

A Forrester Total Economic Impact™
Study Commissioned By IBM
July 2020

The Total Economic Impact™ Of IBM Security Verify

Cost Savings And Business Benefits
Enabled By IBM Security Verify

FORRESTER®

Table Of Contents

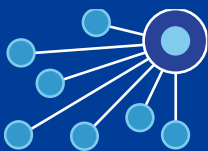
Executive Summary	1
Key Findings	1
TEI Framework And Methodology	3
IBM Security Verify Customer Journey	4
Interviewed Customers	4
The Composite <i>Organization</i>	4
Key Business Goals And Objectives	4
Analysis Of Benefits	6
Infrastructure Cost Avoidance Benefits	6
IT Administrator Benefits	7
Developer Benefits	8
User Benefits	10
Unquantified Benefits	10
Flexibility	10
Analysis Of Costs	12
Costs To Build, Maintain, And Improve The Hybrid IBM Security Verify Environment	12
IBM Security Verify Fees	13
Financial Summary	15
IBM Security Verify Overview	16
Appendix A: Total Economic Impact	17
Appendix B: Endnotes	18

Project Director:
Bob Cormier
Vice President and Principal Consultant

Selected Key Metrics



Developer benefits:
\$268,580 over three years



User benefits:
\$10.1 million over three years



Infrastructure cost avoidance
benefits — \$81,818

Total quantified benefits:
\$10.6 million
(risk- and PV-adjusted)

Executive Summary

IBM Security Verify provides identity-as-a-service (IDaaS) for every user, including single sign-on (SSO), risk-based multifactor authentication (MFA) and adaptive access, user lifecycle management, privacy consent, and identity analytics. It comes with thousands of prebuilt connectors to help organizations quickly provide access to popular software-as-a-service (SaaS) apps and prebuilt templates to help integrate in-house apps.

IBM commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and objectively examine the potential ROI that organizations may realize by investing in IBM Security Verify. The purpose of this study is to provide readers and prospects with a framework to evaluate the potential financial impact of IBM Security Verify on their organizations.

To better understand the benefits, costs, flexibility, and risks associated with this investment, Forrester conducted in-depth interviews with two customers using IBM Security Verify. We have used data gathered from these interviews to create a composite *Organization* that illustrates the quantifiable benefits and costs of investing in IBM Security Verify, specifically SSO and MFA. This global composite *Organization* has 15,000 employees and contractors benefiting from IBM Security Verify. Previously, the composite used on-premises access management technologies from other vendors.

For more information, see the section titled *The Composite Organization*.

Key Findings

Quantified benefits. The composite *Organization* experiences the following risk-adjusted, present-value (PV) quantified benefits, totaling \$10,552,942 over three years, compared to its previous environment (see the Analysis Of Benefits section for more details):

- › **Infrastructure cost avoidance benefits** — \$81,818.
- › **IT administrator benefits** — \$100,718.
- › **Developer benefits** — \$268,580.
- › **User benefits** — \$10,101,826.

In addition to the quantified benefits listed above, the interviewed customers discussed qualitative features or benefits from using IBM Security Verify (see the Unquantified Benefits section for more details).

Costs. The *Organization* experiences the following risk-adjusted and PV costs totaling \$1,468,324 over three years (see the Analysis Of Costs section for more details):

- › **Costs to build, maintain, and improve the hybrid IBM Security Verify environment** — \$522,247.
- › **IBM Security Verify fees** — \$946,077.

Forrester's interviews and subsequent financial analysis found that the *Organization* experiences benefits of \$10,552,942 over three years versus costs of \$1,468,324, adding up to a net present value (NPV) of \$9,084,618, with a payback period of less than six months and an **ROI of 619%**.



ROI
619%



Benefits PV
\$10,552,942



NPV
\$9,084,618



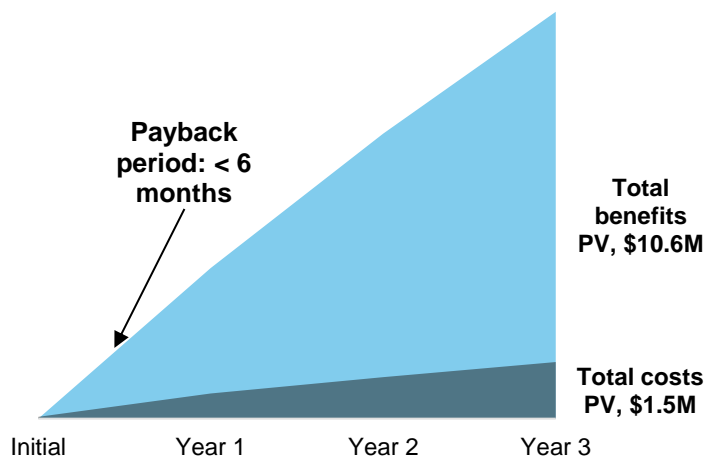
Payback
<6 months

If risk-adjusted costs, benefits, and ROI still demonstrate a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as realistic expectations, as they represent the expected value considering risk. Assuming normal success at mitigating risk, the risk-adjusted numbers should more closely reflect the expected outcome of the investment.

Forrester Note: Optimizing existing identity access management (IAM) resources for the cloud without sacrificing previous on-premises investments is critical, but how can you sell this to your senior management? Many companies have been unable to start their IAM cloud projects because the CISO and other technology management leaders failed to demonstrate a compelling and positive ROI to the CIO and business stakeholders. Without such a business case, some may look at IAM solutions for the cloud as a cost item undeserving of any budget.

With this Forrester case study, readers can gain executive and business support with quantifiable costs and benefits. Like any business plan, IAM solutions for the cloud requires a cost-benefit analysis to justify spending for the project and garner executive support. Quantifying the benefits and costs as we've done in this case study will give readers specific results — readily usable in a presentation to senior stakeholders when asking for an increase to their budget for IAM solutions for the cloud.

Financial Summary



The TEI methodology helps companies demonstrate, justify, and realize the tangible value of IT initiatives to both senior management and other key business stakeholders.

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering investing in IBM Security Verify.

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 IBM Security Verify can have on an organization:



DUE DILIGENCE

Interviewed IBM stakeholders to gather data relative to the marketplace.



CUSTOMER INTERVIEWS

Interviewed two customers using IBM Security Verify to obtain data with respect to costs, benefits, flexibility, and risks.



COMPOSITE ORGANIZATION

Designed a composite *Organization* based on characteristics of the interviewed customers.



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 interviewed customers.



CASE STUDY

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

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by IBM 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 IBM Security Verify.

IBM 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.

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

IBM Security Verify Customer Journey

BEFORE AND AFTER IBM SECURITY VERIFY INVESTMENT

Interviewed Customers

For this study, Forrester conducted interviews with the two IBM Security Verify customers described below, each requesting anonymity:

CUSTOMER DESCRIPTION	NUMBER OF IBM USERS	INTERVIEWEE	MONTHS USING IBM SECURITY VERIFY
A leading logistics organization in EMEA	4,000	Application manager	15
North American semiconductor company	15,000	Security analyst	18

The Composite *Organization*

To better understand the benefits, costs, flexibility, and risks associated with this investment, Forrester conducted in-depth interviews with two customers using IBM Security Verify. We have used data gathered from these two interviews to create a composite *Organization* that illustrates the quantifiable benefits and costs of investing in IBM Security Verify offerings, specifically SSO and MFA. This global composite *Organization* has 15,000 employees and contractors benefiting from IBM Security Verify. Previously, the composite used on-premises IAM products from another vendor.

As with most IBM Security Verify customers, the composite *Organization* has chosen to have a hybrid deployment in support of its cloud roadmap with a combination of keeping its legacy on-premises products and investing in IBM Security Verify.

The *Organization* benefits from a lower cost cloud model and the ability to do things faster, such as adding multifactor authentication to applications; this had taken 30 days to do with the on-premises solutions but takes only a few hours with IBM Security Verify.

The *Organization* also reduces infrastructure and labor costs for development, QA, and production environments.

"IBM Security Verify is a very comprehensive platform with SSO, MFA, and identity governance suitable for all our constituents including business-to-employee, business-to-business, and business-to-consumer use cases."

Security analyst



Key Business Goals And Objectives

After extensive review processes evaluating several vendors, the interviewed customers selected IBM Security Verify as, overall, they believed IBM's cloud offerings could satisfy the following business goals and objectives, also shared by the composite *Organization*:

- › Allow employees and contractors to log in with single sign-on.
- › Streamline the onboarding process for new applications and MFA methods.
- › Save IT from password and access requests.
- › Leverage existing on-premises IAM investments for a hybrid solution.

- › Support Zero Trust initiatives by better utilizing identity context.
- › Identify and mitigate risks with better reporting and analytics.

The customer interviews revealed beneficial functionality attributed to their investments in IBM Security Verify as listed below (specific financial benefit details are available in the Analysis Of Benefits section):

- › Infrastructure cost avoidance benefits — \$81,818.
- › IT administrator benefits — \$100,718.
- › Developer benefits — \$268,580.
- › User benefits — \$10,101,826.

In addition to the benefits listed above, the interviewed customers discussed qualitative features or benefits from using IBM Security Verify (see the Unquantified Benefits section for more details).

“IBM Security Verify has a clean, business-friendly interface, delivered from the cloud. It helps us reduce our total cost of ownership and reduce our dependence on specialized and hard-to-find security skills.”

Application manager



Analysis Of Benefits

QUANTIFIED BENEFIT AND COST DATA

Total Benefits — The *Organization*

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Infrastructure cost avoidance benefits	\$90,000	\$0	\$0	\$90,000	\$81,818
Btr	IT administrator benefits	\$40,500	\$40,500	\$40,500	\$121,500	\$100,718
Ctr	Developer benefits	\$108,000	\$108,000	\$108,000	\$324,000	\$268,580
Dtr	User benefits	\$4,062,094	\$4,062,094	\$4,062,094	\$12,186,281	\$10,101,826
Total benefits (risk-adjusted)		\$4,300,594	\$4,210,594	\$4,210,594	\$12,721,781	\$10,552,942

Note Atr, Btr, Ctr and Dtr refer to benefit totals in the tables below.

Infrastructure Cost Avoidance Benefits

As with the interviewed customers, the composite *Organization* chooses a hybrid IAM deployment with a combination of keeping its legacy on-premises products and investing in new IBM Security Verify products. The *Organization* benefits from a lower cost cloud model related to its legacy on-premises infrastructure costs, as it does not have to replace IAM servers at end-of-life cycles.

Modeling and assumptions. The *Organization* avoids IAM-related, on-premises hardware replacement costs as follows: an estimated 10 servers at \$10,000 each for all environments (development, QA, and production) for basic high availability. Forrester assumes the *Organization* avoids the cost of replacing 10 servers during Year 1 of our analysis.

Risks. Forrester has risk-adjusted this benefit downward by 10% in the table below due to the wide range of results among interviewed customers, including the variability of end-of-life timing for servers.

This yields a three-year, risk-adjusted PV of \$81,818.

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the *Organization* expects risk-adjusted total benefits to be a PV of more than \$10.5 million.

Infrastructure Cost Avoidance Benefits: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
A1	Number of IAM servers — cost avoidance	<i>Organization</i>	10	0	0
A2	Average cost per server	Industry average	\$10,000	\$0	\$0
At	Infrastructure cost avoidance benefits	A1*A2	\$100,000	\$0	\$0
	Risk adjustment	↓10%			
Atr	Infrastructure cost avoidance benefits (risk-adjusted)		\$90,000	\$0	\$0

IT Administrator Benefits

IBM Security Verify's administrative dashboard provides a global overview of user activity on a daily, weekly, and ongoing basis. Administrators can view successful and failed logins, SSO connections, and geographic activity trends. IBM Security Verify's reporting includes application usage reports to spot trends, monitor performance, investigate patterns and anomalies in user behavior, and monitor suspicious user activity.

Administrators can enable various authentication methods for each new application and then start to onboard users and groups.

In addition, IBM Security Verify supports many SaaS applications and allows administrators to bridge to the cloud with custom configurations for on-premises applications. The "add application" interface lets administrators configure an application's general settings and assign a delegated business owner to manage the application.

Line-of-business managers who have been delegated application approval authority to give their employees access can do so without waiting on IT. The IBM Security Verify dashboard provides managers with a detailed view of pending approval requests.

Finally, IT administrators can control user application entitlements for different classifications of users, i.e., employees, managers, contractors, and customers.

Modeling and assumptions. The *Organization* saves one-half FTE due to the following features and functionality of IBM Security Verify:

- › The ability to more efficiently monitor user behavior with dashboard and custom reporting.
- › Simpler and more secure integration with common user and cloud directories.
- › Instant access to many cloud applications and the ability to bridge on-premises and legacy applications.
- › The ability to delegate user provisioning and deprovisioning to line-of-business managers, reducing IT administrators' workloads.
- › The ability to apply simple controls for conditional, risk-based MFA.

Forrester assumes a fully loaded annual labor cost of \$90,000 for IT administrators. The annual benefit is a non-risk-adjusted \$45,000.

Risks. Forrester has risk-adjusted the savings benefit downward by 10% in the table below due to the wide range of benefit and salary results among interviewed customers.

This yields a three-year, risk-adjusted PV of \$100,718.

IT Administrator Benefits: Calculation Table					
REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
B1	Labor savings (FTEs)	Interviews	0.5	0.5	0.5
B2	Fully loaded costs per IT administrator	Industry average	\$90,000	\$90,000	\$90,000
Bt	IT administrator benefits	B1*B2	\$45,000	\$45,000	\$45,000
	Risk adjustment	↓10%			
Btr	IT administrator benefits (risk-adjusted)		\$40,500	\$40,500	\$40,500

Developer Benefits

Developers can use IBM Security Verify APIs to integrate identity-related functions such as user management and authentication into applications. Using the dashboard, developers can see an overview of logins, SSO connections, and connected applications. From the configuration page, developers can manage the IBM Security Verify APIs that are being used in the applications and the granted permissions. Also, from the configuration page, developers can select from a variety of API clients to integrate into applications. In addition, developers can select a custom application template to integrate new OpenID Connect (OIDC) applications for single sign-on. Developers are building custom applications using step-by-step instructions and guided, wizard-like experiences to integrate the applications. Finally, developers are monitoring the performance of applications and digging into authentication event details to troubleshoot bugs.

Modeling and assumptions. The average application developer whose tasks include integrating identity-related functions into applications saves approximately 10% of their overall development time due to the features and functionality listed above.

The *Organization* has 10 developers saving a collective 10% (equal to one FTE). Forrester uses a fully loaded annual labor cost of \$120,000 for these developers. The annual benefit is a non-risk adjusted \$120,000.

Risks. To be conservative, Forrester has risk-adjusted (reduced) savings by 10% to reflect interviewed customers' variations in numbers of developers and regional variances in labor costs.

Our analysis yields a three-year risk-adjusted total PV of \$268,580.

Benefit risk is the risk that the business or technology needs of the organization may not be met by the investment, resulting in lower overall total benefits. The greater the uncertainty, the wider the potential range of outcomes for benefit estimates.

Developer Benefits: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
C1	Number of developers positively impacted	Organization	10	10	10
C2	Percent of each developer's time doing identity-related tasks	Interviews	10%	10%	10%
C3	Fully loaded costs of developers	Industry average	\$120,000	\$120,000	\$120,000
Ct	Developer benefits	$C1 \times C2 \times C3$	\$120,000	\$120,000	\$120,000
	Risk adjustment	↓10%			
Ctr	Developer benefits (risk-adjusted)		\$108,000	\$108,000	\$108,000

User Benefits

When users (employees or contractors) log into applications that require MFA, they can choose their most convenient authentication method, including passwordless options. From the launchpad, users can access the applications they are entitled to use, either with one click or using MFA. Users can browse company-approved applications and request access to those applications and provide justification if needed. Once access is approved either by IT or a delegated line-of-business manager, users can change their passwords and register authentication devices, i.e., smartphones for their accounts.

Modeling and assumptions. The average user saves 20 minutes per week due to the following features and functionality of IBM Security Verify:

- › A consistent, branded login experience across all platforms.
- › A simple user launchpad for access to applications.
- › User-centric security settings for device registration and password changes.

There are 15,000 employees and contractors who benefit from IBM Security Verify. At 20 minutes per week, each user saves 17.3 hours per year, rounded.

Risks. To be conservative, the savings below are risk-adjusted downward by 50% to reflect variations in interviewed customers' saved hours per user and regional labor compensation variances. This yields a three-year, risk-adjusted total PV of \$10,101,826.

"We have employees and contractors all over the world; in North America, EMEA and APAC, all benefiting from IBM Security Verify."

Security analyst



User Benefits: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
D1	Number of users	<i>Organization</i>	15,000	15,000	15,000
D2	Time saved per week per user (20 minutes or one-third of an hour)	Interviews/hours	0.3333	0.3333	0.3333
D3	Hours saved per year per user (rounded value shown)	D2*52 (weeks)	17.3	17.3	17.3
D4	Average hourly salary of users	Industry average \$65,000/2,080	\$31.25	\$31.25	\$31.25
Dt	User benefits	D1*D3*D4	\$8,124,188	\$8,124,188	\$8,124,188
	Risk adjustment	↓50%			
Dtr	User benefits (risk-adjusted)		\$4,062,094	\$4,062,094	\$4,062,094

Unquantified Benefits

In addition to the quantified benefits listed above, the interviewed customers discussed qualitative features or benefits from using IBM Security Verify, including:

- › **Preventing employees and contractors from leaking sensitive data and intellectual property.** According to respondents to Forrester's latest security survey, internal incidents caused 23% of the breaches of sensitive data at enterprises in the past 12 months.¹ Employees can leak data unwittingly or intentionally, often with catastrophic results for the organization.
- › **Maintain a competitive advantage and business agility in the age of digital business.** Digital transformation demands mapping of digital and nondigital assets to humans. Solid and secure identity and access management processes are the cornerstone of a secure digital business. Providing a consistent, secure, enjoyable, or at least easy-to-use technology environment — in which customers and enterprise and business partner users don't spend eons waiting to get all the necessary data and application access or to have their passwords reset — is an important component of maintaining competitive advantage.

"I know the benefits created by Security Verify have exceeded the costs. We are saving money in the areas of infrastructure cost avoidance, IAM administration, and the ability of developers to integrate identity-related functions into applications."

Security analyst



Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from customer to customer. There are scenarios in which a customer might choose to implement IBM Security Verify and later realize additional uses and business opportunities, as follows:

- › **The future ability to support an increasingly diverse device and application ecosystem such as internet of things (IoT).** The number of IoT-enabled connected devices will continue to grow in the future, whether it's wearables, embedded sensors, home appliances, vehicles, or heavy assets such as machinery.
- › **Use of enhanced security features.** Each customer was either using or interested in using the following MFA features: protecting accounts with an additional security layer; meeting compliance mandates with a common approach to MFA across applications, VPN, Windows desktops, and Linux; and infusing multiple modern user authentication options per resource, like SMS/email one-time passwords, IBM Verify app push notifications, fingerprint, face recognition, QR codes, FIDO2, and more.
- › **The ability to expand usage to the consumer population.** Each customer was focusing its initial deployment of IBM Security Verify on the workforce population. Customers are interested in deploying SSO and MFA capabilities to their significant consumer populations to realize the benefits of providing a secure yet seamless experience for their consumers.

The concept of flexibility is further described in Appendix A.

Flexibility, as defined by TEI, represents an investment in additional capacity or capability that could be turned into business benefit for a future additional investment. This provides an organization with the "right" or the ability to engage in future initiatives but not the obligation to do so.

Analysis Of Costs

Total Costs

REF.	BENEFIT	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Etr	Costs to build, maintain, and improve the hybrid IBM Security Verify environment	\$33,231	\$288,000	\$144,000	\$144,000	\$609,231	\$522,247
Ftr	IBM Security Verify fees	\$15,000	\$374,400	\$374,400	\$374,400	\$1,138,200	\$946,077
	Total costs (risk-adjusted)	\$48,231	\$662,400	\$518,400	\$518,400	\$1,747,431	\$1,468,324

Costs To Build, Maintain, And Improve The Hybrid IBM Security Verify Environment

Initially, the build and deployment processes at the composite *Organization* involve IT administrators spending 480 hours planning the migration from legacy IAM products to IBM Security Verify products for those applications that would be moved to the cloud. In Year 1, two FTEs support identity management development, maintenance, and improvements. In Years 2 and 3, one FTE supports ongoing maintenance, improvements, and administration.

Modeling and assumptions. Forrester uses an industry average fully loaded annual compensation rate of \$120,000 per year or \$57.69 (rounded) per hour for IT administrators.

Risks. Forrester has risk-adjusted these costs upward by 20% to reflect the variability of each interviewed customer's deployments and regional labor compensation variances.

The *Organization's* total labor costs to build, maintain, and improve IBM Security Verify are a risk-adjusted total PV of \$522,247.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the *Organization* expects total risk-adjusted costs to be a PV of almost \$1.5 million.

Costs To Build, Maintain, And Improve The Hybrid IBM Security Verify Environment: Calculation Table

REF.	COST	CALC./SOURCE	INITIAL	YEAR 1	YEAR 2	YEAR 3
E1	Labor hours to build and deploy	Interviews/hours	480	0	0	0
E2	Labor hours to maintain and improve	Interviews/hours	0	4,160	2,080	2,080
E3	Cost per FTE (rounded value shown)	120,000/2,080 hours	\$57.69	\$57.69	\$57.69	\$57.69
Et	Costs to build, maintain, and improve the hybrid IBM Security Verify environment	E1+E2*E3	\$27,692	\$240,000	\$120,000	\$120,000
	Risk adjustment	↑20%	□			
Etr	Costs to build, maintain, and improve the hybrid IBM Security Verify environment (risk-adjusted)		\$33,231	\$288,000	\$144,000	\$144,000

IBM Security Verify Fees

According to IBM, its Security Verify platform only charges for actual usage, so customers can add/remove users or even product use cases within Security Verify at their own pace. Security Verify pricing uses resource units as a metric to quantify a customer's dynamic usage between user populations and product use cases. Customers estimate the size of their workforce and consumer populations, average number of logins per year, and product use cases for each population.

Modeling and assumptions. The *Organization* incurs \$15,000 in professional services fees related to IBM helping with the implementation. IBM user fees are as follows:

- › Single-sign-on and multi-factor authentication for cloud and on-premises applications with an average of 2,000 logins per person per year: \$2.08 per month for each of the 15,000 employees/contractors or \$374,400 annually.

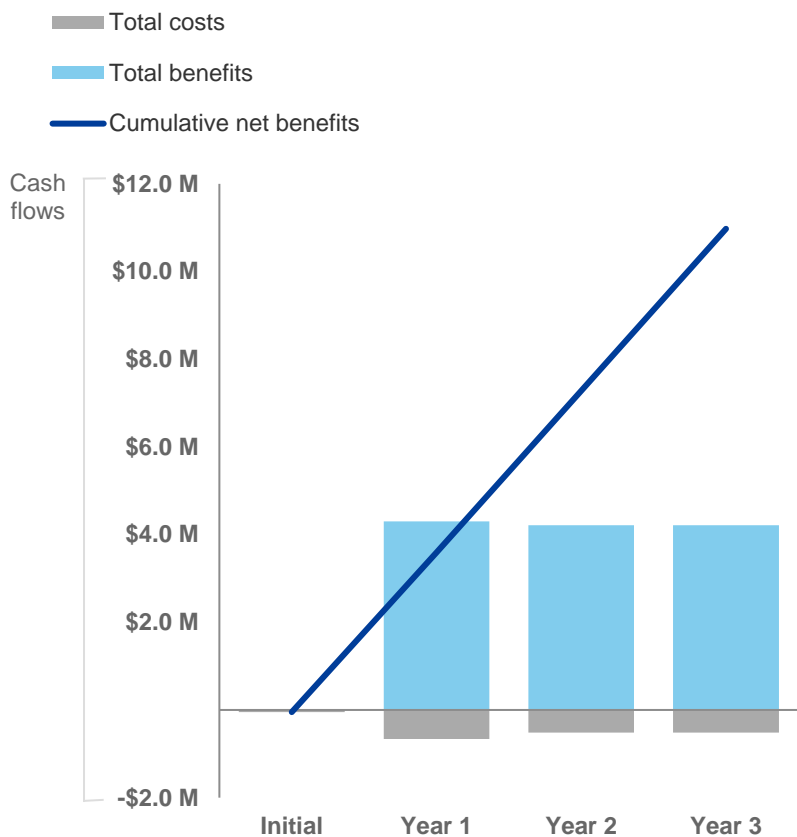
Risks. These costs are fixed quotes from IBM; therefore, Forrester has not risk-adjusted these costs. This yields a three-year total PV of \$946,077.

IBM Security Verify Fees: Calculation Table						
REF.	COST	CALC./SOURCE	INITIAL	YEAR 1	YEAR 2	YEAR 3
F1	Number of employees and contractors	Organization		15,000	15,000	15,000
F2	SSO and MFA for cloud and on-premises applications	Per employee per month/IBM		\$2.08	\$2.08	\$2.08
F3	Total SSO and MFA fees	(F1*F2)*12 months		\$374,400	\$374,400	\$374,400
F4	IBM professional services	Implementation fees/IBM	\$15,000	\$0	\$0	\$0
Ft	IBM Security Verify fees	F3+F4	\$15,000	\$374,400	\$374,400	\$374,400
	Risk adjustment	0%				
Ftr	IBM Security Verify fees (risk-adjusted)		\$15,000	\$374,400	\$374,400	\$374,400

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 interviewed organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.



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

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	(\$48,231)	(\$662,400)	(\$518,400)	(\$518,400)	(\$1,747,431)	(\$1,468,324)
Total benefits	\$0	\$4,300,594	\$4,210,594	\$4,210,594	\$12,721,781	\$10,552,942
Net benefits	(\$48,231)	\$3,638,194	\$3,692,194	\$3,692,194	\$10,974,350	\$9,084,618
ROI						619%
Payback period						< 6 months

If risk-adjusted costs, benefits, and ROI still demonstrate a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. Assuming normal success at mitigating risk, the risk-adjusted numbers should more closely reflect the expected outcome of the investment.

IBM Security Verify Overview

The following information is provided by IBM. Forrester has not validated any claims and does not endorse IBM Security Verify or its offerings.

ABOUT IBM SECURITY VERIFY

Provides identity-as-a-service for every user, including SSO, risk-based MFA and adaptive access, user lifecycle management, and identity analytics. It comes with thousands of prebuilt connectors to help customers quickly provide access to popular SaaS apps and prebuilt templates to help integrate in-house apps. Key features include the ability to:

- › Log in with federated single sign-on across cloud, mobile, and on-premises apps.
- › Enhance security with modern multifactor authentication methods.
- › Free up the help desk with user self-care options.
- › Adapt for context using risk-based authentication, IBM Trusteer integration, and adaptive access control.
- › Identify and mitigate access risks with identity analytics.
- › Enable user provisioning and lifecycle management.
- › Automate recertification campaigns.
- › Extend SSO to UEM with IBM Security MaaS360 integration.
- › Extend Zero Trust workflows with IBM QRadar and Resilient integration.
- › Protect on-premises applications from the cloud using a lightweight application gateway.
- › Troubleshoot events with live activity reports and diagnostics.
- › Empower managers to control access with delegation.

For more information about these features, please go to:

<https://www.ibm.com/products/verify-for-workforce-iam/details>

Appendix A: Total Economic Impact

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

Total Economic Impact Approach



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



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



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



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

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



PRESENT VALUE (PV)

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



NET PRESENT VALUE (NPV)

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



RETURN ON INVESTMENT (ROI)

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



DISCOUNT RATE

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



PAYBACK PERIOD

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

Appendix B: Endnotes

¹ Source: Forrester Analytics Business Technographics® Security Survey, 2020