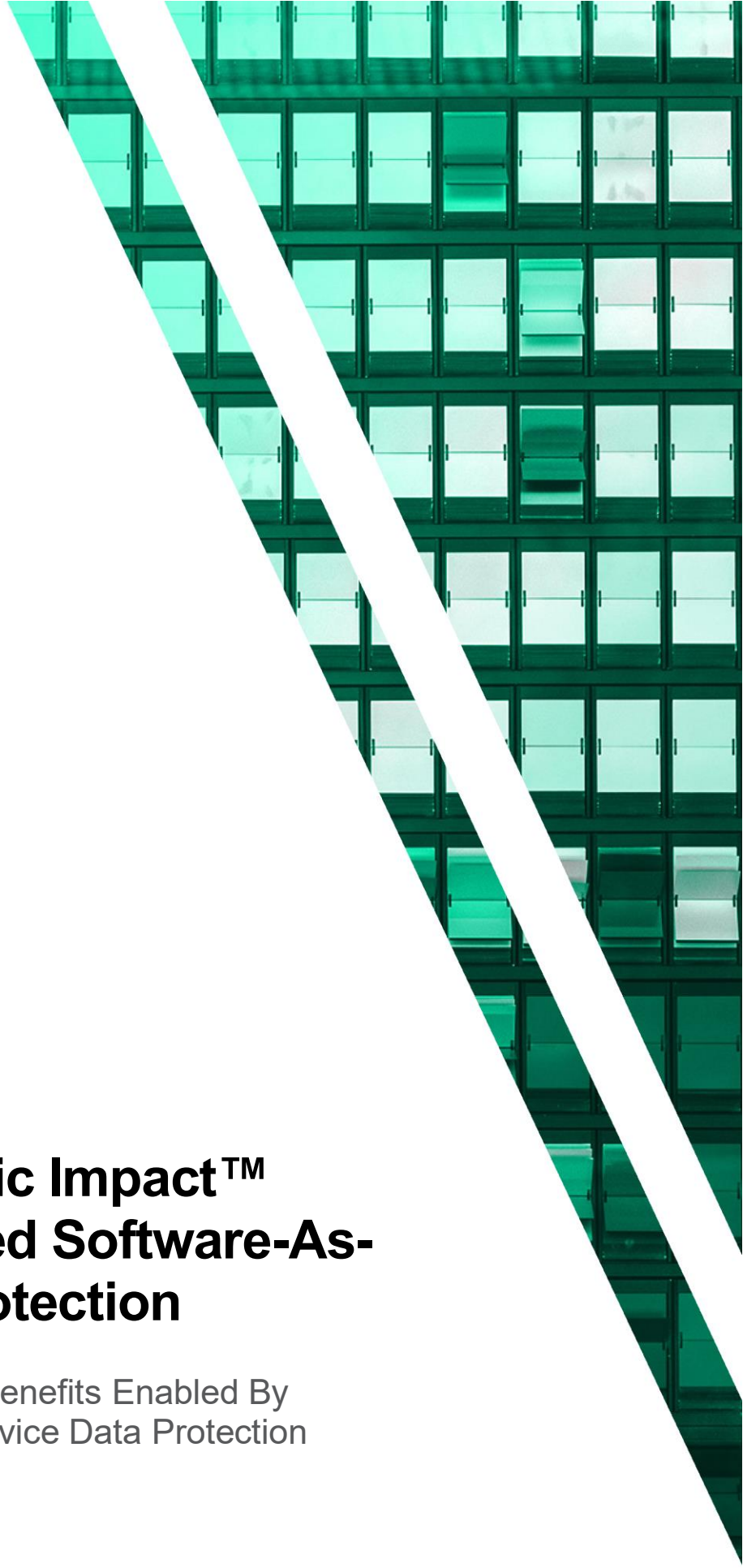
FORRESTER®



# The Total Economic Impact™ Of Keepit Dedicated Software-As-A-Service Data Protection

Cost Savings And Business Benefits Enabled By Dedicated Software-As-A-Service Data Protection

**DECEMBER 2021**

## Table Of Contents


**Executive Summary ..... 1**

**The Keepit Dedicated SaaS Data Protection Customer Journey ..... 6**

Key Challenges ..... 6

Composite Organization ..... 7

**Analysis Of Benefits ..... 8**

Reduced Impact Of A Ransomware Attack ..... 8

Reduced SaaS Licensing Costs ..... 9

Reduced Archiving Costs ..... 10

Reduced Auditing And Legal Costs ..... 11

IT Administrator Offboarding And Restoring Efficiencies ..... 13

SaaS User Productivity Impact ..... 14

Unquantified Benefits ..... 15

Flexibility ..... 16

**Analysis Of Costs ..... 17**

Software License Fees ..... 17

Other Costs ..... 18

**Financial Summary ..... 19**

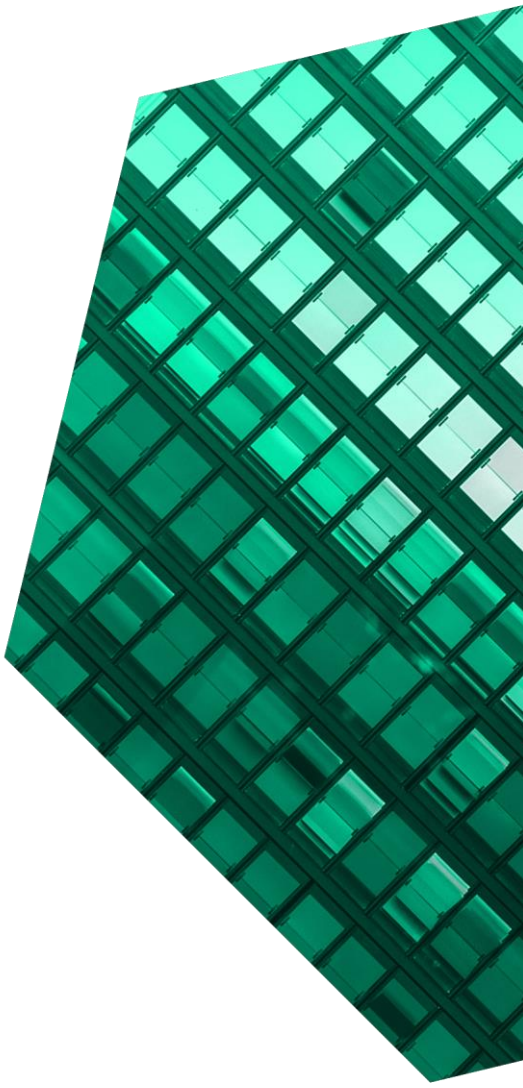
**Appendix A: Total Economic Impact ..... 20**

**Appendix B: Supplemental Material ..... 21**

**Appendix C: Endnotes ..... 21**



*Consulting Team: Jan ten Sythoff*

## Executive Summary

Organizations are responsible for protecting their data and configuration settings when using software as a service (SaaS). Keepit safeguards all important SaaS data and enables IT administrators to quickly find, restore, and archive it. This analysis found that Keepit delivers benefits including significant cost savings and time efficiencies through administration and compliance-based use cases. It is also an important component of a recovery system in the event of a ransomware attack and it improves compliance and business agility.

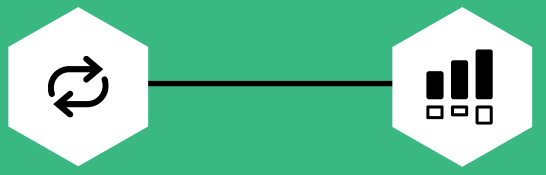
Keepit Dedicated SaaS Data Protection is a cloud-based backup and recovery solution for several core collaboration SaaS applications, such as email, file storage, communications, and CRM. It enables IT administrators and application owners to quickly search for, find, and restore messages, files, and other data types whenever such data is lost or unavailable because of events like ransomware attacks.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five decision-makers with experience using Keepit Dedicated SaaS Data Protection. For the purposes of this study, Forrester aggregated the experiences of the interviewed decision-makers and combined the results into a single composite organization.

Prior to using Keepit Dedicated SaaS Data Protection, the interviewed decision-makers relied on their SaaS application vendor's native backup and restore functionality, which was focused on availability of service rather than customer data protection and recovery. This made it limited and insufficient. The decision-makers' organizations were liable if they lost core data such as emails, digital files, and configuration settings. To improve their data resilience, organizations adopted Keepit as they moved from on-premises applications to SaaS-based collaboration and CRM services. The decision-makers' organizations were especially concerned about data loss caused by ransomware attacks or unplanned service outages. Furthermore, they wanted to ease pressures on IT administrators and help desk staff by enabling them to quickly and easily find data and restore it, thus minimizing the impact on employees.

**KEY STATISTICS**



Return on investment (ROI)
**78%**

Net present value (NPV)
**$225K**

After the investment in Keepit Dedicated SaaS Data Protection, the customers saw significant cost and time savings. Key results from the investment include reduced SaaS costs, reduced archiving costs, and

increased efficiency of IT administrators and SaaS users. Some interviewees also reported benefits related to compliance and e-discovery.

## KEY FINDINGS

**Key benefits.** The key benefits include:

- **Reduced impact of a ransomware attack**. Ransomware attacks, which are in the news more and more frequently, can be devastating to organizations, leaving employees unable to use core business applications and access data for days, weeks, and even months at a time. In the case of the composite organization, if such an event were to bring systems down for five days, it could incur costs of $5 million or more. Interviewees highlighted that Keepit is an important component of their disaster recovery plan in the event of a ransomware attack, enabling them to restore access to data and employee productivity in a shorter time. This could potentially save them significant costs and damage to their reputations.

> **"Keepit does not avoid ransomware attacks, but it ensures you are back up and running quickly."**
>
> *Project manager, server specialist, local government*

- **Reduced SaaS licensing fees.** Companies often have to keep ex-employee user accounts active after their end date to access user data which otherwise may have been purged by the SaaS vendor. Keepit retains all former user data as part of the backup after they have left and does not charge for the accounts of ex-employees. As a result, the companies save on three months of SaaS licensing fees for employees who leave the organization, or around 10% of the workforce per year. This number can be much higher if organizations use a lot of temporary staff or contractors. With all historical data available, it simplifies data management and employee onboarding and offboarding.
- **Reduced archiving costs.** The Keepit architecture can be both a backup and archive repository. Organizations can therefore avoid investing into a separate archiving tool in addition to the backup solution. In the case of the composite organization, it was able to save more than $164,000 over the three years. This is equivalent to around $10 per employee per year.
- **Reduced auditing and legal costs.** If data is no longer available for legal or auditing purposes, organizations might incur significant lawyer and auditor costs. Keepit stores core SaaS data for as long as the customer chooses and can make it quickly available, thus saving auditing and legal time. In the case of the composite, seven days of auditor and lawyer costs are avoided every year.
- **IT administrator offboarding and restoring efficiencies.** IT administrators save a lot of time and effort in various use cases through Keepit. For instance, the time required to offboard an employee is reduced from an hour to a matter of minutes. Searching and finding lost files is also much easier and faster, as are other tasks such as employee email address changes.
- **Increased SaaS user productivity.** Employees save time because lost files are restored quickly. Without Keepit, employees would need to reproduce a lost file, spending a lot of time and unnecessary effort.

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

- **Improved compliance.** Certain business sectors, such as finance, have to demonstrate an exit strategy to show they can readily continue

operating without a SaaS service. Keepit helps them achieve this by enabling core data to be accessed and restored. It also emboldens the use of chat and other messaging services because it keeps a record of such interactions, which is important in some industries.

- **Increased flexibility.** Keepit enables organizations to be more flexible and agile in several ways. As a cloud-based service, it does not require hardware provisioning or software maintenance, and it easily scales up or down. One interviewee was also able to use it to consolidate SaaS user accounts when their organization merged with another. Keepit readily fits as part of a digital transformation to an agile, cloud-based IT set-up.
- **Avoided costs of on-premises backup.** Those organizations that replace their on-premises backup systems with Keepit achieve different benefits, which depend on the relative performance of the two options. On-premises backup incurs additional costs, including regular maintenance and upkeep of the servers and software.
- **Transparent and predictable pricing.** Keepit charges based on an all-inclusive per-user, per-month fee. There are no additional charges based on usage, storage amount, or data capacity. This means that costs are predictable.
- **Reduced impact of SaaS outage.** In the event of the SaaS service becoming unavailable, IT administrators can quickly access important data for some key users, reducing the impact of the outage.

**Costs.** Risk-adjusted PV costs include:

- **Licensing fees.** Keepit charges based on the number of active users utilizing the application.
- **Other costs.** Additional costs related to the implementation and maintenance of the solution are minimal. New customers are set up quickly and ongoing maintenance is also minimal. As an organization's needs change, the solution scales up and down with no intervention required.

The decision-maker interviews and financial analysis found that a composite organization with no additional backup in place on top of their SaaS provider, experiences benefits of more than $514,000 over three years versus costs of about $289,000, adding up to a net present value (NPV) of almost $225,000 and an ROI of 78%.

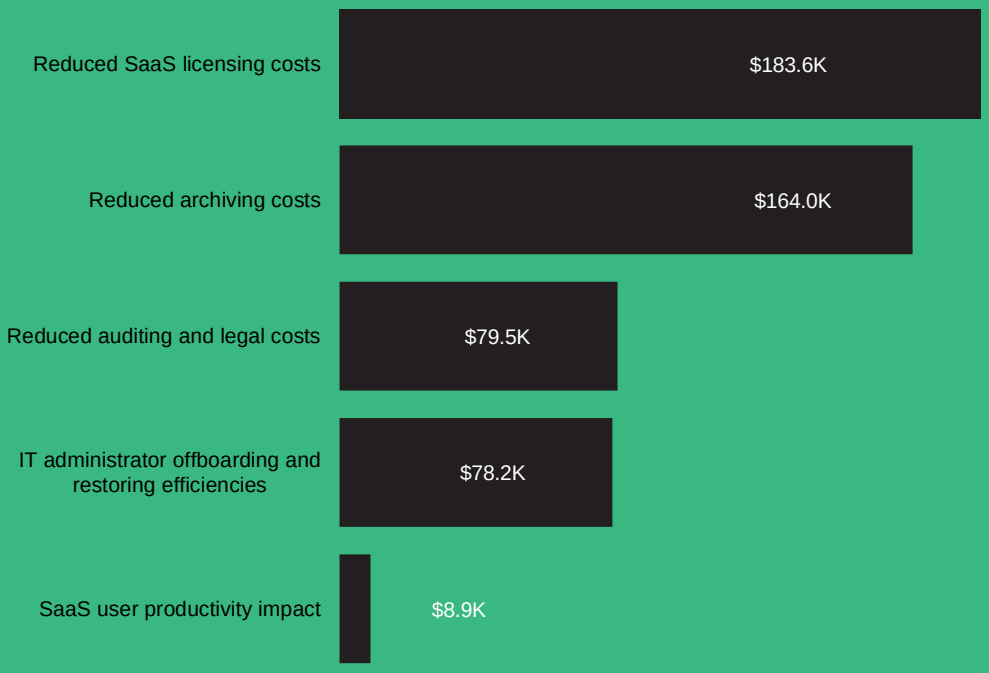
ROI
**78%**

BENEFITS PV
**$514K**

NPV
**225K**

PAYBACK
**<6 months**

**Benefits (Three-Year)**




**Keepit safeguards core data, which helps it reduce the impact of events such as ransomware and malicious software attacks. Furthermore, it reduces cloud and data costs and improves IT efficiency.**

## 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 Dedicated SaaS Data Protection.

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 Dedicated SaaS Data Protection can have on an organization.

# The Keepit Dedicated SaaS Data Protection Customer Journey

Drivers leading to the Keepit Dedicated SaaS Data Protection investment

**Interviewed Decision-Makers**

| Interviewee | Industry | Previous setup | Number of SaaS users |
|---|---|---|---|
| Infrastructure architect | Construction supplies | No additional backup on top of SaaS provider | 11,000 |
| Project manager, server specialist | Local government | No additional backup on top of SaaS provider | 4,500 |
| Head of digital workplace and support services | Financial services | On-premises application and backup | 3,600 |
| IT infrastructure manager | Manufacturing | On-premises application and backup | 3,000 |
| Group head of infrastructure | Manufacturing and logistics | No additional backup on top of SaaS provider | 2,000 |

## KEY CHALLENGES

Before investing with Keepit, three out of the five interviewed decision-makers' organizations had no additional backup for their SaaS service, believing that the SaaS vendor provided sufficient backup capabilities for the customer data. The other two decision-makers' organizations migrated to a full cloud setup, moving both their collaboration suite and backup on-premises applications to the cloud at the same time. In the latter case, the benefits from working with Keepit are largely around not having to manage on-premises infrastructure.

The interviewed decision-makers' organizations struggled with common challenges, including:

- **Lack of backup for key SaaS applications.** Several interviewed decision-makers said that when their organizations moved email and file storage applications to the cloud, they believed that the SaaS vendor's service included sufficient backup and restore capabilities for customer-created data. However, there was no long-term backup included, leaving organizations at risk of losing important long-term data.
- **Increasing threat from ransomware attacks.** Complaints about ransomware attacks are on the rise and their impacts have been widely reported, including instances of organizations taking months to recover. In some cases, organizations have had to stop operating altogether. The costs of such attacks are significant and include lost revenue, profit (whether that includes paying the ransom or not), and productivity, as well as damage to an organization's reputation. The time and effort required to recover from a ransomware attack is also considerable.
- **Pressure on IT resources.** IT is often seen as a cost center, resulting in pressure on limited resources to be more efficient, reduce costs, and do more without increased investment. However,

> **"When we initially migrated to [SaaS vendor], we assumed backup and restore [capabilities] were included. It gradually became clear that this was not the case; this backup was limited in scope and did not cover our needs. We were liable to lose data altogether in the long term."**
>
> *Project manager, server specialist, local government*

this is while risks, notably ransomware and other malicious attack risks, are growing.

- **Need to shift to flexible and scalable infrastructure.** As part of their digital transformations, many organizations are moving core systems, including communications and file storage capabilities, to the cloud. Moving to the cloud means IT no longer has to manage infrastructure or spend time on software maintenance.

**"It was unclear how quickly our SaaS vendor would react when we needed to restore data. When you restore data with Keepit, it's much cleaner and easier. You don't receive a single file with a lot of data which you need to unpick."**

*Project manager, server specialist, local government*

## 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 five 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.** A large, regional manufacturing organization with $4 billion in revenue and earnings before interest, taxes, depreciation, and amortization (EBITDA) of $250 million. It has 10,000 employees, half of which are office-based SaaS users. The number of SaaS users is growing by 500 every year. Leadership is also increasingly concerned about malicious attacks and wants to strengthen disaster recovery capabilities. The average SaaS user salary rate is $100,000 and employee turnover rate is 10%.

**Key assumptions**

- **5,000 SaaS users**
- **$4B in revenues**
- **$250M in EBITDA**
- **Email and file storage in the cloud**
- **No backup capability with the SaaS vendor**
- **Growing concerns about ransomware attacks**

**Deployment characteristics.** The organization had moved its email and file storage applications to the cloud several years ago but did not realize that its SaaS service included only a limited backup, with restricted time and data storage, and so did not invest in an alternative backup capability at the time. It was also becoming increasingly concerned about ransomware attacks and wanted to provide better restore capabilities to its users while looking for ways to reduce costs.

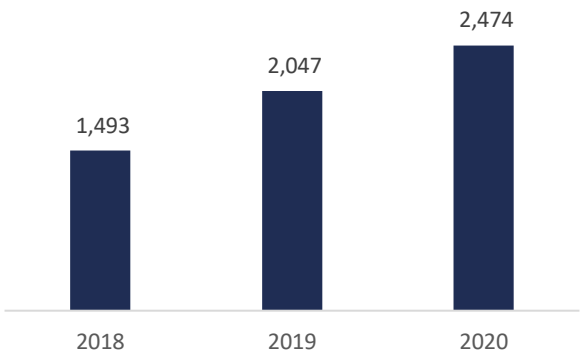
# Analysis Of Benefits

Key benefits as applied to the composite

### REDUCED IMPACT OF A RANSOMWARE ATTACK

The interviewees highlighted that one of the key reasons for investing in Keepit was to safeguard data in the event of a ransomware or other malicious software attack. Such events are becoming more frequent, with a number of recent, high-profile attacks resulting in significant damages and costs.[2]

**Number of ransomware complaints to FBI, 2018 - 2020**




Ransomware attacks affect multiple IT systems and cause devastation to public and private organizations; some have not been able to recover. There are several ways in which costs are incurred:

- **Operational downtime.** With critical systems unavailable, production slows or stops. This can last for weeks, impacting revenue and profit.
- **Productivity loss.** Employees cannot fulfil core tasks because they cannot access systems, data, or communications applications.
- **Reputational damage.** The damage to an organization's reputation, image, and goodwill can be significant; this can include costs relating to customer compensation, legal implications, and PR and marketing efforts.
- **Recovery systems.** The costs of following the recovery process plus the time and effort from internal and external agencies like regulators and consultancies.

> **"In the event of a ransomware attack or technical failure, we have a set of priorities, including enabling frontline staff to establish mail data. For many, this is their primary communications platform and archive; this is where Keepit has an important part to play."**
>
> *Infrastructure architect, construction supplies*

Research shows that, on average, it takes multiple weeks to recover from a ransomware attack and it costs millions of dollars in damages. Forrester research finds many organizations under-prepared for ransomware attacks.[3]

In the case of the composite, if systems are down for five days, the impact on EBITDA (if none is subsequently recovered) is nearly $3.5 million, while the productivity impact for the 5,000 SaaS users is $1.5 million.

> **"My best guess [of the beneficial impact we expect Keepit to have in the event of a ransomware attack] is somewhere between 20-40% reduced cost and a lot of time. In real money it could be anywhere between €50,000 and €500,000."**
>
> *Infrastructure architect, construction supplies*

While the interviewed decision-makers said that their investment in Keepit was, in part, driven by concerns about a ransomware attack, it was difficult for them to quantify the impact as none had been through such an event. The infrastructure architect in the construction supplies industry was able to provide an estimate of somewhere between €50,000 and €500,000. Clearly such an additional benefit would substantially increase the ROI.

**Total Benefits**

| Ref. | Benefit | Year 1 | Year 2 | Year 3 | Total | Present Value |
|---|---|---|---|---|---|---|
| Atr | Reduced SaaS licensing costs | $67,500 | $74,250 | $81,000 | $222,750 | $183,584 |
| Btr | Reduced archiving costs | $32,400 | $70,567 | $101,477 | $204,444 | $164,016 |
| Ctr | Reduced auditing and legal costs | $31,970 | $31,970 | $31,970 | $95,909 | $79,504 |
| Dtr | IT administrator offboarding and restoring efficiencies | $28,738 | $31,611 | $34,485 | $94,834 | $78,159 |
| Etr | SaaS user productivity impact | $3,285 | $3,614 | $3,942 | $10,841 | $8,934 |
| | Total benefits (risk-adjusted) | $163,892 | $212,012 | $252,873 | $628,777 | $514,197 |

### REDUCED SAAS LICENSING COSTS

**Evidence and data.** An important benefit of Keepit is the reduction in SaaS licensing fees. When an employee leaves, organizations typically need to keep the data, including emails, for three months or more, retaining the SaaS subscription for this prolonged period. However, having the data backup instantly accessible in Keepit means an active license is not necessary to keep this data and organizations can see substantial savings. Furthermore, all of the historical data is available at any time, making it much easier for IT administrators to onboard new employees and offboard those leaving.

> **"We save DKK 1,500 to DKK 1,800 [$225 to $270] per employee who leaves as we no longer need to keep the subscription for three months."**
>
> *Head of digital workplace and support services, financial services*

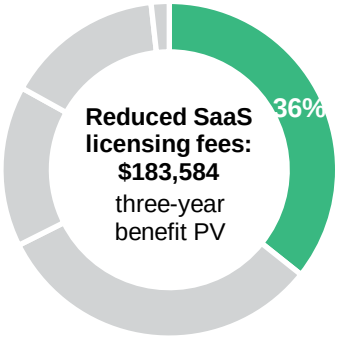
**Modeling and assumptions.** The following metrics were used to quantify this benefit:

- The number of SaaS users leaving was estimated by assuming an employee (SaaS user) turnover rate of 10%. This is a relatively low rate, and it can vary by industry and region.

- 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 can vary from organization to organization because of the SaaS licensing costs, the user turnover rate and the length of time an organization chose to keep the data.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of almost $183,600.

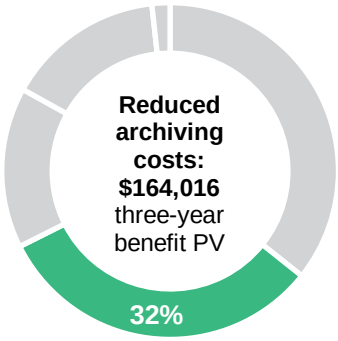



**Reduced SaaS Licensing Costs**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| A1 | Number of SaaS users | Composite | 5,000 | 5,500 | 6,000 |
| A2 | SaaS user turnover | Composite | 10% | 10% | 10% |
| A3 | Number of users leaving | A1*A2 | 500 | 550 | 600 |
| A4 | SaaS license fee per user per month | Composite | $50 | $50 | $50 |
| A5 | Number of months of licensing saved per user leaving | Composite | 3 | 3 | 3 |
| At | Reduced SaaS licensing costs | A3*A4*A5 | $75,000 | $82,500 | $90,000 |
| | Risk adjustment | ↓10% | | | |
| Atr | Reduced SaaS licensing costs (risk-adjusted) | | $67,500 | $74,250 | $81,000 |
| | **Three-year total: $222,750** | | | **Three-year present value: $183,584** | |

### REDUCED ARCHIVING COSTS

**Evidence and data.** The nature of Keepit's architecture means that in addition to being a data backup, it can also be used as a data archive. Older data that is seldom accessed but needs to be retained is often archived, but the related costs can be saved by using Keepit instead of an alternative tool. This also reduces IT administration effort by



reducing the number of tools that need to be supported and maintained.

**Modeling and assumptions.** To quantify this benefit, we assumed that:

- Each SaaS user has 15 GB of data that needs to be archived in Year 1, 22 GB of data Year 2, and 29 GB in the third year. These numbers come from average amounts of annual archived data reported by the five decision-makers.
- One hundred percent of this data is archived.
- The cost of archiving data is $0.04 per gigabyte per month, in line with current cloud storage pricing for quick access to data and including additional storage costs associated with data indexing.
- The data overhead or egress cost for accessing the data is 35%.

**Risks.** The amount of data organizations need to be archived might be different than the composite organization, changing the value of the benefit.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of more than $164,000.

**Reduced Archiving Costs**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| B1 | Number of SaaS users | Composite | 5,000 | 5,500 | 6,000 |
| B2 | Average SaaS data per user per month (gigabytes) | Interviews | 15 | 22 | 29 |
| B3 | Average monthly SaaS data (gigabytes) | B1*B2 | 75,000 | 121,000 | 174,000 |
| B4 | Cost of data archiving (per gigabyte per month) | Assumption | $0.04 | $0.04 | $0.04 |
| B5 | Data overhead or egress costs | Assumption | 35% | 35% | 35% |
| Bt | Reduced archiving costs | B3*B4*12*(1+B5) | $36,000 | $78,408 | $112,752 |
| | Risk adjustment | ↓10% | | | |
| Btr | Reduced archiving costs (risk-adjusted) | | $32,400 | $70,567 | $101,477 |
| | **Three-year total: $204,444** | | | **Three-year present value: $164,016** | |

### REDUCED AUDITING AND LEGAL COSTS

**Evidence and data.** Interviewed decision-makers said that they sometimes need to provide proof of actions taken, instructions given, or other information about past events for legal or auditing purposes.

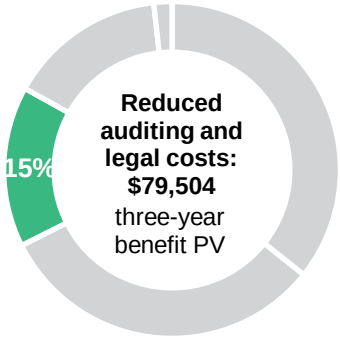
- Interviewees were able to find files and emails from particular dates very quickly and easily, saving time in searching for other means of providing such evidence.
- In some cases, this can mean substantial cost savings. The interviewee from the financial services organization said they lost a key document in the midst of merger discussions and finding and restoring it quickly and easily saved a lot of time and money.

**Modeling and assumptions.** In order to quantify this benefit, Forrester assumed that:

- 40 hours of legal team time are saved annually because lost documents, emails, and data can quickly be located and restored.
- For the same reasons, 8 hours of auditing time are saved every quarter.
- Lawyer and auditor hourly fees are $500.
- The average IT administrator has a salary of $75,000, equivalent to a fully loaded hourly rate of about $55.
- IT administrators also save the equivalent time in this use case because of easier and faster document discovery and restore functions.

**Risks.** Some of the interviewed decision-makers had not used Keepit for these use cases yet but expected to in the future. This could also be true for other organizations.

**Results:** To account for these risks, Forrester adjusted this benefit downward by 20%. This resulted in a three-year, risk-adjusted total PV of over $79,500.




**Reduced Auditing And Legal Costs**

| Ref. | Metric | Source | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|
| C1 | Legal hold and e-discovery efficiencies | Interviews | 40 | 40 | 40 |
| C2 | Auditing efficiencies | Assumption | 32 | 32 | 32 |
| C3 | Average lawyer and auditor hourly rate | Assumption | $500 | $500 | $500 |
| C4 | Lawyer and auditing efficiency | (C1+C2)*C3 | $36,000 | $36,000 | $36,000 |
| C5 | IT administrator hourly rate (based on fully loaded $75,000 salary) | TEI standard | $55 | $55 | $55 |
| C6 | Related IT administrator efficiencies | (C1+C2)*C5 | $3,962 | $3,962 | $3,962 |
| Ct | Reduced auditing and legal costs | C4+C6 | $39,962 | $39,962 | $39,962 |
| | Risk adjustment | ↓20% | | | |
| Ctr | Reduced auditing and legal costs (risk-adjusted) | | $31,970 | $31,970 | $31,970 |
| | **Three-year total: $95,909** | | | **Three-year present value: $79,504** | |

### IT ADMINISTRATOR OFFBOARDING AND RESTORING EFFICIENCIES

**Evidence and data.** All interviewed decision-makers highlighted that Keepit makes it easier for IT administrators to complete various tasks, thus improving their efficiency. Employee offboarding and document or folder restores are two important tasks they were able to be more efficient.

- The IT infrastructure manager in the manufacturing sector told us: “Previously, it took about an hour to manually move data when an employee was leaving. This now takes a minute”.
- Another interviewee told Forrester, “Keepit keeps the data of employees who leave for a year — this is a great licensing feature, otherwise the data of those users could be lost.”
- It was also clear that finding lost files, folders, or emails could take IT administrators a lot of time to find and restore. With Keepit, they were able to locate and restore data quickly and easily, giving them time back for more productive tasks.
- One interviewed decision-maker said that their organization also saved time when changing user email addresses, although this is a less common use case.

> **“Previously, it took about an hour to manually move data when an employee was leaving. This now takes a minute.”**
>
> *IT infrastructure manager, manufacturing*

**Modeling and assumptions.** In order to quantify the value of this benefit, it was assumed that:

- The composite has 5,000 users, growing to 5,500 in Year 2 and 6,000 in Year 3.
- The average employee and SaaS user turnover rate is 10%, a typical benchmark for many industries. This can be much higher, particularly in cases where a lot of contractors and temporary staff are used.
- The average time an IT administrator has to spend managing the data of an employee who leaves is one hour without Keepit.
- On average, there is one restore per 100 employees per year.
- For every restore, the IT administrator saves, on average, an hour of work time. This is because of Keepit’s easy search and restore capability.
- The average IT administrator has a salary of $75,000, equivalent to a fully loaded hourly rate of around $55.

**Risks.** The amount of time saved by IT administrators could vary depending on an organization’s previous process, different staff turnover rates or lower frequency of restores

**Results.** To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of almost $78,200.

| IT Administrator Offboarding And Restoring Efficiencies | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| D1 | Number of SaaS users | Composite | 5,000 | 5,500 | 6,000 |
| D2 | SaaS user turnover rate | Assumption | 10% | 10% | 10% |
| D3 | Number SaaS users offboarding | D1*D2 | 500 | 550 | 600 |
| D4 | Average time saving per employee offboarded (hours) | Interviews | 1.0 | 1.0 | 1.0 |
| D5 | Total employee offboarding time saving (hours) | D3*D4 | 500 | 550 | 600 |
| D6 | Number of restores (1 per 100 users) | 0.01*D1 | 50 | 55 | 60 |
| D7 | Average time saving per restore (hours) | Interviews | 1 | 1 | 1 |
| D8 | IT administrator hourly rate (based on fully loaded $75,000 salary) | TEI standard | $55 | $55 | $55 |
| Dt | IT administrator offboarding and restoring efficiencies | (D5+(D6*D7))*D8 | $30,250 | $33,275 | $36,300 |
| | Risk adjustment | ↓5% | | | |
| Dtr | IT administrator offboarding and restoring efficiencies (risk-adjusted) | | $28,738 | $31,611 | $34,485 |
| | **Three-year total: $94,834** | | | **Three-year present value: $78,159** | |

### SAAS USER PRODUCTIVITY IMPACT

**Evidence and data.** The interviewed decision-makers highlighted that Keepit enabled their organizations' IT administrators to more quickly find and restore documents, files, and folders that employees lost. Employees mistakenly misplaced everything from files to complete email folders, which can take a long time for IT administrators to locate and then restore. Decision-makers also said that Keepit was also an excellent backup if unhappy employees deleted files deliberately. Interviewees shared how often they need to restore data, and how much time this typically saved.

**Modeling and assumptions.** This benefit was quantified by assuming that:

- IT administrators need to restore an average of one file per 100 users per year. In the case of the composite organization, this equates to 50 restores in Year 1, 55 in Year 2, and 60 in Year 3.
- For each restore, an employee saves an average of 2 hours not having to recreate a lost document, folder, or email.

> **"We lost an important 2 GB file, it would have taken two days to bring it back, but with Keepit it took just minutes. They make it very easy to restore single files and folders."**
>
> *Head of digital workplace and support services, financial services*

**Risks.** Every organization is unique, and some might need to restore data less frequently than the composite organization, lowering this benefit's value.

**Results.** To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of over $8,900.

| SaaS User Productivity Impact | | | | | |
|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Year 1** | **Year 2** | **Year 3** |
| E1 | Number of SaaS users | Composite | 5,000 | 5,500 | 6,000 |
| E2 | Number of restores | Composite | 50 | 55 | 60 |
| E3 | Time saving per restore (hours) | Interviews | 2 | 2 | 2 |
| E4 | Average SaaS user hourly rate (based on fully loaded $100,00 salary) | TEI standard | $73 | $73 | $73 |
| E5 | Productivity conversion factor | TEI standard | 50% | 50% | 50% |
| Et | SaaS user productivity impact | E2*E3*E4 | $3,650 | $4,015 | $4,380 |
| | Risk adjustment | ↓10% | | | |
| Etr | SaaS user productivity impact (risk-adjusted) | | $3,285 | $3,614 | $3,942 |
| | **Three-year total: $10,841** | | | **Three-year present value: $8,934** | |

### UNQUANTIFIED BENEFITS

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

- **Reduced impact of SaaS service outage**. Some of the interviewed decision-makers said that one of the reasons for investing in Keepit was in the event of a SaaS service outage or other technical failure. Such events mean users cannot access SaaS applications or data. Keepit reduces the impact of such an event as IT administrators can provide data access to key users.
- **Better compliance.** The head of digital workplace and support services in the financial services sector highlighted that adopting Keepit made it that their organization could reduce its efforts to demonstrate compliance. There were two reasons for this:
  - The financial regulator requires that organizations in the financial services sector have a clear exit strategy. The organization has to demonstrate they can easily set up their cloud-based core systems on-premises if needed. Keepit provides the organization with access to all the data it needs to set-up email and shared folder repository systems on-premises.
  - Chat-based applications can become an official communications channel. Some users in the financial services organization were reluctant to use chat-based applications for official communications because the messages can easily be deleted. By having a strong backup and restore solution, users felt more confident using more efficient communications tools other than email for some use cases and tasks, knowing that the data is always quickly and easily available.

- **Avoided costs of on-premises back-up.** Decision-makers' organizations that replace their on-premises backup systems with Keepit achieve different benefits, which depend on the relative performance of the two options. However, an on-premises backup solution incurs additional costs including regular maintenance and upkeep of the servers and software that Keepit avoids.
- **Transparent and predictable costs**. Interviewees highlighted that they liked the fact that there were no hidden or variable costs for Keepit. Other backup tools their organizations had used in the past were priced on the amount of storage or data used. This meant that costs could vary from one month to the next and that there could be unexpected additional hidden costs.
- **Reduced reliance on SaaS vendor**. One interviewee told Forrester that one of the reasons their organization choose Keepit was to be less reliant on their SaaS provider. The organization wanted to have a different vendor with a separate copy of the data. Not only does this reduce risks, but it can also help in contract renewal negotiations.

**FLEXIBILITY**

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

- **Reducing reliance on on-premises equipment**. Many organizations are benefiting from the flexibility and efficiency of cloud-based SaaS services. Leveraging technology to become more agile and flexible is typically part of an organization's digital transformation. Using a cloud backup and recovery service such as Keepit is very much in line with such strategies. For instance, as the number of SaaS users increases or decreases, Keepit automatically scales its services up or down as needed without any IT intervention. This also negates the need for upgrading system software and managing infrastructure.

> **"When we merged [with another organization], we did not need to worry about the 15 TB of data from the employees who had left. This saved a lot of uncertainty and cost."**
>
> *Head of digital workplace and support services, financial services*

- **In the event of an acquisition or merger, IT administrators can more easily migrate and consolidate user accounts and data.** As a result, IT teams are more agile and flexible in being able to integrate different systems and data repositories.
- **Using Keepit for additional SaaS services.** Keepit provides backup and recovery for various SaaS solutions. One interviewee told us their organization had to use multiple communications and productivity suites. Keepit makes it easier for IT administrators by letting them use the same backup and recovery solution for both.

> **"There is some benefit in having the same provider across both [productivity suites]."**
>
> *Group head of infrastructure, manufacturing and logistics*

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

# 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** |
| Ftr | Software license fees | $0 | $105,000 | $115,500 | $126,000 | $346,500 | $285,575 |
| Gtr | Other costs | $2,420 | $484 | $484 | $484 | $3,872 | $3,624 |
| | Total costs (risk-adjusted) | $2,420 | $105,484 | $115,984 | $126,484 | $350,372 | $289,199 |

### SOFTWARE LICENSE FEES

**Evidence and data.** Keepit is licensed on a per-user, per-month basis. The monthly rate is constant and does not depend on the amount of storage used or other variables, so IT costs are predictable.

**Modeling and assumptions.** The number of users grows from 5,000 in Year 1 to 5,500 in Year 2 and 6,000 in Year 3. The annual cost per user per year is $20.

**Risks.** Software license fees can vary depending on factors specific to each organization such as regional distribution and size; prices can also change over time.

**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 almost $285,600.

| Software License Fees | | | | | | |
|---|---|---|---|---|---|---|
| **Ref.** | **Metric** | **Source** | **Initial** | **Year 1** | **Year 2** | **Year 3** |
| F1 | Number of SaaS users | Composite | | 5,000 | 5,500 | 6,000 |
| F2 | Cost per user (annual) | Assumption | | $20 | $20 | $20 |
| Ft | Software license fees | F1*F2 | $0 | $100,000 | $110,000 | $120,000 |
| | Risk adjustment | ↑5% | | | | |
| Ftr | Software license fees (risk-adjusted) | | $0 | $105,000 | $115,500 | $126,000 |
| | **Three-year total: $346,500** | | | **Three-year present value: $285,575** | | |

## OTHER COSTS

**Evidence and data.** In addition to the license fees, there were some minimal additional costs associated with the Keepit solution. It is very easy and quick to install and use. One interviewee said the implementation took less than half an hour, and the IT administrators needed just five minutes to becomes familiar with the interface.

> **"There was no training required, the IT admins could all understand it within 5 minutes."**
>
> *IT infrastructure manager, manufacturing industry*

**Modeling and assumptions.** According to the interviewed decision-makers, the average amount of time required for implementation and planning with Keepit was just 15 hours with the exception of one case that took 50 hours. To account for the different experiences, Forrester assumes 40 hours for implementation. The initial back-up time might also vary depending on the data transfer rate.

There is also very minimal ongoing maintenance and administration required, as the Keepit service scales up and down automatically. In the case of the composite organization, Forrester has assumed just 2 hours are required every quarter for an IT administrator, totaling 8 hours per year.

**Risks.** There are several factors that might change how much an organization pays in other costs. This includes differences in time required for implementation, planning, maintenance, and administration.

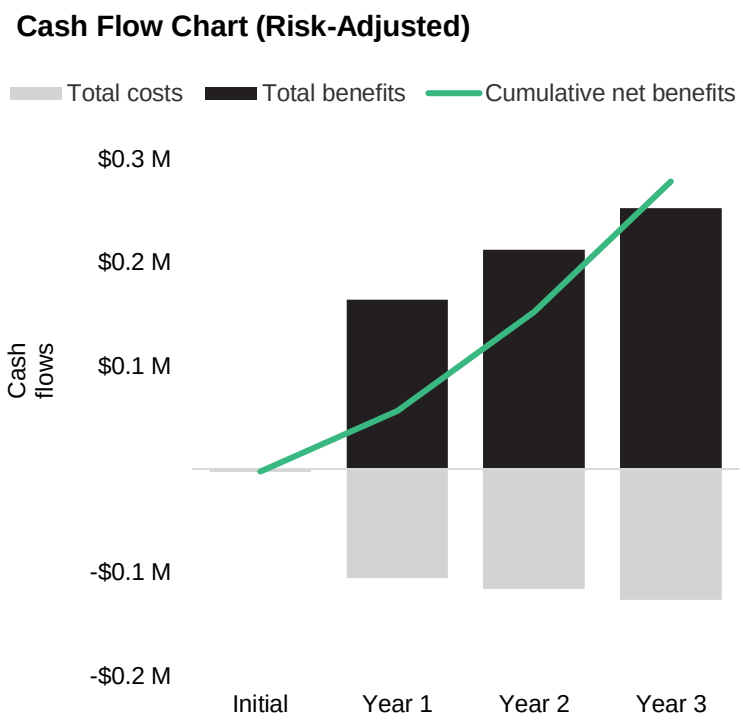
**Results.** To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $3,624.

**Other Costs**

| Ref. | Metric | Source | Initial | Year 1 | Year 2 | Year 3 |
|---|---|---|---|---|---|---|
| G1 | Implementation and planning effort (hours) | Interviews | 40 | | | |
| G2 | Maintenance and administration effort (hours) | Composite | 0 | 8 | 8 | 8 |
| G3 | IT administrator hourly rate (based on fully loaded $75,000 salary) | TEI standard | $55 | $55 | $55 | $55 |
| Gt | Other costs | (G1+G2)*G3 | $2,200 | $440 | $440 | $440 |
| | Risk adjustment | ↑10% | | | | |
| Gtr | Other costs (risk-adjusted) | | $2,420 | $484 | $484 | $484 |
| | **Three-year total: $3,872** | | | **Three-year present value: $3,624** | | |

# 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 | ($2,420) | ($105,484) | ($115,984) | ($126,484) | ($350,372) | ($289,199) |
| Total benefits | $0 | $163,892 | $212,012 | $252,873 | $628,777 | $514,197 |
| Net benefits | ($2,420) | $58,408 | $96,028 | $126,389 | $278,405 | $224,998 |
| ROI | | | | | | 78% |
| 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: Supplemental Material

*Related Forrester Research*

"The State Of Disaster Recovery Preparedness In 2020," Forrester Research, Inc., August 24, 2020.

"Ransomware Is A Business Continuity Issue," Forrester Research, Inc., May 22, 2018.

"Back Up Your SaaS Data — Because Most SaaS Providers Don't," Forrester Research, Inc., December 29, 2017.

## Appendix C: 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: "Internet Crime Report 2020," Internet Crime Complaint Center (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf).

[3] "Source: The State Of Disaster Recovery Preparedness In 2020," Forrester Research, Inc., August 24, 2020.


FORRESTER®