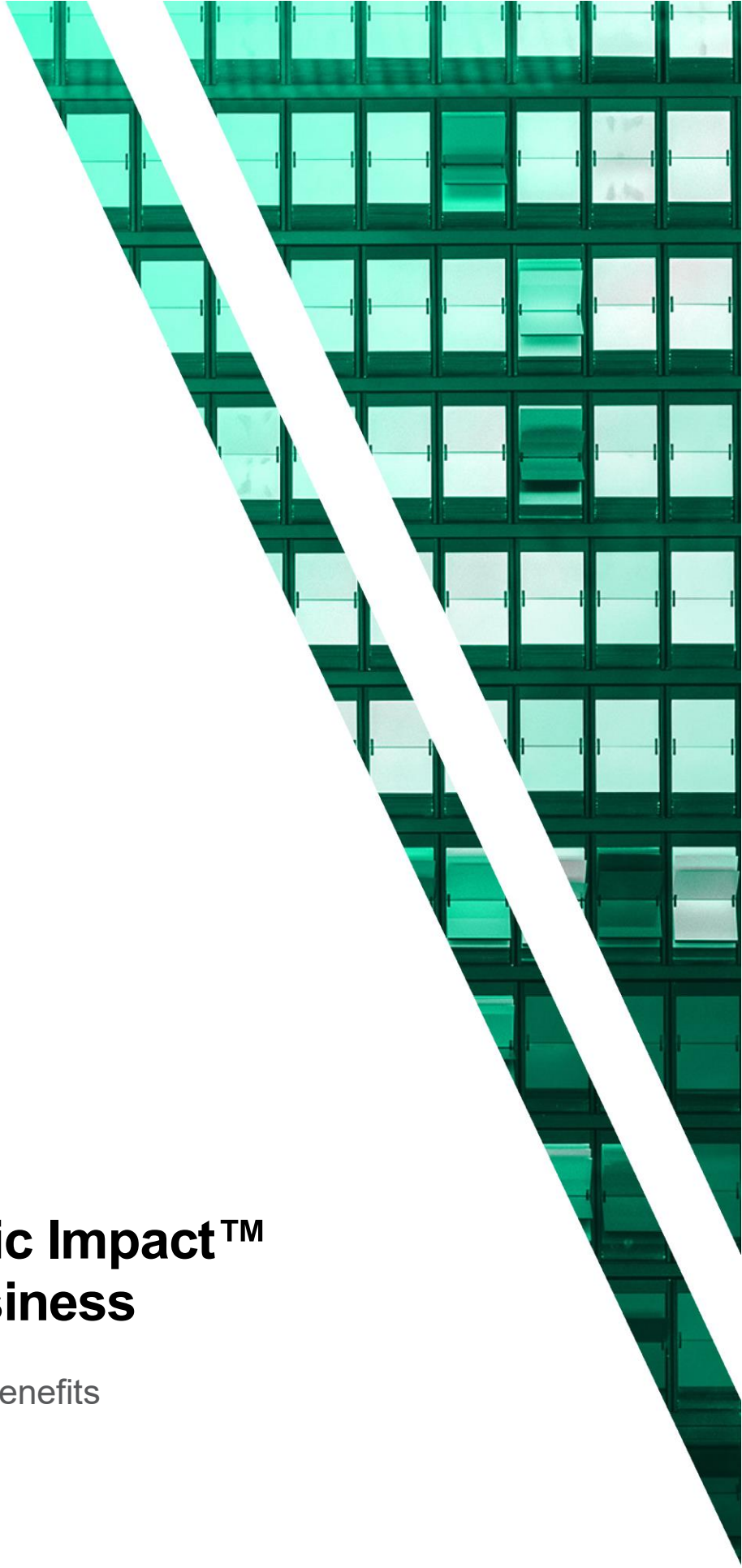
FORRESTER®



The Total Economic Impact™ Of 1Password Business

Cost Savings And Business Benefits Enabled By 1Password

JANUARY 2023

Table Of Contents

Executive Summary 1

The 1Password Business Customer Journey..... 7

Key Challenges 7

Composite Organization 8

Analysis Of Benefits 10

IT Desktop And Mobile Support Team Efficiency Increase From 1Password 10

Employee Productivity Increase Due To 1Password 12

IT Team Productivity Increase From Vaults And Reporting With 1Password 14

Unquantified Benefits.....16

Flexibility 17

Analysis Of Costs 18

Annual License Costs.....18

IT Team Implementation And Ongoing Management Costs 19

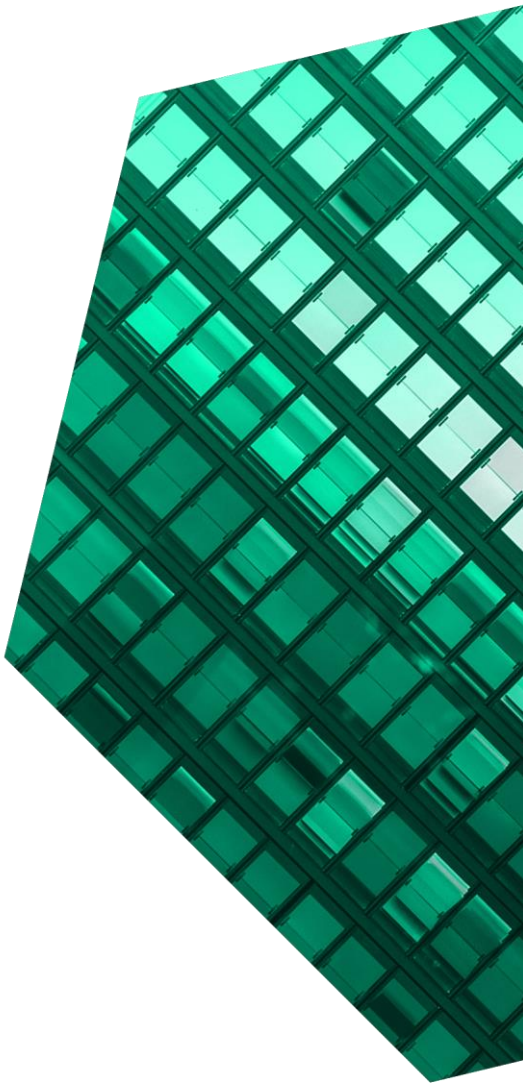
Training For A Fully Integrated Solution 20

Financial Summary 21

Appendix A: Total Economic Impact.....22

Appendix B: Endnotes.....23

Consultant: *Lalé Varoglu*



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and 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. For additional information, go to forrester.com.

Executive Summary

Cybersecurity is paramount as companies transition operations to digital environments, allowing employees to access tools and systems remotely. 1Password Business is an encrypted password solution that provides users with secure access via autofill logins, autogenerated strong passwords, and vault features. 1Password offers these capabilities on any platform or device, promoting global security, increasing IT staff and employee productivity, and helping organizations deliver a high return on investment.

1Password Business is an end-to-end encrypted password solution that creates an improved security environment by providing greater visibility into potential breaches and prompting employees to adopt better password management habits. 1Password achieves this by enabling employees to sign on to all their solutions with just one login, eliminating the need to store, remember, or reuse multiple passwords.

In addition to autofill and autocreation of complex passwords, 1Password also features vaults that allow employees to access shared team applications and services quickly and securely. They can store and share credentials to software solutions, documents, and corporate credit card information. And while 1Password stores customer vault and password data on its proprietary servers, the data is secured with end-to-end encryption, resulting in customer data being inaccessible even to 1Password.

KEY STATISTICS

Return on investment (ROI)
206%

Net present value (NPV)
$853K

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives with experience using 1Password. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization. The composite is an online technology services company, headquartered in North America with global operations. The company generates $350 million in annual revenue, has 1,500 employees, and grows 20% annually during the three-year TEI analysis period.

Total three-year PV benefits

$1.3 million

Prior to 1Password, the security environments of the interviewees' organizations were complex and problematic. Lacking a cohesive password solution, employees often signed in with self-selected password managers, or they stored passwords in spreadsheets, on physical notepads, and on sticky notes. Employees frequently used the same recycled password, sometimes as simple as "password123," for multiple applications with shared access.

According to a 2022 Cost Of A Data Breach report, 19% of security breaches are caused by stolen or compromised credentials, with an average cost of $4.54 million per incident.[2] Forrester analysts estimate that each breach takes approximately 200 days to remediate.

In this prior unsecure password environment, one of the organizations experienced a security breach that caused operational disruptions, data loss, and financial risk, requiring significant resources to resolve.

The interviewees added that this level of exposure also raised GDPR concerns, an increasingly complicated privacy and compliance issue for European customers.

Furthermore, in the absence of a unified password solution, IT teams lacked the visibility and control over their security infrastructure. They spent considerable time solving login- and password-related issues. This was a complex and laborious process and required IT team members to investigate different solutions and involved multiple teams across the company to resolve the issue.

After adopting 1Password Business as a globally integrated solution, the interviewees were able to reduce the security threat exposure of their organizations and gain substantial time and productivity efficiencies for both IT teams and end users.

With the solution, employees replaced lists of passwords with just one, secure 1Password account. They used 1Password's autofill capabilities for online login and account creation. In addition, 1Password's vaults feature gave them the ability to share sensitive information in an automated, safe, and structured way.

1Password enabled the IT team to gain and maintain control and visibility surrounding their employee security for apps, credentials, and logins, enhancing the organization's global security. The IT team became better equipped to resolve login and credential issues in a timely and more proactive manner, helping them to mitigate risk, prevent security breaches, and ensure compliance.

KEY FINDINGS

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

- **Increased efficiency of IT desktop and mobile support team valued at $286,000.** With 1Password, employees are able to log in to websites quickly and create complex passwords. They no longer store their passwords on spreadsheets or notepads, which are frequently lost or forgotten and require IT support intervention to regain system access. As a result, the number of IT helpdesk support tickets is reduced by 70%, creating 291 hours per IT team member annually.

  In addition, 1Password's built-in Insights tool alerts the IT team of weak passwords and compromised websites, so that they can take preventive measures against potential security breaches.

- **Employee productivity increase valued at $158,000.** End users no longer need to remember passwords, maintain lists, or depend on an IT helpdesk support team's schedule to resolve password issues. Processes involving password management are now automated, encrypted, and located in one system, accessible

from any platform or device. Time spent resetting passwords or waiting to gain access to systems is eliminated, saving over 1,400 employee hours a year for the company.

Furthermore, end users receive alerts from 1Password in case of weak or compromised passwords and websites, prompting them to use strong passwords and change their passwords frequently to ensure security of their accounts.

- **IT team productivity increase from vault feature and reporting valued at $408,000.** With 1Password's vault feature, project teams can request that IT engineers create a shared vault to safely store documents, login credentials, confidential information, and tools for team members to access. Before vaults, IT engineers had to research the systems required, collect access credentials, and then set up each team member individually. The ability to create a dedicated vault streamlines the employee onboarding process and saves 416 hours per involved IT team member annually.
- **Employee efficiency increase from 1Password vaults valued at $414,000.** Rather than storing and sharing private information in an email, worksheet, or sticky note, which leads to spending extra time locating information, as well as dealing with issues when information is misplaced, 1Password allows employees the ability to access and share sensitive information such as login data and documents in a secure manner.

  In addition, IT managers are able to onboard team members to a project vault quickly, such as granting access to the information, solutions, and tools required for their individual projects, resulting in a total time savings of 3,750 employee hours per year.

Unquantified benefits. Benefits that provide value for the composite organization but are not quantified in this study include:

- **Increased security breach avoidance through visibility, control, and enhanced employee experience.** 1Password's built-in Insights tool notifies the IT team and the end user when an email address or password is compromised, enabling them to act quickly.

  Also, 1Password provides the IT teams with the ability to integrate their own control systems directly into the solution, giving them additional visibility and control. Having a cohesive, streamlined, and secure solution deployed across the organization, the IT team is able to focus on higher-value tasks, resulting in improved end user engagement and satisfaction.
- **Ability to do more with fewer systems.** With 1Password, the IT team establishes one enterprise account and shares login credentials and MFA codes instead of each individual employee signing up for numerous apps and services independently.

  Organizations have more flexibility in how they manage access to apps and are less susceptible to upgrade charges for single sign-on (SSO) when purchasing additional software from third-party vendors, while maintaining the same level of security.
- **Creation of time savings for developers.** Developers can secure their credentials in 1Password and then access throughout their code and development environments via references.

  Using 1Password as a central source of truth eliminates plaintext secrets in code, which helps reduce errors and streamlines updating and sharing credentials across teams.

- **Cultivating strong partnerships with customers.** 1Password establishes deep, long-term relationships with its customers, is responsive to their needs, and builds innovative solutions accordingly.
- **Ability to create and teach security hygiene at home.** 1Password's extended coverage to employees' families not only creates a secure digital environment at home but also equips them to teach better security practices to their children, keeping their families safe.

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

- **Licensing costs are $340,000 over three years.** 1Password Business' licensing fee totals $66 per user per year. Forrester determines that this price is a reasonable estimate for the size of the composite. 1Password has additional pricing options[3].
- **The IT team's implementation and ongoing management costs amount to $38,000 over three years.** In the beginning, two IT managers and one senior procurement officer are involved in preparing internal documentation, coordinating with the 1Password team, and granting initial access. The composite provides all training in-house.
- **Training for a fully integrated solution costs $36,000 over three years.** The composite organization achieves an 87% adoption rate in the first year with 1Password Business. To migrate employees from a previous password manager typically takes about 30 minutes, including training and setup. Employees with no password manager experience require about 1 hour to train.

  As the company grows 20% annually, each new employee onboarded to 1Password requires a 30-minute training.

The representative interviews and financial analysis found that a composite organization experiences benefits of $1.3 million over three years versus costs of $414,000, adding up to a net present value (NPV) of $853,000 and an ROI of 206%.

ROI
206%

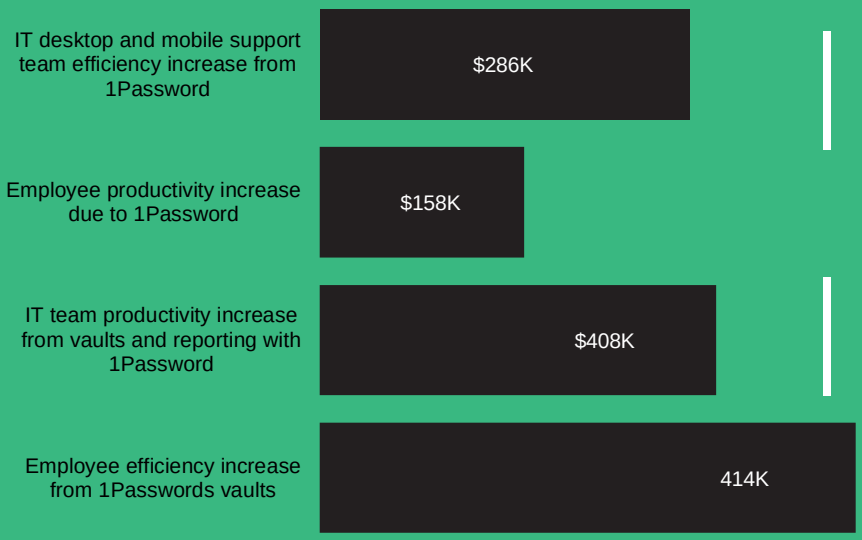
BENEFITS PV
1.3M

NPV
$853K

PAYBACK
<6 months

HELPDESK TICKET REDUCTION
70%

Benefits (Three-Year)



With 1Password, total employee efficiency increased by 4,310 hours per year from password reset related issues.

With 1Password's vault feature, the composite organization saved close to 8,000 employee hours per year.

"1Password carved itself a niche; nothing else offers the same functionality such as security (login and vault), ease of use, and scalability for password management."

— IT manager, fintech

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 1Password Business.

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 1Password can have on an organization.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by 1Password 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 1Password Business.

1Password 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.

1Password provided the customer names for the interviews but did not participate in the interviews.

DUE DILIGENCE

Interviewed 1Password stakeholders and Forrester analysts to gather data relative to the Business solution.

INTERVIEWS

Interviewed six representatives at organizations using 1Password Business 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.

The 1Password Business Customer Journey

Drivers leading to the 1Password investment

Interviews			
Role	**Industry**	**Region**	**Number Of Employees**
IT manager	Fintech	HQ in North America	1,500
IT manager	Cybersecurity	HQ in Europe with global operations	380
IT manager	Cybersecurity	HQ in Europe with global operations	380
Senior director, communications	Cybersecurity	HQ in Europe with global operations	380
IT manager	Consulting	HQ in North America with global operations	1,300
IT manager	Educational technology	HQ in North America with global operations	1,700

KEY CHALLENGES

Prior to 1Password Business, the interviewees' organizations lacked a global, unified password solution, creating potential vulnerabilities in their security environment. As a result, some found their own solutions to remember their login information, such as downloading a password manager for individual or team use. This method led to the deployment of multiple and unmanaged password solutions across the organization.

Others maintained lists of passwords on spreadsheets and notepads, or they placed handwritten sticky notes on laptops. Additionally, and even less secure, many created easily predictable passwords, such as "password123," and used the same ones repeatedly, exposing organizations to security risk.

The interviewees' organizations shared common challenges prior to the use of 1Password, including:

- **Increased concern over employee security, data breaches, and GDPR compliance.** In the absence of a centralized, cohesive password manager used across the organization, management was concerned about the methods employees adopted to manage passwords, credentials, and sensitive login data. One of the interviewees reported a security breach, which was time-consuming to resolve and raised GDPR compliance concerns.
- **Reduced employee productivity due to password- and login-related issues.** The amount of time to reset an end user's password depended on the IT helpdesk support's queue, project load, and priorities. In the legacy environment, the helpdesk support team was overburdened by the number of daily tickets

> **"1Password created better password management habits and a more secure technology environment."**
>
> *IT manager, educational technology*

"The benefits of 1Password are not just-in-time saving efficiencies. It is increasing the security of our internal systems."

IT manager, consulting

requesting password resets, resulting in significant, unproductive downtime for the impacted end users. End users requesting resets could not get back to work until their issues were resolved.

- **Little visibility or control over the global security environment.** IT managers required complete access to manage and control all the systems and accounts in their organization. Prior to 1Password Business, they lacked the visibility to determine the available systems, manage user credentials, and distribute access to respective groups. This information was not readily available, and considerable research was required to gather this data and create alignment among teams.
- **Security concerns over previous password solutions.** Due to the high-risk nature of their data, the interviewees proactively tracked their password managers' performance on well-known security advisory websites, which regularly report current security vulnerabilities. When they realized that the prior solutions created vulnerabilities and security gaps, they sought a new platform.

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Be implemented across the business easily, eliminating security vulnerabilities.
- Integrate seamlessly with common web browsers and be accessible from any platform or application.
- Enable users to manage, store, and share sensitive information and secrets.

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 six 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. The composite is a global online technology services company, headquartered in North America, with $350 million annual revenue, 1,500 employees, and an annual 20% growth rate. The number of helpdesk and mobile support staff totals 10.

Deployment characteristics. The composite objective is to integrate 1Password Business globally at an adoption target rate of 85% to 90% within three years. Three hundred employees are already existing users of 1Password. In Year 1, 1,000 employees

Key Assumptions

- **$350 million in revenue**
- **1,500 employees globally**
- **20% annual growth**
- **IT support team is 10 people**
- **Multiple security solutions in place (SSO, MFA, 2FA)**
- **1Password adoption target is 85% to 90% over three years**

migrate to 1Password and are fully trained, including 200 employees without any prior password manager experience. As the company grows, in Years 2 and 3, all new employees are onboarded to 1Password.

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	IT desktop and mobile support team efficiency increase from 1Password	$96,824	$116,189	$135,554	$348,566	$285,889
Btr	Employee productivity increase due to 1Password	$52,815	$63,504	$76,416	$192,734	$157,908
Ctr	IT team productivity increase from vaults and reporting with 1Password	$138,320	$165,984	$193,648	$497,952	$408,413
Dtr	Employee efficiency increase from 1Passwords vaults	$138,938	$166,725	$200,070	$505,733	$414,412
	Total benefits (risk-adjusted)	$426,896	$512,402	$605,687	$1,544,985	$1,266,622

IT DESKTOP AND MOBILE SUPPORT TEAM EFFICIENCY INCREASE FROM 1PASSWORD

Evidence and data. The interviewees stated that the adoption of 1Password Business across the organization led to significant productivity increase for their IT team.

- With 1Password's ability to autofill, save, and create passwords, employees only needed to know their single 1Password account rather than trying to maintain lists of login information in spreadsheets, notebooks, and notepads. As a result, the number of tickets submitted to IT desktop and mobile support for password resets dropped significantly.
- In addition, IT teams found 1Password's random password generation functionality very beneficial. Each IT team member was able to automatically create very strong passwords and securely share them with the team to administer their interfaces.

  Having an accessible and secure password manager for teams/projects saved IT managers time from having to research, locate, and distribute login credentials, leading to increased productivity. An IT manager from a fintech company noted that "1Password had been a core staple of our environment for many years."
- 1Password's domain breach report alerts the IT team of weak passwords and compromised websites, so that they can take proactive measures against any potential security breaches quickly and ensure password compliance across their organization.
- 1Password Business also allowed IT teams to perform additional tasks with ease, such as creating and distributing shared login information to websites, tools, and private online events.

> **"I can't remember how many times I've shown people how to quickly generate the new password within 1Password, which is to me, super, super quick and easy."**
>
> *IT manager, cybersecurity*

Modeling and assumptions. Based on the customer interviews, Forrester estimates the following for the composite organization:

- The composite uses 1Password Business in addition to other authentication methods such as SSO, 2FA, and MFA.
- In the prior legacy environment, the IT desktop and mobile support team dedicates 20% of time to password resets.
- With 1Password Business, the IT desktop and mobile support team is able to reduce tickets and increase team efficiency by 70%.
- Total time savings for the IT support team amounts to 2,910 hours per year.

Risks. The realization of this benefit will vary with:

- The size of the organization and the IT desktop and mobile support team.
- The 1Password adoption rate across the organization.
- Salary levels, depending on skills and geographical location.

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 $286,000.

IT Desktop And Mobile Support Team Efficiency Increase From 1Password

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	IT desktop and mobile support team full-time equivalent (20% annual growth)	Composite	10	12	14
A2	Percent of time spend on password resets	Interviews	20%	20%	20%
A3	Average hourly rate per fully burdened IT generalist	TEI standard	$35	$35	$35
A4	Percent captured with 1Password	Interviews	70%	70%	70%
At	IT desktop and mobile support team efficiency increase from 1Password	A1*A2*A3* A4*2,080	$101,920	$122,304	$142,688
	Risk adjustment	↓5%			
Atr	IT desktop and mobile support team efficiency increase from 1Password (risk-adjusted)		$96,824	$116,189	$135,554
	Three-year total: $348,566		**Three-year present value: $285,889**		

EMPLOYEE PRODUCTIVITY INCREASE DUE TO 1PASSWORD

- **Evidence and data.** Interviewees stated that their organizations adopted 1Password Business to increase employee security; however, they experienced additional uses and benefits from the solution.
- The employees used 1Password for its autofill login and complex password creation capabilities, no longer keeping sensitive information in spreadsheets or physical notepads. An IT manager at an educational technology organization noted: "When you enter a new username and password for a site, it prompts you to save it in 1Password; that's just a time-saver. You don't have to open the tool, add the site, add username and password, it just dynamically does that."
- 1Password login information saved to the app or website in form of credentials and passwords provided quick and easy sign-on experience.
- 1Password notified end users of any login abnormalities and compromised credentials or websites, granting them visibility into their own security breach risk exposure and instilling better password management habits.
- The employees no longer depended on IT desktop support's timelines to reset their passwords.
- 1Password's license includes separate family accounts for personal use, further reducing the risk from being victims to hacking or malware at home.

> **"One of the reasons we use 1Password software is because we have very high levels of trust in the system and the service."**
>
> *IT manager, fintech*

Modeling and assumptions. Based on customer interviews, we assume the following for the composite organization:

- The composite achieves an 87% adoption rate with 1Password in its first year.
- The organization experiences a 70% reduction in password reset issues due to an effective 1Password implementation, saving 1,400 employee hours annually.
- The employee productivity realization factor considers that the time employees save from login-related issues may not directly translate to a productivity increase.

Risks. The optimization of this benefit will vary with:

- The organization's security structure and its legacy password manager solutions.
- 1Password adoption levels.
- The size of the organization, number of its employees, and its growth rate.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $158,000.

Employee Productivity Increase Due To 1Password

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Total number of full-time employees excluding desktop and mobile support (20% annual growth)	Composite	1,500	1,800	2,160
B2	Number of login/password issues before 1Password (per week)	Composite	135	162	194
B3	Percent reduction in password-related issues	Interviews	70%	70%	70%
B4	Number of login/password issues with 1Password (per week)	B2*(1-B3)	41	49	58
B5	Average time spent in restoring passwords (minutes)	Composite	35	35	35
B6	Total time savings from resolving password issues due to 1Password (in hours)	(B2-B4)* (B5/60)*52	2,851	3,428	4,125
B7	Employee productivity realization factor	TEI standard	50%	50%	50%
B8	Average hourly rate per fully burdened business user	TEI standard	$39	$39	$39
Bt	Employee productivity increase due to 1Password	B5*B6*B7	$55,595	$66,846	$80,438
	Risk adjustment	↓5%			
Btr	Employee productivity increase due to 1Password (risk-adjusted)		$52,815	$63,504	$76,416
	Three-year total: $192,734	**Three-year present value: $157,908**			

IT TEAM PRODUCTIVITY INCREASE FROM VAULTS AND REPORTING WITH 1PASSWORD

Evidence and data. IT teams set up 1Password vaults to create a secure solution to store credentials, share information, and manage secrets, login data, credit card numbers, and passwords.

- With 1Password, creating a shared vault and assigning end users were seamless processes compared to the work that would be required to set up the system each time a team needed a solution in place.
- Through the vault's search function, the IT team located necessary information in a faster and more effective manner.
- 1Password's reporting feature gave interviewees additional visibility to login and system access activity and ensured compliance with company policies.

Modeling and assumptions. The composite organization's IT team saves a total of 8 hours per week from vault and reporting capabilities, including:

- The ability to create shared vaults for project teams allows the desktop support team to save 6 hours per week per team member.
- Two hours are saved per week per desktop support team member with automated reporting tools. Login reporting in the previous environment required team members to gather the relevant data manually from individuals separately.
- Onboarding and offboarding is easier and faster.
- Total time savings for the IT team amounts to 4,160 hours annually.

Risks. The optimization of this benefit will vary with:

- The size of the IT team dedicated to 1Password.
- The level of deployment of the solution.
- The number of employees and projects an IT engineer needs to set up annually.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $408,000.

> **"In IT, we have a bunch of locally running tools where we'll have shared credentials. So, using the shared vault allows us to secure them properly and easily share that information."**
>
> *IT manager, consulting*

IT Team Productivity Increase From Vaults And Reporting With 1Password

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	IT desktop and mobile support team full-time equivalent	A1	10	12	14
C2	Average hourly rate per fully burdened IT generalist	TEI standard	$35	$35	$35
C3	Time saved by creating shared vaults and reporting with 1Password (per week)	Interviews	8	8	8
Ct	IT team productivity increase from vaults and reporting with 1Password	C1*C2*C3*52	$145,600	$174,720	$203,840
	Risk adjustment	↓5%			
Ctr	IT team productivity increase from vaults and reporting with 1Password (risk-adjusted)		$138,320	$165,984	$193,648
	Three-year total: $497,952		**Three-year present value: $408,413**		

EMPLOYEE EFFICIENCY INCREASE FROM 1PASSWORDS VAULTS

Evidence and data. In addition to IT team efficiencies, the organizations' end users significantly benefitted from the vault feature. The interviewees reported:

- End user productivity increased because onboarding was a secure one-time event that no longer required researching and identifying adequate tools and provisioning access individually. In the absence of the vault capability, granting access and permissions was chaotic and laborious, and the methods used to share information unsecure.
- In addition, each employee received access to a private, personal vault, which is viewable only by the owner and where login credentials, corporate credit cards, confidential information, and other sensitive documents can be safely stored.

Modeling and assumptions. The composite organization estimates:

- Each employee saves approximately 5 hours per year from having immediate automated access to their shared systems and documents.
- The total employee time savings from vaults are 3,750 hours per year.

> **"For our project teams, they put in a simple request to IT, IT creates a shared vault, adds the users and they're ready to go. And so, it's a pretty seamless process."**
>
> *IT manager, consulting*

Risks. The ability to optimize these benefits will vary with:

- The size of the organization and workforce.
- The rate of deployment of 1Password's vault feature and integration with other security solutions.
- The number of IT employees assigned to support 1Password, their hourly rate, skill level, and geographical location.

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $414,000.

Employee Efficiency Increase From 1Password's Vaults					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of employees	B1	1,500	1,800	2,160
D2	Time saved by using 1Password's vault feature (in hours)	Interviews	5	5	5
D3	Total time saved by using vaults (in hours)	D1*D2	7,500	9,000	10,800
D4	Average hourly rate per fully burdened business user	TEI standard	$39	$39	$39
D5	Employee productivity realization factor	TEI standard	50%	50%	50%
Dt	Employee efficiency increase from 1Password's vaults	D3*D4*D5	$146,250	$175,500	$210,600
	Risk adjustment	↓5%			
Dtr	Employee efficiency increase from 1Passwords vaults (risk-adjusted)		$138,938	$166,725	$200,070
	Three-year total: $505,733		**Three-year present value: $414,412**		

UNQUANTIFIED BENEFITS

Customers experienced additional benefits that provide value for the composite but were not able to quantify include:

- **Increased security breach avoidance through visibility, control, and enhanced employee experience.** According to IBM's 2022 cost of a data breach report[2], use of stolen or compromised credentials remains the most common cause of a data breach and is considered the primary attack vector.

  1Password's built-in Insights tool notifies the IT team and the end users when an email address is used to access a compromised website or if there are multiple passwords being reused on multiple devices, enabling team members to take the necessary action quickly.

  Also, the organizations' IT teams can integrate security information and event management (SIEM) control systems directly into 1Password to read logins, audit logs, and locations. This equips them with additional clarity, visibility, and control, promoting satisfaction in their day-to-day operations.

- **Ability to do more with fewer systems.** 1Password enables interviewees' organizations to store and share login credentials and MFA codes in a secure centralized manner, replacing the need for employees to purchase their own apps and solutions independently.

> **"1Password's domain breach report enabled us to identify potential password breaches and helped us avoid any incidents."**
>
> *IT manager, educational technology*

In addition, organizations have more flexibility in how they manage credentials and access for apps and are less susceptible to SSO upgrade charges with third-party software vendors. An IT manager at a fintech company stated, "From a security perspective, 1Password allows us to store MFA codes and maintain an equal level of security while we spend less money to get the service we need from that third party."

- **Creation of time savings for developers.** Developers can secure their credentials in 1Password and then access throughout their code and development environments via references. Using 1Password as a central source of truth eliminates plaintext secrets and helps reduce errors in code.

  This process not only streamlines updating and sharing credentials across teams but also improves security. According to an IT manager at an educational technology company: "It's primarily a security gain. If somebody was to hack into our system, they're not going to be exposed to any of those credentials which are securely stored and accessed through 1Password."

- **Cultivating strong partnerships with customers.** 1Password establishes robust relationships with its customers and prioritizes innovations based on their needs and future technology. An IT manager at a cybersecurity company stated, "We work with a lot of different companies and vendors, and I can't think of one that we have a better relationship with than the one we have one with 1Password."

- **Ability to create and teach security hygiene at home.** 1Password's extended coverage to employees' families not only creates a secure digital environment at home but also equips them to teach better security practices to their children, keeping their families safe.

FLEXIBILITY

The value of flexibility is unique to each customer. There are multiple scenarios in which a customer might implement 1Password Business and later realize additional uses and business opportunities, including:

- **Comfort and peace of mind with 1Password.** With the integration of necessary controls, oversight, and reporting features**,** interviewees stated that IT security team members feel more comfortable with day-to-day operations. 1Password gave them peace of mind because employees were using a more secure solution to sign in and share data.

  1Password's end-to-end encryption gave employees an extra layer of protection and secure access to any application or service, allowing individuals and teams to safely share sensitive information.

- **Ability to store highly secure credentials creates agility.** With 1Password, IT managers can store API credentials, which provides agility for those teams, ensures that their own offering is functioning more smoothly, and simplifies their workflows.

- **Accessing 1Password from any device or operating system promotes flexibility.** The ability to access 1Password from desktop or mobile and from any operating system provides the end users and the IT team with enhanced flexibility, while keeping information secure.

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**
Etr	Annual license costs	$0	$113,850	$136,620	$163,944	$414,414	$339,583
Ftr	IT team implementation and ongoing management costs	$23,288	$9,660	$3,864	$3,864	$40,676	$38,166
Gtr	Training for a fully integrated solution	$0	$24,570	$11,057	$6,143	$41,769	$36,089
	Total costs (risk-adjusted)	$23,288	$148,080	$151,541	$173,951	$496,859	$413,838

ANNUAL LICENSE COSTS

Evidence and data. Interviewees noted that after migrating to 1Password, their organizations' cost savings from discontinued solutions were offset by the significant increase in the number of users.

Modeling and assumptions. Based on the customer interviews, Forrester estimates the following for the composite organization:

- The composite's first year annual license costs for 1Password Business solution are $99,000.
- The composite's global security objective is to implement 1Password at an adoption rate of 85% to 90%. The organization issues all employees a license to access password management and vault features.

Risks. Licensing fees may vary depending on:

- The size of the organization.
- The number of employees migrating to 1Password.
- The organizational security objectives, rate of adoption, and commitment to achieve it.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $340,000.

Annual License Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Business license fee per year	1Password		$66	$66	$66
E2	Number of licenses	Composite		1,500	1,800	2,160
Et	Annual license costs	E1*E2	$0	$99,000	$118,800	$142,560
	Risk adjustment	↑15%				
Etr	Annual license costs (risk-adjusted)			$113,850	$136,620	$163,944
	Three-year total: $414,414			**Three-year present value: $339,583**		

IT TEAM IMPLEMENTATION AND ONGOING MANAGEMENT COSTS

Evidence and data. Organizations deployed 1Password gradually over a period of six to nine months to ensure its success.

- The initial implementation process required that the IT team act as champions of 1Password to influence leaders and employees to "buy in," as the migration was optional, not obligatory.
- All organizations opted for in-house training based on 1Password videos, documents, and other materials. IT managers also created shared vaults for teams, projects, and onboarding processes across the organization.
- Once the systems were in place, ongoing management was minimal and limited to onboarding, offboarding, and troubleshooting.

Modeling and assumptions. For the financial analysis, Forrester assumes:

- Deployment requires three people: two IT managers and one senior procurement officer to prepare internal documentation, coordinate with 1Password, and gain preliminary access.
- In the first year, IT staff deploys 1Password to end users by setting up internal training platforms and promotional campaigns, sending invites for end users, and providing instructions and documentation.
- In Years 2 and 3, the training platform and internal educational campaigns are established; IT team members primarily focus on onboarding new employees and troubleshooting any issues.

Risks. Implementation costs may vary due to the size of the organization and the IT team, salary and skill levels, and geographical location. Additionally, the level of IT commitment can impact the speed of adoption, training, and implementation.

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $38,000.

IT Team Implementation And Ongoing Management Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Number of full time equivalent (FTE) deploying 1Password	Composite	3			
F2	Hourly rate per person of a fully burdened IT managers and team working on implementation	TEI standard	$45			
F3	Total hours for the initial implementation per person (over 3-to-6-month period)	Interviews	150			
F4	Subtotal: Implementation costs	F1*F2*F3	$20,250			
F5	Number of full time equivalent (FTE) managing 1Password	Composite		2	2	2
F6	Hourly rate per IT managers and team managing 1Password	TEI standard		$35	$35	$35
F7	Number of hours per IT resource (monthly)	Interviews		10	4	4
F8	Subtotal: Ongoing management costs	F5*F6*F7		$8,400	$3,360	$3,360
Ft	IT team implementation and ongoing management costs	F4+F8	$20,250	$8,400	$3,360	$3,360
	Risk adjustment	↑15%				
Ftr	IT team implementation and ongoing management costs (risk-adjusted)		$23,288	$9,660	$3,864	$3,864
	Three-year total: $40,676			**Three-year present value: $38,166**		

TRAINING FOR A FULLY INTEGRATED SOLUTION

Evidence and data. The interviewees stated that:

- The initial deployment was conducted with a small employee base and subsequently expanded to other employees.
- The ease of migration from another solution was contingent on the existence and efficacy of an outgoing solution's export function that rendered the process seamless.
- Each employee's training varied according to the level of familiarity with password managers. The employees with previous password manager experience took 30 minutes to 1 hour to train, and the ones lacking previous experience required 1 to 2 hours.

Modeling and assumptions. The composite organization is an online technology services company. The employees are proficient in using various password solutions.

- The employees 86% adoption rate of 1Password is as follows: 20% of employees are previous 1Password subscribers, 53% have experience with other password solutions, and 13% have no experience using a password manager.
- The employees receive training according to their expertise with a password manager.

Risks. The training costs will vary with the size of the company, its industry, and culture, such as:

- The types of solutions to be replaced.
- The organization's and employees' commitment to adopt 1Password.
- The availability and deployment of the tools and systems necessary to achieve their objectives.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $36,000.

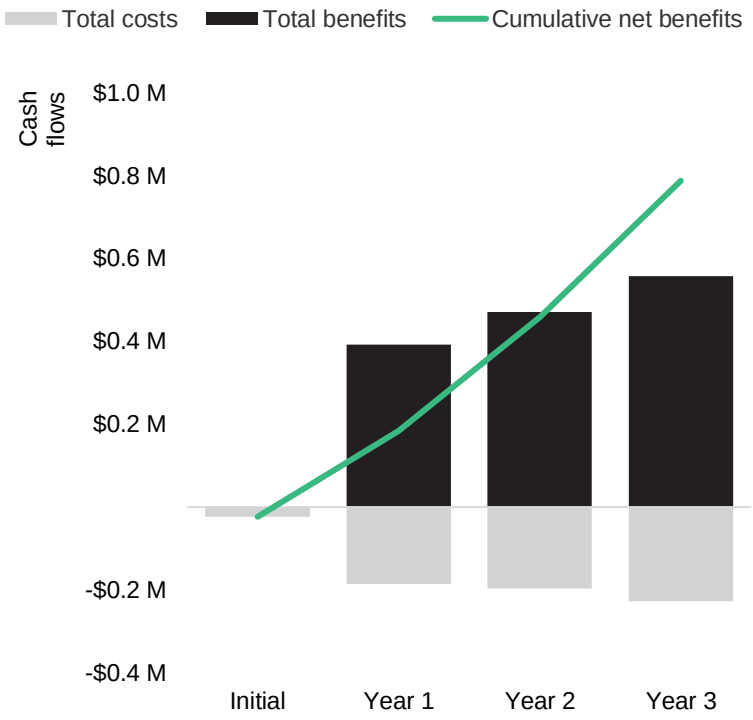
Training For A Fully Integrated Solution

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Number of employees migrating from another password solution	Composite		800	540	300
G2	Training and setting up (in hours)	Interviews		0.5	0.5	0.5
G3	Total hours spent for adoption	(G1*G2)		400	270	150
G4	Number of employees being introduced to a password solution for the first time	Composite		200		
G5	Training and setting up (in hours)	Interviews		1.0		
G6	Total hours spent for adoption	G4*G5		200		
G7	Average hourly rate per fully burdened business user	TEI standard		$39	$39	$39
Gt	Training for a fully integrated solution	(G3+G6)*G7	$0	$23,400	$10,530	$5,850
	Risk adjustment	↑5%				
Gtr	Training for a fully integrated solution (risk-adjusted)		$0	$24,570	$11,057	$6,143
	Three-year total: $41,769			**Three-year present value: $36,089**		

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, 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 and 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	($23,288)	($148,080)	($151,541)	($173,951)	($496,859)	($413,838)
Total benefits	$0	$426,896	$512,402	$605,687	$1,544,985	$1,266,622
Net benefits	($23,288)	$278,816	$360,861	$431,737	$1,048,127	$852,784
ROI						206%
Payback period (months)						<6

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: "Cost of a data breach 2022," IBM Security, July 2022.

[3] 1Password Business pricing options.


FORRESTER®