FORRESTER®

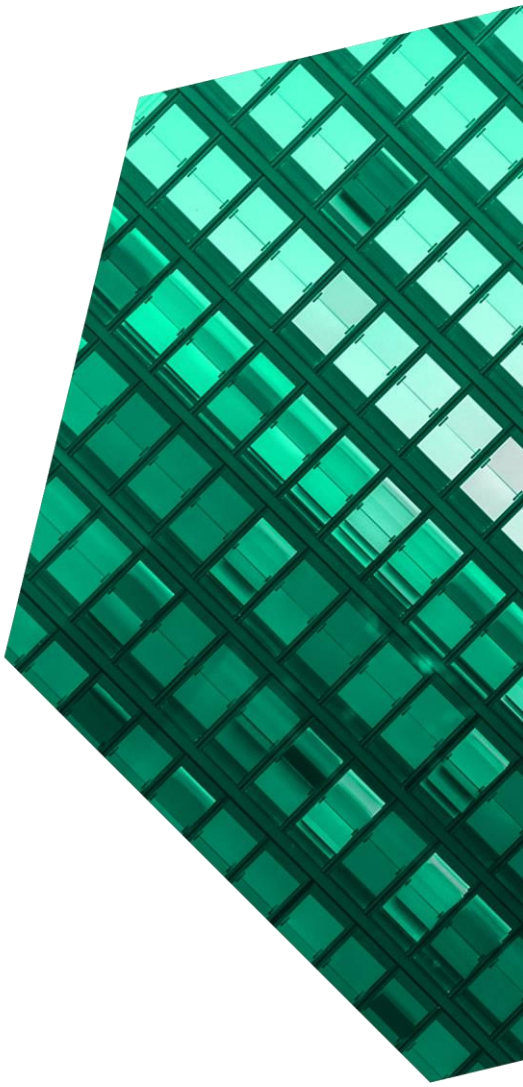
The Total Economic Impact™ Of The Maverics Identity Orchestration Platform

Cost Savings And Business Benefits Enabled By Strata Identity's Maverics Identity Orchestration Platform

OCTOBER 2023

Table Of Contents

Consultant: *James Davis*



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.

Executive Summary

Enterprises eager to embrace digital or cloud transformation (including the adoption of a multicloud approach), are often held back by the limitations of their current IAM systems, which makes modernization costly and overly complex. Strata Identity's Maverics Identity Orchestration Platform can significantly reduce these costs and speed up modernization projects while also offering the flexibility and agility needed to adopt new IAM systems and identity services.

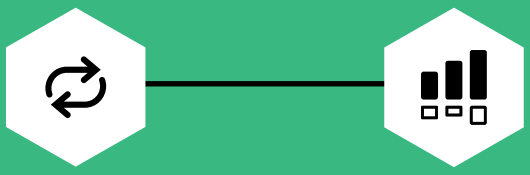
Strata Identity provides a unified platform for integrating any identity service or provider with an organization's applications to manage identity for workforce and customer identity needs. Strata's Maverics Identity Orchestration Platform enables organizations to migrate their identity infrastructures away from legacy identity providers (IDPs) to modern alternatives, thereby reducing operational complexity and costs. Maverics also offers enterprises the flexibility to integrate additional identity access management (IAM) vendors and quickly adopt new services in the future as their security and access needs change.

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

Time savings when migrating a high-complexity application with Maverics

1,950 hours

KEY STATISTICS



Return on investment (ROI)

407%

Net present value (NPV)

$11.12M

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed four representatives with experience using Maverics. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is a financial services organization with 25,000 employees and revenue of $5 billion per year. The organization has 400 enterprise applications, and it aims to migrate 200 of them to a modern, cloud-based IDP.

Prior to using Maverics, interviewees' organizations relied on individual developers to modernize application code or custom build integrations to work with a new IDP. Many faced unrealistic time constraints due to their existing IDPs reaching end of life (EOL). Additionally, the available migration options for legacy applications were limited and cost prohibitive. The organizations found identity management tools (e.g., application gateways,

reverse proxy products, and others required for authorization and directory services) to be too rigid. Moreover, the organizations needed a way to reduce the risk of vendor lock-in in the event that key IAM components (e.g., software for directory services) were discontinued.

After the investment in Maverics, interviewees' organizations expedited the migration of both legacy and standards-based applications to their new identity providers, which streamlined identity management and allowed them to comply with data-access and security regulations. Maverics not only cut down the time needed for application migration, but it also drove considerable cost savings due to lower licensing and maintenance fees post-migration. And because Maverics is a software-as-a-service (SaaS) offering, the organizations greatly reduced time spent maintaining legacy IDPs.

Interviewees described using Maverics to orchestrate identity for employees and business partners as part of broader initiatives such as migrating to the cloud, improving security and user experience for SaaS and external-facing websites, and increasing the speed of integration for corporate acquisitions.

KEY FINDINGS

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

- **Avoided costs of rewriting applications.** With Maverics, the composite organization migrates both nonstandard and modern enterprise applications in significantly less time compared to manually rewriting the apps to work with the target IDPs. This results in considerable cost savings. Over three years, the shorter development cycle is worth more than $10 million to the composite organization.
- **Cost savings due to the retirement of expensive legacy IAM infrastructure and services.** Adopting Maverics enables the composite organization to eliminate expensive licensing contracts for legacy products, which results in savings of $600,000 per year. The composite organization also saves on required professional services support costs associated with the legacy products. Over three years, the composite's savings due to the retirement of its legacy IAM infrastructure cycle are worth $2.1 million.
- **Reduced staffing for security and IT operations, which enables information security engineers to handle revenue-producing tasks.** The composite's prior solution required five FTEs to maintain the software, manage code, and execute other necessary changes. With Maverics, these employees shift to other security tasks, including management of modern IDP services for the organization's public-facing website. Maverics also enables the composite to update an internal employee training program without manual intervention, saving 1,400 hours of labor. Over three years, the security and IT operations cost savings total $1.7 million.

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

- **Mitigated risk of vendor lock-in.** The use of the Maverics platform enables the composite organization to easily migrate applications between IDP vendors and adopt advanced identity services such as passwordless multifactor authentication. Adopting Maverics enables the organization to mitigate the risk of a need for an expensive lift-and-shift migration in the future.
- **Accelerated integration of acquisitions.** The composite organization typically acquires other companies each year. Using Maverics enables coexistence and easier integration of existing IDP systems the acquired companies deployed.

- **Improved security posture.** By leveraging Strata's technology to migrate to a modern identity provider, the composite organization improves its security posture with the quicker deployment of multifactor authentication on complex applications. Maverics has the ability to provide a single view of users and roles, which enables better control over access and improves security.
- **Reduced code maintenance.** Strata performs the upgrades and code maintenance for Maverics, which allows the composite organization to focus on any needed core application code updates. The update process is accelerated by the ability to use existing DevOps automation tools.

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

- **Maverics licensing fees.** Pricing is based on the number of applications in production at a list price of $250 per application per month. The composite organization migrates 200 applications using Maverics at a yearly cost of $600,000. It also pays a fee based on the number of IDP integrations, which is priced at $2,500 per IDP per month. Because the composite has four IDP integrations, the resulting cost is $120,000 per year. The three-year PV cost of Maverics licensing for the composite is $1.8 million.
- **Total implementation costs.** The composite organization requires 1,000 hours to analyze its application environment and its links to IAM systems. Over the three-year period, the composite migrates 25 high-complexity applications and 175 low-complexity applications using Maverics. It spends 500 hours migrating applications in Year 1 and 1,000 hours in years 2 and 3. The composite's three-year PV cost of implementing Maverics is $355,000.
- **Professional support services.** The composite organization purchases a 100-hour block of professional services to support internal staff during the initial project implementation and rollout. Additionally, the organization contracts for enterprise-level technical support at a cost of $172,500 per year. The composite's three-year PV cost of professional support services is $476,000.
- **Initial and ongoing costs.** The composite's initial training costs include five senior developers who spend 10 hours in training for Maverics. Ongoing system management of Strata software requires one software developer in Year 1 and two developers in years 2 and 3, and each developer spending 200 hours to maintain the software. The composite's three-year PV of initial and ongoing costs is $90,000.

The representative interviews and financial analysis found that a composite organization experiences benefits of $13.85 million over three years versus costs of $2.73 million, adding up to a net present value (NPV) of $11.12 million and an ROI of 407%.

ROI of Maverics Identity Orchestration Platform

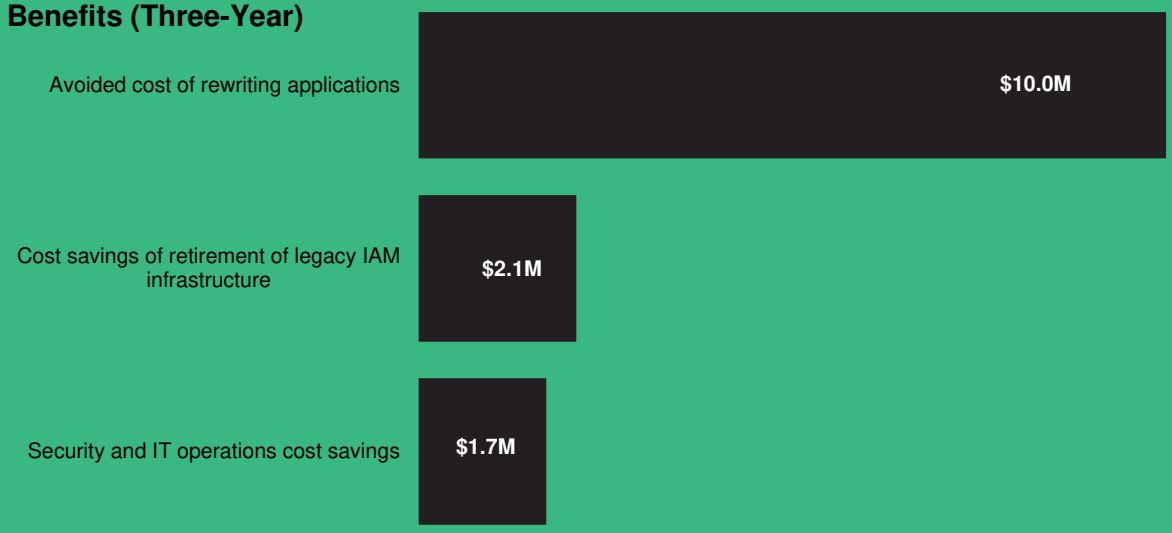
407%

ROI
407%

BENEFITS PV
$13.85M

NPV
$11.12M

PAYBACK
<6 months



“Having to maintain legacy code is a huge time suck for my team. [With Strata,] I’m getting a lot more time to work on revenue-generating code instead of maintenance code.”

— Senior VP of technology, financial services

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 the Maverics Identity Orchestration Platform.

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 Maverics can have on an organization.

DUE DILIGENCE

Interviewed Strata Identity stakeholders and Forrester analysts to gather data relative to the Maverics Identity Orchestration Platform.

INTERVIEWS

Interviewed four representatives at organizations using Maverics 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 Maverics Identity Orchestration Platform Customer Journey

Drivers leading to the Maverics investment

Interviews

Role	Industry	Region	Use cases	Employees
Senior VP of technology	Financial services	Western US	• Migrate to new IDP • Control access to apps	550
Security manager, IAM	State government	US	• Add modern authentication to apps • Enable access to cloud services	>50,000
Principal engineer	Financial services	Eastern US	• Migrate to new IDP • Protect access to critical local apps	25,000
Information security manager	Retail	US	• Migrate to new IDP • Control access to apps	>50,000

KEY CHALLENGES

Before implementing the Maverics Identity Orchestration Platform, interviewees' organizations struggled with the need for manual code changes to each application while quickly modernizing their IDPs. Enterprisewide initiatives included moving to a new or additional cloud infrastructure service provider, adopting new SaaS applications, and increasing flexibility required to adapt to changes in business strategy and needs. These modernization initiatives were designed to improve IAM processes by leveraging technology such as user-friendly, passwordless authentication. However, IT and security teams were under pressure and faced deadlines brought on by different IAM vendors ending support for legacy identity providers.

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

- **High cost of updating legacy applications to standards-based cloud identity management systems.** Efforts to modernize IAM systems were necessitated by looming product end-of-life or end-of-service with the organizations' existing IAM vendors. They had hundreds or even thousands of applications to update, and many legacy applications were mission critical. Rewriting applications (i.e., refactoring) would be time consuming and prohibitively expensive. Not migrating meant spending millions of dollars per year on licensing and support services as well as increasing the risk of security incidents.

  The senior VP of technology at a financial services company said: "[Because] we were no longer going to be able to get security updates, we felt like we were between a rock and a hard place. We had to find some solution to migrate out of our [previous] IDP and move to a proper IDP [and] then do the pen tests I regularly conduct every quarter."

- **Vendor lock-in, which could result in costly service and support contracts for obsolete products.** Interviewees said their organizations examined using stopgap measures such as expensive vendor-specific application gateways to enable legacy applications to access modern IDPs. The alternative was to continue using legacy identity solutions by signing long-term contracts for service and support in addition to

paying licensing fees that could reach millions of dollars per year.

- **A need to update applications as additional cloud service and identity providers are adopted.** Interviewees' organizations had sizeable portfolios of applications, and each time a new cloud service provider was used, a portion of the portfolio needed to be refactored. Any time their organizations acquired another company, the same process of integrating different IAM and IDPs would occur. Interviewees said they did not want their organizations to combine tools from a variety of authorization and directory providers to build the identity access functionality they needed.

"We weren't looking for three or four tools that would be best of breed to try to make this all work. We wanted one single tool that could fix all the problems."

Senior VP of technology, financial

SOLUTION REQUIREMENTS

The interviewees' organizations searched for a solution that could:

- Link on-premises databases and applications to the cloud.
- Enable quick migration of existing applications to Microsoft Entra Verified ID, Okta, Oracle Cloud, and other vendors.
- Centralize identity management across a variety of tools to improve the orchestration of roles and access.
- Allow for easy integration of any new tools.
- Reduce the risk of vendor lock-in from future EOL notices in areas such as directory services products.
- Be flexible enough to support future requirements such as anticipated regulatory standards for data access and security.

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite company, and an ROI analysis that illustrates the areas financially affected. The composite organization is representative of the four interviewees, and it is used to present the aggregate financial analysis in the next section. The composite organization has the following characteristics:

Description of composite. The US-based financial services company generates $5 billion in revenue annually, and it operates in numerous states via branch offices as well as online services. The organization has 25,000 employees including 2,500 IT employees and an IAM team with five full-time employees. It has 400 applications that serve a variety of back- and front-office functions.

Deployment characteristics. The organization prioritizes the migration of 200 applications to a new IDP because many use legacy proprietary authentication protocols that are associated with products that are no longer being serviced. Other applications use standard protocols but still require some refactoring as the company moves to standardize on a cloud-based IDP.

Key Assumptions

- **$5 billion annual revenue**
- **US operations**
- **25,000 employees**
- **Migrates 200 of 400 enterprise applications to new identity provider**

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	Avoided cost of rewriting applications	$2,030,625	$4,061,250	$6,412,500	$12,504,375	$10,020,234
Btr	Cost savings of retirement of legacy IAM infrastructure	$569,813	$863,831	$1,177,290	$2,610,934	$2,116,437
Ctr	Security and IT operations cost savings	$577,030	$671,840	$839,800	$2,088,670	$1,710,767
	Total benefits (risk-adjusted)	$3,177,468	$5,596,921	$8,429,590	$17,203,979	$13,847,438

AVOIDED COST OF REWRITING APPLICATIONS

Evidence and data. Interviewees' organizations invested in the Maverics platform to migrate legacy and modern enterprise applications to new IDPs with significantly less engineering effort and cost compared to other vendors they evaluated.

- The organizations identified key applications that needed to be migrated first and found they were able to migrate upwards of 15 complex legacy applications in the first year of use with single applications finished in a matter of weeks instead of requiring multiple months of engineering effort.
- The security manager, IAM, at a state government agency said their organization's IT department migrated its first legacy application in six weeks. With its previous solution the organization required two developers to work an estimated 5,000 hours migrating a more complex application. But with Maverics, this takes 1,700 hours. The interviewee said they expect it to take less than a week to migrate each modern application.
- A senior VP of technology in the financial services industry said that with Maverics, their organization replaced single sign-on (SSO) for 60 websites that would otherwise require custom code to use a new IDP. The organization saved an estimated $500,000 because of the time saved compared to rewriting each site for use with the new IDP. The manual approach to modernizing the SSO would have required three mid-level developers working over the course of a month to create a single SSO for the new IDP. But using Maverics, a single developer could integrate the SSO for a web app in 4 hours.
- The principal engineer at a financial services firm in the banking industry said their organization needed to migrate mission-critical applications to a new IDP because support for its current system was going to be discontinued. The organization used one of the 50 key applications to be migrated for transactions conducted with the Fedwire payment system, so any downtime meant lost revenue. The organization saved an estimated $380,000 in application rewriting costs for that one application using Maverics, and it experienced zero application downtime.
- The information security manager for a large retailer said: "We had 200 applications that we had planned to migrate away from our legacy SSO solution. In the first year, we quickly migrated half of the low-hanging fruit that was owned by the various security teams." In the second year, the organization also migrated more complex applications, which the interviewee

estimated would have taken 2,000 hours per complex application to manually rewrite and test code. The organization considered approximately 20 of the 200 applications to be complex.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- Analysis of the composite's IT environment and application dependencies identifies 400 enterprise applications. Of these, 200 are prioritized for migration to a new IDP. These applications are either for internal use by employees or business partners.
- Of the 200 applications, 25 are considered "high complexity" because of a combination of factors, including the amount of code, the use of proprietary protocols for authentication, and third-party callouts for authorization rules. Each high-complexity application takes 2,000 hours to refactor.
- The remaining 175 applications are considered "low-complexity" and "middle-complexity" due to smaller code bases. Many also use a standardized authentication protocol such as Security Assertion Markup Language (SAML) or OpenID Connect (OIDC). However, they are being refactored because the composite wants to provide an easier migration path in the future, including the integration of on-premises directory systems with cloud-based systems. Other scenarios include the consolidation of IAM and IDP vendors while maintaining access to cloud-based applications. Each low- to middle-complexity application takes 550 hours to refactor.
- The average fully burdened cost of a developer is $95 per hour.

Risks. The impact of this benefit may vary based on the following factors:

- The IT staff's level of experience in estimating the time required to modify an application, which may be affected by their familiarity with and access to the legacy code base and the code quality.
- The experience level of developers.
- The cost of compensation for developers.
- Regulatory requirements, which vary by industry.

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 $10 million.

> **"We had to have an expensive consultant write new code for an end-of-life platform. … It hurt my soul. But what do you do? Our app needs some changes, and this impacts how users log in."**
>
> *Security manager, IAM, state government*

Avoided Cost Of Rewriting Applications					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	High-complexity applications migrated with Strata Identity	Composite	5	10	10
A2	Estimated time to refactor high-complexity applications (hours)	Interviews	2,000	2,000	2,000
A3	Low-complexity applications migrated with Strata Identity	Composite	25	50	100
A4	Estimated time to refactor low-/medium-complexity applications (hours)	Interviews	550	550	550
A5	Subtotal: Total annual time saved (hours)	(A1*A2)+(A3*A4)	23,750	47,500	75,000
A6	Average fully burdened hourly cost of a developer FTE	TEI standard	$95	$95	$95
At	Avoided cost of rewriting applications	A5*A6	$2,256,250	$4,512,500	$7,125,000
	Risk adjustment	↓10%			
Atr	Avoided cost of rewriting applications (risk-adjusted)		$2,030,625	$4,061,250	$6,412,500
	Three-year total: $12,504,375		**Three-year present value: $10,020,234**		

COST SAVINGS OF RETIREMENT OF LEGACY IAM INFRASTRUCTURE

Evidence and data. Interviewees said that their organizations' prior IAM systems were expensive in terms of licensing, professional support costs, and the costs of ongoing maintenance. Some were faced with the need to sign costly support services contracts that could exceed the cost of licenses for soon-to-be EOL products. Their prior IAM systems required on-premises equipment that also added to the overall costs of the solutions.

After implementing Maverics, the organizations were able to deprecate the software and either decommission or repurpose the underlying servers, storage, and networking equipment infrastructures. This resulted in significant savings.

- The security manager, IAM, of a state government agency said their organization faced a deadline to migrate a critical and complex application that used a legacy on-premises IDP to a new IDP that was cloud-based. The interviewee reported the agency needed to hire an expensive consultant to write new code for an end-of-life platform. With Maverics, it migrated to the new system by the deadline without the need for outside services. The security manager said the agency saved an estimated $3 million per year on licensing costs and infrastructure even when accounting for the cost of the new system.
- The principal engineer for a financial services firm said: "[We've] got so many different weird things in [our industry], and then everybody goes out and gets their own application that needs SSO or needs to run on dedicated servers. We don't have anything out there [that is sharing infrastructure]."

  Using Maverics enabled the organization to free up at least 20 Windows and hyperconverged infrastructure components (HCIs) required by its prior IAM solution. The interviewee reported that HCI systems — which combine computing, networking, and storage into a single cluster — and Windows servers cost between $10,000 to $20,000 each and that annual maintenance costs were $375,000 and $115,000 for infrastructure.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization saves $600,000 per year on avoided licensing costs for the prior solution.

"[My organization] will save about $3 million per year once [it migrates] off [its prior solution] and [shuts] it down."

Security manager, IAM, state government

- The composite organization saves $865,000 over a three-year period for services and support costs. These costs for the EOL solution start at 18% of the licensing cost in Year 1 and increase by 5% in Year 2 and by 10% in Year 3 to reflect the higher prices the vendor charges for supporting a discontinued product.
- The composite organization experiences savings of $115,000 per year on hardware costs.
- Because the composite retires its prior solution, the organization saves $281,000 per year on administration and maintenance costs.
- The composite organization recaptures 50% of cost savings in Year 1, 75% in Year 2, and 100% in Year 3 as the migration and reassignment of staff is fully completed.

Risks. Benefits realized may vary based on the following factors:

- The licensing costs of the organization's legacy IAM solution, which varies from vendor to vendor.
- The amount of professional services and support the organization requires.
- The salaries of staff who perform administration and maintenance on the systems.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $2.1 million.

Cost Savings Of Retirement Of Legacy IAM Infrastructure

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Avoided licensing costs of legacy IAM infrastructure	Composite	$600,000	$600,000	$600,000
B2	Third-party professional services (including support for EOL products)	Composite	$270,000	$283,500	$311,850
B3	Hardware or cloud resource costs	Interviews	$115,000	$115,000	$115,000
B4	Legacy system administration and maintenance costs	Interviews	$281,250	$281,250	$281,250
B5	Percent of cost recaptured	Composite	50%	75%	100%
Bt	Cost savings of retirement of legacy IAM infrastructure	(B1+B2+B3+B4) *B5	$633,125	$959,813	$1,308,100
	Risk adjustment	↓10%			
Btr	Cost savings of retirement of legacy IAM infrastructure (risk-adjusted)		$569,813	$863,831	$1,177,290
	Three-year total: $2,610,934		**Three-year present value: $2,116,437**		

SECURITY AND IT OPERATIONS COST SAVINGS

Evidence and data. Interviewees noted that legacy SSO and IDP solutions required significant resources to manage on an ongoing basis. Their organizations sourced these systems from different vendors, and all were deployed on-premises. The systems required varying degrees of manual software updates conducted by staff along with associated hardware, storage, and networking equipment needed to run the vendor's software. In addition, unscheduled patches for security issues added to the required maintenance time. Updates represented a security issue because any gap between vulnerability disclosure and system patching represented increased risk for breaches.

Interviewees reported that after implementing Maverics, their organizations reduced time spent on software maintenance because the platform can be deployed as a hybrid, air-gapped SaaS product. Some of the organizations were able to repurpose staff to higher-value tasks, and others were able to assign more junior staff to regular configuration changes, which is something they couldn't do with the prior solution. The ability to automate maintenance and configuration processes saved time and reduced security issues and downtime due to misconfiguration errors during manual data entry.

- The principal engineer at a financial services organization said their team experienced a lot of "headaches" with its prior IAM solution and that it required a team of nine full-time employees to manage both the employee- and customer-facing applications. They said: "Over the years, we've had so many issues with it. … People didn't trust it to do simple things like patching and rebooting the servers."
  They said Strata's Maverics platform saved the time needed for change requests along with the manual patching and rebooting of systems, and that this enabled the organization to shift the employees to managing authorization and security for customers, including for a website that has millions of unique visitors each month.
- The security manager, IAM, for a state government agency said their organization's prior solution required the coordination of five staff members and 4 hours for a major version upgrade, but this is now automated with Maverics. They said: "It's a SaaS solution. They'll keep their application at the latest version, and all my staff does now is make any modifications to applications that might impact the connection to that SaaS solution."
- The senior VP of technology at a financial services organization stated that their firm's prior IAM solution required an estimated 1.5 FTEs of developer time to maintain legacy code (including time spent on product upgrades and patches), while Maverics only required 8 hours per month from a junior developer. The prior solution also lacked the ability to centralize identity management, which required tabular data exports that needed manual audits. Maverics simplified the process of updating access and permissions for 200 different roles and 10,000 users per month, and the interviewee said it will enable the organization to meet future standards for data access and security.
- The principal engineer of a financial services firm said that their organization has an extensive training program on the company intranet, and it requires authentication to monitor employees' progress and completion. The content contains links that direct employees to SharePoint documents, and updating those documents to be compatible with a new IDP would mean changing roughly 2,800 links across hundreds of files. The company created a service extension with Maverics that automatically rebuilds the link request and sends the information to the new IDP, saving an estimated 1,400 hours of labor and enabling the migration to be completed on time.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- After implementing Maverics, the composite reassigns a total of three information security engineers to other tasks in Year 1, with a total of four and five reassigned in years 2 and 3, respectively.
- The average fully burdened cost of a full-time information security engineer is $85 per hour.
- The composite saves 1,400 hours on intranet maintenance in Year 1.
- The average fully burdened cost of a full-time SharePoint administrator is $55 per hour.

Risks. Benefits realized may vary based on the following factors:

- The complexity of the organization's existing IAM environment and the number of IDPs needed.
- The number of employees, which correlates with managing access permissions and roles.
- The compensation rates of information security engineers.
- The organization's ability to extend IAM systems for use cases beyond traditional access management (e.g., proxy-based rebuilding of hyperlink requests).

Results. To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year, risk-adjusted total PV of $1.7 million.

"There were a lot of headaches with [the prior vendor]. Now, [my organization is] running Strata, and they patch and reboot on their own. There are no issues whatsoever."

Principal engineer, financial services

Security And IT Operations Cost Savings

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Information security engineer FTEs reassigned	Composite	3	4	5
C2	Average fully burdened hourly cost of an information security engineer FTE	TEI standard	$85	$85	$85
C3	Subtotal: Information security engineer cost savings	C1*(C2*2080)	$530,400	$707,200	$884,000
C4	Intranet maintenance time savings (hours)	Interviews	1,400	0	0
C5	Average fully burdened hourly cost of a SharePoint administrator FTE	TEI standard	$55	$55	$55
C6	Subtotal: Intranet maintenance cost savings	C4*C5	$77,000	$0	$0
Ct	Security and IT operations cost savings	C3+C6	$607,400	$707,200	$884,000
	Risk adjustment	↓5%			
Ctr	Security and IT operations cost savings (risk-adjusted)		$577,030	$671,840	$839,800
	Three-year total: $2,088,670		**Three-year present value: $1,710,767**		

UNQUANTIFIED BENEFITS

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

- **Mitigated risk of vendor lock-in.** Interviewees noted that getting out of vendor lock-in with prior solutions was a key reason for selecting Strata's Maverics. Even for applications that already used standards-based authentication protocols, their organizations used Maverics as an identity orchestration layer to insulate themselves from the product deprecation and vendor consolidation they expect in the future. The principal engineer at a financial services firm said: "The writing's on the wall. Our vendor isn't putting further development into the product we use for our on-premises directory service. We still need to have an identity provider rooted on-premises so key applications don't have cloud dependency." They added that their organization can use Maverics to orchestrate the authentication by pulling information from the legacy on-premises IDP system and using that data to build the authorization token that the new IDP uses with some configuration changes instead of recoding applications entirely.
- **Accelerated integration of acquisitions.** A scenario related to vendor lock-in plays out in corporate M&A transactions as IT departments are tasked with integrating new identity providers to allow employees at acquired companies access to necessary applications. The senior VP of technology at a financial services provider said their company acquires dozens of companies each year: "Last year, we were sometimes acquiring two companies per week. There's a lot of integration work to be done. There's an opportunity for [Maverics] to help solve some of the issues we're having with using Azure AD to handle everything."
- **Improved security posture.** Interviewees said that using a modern IDP was critical to efforts to improve their organizations' security in the near term and to make auditing easier in the future when expected regulations come into play. The senior VP of technology at a financial services organization said: "[With our previous solution] we [didn't] know really who [had] access to what unless we [sat] down and [did] a manual audit." The problem is that the organization shares marketing and other materials with external partners with employees who change roles or leave those companies. The interviewee said: "They may be looking at stuff that they shouldn't anymore because it's hard to identify." The organization used Maverics to orchestrate the movement of data out of the old system and into the new IDP, and the senior VP said Maverics improved security by providing a single view of users and their roles to manage permission to applications and content.
- **Reduced code maintenance.** Interviewees said that with Maverics upgrades and code maintenance performed by Strata, the ability to automate changes to applications could be simplified through automation tools. The security manager, IAM, at a state government agency said: "The nice thing about Strata is we can use automation tools for managing their upgrades and maintenance. That's not going to take resources at all."

FLEXIBILITY

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

- **Futureproofing against potential changes in protocols or other industry standards for authentication.** The senior VP of technology at a financial services organization said: "We didn't want to have to worry about new protocols or

new authentication types. We wanted some level of comfort that the product was going to be kind of kept up to date with any new stuff [such as a change in the SAML protocol]. We wanted the tool to be kind of a Swiss Army knife as far as protocol and types of authentication mechanisms were concerned."

- **Customizing Maverics for unique use cases.** Interviewees said another benefit of Maverics is having the ability to leverage its capabilities for uses beyond authentication by enabling the creation of service extensions to the platform. The principal engineer at a financial services organization said their firm created an extension, tested it, and deployed it in a matter of hours: "The Strata product is very customizable," they said. "[We're] deploying the application to [our] servers through automation using standard CI/CD pipeline tools. Not every company might have the people on staff to set up something like that. But if they don't, the Strata team does."
- **Integrating with DevOps tooling.** Interviewees said their organizations used the UI as a standard method for customers to configure Maverics, but they said they liked having the ability to choose between using the UI or scripting changes via automation tools, which they described as a time-saving feature. The senior VP of technology at a financial services organization said: "We liked [Maverics] because we felt like the configuration was simple enough that almost anybody could do it. We could integrate YAML (yet another markup language) scripts directly into our CI/CD pipeline eventually and automate the whole thing versus going into a UI."

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

"The flexibility of the solution, the extensibility/customization, and the white-glove service we received from the Strata team made it extremely attractive and helped us accomplish our goals."

Information security manager, retail

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**
Dtr	Maverics licensing fees	$0	$720,000	$720,000	$720,000	$2,160,000	$1,790,533
Etr	Total implementation costs	$92,000	$54,625	$109,250	$163,875	$419,750	$355,070
Ftr	Total professional support services	$26,250	$189,000	$189,000	$189,000	$593,250	$496,265
Gtr	Initial and ongoing costs	$5,775	$21,105	$41,055	$41,055	$108,990	$89,736
	Total costs (risk-adjusted)	$124,025	$984,730	$1,059,305	$1,113,930	$3,281,990	$2,731,604

MAVERICS LICENSING FEES

Evidence and data. Pricing for the prior solutions of the interviewees' organizations had an array of variables for licensing on a perpetual or term basis, and some IAM components came as part of an offering tier. Interviewees said their firms' legacy IAM products typically price on a per-subscriber (e.g., per-employee) basis and that this often leaves organizations with costs based on licenses that aren't used.

The principal engineer for a financial services company said: "Our migration ranged from applications as small as something that's being logged into maybe, like, 30 people to applications that's logged in to buy our entire workforce, which is about 25,000 users."

They also noted that having fees based on the number of applications and IDP integrations instead of users was one of the factors that made Strata licensing more attractive than pricing for their organization's prior solution.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- After assessing its application portfolio, the composite organization plans to migrate 200 applications during a three-year period. The company pays a fee of $250 per application.
- The composite organization has four IDP integrations based on its use of multiple cloud services. The cost of each integration is $2,500 per IDP per month.
- Pricing may vary. Contact Strata Identity for additional details.

Risks. The licensing costs can vary based on factors such as:

- The organization's number of applications.
- The organization's number of IDP integrations.

Results. While organizations will experience different costs based on these variables, Forrester used standard list pricing from Strata. Therefore, Forrester did not add any risk adjustment, yielding a three-year, total PV (discounted at 10%) of $1.8 million.

Maverics Licensing Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
D1	Total applications in production	Composite	0	200	200	200
D2	Monthly subscription fee per application	Interviews	$0	$250	$250	$250
D3	Subtotal: Total Maverics application fees	D1*(D2*12)	$0	$600,000	$600,000	$600,000
D4	IDP integrations	Composite	0	4	4	4
D5	Monthly subscription fee per IDP per month	Interviews	$0	$2,500	$2,500	$2,500
D6	Subtotal: Total Maverics IDP integration fees	D4*(D5*12)	$0	$120,000	$120,000	$120,000
Dt	Maverics licensing fees	D3+D6	$0	$720,000	$720,000	$720,000
	Risk adjustment	0%				
Dtr	Maverics licensing fees (risk-adjusted)		$0	$720,000	$720,000	$720,000
	Three-year total: $2,160,000			**Three-year present value: $1,790,533**		

TOTAL IMPLEMENTATION COSTS

Evidence and data. Interviewees described a range of tasks in the process of migrating applications from their organizations' prior IAM environments, including:

- Analyzing the identity and application environment to quantify the number of applications to be migrated.
- Conducting an initial proof-of-concept trial on a single application.
- Classifying and prioritizing applications into categories such as "high complexity" and "medium- and low-complexity" and planning out a timeline for the migration process.
- Coordinating with security teams and application owners on cutover procedures and timing.

Interviewees also provided the following details:

- The senior VP of technology for a financial services firm said their organization had a team of three employees work on the proof-of-concept for approximately 9 hours per week over a six-week period and that it used roughly the same resources to plan the implementation. The organization assigned a mid-level developer to refactor applications for the Maverics platform, and the interviewee said the process took 4 hours per application. The prior solution required three developers working a total of four weeks for a single new application integration.
- The information security manager for a retail company said: "Low-complexity applications were very simple and took us minutes to transfer configurations. We'd then just need to coordinate with app owners on a cutover and that time would vary, but [it] resulted in basically zero downtime." They added that high-complexity applications added some application testing time but said, "Transferring configurations was also quick, and

we could reuse a lot of configurations." They also noted that high-complexity applications each required 2 hours of engineering and testing time.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization spends 1,000 hours analyzing its identity and application environment.
- The composite organization uses IT analysts to perform this task.
- The average fully burdened cost of an IT analyst FTE is $80 per hour.
- In Year 1, the composite organization migrates five high-complexity applications. In each of years 2 and 3, it migrates 10 high-complexity applications for a total of 25.
- The composite requires 50 hours of effort to migrate one high-complexity application with Maverics.
- In Year 1, the composite migrates 25 low-complexity applications. It migrates another 50 applications in Year 2 and another 100 in Year 3.
- The effort required to migrate one low-complexity application is 10 hours.

Total applications migrated with Maverics

200

Risks. Implementation costs may vary based on the following factors:

- The level of experience the organization's staff has in estimating time required to modify an application.
- Time estimates, which may be affected by familiarity with the code base, access to the legacy code base, and the code quality.
- The experience level of developers on staff.
- The total number of applications and their complexity.
- The compensation rates of developers.

> **"One of the main selection criteria we were looking at was ease of implementation because we don't have a ton of developers that I can put on this project."**
>
> *Senior VP of technology, financial services*

Results. To account for these risks, Forrester adjusted this cost upward by 15%, yielding a three-year, risk-adjusted total PV of $355,000.

Total Implementation Costs						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
E1	Average time required to analyze identity and application environment (hours)	Interviews	1,000	0	0	0
E2	Average fully burdened hourly cost of an IT analyst FTE	TEI standard	$80	$80	$80	$80
E3	Subtotal: Analyze identity and application environment	E1*E2	$80,000	$0	$0	$0
E4	High-complexity applications migrated	Interviews	0	5	10	10
E5	Average time required to migrate one high-complexity application with Strata Identity (hours)	Composite	0	50	50	50
E6	Low-complexity applications migrated	Interviews	0	25	50	100
E7	Average time required to migrate one low-complexity application with Strata Identity (hours)	Composite	0	10	10	10
E8	Total time to migrate applications (hours)	(E4*E5)+(E6*E7)	0	500	1,000	1,500
E9	Average fully burdened hourly cost of a developer FTE	TEI standard	$0	$95	$95	$95
E10	Subtotal: Internal implementation costs	E8*E9	$0	$47,500	$95,000	$142,500
Et	Total implementation costs	E3+E10	$80,000	$47,500	$95,000	$142,500
	Risk adjustment	↑15%				
Etr	Total implementation costs (risk-adjusted)		$92,000	$54,625	$109,250	$163,875
	Three-year total: $419,750			**Three-year present value: $355,070**		

TOTAL PROFESSIONAL SUPPORT SERVICES

Evidence and data. Interviewees said their organizations utilized the professional services of Strata for both implementation and ongoing support. They noted that these costs were significantly lower compared to the costs of their prior vendors, and they attributed this to the ease of implementation of Maverics and its SaaS deployment model.

Modeling and assumptions. Forrester assumes the following about the composite organization:

- The composite organization buys an optional 100 hours of professional services from Strata to assist with the implementation of Maverics.
- The composite organization buys technical support services. These services are priced at 25% of the total licensing cost.

Risks. Professional services costs may vary based on the following factors:

- The level of experience staff has with deploying and managing IAM technologies.
- The criticality of an application to core business operations where the cost of downtime can significantly exceed the cost of external support services.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $496,000.

Total Professional Support Services						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
F1	Technical support	Composite	$0	$180,000	$180,000	$180,000
F2	100-hour block of professional services	Composite	$25,000	$0	$0	$0
Ft	Total professional support services	F1+F2	$25,000	$180,000	$180,000	$180,000
	Risk adjustment	↑5%				
Ftr	Total professional support services (risk-adjusted)		$26,250	$189,000	$189,000	$189,000
	Three-year total: $593,250			**Three-year present value: $496,265**		

INITIAL AND ONGOING COSTS

Evidence and data. Interviewees said their organizations incurred costs for initial training on the Maverics platform as well as ongoing costs for administration. Interviewees found that onboarding with Strata generally provided all the training needed to use the platform and that their organizations could perform ongoing management using fewer resources than with their prior solutions.

- Interviewees noted that familiarity with modern identity technology and protocols provided the basis for quickly using the Maverics platform. The security manager, IAM, at a state government agency said: "[the YAML language for configuration files used by both Maverics and other DevOps tools is] well-known within our technical teams. There's not a lot [needed] there on training, and [my organization is] not paying [for] any additional training on Maverics."
- The senior VP of a financial services firm said their organization assigned a junior developer to conducting ongoing management. They estimated the developer spends 4 hours per month on maintenance and configuration tasks.
- The security manager, IAM, at a state government agency said: "The nice thing about [Maverics] is we have an automated method for managing the upgrades and maintenance. That's not going to take resources at all."
- The principal engineer for a financial services firm said their organization only requires one FTE working 4 hours per week on maintenance and configuration tasks.

Modeling and assumptions. Forrester assumes the following for the composite organization:

- For ongoing maintenance and administration of the Maverics platform, the composite organization uses one software developer in Year 1 and two developers in years 2 and 3. These employees spend a total of 200 hours on these tasks each year.
- This average fully burdened rate of a developer FTE is $95 per hour.
- The composite organization trains five senior developers to use the Maverics platform during the initial phase of the project. The training program takes 10 hours, and these developers then train one other employee on the software in the subsequent years.
- The average fully burdened rate of a senior developer FTE is $110 per hour.

Risks. Initial and ongoing costs may vary based on the following factors:

- The level of experience the organization's staff has with DevOps tools and managing IAM technologies.
- The compensation rates of developers.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $88,000.

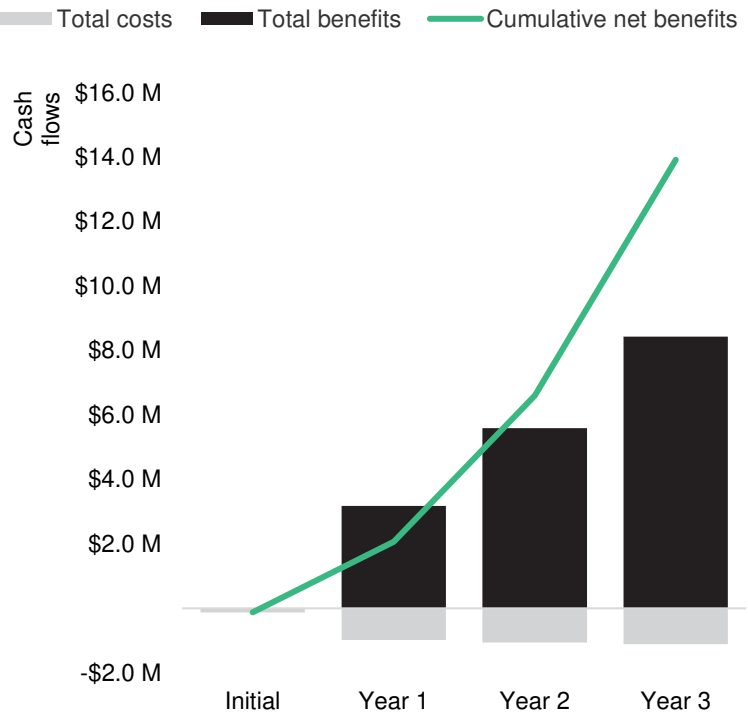
Initial And Ongoing Costs

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
G1	Software developers	Composite	0	1	2	2
G2	Average fully burdened hourly cost of a software developer	TEI standard	$0	$95	$95	$95
G3	Time developers spend on ongoing maintenance and administration of the Maverics platform (hours)	Composite	0	200	200	200
G4	Subtotal: Administrative cost of software developers	G1*G2*G3	$0	$19,000	$38,000	$38,000
G5	Senior developers trained to use the Maverics platform	TEI standard	5	1	1	1
G6	Average fully burdened hourly cost of a senior developer	TEI standard	$110	$110	$110	$110
G7	Training time (hours)	Interviews	10	10	10	10
G8	Subtotal: Training costs	G5*G6*G7	$5,500	$1,100	$1,100	$1,100
Gt	Initial and ongoing costs	G4+G8	$5,500	$20,100	$39,100	$39,100
	Risk adjustment	↑5%				
Gtr	Initial and ongoing costs (risk-adjusted)		$5,775	$21,105	$41,055	$41,055
	Three-year total: $108,990		**Three-year present value: $89,736**			

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, 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	($124,025)	($984,730)	($1,059,305)	($1,113,930)	($3,281,990)	($2,731,604)
Total benefits	$0	$3,177,468	$5,596,921	$8,429,590	$17,203,979	$13,847,438
Net benefits	($124,025)	$2,192,738	$4,537,616	$7,315,660	$13,921,989	$11,115,834
ROI						407%
Payback						<6 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

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

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

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

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

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

PRESENT VALUE (PV)

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

NET PRESENT VALUE (NPV)

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

RETURN ON INVESTMENT (ROI)

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

DISCOUNT RATE

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

PAYBACK PERIOD

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

Appendix B: Supplemental Material

Related Forrester Research

"The Forrester Tech Tide™: Identity And Access Management (IAM), Q1 2023," Forrester Research, Inc., February 8, 2023.

"The Forrester Wave™: Customer Identity And Access Management, Q4 2022," Forrester Research, Inc., November 7, 2022.

Appendix C: Endnotes

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


FORRESTER®