can be mitigated through Keepit's software-as-a-service (SaaS) data protection solution. It can also lead to cost savings and time efficiencies for IT administrators and make the day-to-day operations of SaaS backup more efficient, saving time and money.

Keepit is a SaaS data protection platform for companies with data stored in the cloud. Keepit is a vendor-neutral and independent cloud dedicated to SaaS data protection based on a blockchain-verified solution. Keepit protects data in key business applications including the most popular productivity suites, CRM solutions, and directory services. It enables IT administrators and application owners to quickly search for, find, and restore messages, files, and other data types whenever such data is lost or unavailable.

Keepit commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying Keepit SaaS data protection.[1] The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of Keepit SaaS data protection on their organizations.

Reduction in time needed to restore data for selected group of users

90%

KEY STATISTICS

Return on investment (ROI)

163%

Net present value (NPV)

$821.8K

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Keepit. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a manufacturing organization with $2 billion in annual revenue.

Prior to using Keepit SaaS data protection, these interviewees noted how their organizations relied on on-premises data backup solutions or did not have a backup solution in place at all. Their organizations developed the need for a cloud-based backup when they migrated their core productivity applications into the cloud and realized that their cloud vendors' storage did not provide sufficient backup capabilities. The interviewed decision-makers had growing concerns about ransomware attacks and, hence, needed a solution to back up their data. Additionally, they were looking for an easy-to-use solution that could support them in their cloud transition. It's important to note that Forrester Research recommends that an essential piece of an organization's overall ransomware protection plan is a backup tool for critical data.[2]

After the investment in Keepit, the interviewees noted that the Keepit solution better protected their organizations than hosting data on-premises due to the solution's multicloud nature. Key results from the investment include faster and more accurate recovery from ransomware attacks, reduced SaaS licensing costs, on-premises backup cost avoidance, and increased SaaS users productivity.

KEY FINDINGS

Quantified benefits. Three-year, risk-adjusted present value (PV) quantified benefits for the composite organization include:

- **Faster and more accurate recovery from a ransomware attack.** The Keepit solution gives the composite organization the ability to restore and recover backed up data in a quick, efficient, and accurate manner. This is critical for the composite to quickly recover in the event of a successful ransomware attack. The Keepit solution limits the impact of a ransomware attack for the composite by allowing it to recover and restore data quickly, preventing data loss and reducing downtime. This benefit is worth $819,100.
- **Reduced SaaS licensing costs.** The composite organization retains data from former employees after they leave the organization for compliance reasons and therefore needs to continue to pay SaaS fees even after a user has left. Due to the nature of Keepit and its ability to keep unlimited data backup accessible, the composite organization eliminates these licensing costs for three months for around 10% of its workforce. With all historical data available, it also simplifies data management and employee onboarding and offboarding. This reduces SaaS licensing costs by $351,400 over three years.
- **On-premises backup cost avoidance.** By adopting Keepit for cloud backup, the composite organization avoids the associated costs that comes with an on-premises solution. It not only experiences important maintenance time savings, but also reduces the amount of hardware that needs to be upgraded. Through Keepit, the composite organization also benefits from paying its license fee to Keepit on a per-seat basis rather than paying based on the amount of data stored in the backup solution. This results in on-premises backup cost avoidance of $134,000 over three years.
- **SaaS user productivity impact.** Through Keepit, the composite organization's IT administrators find and restore files and data faster and more efficiently, saving $21,400 over three years.

Unquantified benefits. Benefits that provide value for the interviewees' organizations but are not quantified in this study include:

- **Using Keepit as a data archive.** Interviewees noted the Keepit platform could be used as a data archive on top of being primarily a backup

> **"It's important to have the confidence to have all data available all the time. If something happens, from small instances to big ones, we are able to restore data."**
>
> *Senior system manager, automotive association*

solution, which could result in cost savings on archiving solutions.

- **Ease of use and penetration testing time savings.** Interviewees noted that the Keepit platform was easy to use and had great user experience and interface. This made it possible for non-IT users or those without much IT knowledge to comfortably use the Keepit solution and perform restores. Additionally, penetration tests were included in the Keepit solution, allowing Keepit users to avoid allocating resources towards these tests on a regular basis.

- **Leveraging Keepit for auditing.** The Keepit solution supported the interviewees' organizations, allowing them to quickly find files that may be needed for audit purposes. This saved employees' time finding and locating specific files.

Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Subscription fees.** Keepit charges the composite organization based on the number of seats utilizing the application.

- **Other costs.** Other costs include implementation and ongoing management of the Keepit solution. These are minimal for the composite organization because users are onboarded quickly and there is very little management effort required.

The representative interviews and financial analysis found that a composite organization experiences benefits of $1.33 million over three years versus costs of $504,100, adding up to a net present value (NPV) of $821,800 and an ROI of 163%.

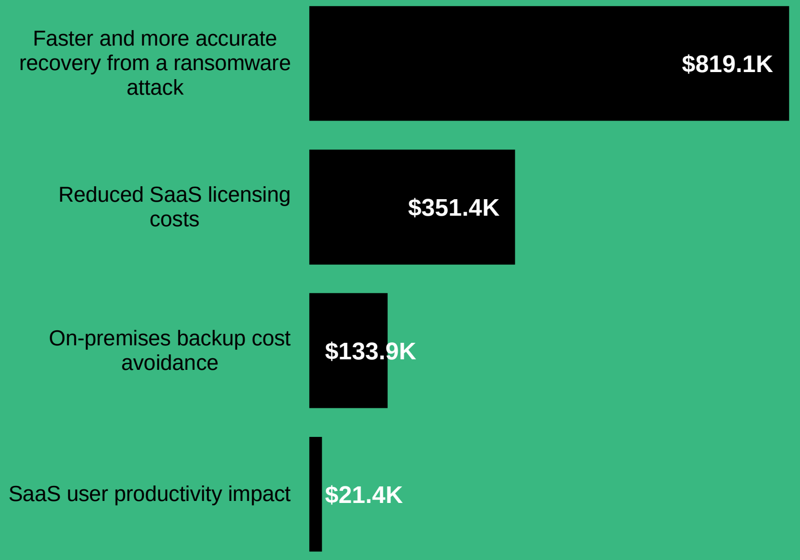
ROI
163%

BENEFITS PV
$1.3M

NPV
$821.8K

PAYBACK
<6 months

Benefits (Three-Year)



> **“The word essential is not an exaggeration in this context. If you have no backup of your data, then you are a threatened species.”**
>
> — Senior consultant, nonprofit

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 Keepit.

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 Keepit can have on an organization.

DUE DILIGENCE

Interviewed Keepit stakeholders and Forrester analysts to gather data relative to Keepit.

INTERVIEWS

Interviewed four representatives at organizations using Keepit SaaS data protection to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees' organizations.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees.

CASE STUDY

Employed four fundamental elements of TEI in modeling the investment impact: benefits, costs, flexibility, and risks. Given the increasing sophistication of ROI analyses related to IT investments, Forrester's TEI methodology provides a complete picture of the total economic impact of purchase decisions. Please see Appendix A for additional information on the TEI methodology.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Keepit and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Keepit.

Keepit reviewed and provided feedback to Forrester, but Forrester maintains editorial control over the study and its findings and does not accept changes to the study that contradict Forrester's findings or obscure the meaning of the study.

Keepit provided the customer names for the interviews but did not participate in the interviews.

The Keepit SaaS Data Protection Customer Journey

🟩 Drivers leading to the Keepit investment

Interviews

Role	Industry	Number Of Seats Backed Up	Previous Setup
Project and workplace services manager	Beverages	21,000	On-premises
IT leader	Nonprofit	14,000	On-premises
Senior system manager	Automotive association	9,000	On-premises
Senior consultant	Nonprofit	2,000	No backup

KEY CHALLENGES

Before investing in Keepit, three out of four interviewees had an on-premises backup solution managed by an external vendor, while one interviewee noted how their organization had no backup in place for their SaaS productivity applications.

The interviewees noted how their organizations struggled with common challenges, including:

- **Progressing their cloud transformation journey.** Interviewees noted that their organizations had an appetite to develop the right IT framework to advance their cloud transformation journey. This would allow them to be more agile and flexible and also would lower the need for in-house IT resources. Considering the increased reliance on SaaS applications, interviewees' organizations also needed to have a backup solution that could match their needs in the SaaS space and protect the data they had in the cloud.

- **Protecting data from the threat of a successful ransomware attack.** All interviewed decision-makers highlighted how they were increasingly aware of the threat ransomware attacks pose on their organizations. The senior system manager at an automotive association notably mentioned: "Everyone knows an attack will happen. It is just a matter of when it will happen." The consequences of a ransomware attack include major financial losses, reputational damage, operational disruption, and intellectual property loss.[3]

- **Protecting against human error.** Additionally, interviewees noted that having data backed up by Keepit's solution reduced the impact of human errors and mistakes.

- **Usability of the backup solution.** Interviewees looked for a solution that would have great usability. Their legacy on-premises backup solutions were too complex for non-IT users or users that do not necessarily possess a lot of IT knowledge to utilize.

> **"With Keepit, we have unlimited storage. We don't have to worry about how much data we back up."**
>
> *Project and workplace services manager, beverages*

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Provide excellent backup capabilities.
- Satisfy compliance requirements around data protection legislation.
- Provide a user-friendly and easy-to-use platform.
- Provide cloud capabilities.

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 interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. A European-headquartered, global manufacturing organization with around $2 billion in revenue. The composite uses Keepit to back up 10,000 seats in Year 1, growing to 10,500 in Year 2, and 11,000 in Year 3. The composite organization backs up the data from a popular SaaS productivity suite; there is also potential to back up directory services data with the Keepit solution. The composite previously used an on-premises backup solution before engaging with Keepit. It is increasingly concerned about ransomware and the potential negative and disruptive impact it could have.

Deployment characteristics. The organization moved its email and file storage applications to the cloud several years ago and leveraged on-premises backup solutions. It then realized how a cloud-based solution, such as Keepit, could be beneficial as it would save various costs and allow for greater flexibility with the amount of data that can be backed up.

Key Assumptions

- **$2 billion annual revenue**
- **10,000 seats backed up**
- **Manufacturing organization**
- **Backing up popular productivity suite with interest in backing up directory services**

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	Faster and more accurate recovery from a ransomware attack	$314,657	$330,390	$346,123	$991,171	$819,149
Btr	Reduced SaaS licensing costs	$135,000	$141,750	$148,500	$425,250	$351,446
Ctr	On-premises backup cost avoidance	$59,888	$50,388	$50,388	$160,664	$133,944
Dtr	SaaS user productivity impact	$8,213	$8,623	$9,034	$25,869	$21,380
	Total benefits (risk-adjusted)	$517,758	$531,151	$554,045	$1,602,954	$1,325,919

FASTER AND MORE ACCURATE RECOVERY FROM A RANSOMWARE ATTACK

Evidence and data. Interviewees highlighted how having the Keepit solution provided their organizations with a sense of security against ransomware attacks, acting as an insurance to their business.

- The interviewees noted their organizations planned for a disaster scenario in case a ransomware attack happened and were aware of the exposure risk and potential losses they could suffer as a result of such an attack. Forrester research recommends that backups are the best insurance policy against an attack, but to be effective they need to be part of a planned and tested backup and recovery process.[4] Three-quarters of security decision-makers suffered a breach in the last 12 months, and the frequency of breaches increased in 2022 by 11% from 2021 and by 24% since 2018, when only 50% of companies have reported a breach.[5]

- Interviewees recognized the value of the Keepit solution because it enabled their organizations to restore data in a much shorter time frame and in a more accurate manner compared to relying on the SaaS applications' own backups.

Modeling and assumptions. To quantify this benefit, Forrester assumes the following:

- The composite organization has a disaster scenario plan in place and has already identified a set of priority users who should be the ones that need to be restored first in the event of a successful ransomware attack. These users are classified as tier-one users as their roles are pivotal to the composite organization's operations and/or ability to mitigate the ransomware attack. The tier-one set of users represents 10% of all the users who have their data backed up in Keepit.

- The time needed to restore the tier-one users is 90% lower than the time the composite would spend restoring its data without Keepit, which has been identified by interviewees to be at least three weeks.

- The tier-two set of users represents the remaining part of the composite users who have their data backed up in Keepit (the remaining 90% of users).

- The time needed to restore the tier-two users is 57% lower than the time the composite would spend restoring its data without Keepit, which has been identified by interviewees to be at least three weeks.
- The number of users whose data is backed up in Keepit grows by 500 users year-on-year.
- The business losses the composite would face in the case of a ransomware attack are calculated purely from a productivity loss standpoint taking into account the users' average salaries.
- It is assumed that only 30% of the total users are actually hit by a potential ransomware attack. This is partly because the composite organization backs up SaaS productivity suite data with Keepit. Ransomware virulence is limited by the architecture of the SaaS platform and spreads slower than in the case of on-premises infrastructure like file servers, company-owned application servers, or core infrastructure like directory services. For the purpose of this study, we assume an attack spreading within user data stored in a popular SaaS productivity suite.
- It is also assumed that the data the composite organization's users have backed up in Keepit is data belonging to a popular SaaS productivity suite and only accounts for 45% of the total user data. In fact, users usually have data stored in other applications, such as CRMs, file servers, other productivity suites, and applications.
- According to a study cosponsored by Keepit, 75% of respondents noted their organization has been hit by ransomware in the past 12 months.[6] Additionally, a Forrester security survey also suggests that 74% of global security decision-makers estimate their organization's sensitive data was breached at least once in the previous 12 months, and 36% estimate three or more breaches.[7] Because of this, this study takes into consideration a 75% likelihood for an organization to be hit by ransomware in the next 12 months.
- According to a Cyentia IRIS report, the expected percentage likelihood of a material financial impact caused by ransomware is approximately 7%.[8] This percentage is representative of an organization being attacked by ransomware and suffering a material business disruption across different teams within the organization, resulting in major financial losses.
- Overall, this benefit has been modeled by looking at the negative quantifiable impact of ransomware attack on the composite organization mainly from a productivity standpoint. There can also be other quantifiable or unquantifiable implications for an organization hit by ransomware, such as operational disruption. This can lead to financial losses as well as reputational damage, while a lack of compliance can lead to fines, which cause financial losses. According to a Forrester survey, 70% of global security decision-makers with security responsibilities said their organization lost $1 million or more from breaches in 2022.[9]

Risks. This benefit may vary for organizations based on:

- The extent to which a well-implemented backup and recovery process is in place.
- The level of importance of the data users have backed up in the Keepit solution.
- The percentage of data users have backed up in the Keepit solution as compared to any other user data that may exist in other applications.
- The speed and extent to which a ransomware attack spreads within an organization.

Results. To account for these risks, Forrester adjusted this benefit downward by 25%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $819,100.

Faster And More Accurate Recovery From A Ransomware Attack

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Number of tier-one selected users for targeted restore	Interview	1,000	1,050	1,100
A2	Average SaaS tier-one user hourly rate	TEI standard	$132	$132	$132
A3	Hours needed for restore without Keepit	Interviews	120	120	120
A4	Business losses during ransomware attack for tier-one users without Keepit	A1*A2*A3	$15,840,000	$16,632,000	$17,424,000
A5	Percentage reduction of time for targeted restore with Keepit	Interviews	90%	90%	90%
A6	Subtotal: Business value recovered from a disaster scenario through Keepit targeted restore	A4*A5	$14,256,000	$14,968,800	$15,681,600
A7	Number of tier-two users	Composite	9,000	9,450	9,900
A8	Average SaaS tier-two user hourly rate	TEI standard	$73	$73	$73
A9	Business losses during ransomware attack for tier-two users without Keepit	A3*A7*A8	$78,840,000	$82,782,000	$86,724,000
A10	Percentage reduction of time for full restore with Keepit	Interviews	57%	57%	57%
A11	Subtotal: Business value recovered from a disaster scenario through Keepit full restore	A9*A10	$44,938,800	$47,185,740	$49,432,680
A12	Percentage of users affected by ransomware attack	Composite	30%	30%	30%
A13	Percentage of users data backed up by Keepit	Composite	45%	45%	45%
A14	Likelihood of ransomware attack in the next 12 months	Keepit	75%	75%	75%
A15	Expected likelihood of material financial impact caused by ransomware	Cyentia IRIS	7%	7%	7%
At	Faster and more accurate recovery from a ransomware attack	(A6+A11)*A12 *A13*A14*A15	$419,543	$440,520	$461,497
	Risk adjustment	↓25%			
Atr	Faster and more accurate recovery from a ransomware attack (risk-adjusted)		$314,657	$330,390	$346,123
	Three-year total: $991,171		**Three-year present value: $819,149**		

REDUCED SAAS LICENSING COSTS

Evidence and data. Interviewees noted that their organizations experienced a reduction in SaaS licensing fees due to using Keepit. Typically, when an employee left, interviewees said their organizations needed to keep the employee's user data, including emails, for three months or more. This meant retaining the SaaS subscription for this prolonged period. However, Keepit allowed them to access the data backup instantly, which meant it was not necessary to keep this data, saving the interviewees' organizations money. Furthermore, this historical data was available at any time, making it much easier for IT administrators to onboard new employees and offboard those leaving.

Modeling and assumptions. To quantify this benefit, Forrester assumes the following:

- The composite experiences an employee (SaaS user) turnover rate of 10%. This rate may vary by industry and region.
- The number of users whose data is backed up in Keepit grows by 500 users year-on-year.
- The average SaaS license fee per user is $50. This is based on rates for popular productivity and communications suites.
- The length of time that data needs to be kept after an employee departure is three months.

Risks. This benefit may vary for organizations based on:

- The turnover rate of an organization.
- The average SaaS license fee per user per month.
- The number of months of licensing that can be saved.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $351,400.

Reduced SaaS Licensing Costs

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Number of SaaS users	Composite	10,000	10,500	11,000
B2	SaaS user turnover	Composite	10%	10%	10%
B3	Number of users turned over	B1*B2	1,000	1,050	1,100
B4	SaaS license fee per user per month	Composite	$50	$50	$50
B5	Number of months of licensing saved per user leaving	Composite	3	3	3
Bt	Reduced SaaS licensing costs	B3*B4*B5	$150,000	$157,500	$165,000
	Risk adjustment	↓10%			
Btr	Reduced SaaS licensing costs (risk-adjusted)		$135,000	$141,750	$148,500
	Three-year total: $425,250		Three-year present value: $351,446		

ON-PREMISES BACKUP COST AVOIDANCE

Evidence and data. Interviewees noted that when their organizations moved from an on-premises backup tool to the Keepit SaaS backup, they realized some cost savings due to no longer having to manage an on-premises solution. This included hardware costs. The interviewees also noted cost advantages from Keepit's pricing model compared to on-premises pricing models. They pointed out how the Keepit pricing model was based only on the number of user seats, giving their organizations significant cost advantages compared to on-premises pricing models, which were based on the amount of data stored in the backup.

Modeling and assumptions. To quantify this benefit, Forrester assumes the following:

- Before Keepit, the composite organization spends 528 hours managing its legacy on-premises backup tool. This reduces to 48 hours with Keepit SaaS backup.
- The savings from not having to manage an on-premises backup tool are representative of one IT administrator's time.
- The composite saves $2,000 on average per month compared to an on-premises backup solution based on the pricing, which is made per seat rather than for the amount of data stored.
- The on-premises solution had a three-year hardware replacement rate, and so the on-premises hardware cost avoidance is assumed to be $10,000 in Year 1.

91%

Reduction in time needed to manage Keepit compared to legacy on-premises backup

> **"It used to take me six to eight weeks a year to manage an on-premises backup solution. Now, with Keepit, I spend only 2 hours a month managing the solution."**
>
> *Senior system manager, automotive association*

Risks. This benefit may vary for organizations based on:

- The time spent by an organization's IT team managing the on-premises solution.
- The number of FTEs involved in managing the on-premises solution.
- The pricing model of an on-premises solution.
- The hardware cost of an on-premises solution.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $134,000.

On-Premises Backup Cost Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Time spent to manage legacy on-premises backup (hours)	Interviews	528	528	528
C2	IT administrator hourly rate	TEI standard	$55	$55	$55
C3	Savings in backup management with Keepit SaaS backup	C1*C2	$29,040	$29,040	$29,040
C4	Monthly savings with Keepit SaaS backup	Interviews	$2,000	$2,000	$2,000
C5	Annual operating costs savings with Keepit SaaS backup	C4*12	$24,000	$24,000	$24,000
C6	Hardware cost avoidance	Composite	$10,000		
Ct	On-premises backup cost avoidance	C3+C5+C6	$63,040	$53,040	$53,040
	Risk adjustment	↓5%			
Ctr	On-premises backup cost avoidance (risk-adjusted)		$59,888	$50,388	$50,388
	Three-year total: $160,664		**Three-year present value: $133,944**		

SAAS USER PRODUCTIVITY IMPACT

Evidence and data. The interviewees highlighted that Keepit made it easier and faster for their organizations' IT administrators to find and restore lost documents, files, and folders. Employees could make mistakes and misplace files, messages, and even complete email folders, which took a substantial amount of time for IT administrators to locate and restore in their previous on-premises environments. Interviewees shared how often they needed to restore data, and how much time this typically saved with Keepit.

Modeling and assumptions. To quantify this benefit, Forrester assumes the following:

- The number of yearly restores is representative of approximately 5% of the number of users.
- The number of users whose data is backed up in Keepit grows by 500 users year-on-year.
- A productivity conversion factor of 50% is applied as a TEI standard.

Risks. This benefit may vary for organizations based on:

- The number of SaaS users in an organization.
- The number of restores done per year.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $21,400.

SaaS User Productivity Impact

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Number of SaaS users	Composite	10,000	10,500	11,000
D2	Number of restores	D1*5%	500	525	550
D3	Time saving per restore (hours)	Interviews	0.5	0.5	0.5
D4	Average SaaS user hourly rate	TEI standard	$73	$73	$73
D5	Productivity conversion factor	TEI standard	50%	50%	50%
Dt	SaaS user productivity impact	D2*D3*D4*D5	$9,125	$9,581	$10,038
	Risk adjustment	↓10%			
Dtr	SaaS user productivity impact (risk-adjusted)		$8,213	$8,623	$9,034
Three-year total: $25,869			Three-year present value: $21,380		

UNQUANTIFIED BENEFITS

Interviewees mentioned the following additional benefits that their organizations experienced but were not able to quantify:

- **Using Keepit as a data archive.** Interviewees mentioned that Keepit could also be used as a data archive on top of being a backup solution primarily. Essentially, the interviewees could construct an archive using Keepit backup. User data that was seldom accessed but needed to be retained was often archived, but the related costs could be saved by using Keepit instead of an alternative tool.
- **Ease of use.** Interviewees have noted that the Keepit solution was easy to learn and use. They said that users and administrators did not need specific prior IT knowledge or skills. Additionally, penetration tests were included with the Keepit solution. Interviewees mentioned that prior to Keepit, these tests would have run on a monthly/bimonthly basis and would require allocation of resources to it. With Keepit's solution, this time commitment could be saved
- **Leveraging Keepit for auditing.** The interviewees noted that they sometimes needed to provide proof of actions taken, instructions given, or other information about past events for legal or auditing purposes. Through Keepit, they could find this type of information and data in a quick and easy way and there was no risk of accidentally deleting or misplacing a file.

FLEXIBILITY

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

- **Decreasing reliance on on-premises infrastructure.** Interviewees noted their organizations increasingly valued the ability to leverage the agility and flexibility of SaaS applications with Keepit. Using a solution like Keepit aligned with their digital transformation journey towards more cloud-based infrastructure approach.
- **Using Keepit for additional applications.** Some interviewees highlighted how their organizations started to leverage Keepit for directory services and user data. This represented an attractive future avenue for these organizations as it allowed for a higher level of protection in case of a ransomware attack. A ransomware attack could spread much more rapidly across directory services data and in this way have a greater impact.

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

> **"The value we get from Keepit comes also from the ease of operation and the ability to attach the future services. We have already started to develop a need for multiple other applications to be backed up with Keepit."**
>
> *Senior consultant, nonprofit*

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	Software subscription cost	$0	$189,000	$198,450	$207,900	$595,350	$492,025
Ftr	Other costs	$4,840	$2,904	$2,904	$2,904	$13,552	$12,062
	Total costs (risk-adjusted)	$4,840	$191,904	$201,354	$210,804	$608,902	$504,087

SOFTWARE SUBSCRIPTION COST

Evidence and data. Interviewees noted that Keepit was charged on a per user basis and the cost per user was fixed and so it did not change based on the amount of data stored in the backup solution.

Modeling and assumptions. To quantify this cost, Forrester assumes the following:

- In Year 1, there are 10,000 users.
- The number of users whose data is backed up in Keepit grows by 500 users year-on-year.
- The cost of the Keepit subscription per user is $18.

Risks. This cost may vary for different organizations based on:

- The number of users whose data is backed up on the Keepit solution.
- The cost per user over the three-year period.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $492,000.

Software subscription cost

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Number of SaaS users	Composite		10,000	10,500	11,000
E2	Cost of software subscription per user	Composite		$18	$18	$18
Et	Software subscription cost	E1*E2	$0	$180,000	$189,000	$198,000
	Risk adjustment	↑5%				
Etr	Software subscription cost (risk-adjusted)		$0	$189,000	$198,450	$207,900
	Three-year total: $595,350			**Three-year present value: $492,025**		

OTHER COSTS

Evidence and data. On top of the subscription fees, the interviewees noted their organizations needed to invest time into the implementation of the Keepit solution as well as ongoing management. Interviewees noted that the implementation was fast and did not require much time for users to learn how to use the solution. The IT leader at the nonprofit organization highlighted how the Keepit solution "works almost without any configuration."

Modeling and assumptions. To quantify this cost, Forrester assumes the following:

- The implementation time needed is 80 hours. This includes time spent on pilots, technical trials, and training users.
- One IT administrator needs to invest 4 hours a month in managing the solution on an ongoing basis.

Risks. This cost may vary for organizations based on:

- The time needed to implement the Keepit solution.
- The time needed to maintain the solution, including any upgrades and support.

> **"The training given by Keepit during the implementation phase was extremely good. In 10 minutes, all my team members were onboard."**
>
> *IT leader, nonprofit*

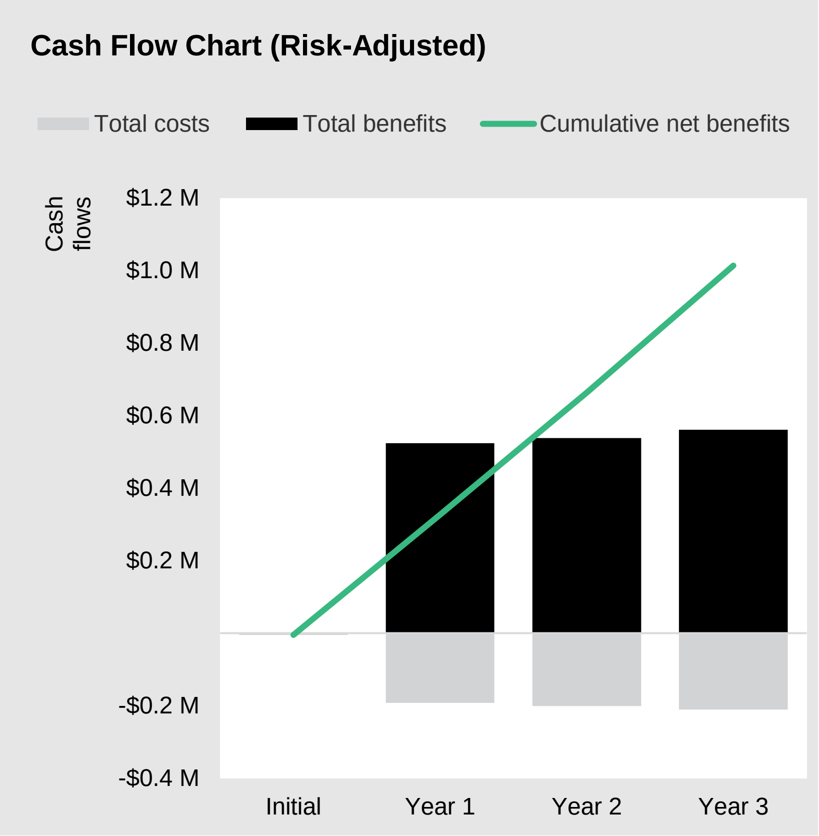
Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $12,100.

Other Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Implementation and planning effort (hours)	Interviews	80			
F2	Maintenance and administration effort (hours)	Interviews		48	48	48
F3	IT administrator hourly rate	TEI standard	$55	$55	$55	$55
Ft	Other costs	(F1+F2)*F3	$4,400	$2,640	$2,640	$2,640
	Risk adjustment	↑10%				
Ftr	Other costs (risk-adjusted)		$4,840	$2,904	$2,904	$2,904
	Three-year total: $13,552			**Three-year present value: $12,062**		

Financial Summary

CONSOLIDATED THREE-YEAR, RISK-ADJUSTED METRICS



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

These risk-adjusted ROI, NPV, and payback period 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	($4,840)	($191,904)	($201,354)	($210,804)	($608,902)	($504,087)
Total benefits	$0	$517,758	$531,151	$554,045	$1,602,954	$1,325,919
Net benefits	($4,840)	$325,854	$329,797	$343,241	$994,052	$821,832
ROI						163%
Payback						<6 months

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] 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.

[2] Source: "The Ransomware Survival Guide," Forrester Research, Inc., November 10, 2021.

[3] Source: Anthony Today, "Impact of Ransomware Attacks on Businesses and Individuals," Medium, February 8, 2023.

[4] Source: "The State Of Ransomware Attacks And Defenses," Forrester Research, Inc., February 2, 2022.

[5] Source: "The State Of Incident Readiness And Response," Forrester Research, Inc., September 25, 2023.

[6] Source: "New Enterprise Strategy Group Study Shows Cyber Attacks Are Rapidly Increasing Despite Security Perimeter and Mitigation Strategies," Keepit, August 29, 2023.

[7] Source: "What 2022's Most Notable Breaches Mean For Tech Execs," Forrester Research, Inc., July 14, 2023.

[8] Source: "Information Risk Insights Study," Cyentia Institute, 2022.

[9] Source: "The State Of Incident Readiness And Response," Forrester Research, Inc., September 25, 2023.""

FORRESTER®