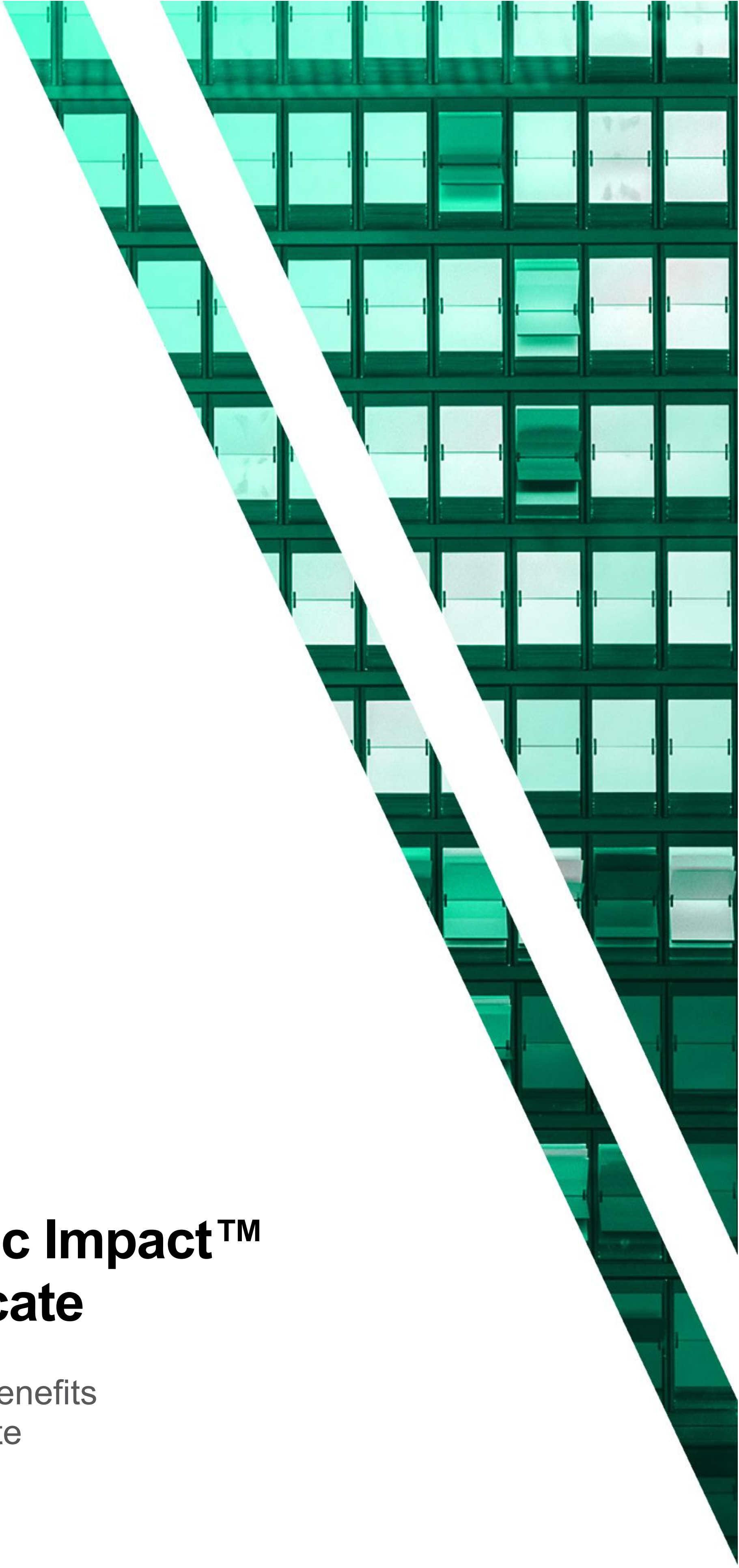
FORRESTER®



The Total Economic Impact™ Of HYPR Authenticate

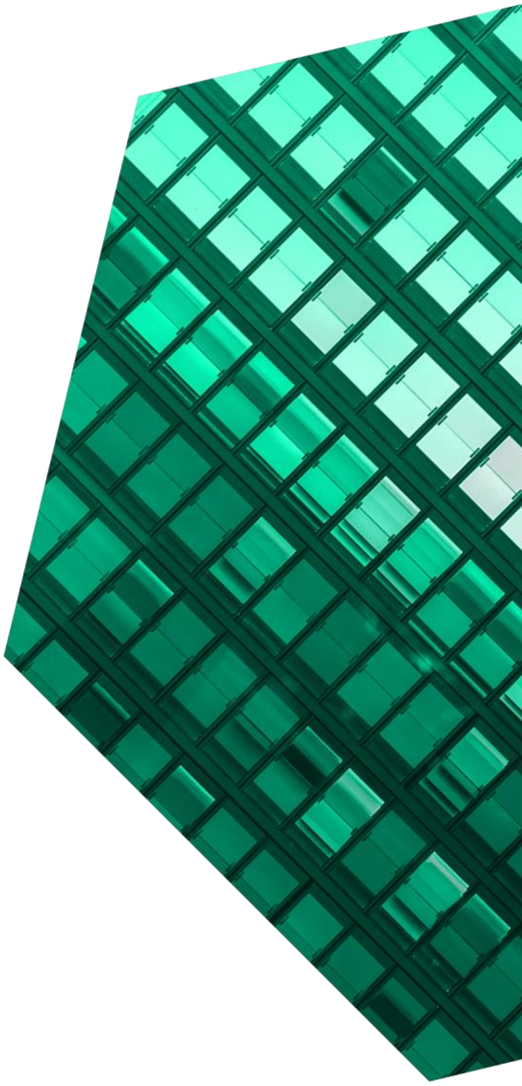
Cost Savings And Business Benefits Enabled By HYPR Authenticate

JULY 2023

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY HYPR

Table Of Contents

Consulting Team: Nikoletta Stergiou
Adam Birnberg



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

Poor workforce password habits undermine the minimum level of security provided by passwords. Passwords drive up operational/help desk costs, sap user productivity, and, when compromised, they can lead to data breaches that damage brand reputation and lead to potential monetary fines.[1] HYPR Authenticate eliminates password use in organizations through a simple, secure passwordless authentication that strengthens security and improves the user experience.

HYPR Authenticate is a simple, secure passwordless authentication solution that conforms to the Fast Identity Online (FIDO) standard recognized by the Cybersecurity and Infrastructure Security Agency (CISA) as the standard for Zero Trust authentication. The solution enables security assurance by eliminating password use and push attacks by putting the user in control and providing a consumer-grade experience through rapid deployment and improved user experience.

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed six representatives of five organizations with experience using HYPR Authenticate. For the purposes of this study, Forrester aggregated the interviewees’ experiences and combined the results into a single composite organization that is highly regulated with $5 billion in annual revenue and 10,000 employees.

KEY STATISTICS

Return on investment (ROI)
324%

Net present value (NPV)
$6.19M

Eliminated password use with HYPR

80%

Interviewees noted that prior to using HYPR Authenticate, their organizations utilized single sign-on (SSO) with passwords and multi-factor authentication (MFA) solutions. In some cases, employees used one-time password (OTP) hard tokens to log into various systems. However, prior attempts yielded limited success, which left interviewees’ organizations with poor user experiences, weak password practices, and frequent and time-consuming password reset and onboarding processes. These practices led to security vulnerabilities, high help desk costs, and end-user downtime that impacted business productivity.

After the investment in HYPR Authenticate, the interviewees' organizations eliminated more than 70% of password use in Year 1, reduced the number of authenticators in their environments, reduced the overall number of password resets, and improved their overall security postures. Key results from the investment include business risk avoidance, help desk support cost reduction, end-user productivity improvement, employee onboarding efficiencies, technology consolidation savings, and reductions in phishing investigations.

KEY FINDINGS

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

- **An 80% reduction of password use that results in business risk avoidance.** The elimination of passwords across the composite organization reduces the risk of attacks related to weak or stolen credentials and phishing, and the organization strives for 100% password elimination. Over three years, business risk avoidance is worth more than $2.7 million to the composite organization.

- **A 95% reduction to help desk support costs related to passwords.** Prior to using HYPR, 50% of the composite's help desk tickets were related to manual administrative password resets. As more users in the organization adopt HYPR, there are fewer help desk tickets related to password resets. Over three years, these avoided support costs are worth more than $2.5 million to the composite organization.

- **End-user productivity savings of nearly $2.7 million due to faster authentication and reduction of password resets.** End-user downtime decreases with less time spent on help desk tickets related to password resets. Furthermore, HYPR Authentication is faster per login than the composite's prior environment. Over three years, end-user productivity savings are worth more than $2.6 million to the composite organization.

- **55% reduction in the time required to onboard new employees who require OTP hard tokens.** Ten percent of the composite's employees require an OTP hard token to access certain applications and systems. With HYPR, the organization eliminates its OTP hard token usage, which increases onboarding efficiencies. Over three years, these efficiencies are worth nearly $61,900 to the composite.

- **Hard-token consolidation savings due to 95% adoption of HYPR.** With HYPR, the composite's end users no longer need OTP hard tokens, which saves the organization on the cost of physical tokens. Over three years, these consolidation savings are worth more than $99,300 to the composite.

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

- **Avoided phishing investigation and response costs.** Passwords leave organizations vulnerable to phishing attacks. With reduced reliance on passwords with HYPR, the composite organization avoids costs associated with account takeover, including costs for phishing investigation and incident response. Depending on the severity and frequency of attacks, these costs can be significant.

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

- **Licensing costs of $1.4 million.** The composite organization uses HYPR's standard licensing, which is based on a per-user basis, but volume pricing is available for larger organizations through enterprise agreements. Over three years, licensing costs are $1.4 million for the composite organization.

- **Deployment costs of $77,000.** The composite's deployment requires several hundred hours because it needs to take change-management steps to promote HYPR adoption across the organization. Initial deployment costs are $77,000 to the composite organization.
- **Ongoing management and end-user training costs totaling $441,000.** A security engineer is responsible for the composite's ongoing management of the HYPR solution. End users find the training to be straightforward, so it requires minimal effort. Over three years, ongoing management and end-user training costs are $441,000 to the composite organization.

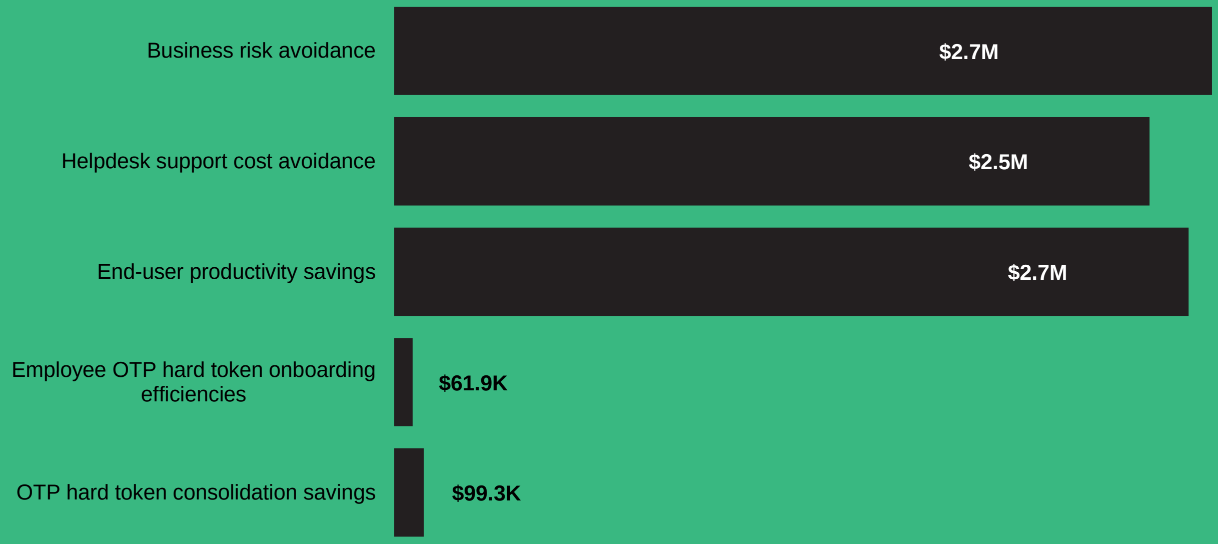
The representative interviews and financial analysis found that a composite organization experiences benefits of $8.10 million over three years versus costs of $1.91 million, adding up to a net present value (NPV) of $6.19 million and an ROI of 324%.

ROI
324%

BENEFITS PV
$8.10M

NPV
$6.19M

Benefits (Three-Year)



> **“[With HYPR,] security becomes easier and better. We can now create a higher overall security posture [internally and externally]. It gives us a strategic advantage and makes us one of the safest companies to do business with, [which] increases overall revenue.”**
>
> — Senior director of identity, security and access management, manufacturing

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 HYPR Authenticate.

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 HYPR Authenticate can have on an organization.

Forrester Consulting conducted an online survey of 351 cybersecurity leaders at global enterprises in the US, the UK, Canada, Germany, and Australia. Survey participants included managers, directors, VPs, and C-level executives who are responsible for cybersecurity decision-making, operations, and reporting. Questions provided to the participants sought to evaluate leaders' cybersecurity strategies and any breaches that have occurred within their organizations. Respondents opted into the survey via a third-party research panel, which fielded the survey on behalf of Forrester in November 2020.

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by HYPR 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 HYPR Authenticate.

HYPR 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.

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

DUE DILIGENCE

Interviewed HYPR stakeholders and Forrester analysts to gather data relative to HYPR Authenticate.

INTERVIEWS

Interviewed six representatives at five organizations using HYPR Authenticate 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 HYPR Authenticate Customer Journey

🟩 Drivers leading to the HYPR Authenticate investment

Interviews

Role	Industry	Region	Annual revenue and FTEs	Number of HYPR users
Director of information security	Financial services	HQ: US Operations: Global	- $928M - 3,000 FTEs	1,000
Senior director of identity, security, and access management	Manufacturing	HQ: US Operations: Global	- $25.8B - 33,000 FTEs	170,000
Partnership manager	Cybersecurity	HQ: Canada Operations: Canada	- $6M - 87 FTEs	n/a
Senior security engineer	Financial services	HQ: US Operations: Global	- $257M - 1,600 FTEs	1,280
- CTO - Senior director of global cyberoperations and intelligence	Transport services	HQ: US Operations: Global	- $13.7B - 69,000 FTEs	77,000

KEY CHALLENGES

Prior to using HYPR, the interviewees' organizations conducted identity authentication through SSO with passwords and MFA solutions, and some employees also used OTP hard tokens. But these solutions had complex processes and poor user experiences (UX), which hampered productivity for end users.

Moreover, the interviewees view passwords as the weakest point in their organizations' security postures and they sought to eliminate passwords for employees.

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

- **Poor UX with other authentication tools and password solutions.** The interviewees shared that password-based authentication such as MFA and SSO often involves multiple steps and complex password policies, which delivers a poor UX for end users. The impact of poor UX is exacerbated when employees must log into multiple systems per day to do their job. The senior director of identity, security, and access management at a manufacturing organization said, "Some people were logging into [software] 60 times a day."

  Poor UX with other authentication solutions caused frustration among end users, which led to meager cyberhygiene. A partnership manager for

> **"It's a risk not to use a passwordless solution today, [and] it's a risk to leave it up to your employees or customers to generate proper cyber hygiene. One of the largest gaps in cyber hygiene today is poor password management."**
>
> *Partnership manager, cybersecurity*

a cybersecurity firm noted: “If you put a bunch of friction in front of [an] individual and you put a bunch of tools in front of that individual that [don’t] help them get their job done, they’re going to take the path of least resistance. And the path of least resistance sometimes is creating really bad passwords or reusing passwords, or not using a vault or not using a passwordless solution.”

Poor UX also caused increased support requests for the organizations’ help desks, especially during scheduled password resets.

- **Weak password practices resulting in security vulnerabilities.** The interviewees shared that passwords are a primary security vulnerability for their organizations and that one of the largest gaps in cyberhygiene today is poor password management. Password-based authentication is susceptible to security breaches including phishing, brute force attacks, password spraying, and credential stuffing.[3] FIDO introduced the FIDO2 protocol in 2016 to help reduce the world’s overreliance on passwords, and the interviewees recognized that their organizations’ prior solutions did not support new industry standards in identity authentication.[4] In their prior environments, the interviewees’ organizations attack surfaces were significantly exposed to these risks.

  The partnership manager at a cybersecurity organization commented: “Password [protection is] one of the largest issues with cyberhygiene today, and it’s one of the highest vulnerabilities probably outside of email. If you have an admin or a user who’s not managing their passwords correctly, you have a massive gap inside of your security posture.”

- **Frequent and time-consuming password reset processes.** Interviewees shared that traditional password-based authentication requires regular password resets on a quarterly basis. The majority of help desk calls are related to passwords or credentials.[5]

  Some interviewees said that in their organization’s prior state, it paid a third-party company to help manage resets while others said their organization’s help desk team managed resets. Password reset processes were complex, and this was heightened when dealing with remote workers.

  The senior director of identity, security, and access management at a manufacturing organization described: “If everything goes wrong, with some cases, we’ve had them where [the employee is] remote in their home, they don’t have [a connection] to the domain, and they don’t have line of sight. And then [if] we don’t have the password kept in our vault service for some reason, they would have to go into the office. … And that could be a day-plus activity.”

- **Time-consuming onboarding processes.** Interviewees said that in addition to their organization’s prior state hampering day-to-day productivity for end users, password-based

“We saw weak password practices going on, and during the middle of the [COVID-19] pandemic, we limited password changes. We were looking for something that would help us eliminate passwords in general to improve ease of use.”

Director of information security, financial services authentication caused employee onboarding into technology/systems to be slow, and it delivered poor employee-experiences (EX).

The partnership manager at a cybersecurity firm shared: “When a new employee comes on, there’s probably a variety of applications they need access to. If you don’t have an ability to manage those passwords and also access those passwords in a seamless way, you’re going to generate friction [and poor] cyberhygiene.”

SOLUTION REQUIREMENTS/INVESTMENT OBJECTIVES

The interviewees’ organizations searched for a solution that could:

- Eliminate passwords and provide an easy, secure login solution.
- Reduce the number of authentication solutions across the organization.
- Layer FIDO2 protocol standards across all apps and services to improve security posture.
- Streamline employee onboarding processes.
- Reduce password resets to improve productivity for help desk staff and end users.

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 global organization is headquartered in the US and is in a highly regulated industry. It generates $5 billion in annual revenue and has 10,000 total employees. The organization grows 5% annually and has 10% attrition that is backfilled.

In its prior environment, the organization used a SSO with password and MFA, and it mandated quarterly password changes with complex requirements for end users. Furthermore, 10% of employees required an OTP hard token to access certain apps and functions.

Deployment characteristics. The composite organization seeks a passwordless solution to eliminate password use, and it invests in HYPR. Adoption of the solution is voluntary across the employee base, and it grows exponentially during three years from 75% adoption in Year 1 to 95% adoption in Year 3.

Key Assumptions

- **$5 billion in annual revenue**
- **10,000 employees**
- **95% HYPR adoption by Year 3**

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	Business risk avoidance	$1,033,212	$1,107,012	$1,180,813	$3,321,036	$2,741,331
Btr	Helpdesk support cost avoidance	$860,625	$1,024,144	$1,201,854	$3,086,623	$2,531,757
Ctr	End-user productivity savings	$905,250	$1,077,256	$1,264,205	$3,246,711	$2,663,065
Dtr	Employee OTP hard token onboarding efficiencies	$23,760	$24,948	$26,195	$74,903	$61,899
Etr	OTP hard token consolidation savings	$33,750	$40,163	$47,132	$121,045	$99,285
	Total benefits (risk-adjusted)	$2,856,597	$3,273,522	$3,720,199	$9,850,318	$8,097,337

BUSINESS RISK AVOIDANCE

Evidence and data. Prior to using HYPR, interviewees' organizations faced business risk challenges related to their environments' login processes. The use of SSO with a password left the organizations at risk of attacks related to weak or stolen credentials that could disrupt end-user productivity and business continuity. As a result, the financial impact of security breaches could cost the organizations thousands to millions of dollars, depending on the severity and frequency of attacks.

With HYPR, the interviewees' organizations avoided potential business risk with the elimination of more than 70% of passwords across their environments.

- The CTO at a transport services organization commented: "From a risk standpoint, the saying is: 'Hackers don't break in. They log in.' That login is usually associated with stolen credentials. [With HYPR,] there's no password to steal anymore. There's a reduction in risk because there's no credential loss based on passwords."
- The partnership manager at a cybersecurity organization noted: "A passwordless solution reduces a lot of friction, and it reduces bad [security] hygiene. When we look at this, this is a very simplistic value proposition for us that is very powerful."
- The senior security engineer at a financial services organization commented: "User passwords may be very weak. With HYPR, there is a big reduction in risk because passwords are no longer around, which is helping the organization be in a more secure state."

> **"Phishing won't work once we have 80% of our organization on HYPR. This is an important success."**
>
> *Senior security engineer, financial services*

- The senior director of identity, security, and access management at a manufacturing organization said: “In our ecosystem today, nobody even knows their password. There are a few people who still use [passwords] for legitimate reasons, [but] we have around 70% [now] moved away from passwords.”

Modeling and assumptions. For the composite organization, Forrester estimates:

- The cost of a security breach for the composite is $854,176, and the organization has three security breaches per year.[6] This cost is inclusive of average remediation and reporting labor costs, average costs of response and notification, fines, damages, compliance costs, customer compensation, average lost business revenues and additional costs to acquire customers, and end-user downtime as it relates to a security breach across the organization.

- 64% of the attacks are related to weak or stolen credentials and phishing.[7]

- With HYPR, the composite eliminates password use by 70% in Year 1, by 75% in Year 2, and by 80% in Year 3.

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

- The company’s size, industry, region, sensitivity and volume of data, and workforce composition.

- The adoption of HYPR across employees to eliminate password use.

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 $2.7 million.

Business Risk Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Cost of a security breach	Forrester research	$854,176	$854,176	$854,176
A2	Security breaches per year	Forrester research	3	3	3
A3	Percent of attacks related to weak or stolen credentials and phishing	Verizon	64%	64%	64%
A4	Percent of password use eliminated with HYPR	Interviews	70%	75%	80%
At	Business risk avoidance	A1*A2*A3*A4	$1,148,013	$1,230,013	$1,312,014
	Risk adjustment	↓10%			
Atr	Business risk avoidance (risk-adjusted)		$1,033,212	$1,107,012	$1,180,813
	Three-year total: $3,321,036		**Three-year present value: $2,741,331**		

HELP DESK SUPPORT COST AVOIDANCE

Evidence and data. Interviewees said that prior to using HYPR, their organizations' help desk teams were overburdened with password/credential-related reset tickets, especially during organization-mandated password resets that typically occur on a quarterly basis. At some of the interviewees' organizations, end users had more than one password, which added to the complexity of managing them all. Furthermore, strict password requirements made it difficult for end users to remember their passwords, which resulted in at least 50% of help desk calls being password-related inquiries.

With HYPR, the organizations alleviated help desk support with the elimination of many password-reset calls as users increasingly adopted the passwordless solution.

- The senior director of identity, security, and access management at a manufacturing organization noted, "[With HYPR,] we're seeing that password [and] password reset … calls are gone."
- The senior director of global cyberoperations and intelligence at a transport services organization noted: "How often you change your passwords [is one less thing to worry about.] Password complexity, the standard sort of baseline definitions of what is our policy and our requirements regarding passwords, and how we enforce it and ensure that people are doing what they're supposed to be doing simply goes away [with HYPR]."
- The CTO at a transport services organization highlighted: "If you talk about password resets and the friction it [causes] to the workforce, it was high. IT costs are reduced because you don't have to reset passwords. There was a specific managed service provider that was [dedicated to] resetting passwords. [With HYPR,] we eliminated [using] that person."

> **"If a service mechanic has 10 calls on his schedule for the day, and he can only make three of them because they spent a couple hours just trying to get their password reset [on their first call], then it hurts the bottom line."**
>
> *CTO, transport services*

> **"[With HYPR,] we're getting a smaller number of [IT] tickets for things like password resets as well as much less disruption from the loss of those credentials."**
>
> *Senior director of global cyberoperations and intelligence, transport services*

Modeling and assumptions. For the composite organization, Forrester estimates:

- There is 5% annual employee growth across three years, leading to 10,000 employees in Year 1, 10,500 employees in Year 2, and 11,025 employees in Year 3.
- Each employee submits an average of six help desk tickets per year.

- Prior to using HYPR, 50% of help desk tickets were related to password resets.
- HYPR is adopted by 75% of employees in Year 1, 85% of employees in Year 2, and 95% of employees in Year 3.
- The average cost of a help desk ticket is $42.50.

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

- The total number of employees and the number of employees who adopt HYPR.
- The number of password-reset tickets per user per year.
- The average cost of a help desk ticket.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2.5 million.

Help Desk Support Cost Avoidance

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Employees	Composite	10,000	10,500	11,025
B2	Help desk tickets per year	Assumption	6	6	6
B3	Percent of help desk tickets related to password resets	Interviews	50%	50%	50%
B4	Number of password-reset tickets before using HYPR	B1*B2*B3	30,000	31,500	33,075
B5	Percent of HYPR adoption across employees	Composite	75%	85%	95%
B6	Password-reset tickets avoided annually with HYPR	B4*B5	22,500	26,775	31,421
B7	Average help desk cost per ticket	Composite	$42.50	$42.50	$42.50
Bt	Help desk support cost avoidance	B6*B7	$956,250	$1,137,938	$1,335,393
	Risk adjustment	↓10%			
Btr	Help desk support cost avoidance (risk-adjusted)		$860,625	$1,024,144	$1,201,854
	Three-year total: $3,086,623		**Three-year present value: $2,531,757**		

END-USER PRODUCTIVITY SAVINGS

Evidence and data. Prior to using HYPR, end users at the interviewees' organizations faced disruptions in their daily operations whenever they had to reach out to the help desk to reset their passwords. In many cases, this occurred more than once per year per end user. Furthermore, end users also lost valuable time with their previous authentication login methods using other MFA solutions. End users typically had to log in to systems multiple times throughout any given day, and processes such as using OTP hard tokens contributed to inconvenient downtime. The impact that this downtime had on an annual basis affected total end-user productivity as minutes added up to hours.

With HYPR, the interviewees' organizations improved their UX, which led to avoided downtime for end users and resulted in end-user productivity savings.

- The CTO at a transport services company noted: "[IT is] not taking [as many password-reset] phone calls on the help desk. There's increased productivity because people don't have to remember where they wrote [their passwords]. When our CEO heard that we didn't have to use passwords [with HYPR], she [asked]: 'Well, what about me? I don't like passwords either.' Once it got going, we couldn't stop that train. Everybody was lining up to be next to remove passwords out of their environment once the word spread that they didn't have to use passwords anymore."
- The senior director of identity, security, and access management at a manufacturing organization noted, "[HYPR] makes it easy for [end users] to register. From a user-experience side, we were able to integrate [HYPR] to our SDK [software development kit]. Now, it's the same UX [on] desktop [and] mobile. That was [a] key [benefit] that people love."
- The partnership manager at a cybersecurity organization commented, "It's a simple click of a button [to leverage] your phone as the FIDO2 token and [access] particular applications."
- The senior security engineer at a financial services organization noted: "With HYPR, users don't have to reset passwords every 90 days. Additionally, single authentication with FIDO2 has saved end users at least 30% of time logging in."

Modeling and assumptions. For the composite organization, Forrester estimates:

- With HYPR, the composite avoids 22,500 password-reset requests in Year 1, 26,775 in Year 2, and 31,421 in Year 3. The average end-user downtime per password reset is 12 minutes.
- There are 7,500 HYPR users in Year 1, 8,925 in Year 2, and 10,474 in Year 3.
- Login times improve for HYPR users. Without HYPR, authentication takes 1 minute per login, and end users authenticate an average of five times per day. With HYPR, end users save 30% of time on authentication.
- The average fully burdened hourly rate of an employee is $40.
- The composite's productivity recapture rate is 50% to account for the fact that not all recovered time is spent productively but may enhance the employee experience (e.g., being able to take longer breaks.)

> **"Authentication [is] faster for [an end user with HYPR] because they don't have to enter [their] username and password."**
>
> *Senior director of identity, security, and access management, manufacturing*

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

- The number of employees and level of HYPR adoption.
- The average downtime per end user related to help desk tickets.
- The number of authentications per user per day.
- The average fully burdened hourly rates of employees.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $2.7 million.

End-User Productivity Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Password-reset tickets avoided with HYPR	B6	22,500	26,775	31,421
C2	**Average end-user downtime per password reset (minutes)**	**Interviews**	**12**	**12**	**12**
C3	Avoided annual end-user downtime related to password resets (hours)	(C1*C2)/60	4,500	5,355	6,284
C4	Average fully burdened hourly rate for an employee	TEI Standard	$40	$40	$40
C5	Subtotal: End-user productivity savings from password resets with HYPR	C3*C4	$180,000	$214,200	$251,360
C6	Employees who use HYPR	B1*B5	7,500	8,925	10,474
C7	Average time per authentication in prior environment (minutes)	Composite	1	1	1
C8	Average authentications per day in prior environment	Composite	5	5	5
C9	Percent of time saved on authentication with HYPR	Interviews	30%	30%	30%
C10	Authentication time savings with HYPR (hours)	(C6*C7*C8*C9*26 0)/60	48,750	58,013	68,081
C11	Subtotal: End-user productivity savings from authentication with HYPR	C4*C10	$1,950,000	$2,320,520	$2,723,240
C12	Productivity recapture	TEI standard	50%	50%	50%
Ct	End-user productivity savings	(C5+C11)*C12	$1,065,000	$1,267,360	$1,487,300
	Risk adjustment	↓15%			
Ctr	End-user productivity savings (risk-adjusted)		$905,250	$1,077,256	$1,264,205
	Three-year total: $3,246,711			**Three-year present value: $2,663,065**	

EMPLOYEE OTP HARD TOKEN ONBOARDING EFFICIENCIES

Evidence and data. Some interviewees said that prior to using HYPR, their organizations had lengthy onboarding processes for new hires. Those who were assigned OTP hard tokens were left in a waiting period as their physical tokens would have to be shipped and delivered before they could begin their work. Depending on the location, this could take anywhere from days to weeks. With HYPR, the organizations eliminated the use of OTP hard tokens, which resulted in faster onboarding for new employees.

The CTO of a transport services organization described: “The only thing we need to do is when a new employee comes on board [is their] manager generates a magic link that goes to that employee that can only be used on that company laptop. They don't put in a password their first time on. They just hit "enter," and it prompts them with a challenge on their personal phone. No longer do we have to mail tokens out or smart cards or bingo cards in some cases where they have to generate that grid. It's just a magic link, and it doesn't matter whether you use an Android or iOS-based device. We send the magic link, and that's used for the MFA authentication."

> **"The obvious value is return on investment in terms of gain, productivity, and onboarding of new employees."**
>
> *CTO, transport services*

Modeling and assumptions. For the composite organization, Forrester estimates:

- The composite's annual employee growth is 5%, and its annual attrition is 10%. This equals 1,500 new employees in Year 1, 1,575 new employees in Year 2, and 1,654 new employees in Year 3.
- Before using HYPR, 10% of the composite's employees were assigned OTP hard tokens.
- Employee onboarding with an OTP hard token takes 16 hours.
- With HYPR, there is a 55% reduction in the time to onboard new employees who require OTP hard tokens as these are eliminated.
- The average fully burdened hourly rate of an employee is $40.
- The composite's productivity recapture rate is 50%.

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

- The percentage of employees who use OTP hard tokens.
- The time spent onboarding employees with OTP hard tokens (including shipping times, etc.)
- The average fully burdened hourly rate of an employee.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $62,000

Employee OTP Hard Token Onboarding Efficiencies

Ref.	Metric	Source	Year 1	Year 2	Year 3
D1	Employees onboarded	(B1*5%)+(B1*10 %)	1,500	1,575	1,654
D2	Percent of employees with OTP hard tokens	Composite	10%	10%	10%
D3	Average time spent to fully onboard new employees onto system in prior environment (hours)	Composite	16	16	16
D4	Time spent onboarding new employees with OTP hard tokens in prior environment (hours)	D1*D2*D3	2,400	2,520	2,646
D5	Percent reduction in time to onboard new employees onto system with HYPR	Interviews	55%	55%	55%
D6	Average fully burdened hourly rate of an employee	Composite	$40	$40	$40
D7	Productivity recapture	TEI standard	50%	50%	50%
Dt	Employee OTP hard token onboarding efficiencies	D4*D5*D6*D7	$26,400	$27,720	$29,106
	Risk adjustment	↓10%			
Dtr	Employee OTP hard token onboarding efficiencies (risk-adjusted)		$23,760	$24,948	$26,195
	Three-year total: $74,903		Three-year present value: $61,899		

OTP HARD TOKEN CONSOLIDATION SAVINGS

Evidence and data. Some interviewees said that prior to using HYPR, their organizations incurred costs related to OTP hard tokens. These included the costs of management resetting them and physically mailing them to employees. The CTO at a transport services organization described: "Like most enterprises in the world, we were using tokens. The ongoing window-washing exercise of trying to mail out tokens, get back tokens, [and] refresh tokens was just a nightmare."

With HYPR, some of the interviewees' organizations were able to eliminate tokens in their environment.

Modeling and assumptions. For the composite organization, Forrester estimates:

- The composite has 10,000 employees in Year 1, 10,500 employees in Year 2, and 11,025 employees in Year 3.
- 10% of employees use OTP hard tokens.
- HYPR adoption across employees is 75% in Year 1, 85% in Year 2, and 95% in Year 3.
- The average unit cost of an OTP hard token is $50.

> **"We don't have any more tokens. There are zero tokens left in the environment for us today, which is huge."**
>
> *CTO, transport services*

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

- The total number of employees and the number of those who adopt HYPR.
- The percentage of employees who use OTP hard tokens.
- The average unit cost of an OTP hard token.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $99,000.

OTP Hard Token Consolidation Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Employees	B1	10,000	10,500	11,025
E2	Percent of employees with OTP hard tokens	Composite	10%	10%	10%
E3	Adoption rate of HYPR across employees	B5	75%	85%	95%
E4	OTP hard token unit cost	Composite	$50	$50	$50
Et	OTP hard token consolidation savings	E1*E2*E3*E4	$37,500	$44,625	$52,369
	Risk adjustment	↓10%			
Etr	OTP hard token consolidation savings (risk-adjusted)		$33,750	$40,163	$47,132
Three-year total: $121,045			**Three-year present value: $99,285**		

UNQUANTIFIED BENEFITS

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

- **Avoided phishing investigation and response costs.** Phishing investigations prove to be a significant cost to organizations because the severity of compromises and attacks can vary. Interviewees said that with HYPR, their organizations decreased the number of phishing incidents where they deployed the solution. The senior director of global cyberoperations at a transport services organization highlighted: “From an incident response perspective, [in] the areas where we don’t have HYPR, we see a lot more activity that we have to deal with based on loss of credentials. Usually, it’s in the form of phishing, [which] leads to longer investigations. [This means] more time and energy from my SOC and

> **“Man-in-the-middle [attacks], credential state theft, and, of course, phishing-resistant MFA: When you don’t have a password in the middle of that, then that risk goes away.”**
>
> *CTO, transport services*

incident response teams to make sure that we've covered all the bases [and identified] all the identities that could potentially be involved."

Please see Appendix B for a framework to estimate the costs your organization may avoid.

FLEXIBILITY

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

- **Lower cyber insurance premiums.** Interviewees noted that using an MFA solution had an impact on reducing their organizations' cyber insurance premiums. The senior director of identity, security, and access management at a manufacturing organization commented, "If you have MFA, it reduces your cyber insurance right away."

  The CTO at a transport services organization commented, "I know that we use it as part of our renewal for our cyber insurance to show a maturity level in our program, and that password and credential theft is lowered based on us using a passwordless, phishing-resistant method of authentication versus traditional passwords."

- **Customer security.** Some interviewees noted the residual impact that HYPR had on not only their organization's workforce, but also on the security of their customers. The CTO at a transport services organization commented, "If we're servicing you as a customer, you don't have to worry about us leaving our book of passwords in a taxicab somewhere because there are no passwords to leave."

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	Licensing	$0	$472,500	$562,275	$659,862	$1,694,637	$1,390,000
Gtr	Deployment	$77,000	$0	$0	$0	$77,000	$77,000
Htr	Ongoing management and end-user training	$0	$176,660	$177,485	$178,354	$532,499	$441,282
	Total costs (risk-adjusted)	$77,000	$649,160	$739,760	$838,216	$2,304,136	$1,908,282

LICENSING

Evidence and data. Interviewees described licensing for HYPR as competitive in the marketplace. Those from larger organizations noted their companies have volume pricing in their enterprise agreements. Other organizations use standard licensing based on a monthly, per user basis.

Modeling and assumptions. For the composite organization, Forrester assumes:

- 75% of the composite's employees adopt HYPR in Year 1, which results in 7,500 total users; 85% adopt it in Year 2, which results in 8,925 total users; and 95% adopt it in Year 3, which results in 10,474 total users.
- The annual list price per user is $60.
- Pricing may vary. Contact HYPR for additional details.

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

- The total number of employees and the number of employees who adopt HYPR.
- Variances in enterprise agreements.

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 $1.4 million.

Licensing

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Users	B1*B5	0	7,500	8,925	10,474
F2	Licensing cost per user	Composite	$0	$60	$60	$60
Ft	Licensing	F1*F2	$0	$450,000	$535,500	$628,440
	Risk adjustment	↑5%				
Ftr	Licensing (risk-adjusted)		$0	$472,500	$562,275	$659,862
	Three-year total: $1,694,637		**Three-year present value: $1,390,000**			

DEPLOYMENT

Evidence and data. Interviewees described proof-of-concept scenarios in which their organizations onboarded and tested the HYPR solution for a couple of months prior to companywide deployment. The organizations offered employees the flexibility to opt in to using the solution, and interviewees noted the biggest challenge was communicating with end users and encouraging them to adopt HYPR. To overcome this, the organizations took action steps to support HYPR users, and this included providing dedicated end-user support teams to assist with questions and onboarding during the initial phases of rolling out HYPR.

Modeling and assumptions. For the composite organization, Forrester assumes:

- Internal security and IT employees spend 200 labor hours implementing, testing, and deploying the solution across the organization.
- The composite dedicates 800 hours to change management across the organization to encourage employees to adopt HYPR as an authentication method. This includes time spent on end-user training.
- The average fully burdened hourly rate of a security engineer is $70.

> **"HYPR API-based authentication is very flexible with workflows and allows you to authenticate people based on the context. We create an authentication layer before they have access to highly privileged [or] secure information."**
>
> *Senior security engineer, financial services*

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

- The size of the organization, which may impact the time spent implementing, testing, and deploying HYPR.
- Change management, which is dependent on the company culture and employee willingness to adopt HYPR.
- The average fully burdened rate of a security engineer.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $77,000.

Deployment

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Internal security and IT labor time for testing (hours)	Composite	200	0	0	0
G2	Time spent for change management (hours)	Composite	800	0	0	0
G3	Average fully burdened hourly rate of a security engineer	Composite	$70	$0	$0	$0
Gt	Deployment	(G1+G2)*G3	$70,000	$0	$0	$0
	Risk adjustment	↑10%				
Gtr	Deployment (risk-adjusted)		$77,000	$0	$0	$0
	Three-year total: $77,000			Three-year present value: $77,000		

ONGOING MANAGEMENT AND END-USER TRAINING

Evidence and data. Interviewees said their organizations' ongoing management of HYPR ranges from requiring a few hours per week to dedicating FTEs to spend most of their time on management depending on the number of HYPR users. Interviewees described end-user training as minimal and straightforward because users typically self-enroll in the solution.

Modeling and assumptions. For the composite organization, Forrester assumes:

- One security engineer FTE is dedicated to ongoing management of HYPR.
- The average fully burdened annual salary of a security engineer is $145,600.
- On average, employee training takes 15 minutes.
- There are 1,500 new employees in Year 1, 1,575 new employees in Year 2, and 1,654 new employees in Year 3.
- The average fully burdened hourly rate of an employee is $40.

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

- The size of the organization, which may require different FTE commitments for ongoing management.
- The average fully burdened hourly rates of employees.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $441,000.

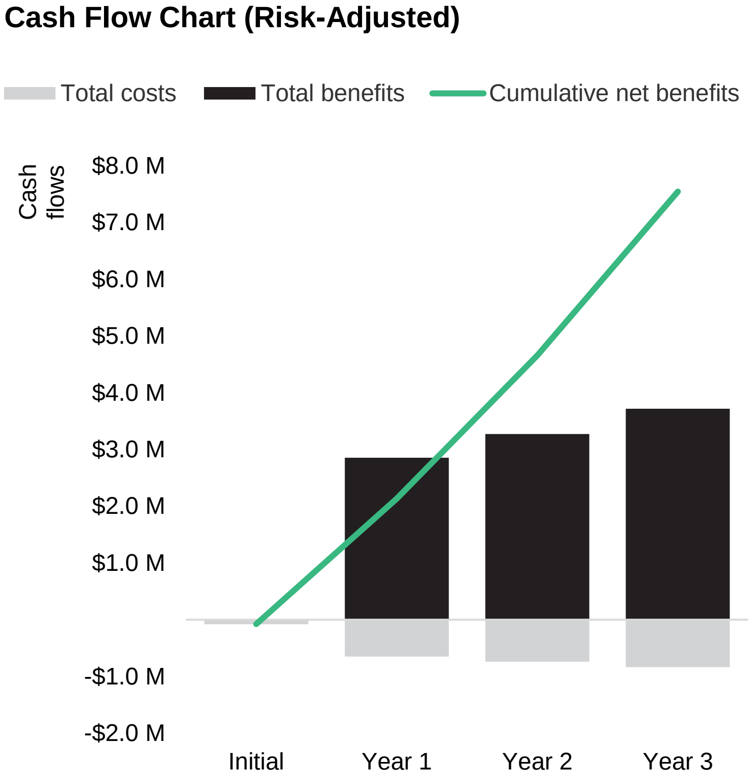
Ongoing Management And End-User Training

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Ongoing management FTEs	Interviews	0	1	1	1
H2	Average fully burdened salary of a security engineer	Composite	$0	$145,600	$145,600	$145,600
H3	Subtotal: Ongoing management costs (rounded)	H1*H2	$0	$145,600	$145,600	$145,600
H4	New employees who require HYPR training	D1	0	1,500	1,575	1,654
H5	Training time for first-time users (minutes)	Interviews	0	15	15	15
H6	Average fully burdened hourly rate of an employee	TEI standard	$0	$40	$40	$40
H7	Subtotal: End-user training costs	(H4*H5*H6)/60	$0	$15,000	$15,750	$16,540
Ht	Ongoing management and end-user training	H3+H7	$0	$160,600	$161,350	$162,140
	Risk adjustment	↑10%				
Htr	Ongoing management and end-user training (risk-adjusted)		$0	$176,660	$177,485	$178,354

Three-year total: $532,499 **Three-year present value: $441,282**

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 and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

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

Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	($77,000)	($649,160)	($739,760)	($838,216)	($2,304,136)	($1,908,282)
Total benefits	$0	$2,856,597	$3,273,522	$3,720,199	$9,850,318	$8,097,337
Net benefits	($77,000)	$2,207,437	$2,533,762	$2,881,983	$7,546,182	$6,189,055
ROI						324%
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: Avoided Phishing Investigation Costs Framework

The framework below provides a way to estimate the cost of phishing investigations your organization may avoid with HYPR. To use this framework, enter your organization's values in rows XX1 and XX5.

Ref.	Metric	Source	Year 1	Year 2	Year 3
XX1	Phishing investigations per year in prior environment	Input			
XX2	Percent of password use eliminated with HYPR	Interviews	70%	75%	80%
XX3	Percent of phishing attempts blocked by multi-factor authentication	Forrester research	96%	96%	96%
XX4	Average time spent per phishing investigation (hours)	Forrester research	3.7	3.7	3.7
XX5	Average fully burdened rate of a security professional	Input			
XXt	Avoided phishing investigation costs	XX1*XX2*XX3*XX4*XX5			

Appendix C: Endnotes

[1] Source: "Using Zero Trust To Kill The Employee Password," Forrester Research, Inc., August 2, 2021.

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

[3] Source: "Using Zero Trust To Kill The Employee Password," Forrester Research, Inc., August 2, 2021.

[4] Source: "Alliance Overview," Fido Alliance, June 2023.

[5] Source: "FIDO Passkeys And The Future Of Customer Authentication," Forrester Research Inc., January 10, 2023.

[6] Source: Forrester Consulting Cost Of A Security Breach Survey, Q4 2020.

[7] Source: "2022 Data Breach Investigations Report," Verizon, June 2022.

FORRESTER®