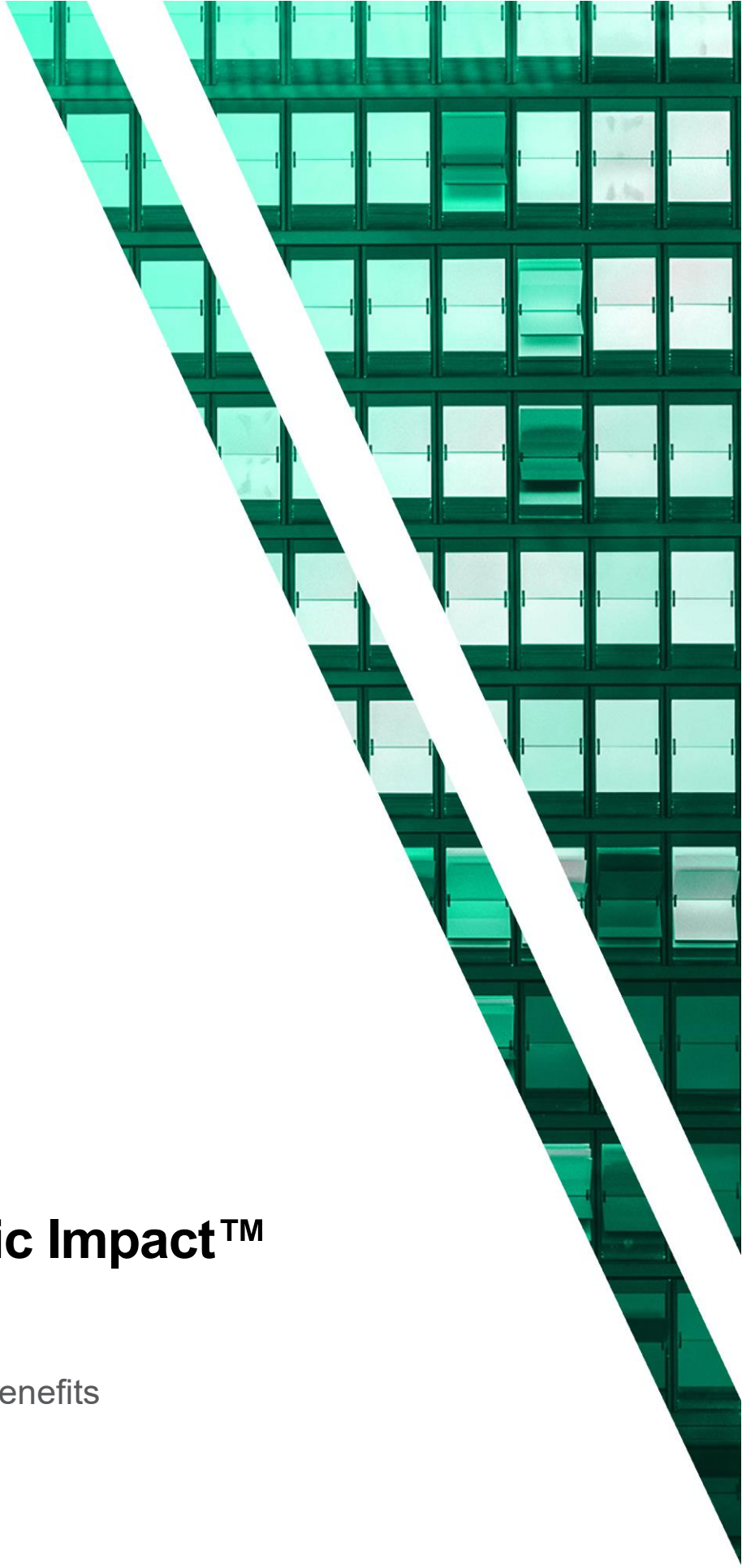
FORRESTER®



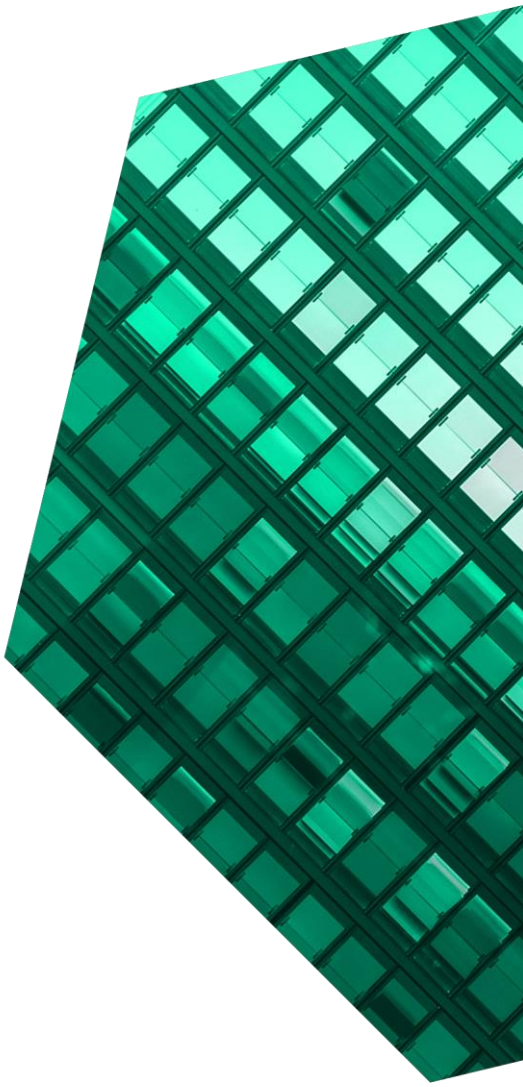
The Total Economic Impact™ Of Microsoft Entra

Cost Savings And Business Benefits Enabled By Microsoft Entra

MARCH 2023

Table Of Contents

Consulting Team: Julia Fadzeyeva
Claudia Heaney



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.

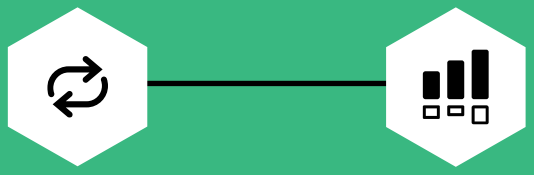
Executive Summary

In a world where 20% of security breaches happen as a result of weak or stolen credentials, identity and access management professionals aim to strengthen security and compliance without creating hurdles to business growth or user experience.[1] The Microsoft Entra family of products helps organizations strengthen security posture while also eliminating complexity and extra costs by simplifying and modernizing the IAM technology stack, shortening product development timelines, and improving user productivity.

Microsoft Entra brings together identity and access solutions into a comprehensive product family for multicloud environments. Microsoft Entra helps organizations protect access to any app or resource for any user or workload, verify and secure every identity and every access request, discover permissions and govern access, and simplify user experience with intelligent real-time access controls all in one place. This study focuses on three products from the Microsoft Entra family: Azure Active Directory (Azure AD), Microsoft Entra Permissions Management, and Microsoft Entra Verified ID.

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

KEY STATISTICS



Return on investment (ROI)
240%

Net present value (NPV)
$8.57M

Reduced likelihood of a breach
20%

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed 10 representatives of eight organizations with experience using Azure AD, Microsoft Entra Permissions Management, and Microsoft Entra Verified ID. For the purposes of this study, Forrester aggregated the interviewees' experiences and combined the results into a single composite organization that is an organization with 10,000 employees and 10 identity and access management (IAM) professionals.

These interviewees noted that prior to using Microsoft Entra, their organizations used on-premises Active Directory and various identity federation systems for legacy applications plus several different cloud-based identity solutions for software-as-a-service (SaaS) and line-of-business apps. In this complex environment, it was not easy for the organizations to provide the level of security and regulatory compliance they sought to achieve. It was also

expensive to maintain and manage the disparate IAM tools, and end users craved more consistent and streamlined authentication experiences.

After the investment in Microsoft Entra, the interviewees' organizations strengthened their security postures, reduced complexity and cost of IAM technologies and infrastructures, empowered developers to build new products faster, and improved end-user and partner experiences.

KEY FINDINGS

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

- **$2.1 million in savings due to reduction of legacy infrastructure and previous IAM solutions.** Moving from on-premises identity federation systems like Active Directory Federation Services (AD FS) and a combination of several IAM point-solutions to Microsoft Entra allows the composite organization to eliminate infrastructure and associated management effort, and it significantly lowers its software license costs.
- **50% increase to IAM team efficiency.** The composite organization relies on several Microsoft Entra products to streamline onboarding, provisioning, and offboarding, to reduce manual effort required for compliance-related data collection and management, and to automate multicloud permissions management. This frees its dedicated IAM team to focus on more strategic business objectives.
- **20% reduced likelihood of a breach from strengthened security posture.** By securing all applications and identities with Azure AD, the composite organization improves visibility, implements more granular risk-based policies, and ensures protection against phishing, credential stuffing, and other malicious techniques that exploit compromised user credentials. With Microsoft Entra Permissions Management, the organization also rightsizes unused and excessive permissions and automates on-demand, time-bound privilege escalations to further reduce security risks.
- **Shortened time to receive access to resources by 90% due to improved product development velocity.** Previously, when the composite's developers requested new permissions, their projects could be interrupted by an average of two days while they waited for access. With Microsoft Entra Permissions Management, they receive access within hours, which saves them time and helps keep development projects on schedule.
- **75% reduction to password reset requests due to self-service.** By enabling self-service password resets, the composite organization empowers users to reset their own passwords. This aligns the experience to user expectations and significantly reduces the number of password reset requests submitted to the help desk.
- **Average productivity increase of 13 hours per year for business end users.** The composite considers more time available to get work done as a proxy for improved business outcomes because the value someone adds should be at least equal to what they are paid.

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

- **Working with Microsoft as a trusted IAM partner.** All interviewees said that working with fewer vendors is easier and that Microsoft provides very good customer service and support.
- **Ensuring compliance with regulatory standards.** Several interviewees' organizations operate in highly regulated markets, and moving

to the cloud with Microsoft Entra helped them adhere to their industries' requirements.

- **Using External Identities in Microsoft Entra to streamline secure access for partners.** Several of the interviewees' organizations use Microsoft Entra to securely interact with partners, distributors, suppliers, or vendors without incurring the costs and security risks of managing those peripheral identities.

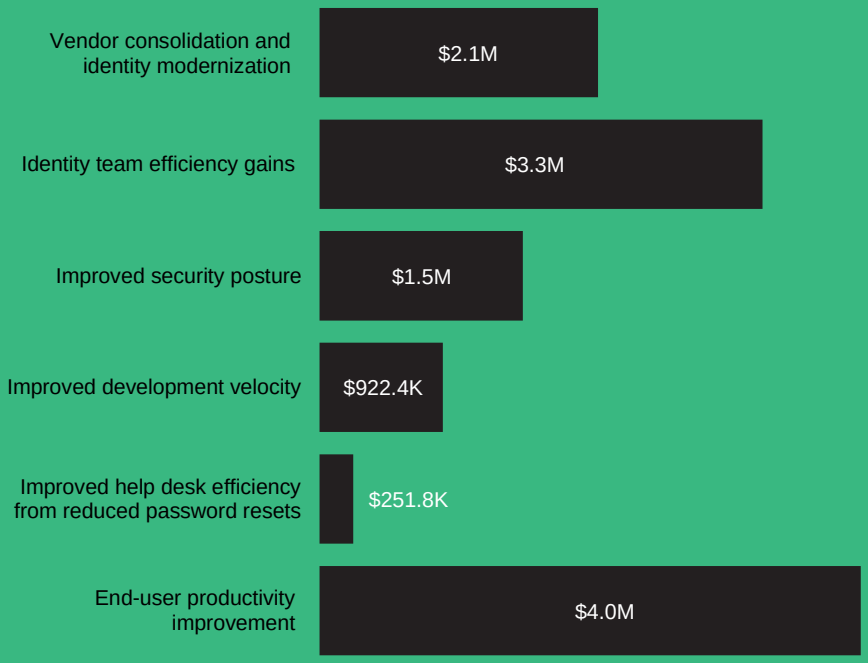
Costs. Three-year, risk-adjusted PV costs for the composite organization include:

- **Microsoft license fees of $2 million.** The composite organization pays license costs based on the number of Azure AD users per month and the number of resources per cloud who use Permissions Management.
- **Internal effort costs of $1.5 million.** The internal efforts associated with the composite's Microsoft Entra investment include a six-month initial rollout, app integration, training for the IAM team, and ongoing management of the Entra product family and relevant projects.

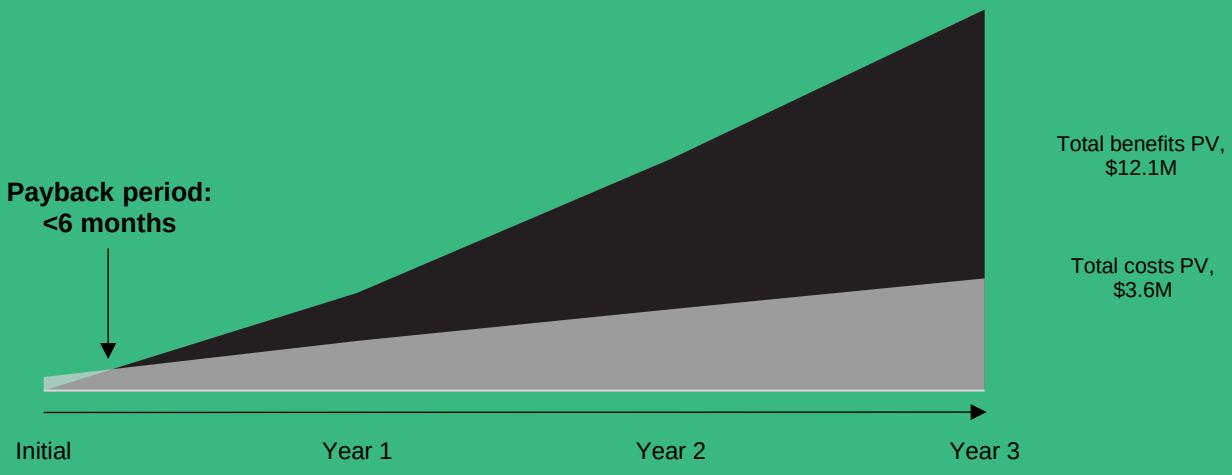
The representative interviews and financial analysis found that a composite organization experiences benefits of $12.14 million over three years versus costs of $3.57 million, adding up to a net present value (NPV) of $8.57 million and an ROI of 240%.

ROI	BENEFITS PV	NPV	PAYBACK
240%	**$12.14M**	**$8.57M**	**<6 months**

Benefits (Three-Year)



Financial Summary



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 Microsoft Entra.

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 Microsoft Entra can have on an organization.

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

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Microsoft 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 Microsoft Entra.

Microsoft 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.

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

DUE DILIGENCE

Interviewed Microsoft stakeholders and Forrester analyst to gather data relative to Microsoft Entra.

INTERVIEWS

Interviewed 10 representatives at eight organizations using Microsoft Entra 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 Microsoft Entra Customer Journey

Drivers leading to the Microsoft Entra investment

Interviews

Role	Industry	Region	Number of employees
Director of solutions architecture	Insurance	HQ: Europe Operations: Global	55,000
Identity and access team lead	Software	HQ: US Operations: Global	3,000
Principal IT engineer	Semiconductor	HQ: US Operations: Global	45,000
Senior security engineer	Software	HQ: US Operations: Global	25,000
Head of enterprise security architecture	Insurance	HQ: US Operations: Global	95,000
Senior IT system engineer	Manufacturing	HQ: Europe Operations: Europe	12,000
Co-founder and chief technology officer; Founder and chief executive officer	Security	HQ: Canada Operations: Canada	<50
Senior manager for productivity services and networking automations; Senior solutions architect, identity and access management space	Software	HQ: US Operations: Global	13,000

KEY CHALLENGES

Before adopting Microsoft Entra, interviewees' organizations managed identity and access with multiple point solutions. The complexity of managing and integrating multiple tools resulted in inefficient use of both financial and labor resources.

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

- **Legacy solutions did not provide adequate security and did not satisfy compliance requirements.** Attacks targeting weak credentials for employees or partner third parties became more frequent and complex over time, and interviewees said that meeting these threats required modern tools that are well-integrated with each other. A director of solutions architecture at an insurance company said, "A lot of the businesses we are in are strictly regulated and we have to have these kinds of controls in place."

> **"We just tried to replicate what we had on-prem, and we thought that we should be able to manage this challenge in cloud using our on-prem practices and tools. Very quickly, we figured out it was not good enough."**
>
> *Head of enterprise security architecture, insurance*

- **Historically accumulated IAM tools introduced high complexity and costs.** The director of solutions architecture – whose insurance organization holds a Microsoft 365 E5 license – told Forrester: "In the past, a lot of folks have gone out and bought tools with comparable capabilities at the highest price point. We wanted

to reevaluate and try to leverage more of the Microsoft tools to get a return on investment." In addition to controlling license costs, interviewees indicated that setting and managing their organizations' prior point solutions required significant effort.

- **End-user and business productivity suffered with prior solutions.** Interviewees recognized the need for IT and IAM teams to enable business growth and contribute to employee productivity rather than create interruptions, delays, and frustration. Their organizations' legacy on-premises identity and access management solutions made it too difficult for employees to maintain their working flows and stay productive.

INVESTMENT OBJECTIVES

The interviewees' organizations searched for a solution that could:

- Strengthen security through modern authentication capabilities that could offer strong protection again credential-related attacks.
- Improve regulatory compliance.
- Reduce costs through license rationalization.
- Reduce the level of effort of managing IAM tools and infrastructure without significant additional training.

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 interviewees' 10 interviewees, and it is used to present the aggregate financial analysis in the next section.

Description of composite. The composite organization is a global, business-to-business (B2B) organization with 10,000 full-time employees. It employs 10 IAM professionals who interact with Microsoft Entra solutions on a regular basis.

Before implementing Microsoft Entra, the composite organization had several IAM solutions in place that

"It was our strategic goal to move to a cloud identity first. We wanted to have Azure AD as our source of authority because it is the one place where we truly have a single identity. Whereas on-prem, a lot of people had many different identities to do many different things in the various domains. So, our strategic direction is cloud first."

Director of solutions architecture, insurance

"A trigger catalyst for us to move to Azure AD from AD FS was the fact that credential stuffing had become a problem. It was easy to figure out [our] CEO's username, and that was a big problem on the AD FS side. Moving to Azure AD has meant that we have not had to deal with credential-stuffing attacks."

Identity and access team lead, software

supported a core set of applications based on nonmodern authentication methods. Users needed to remember multiple credentials, IT had very little visibility into who accessed applications, and there were no self-service capabilities enabled for IAM issues. With multiple solutions not seamlessly integrated, the organization was concerned about security gaps and heightened risks.

Deployment characteristics. The composite organization enables single sign-on (SSO), requires multifactor authentication (MFA) for all applications and all users, and allows employees to access applications through managed mobile devices, desktops, or laptops. The IT team integrates security logs with the enterprise security information and event management (SIEM) solution to improve visibility and the SecOps team's ability to investigate and remediate incidents.

KEY ASSUMPTIONS

- **10,000 employees**
- **10 IAM professionals use Microsoft Entra**
- **Enables SSO and MFA for all employees**

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	Vendor consolidation and identity modernization	$866,250	$832,500	$810,000	$2,508,750	$2,084,082
Btr	Identity team efficiency gains	$675,000	$1,377,000	$2,079,000	$4,131,000	$3,313,636
Ctr	Improved security posture	$505,130	$673,506	$673,506	$1,852,142	$1,521,840
Dtr	Improved development velocity	$0	$584,640	$584,640	$1,169,280	$922,422
Etr	Improved help desk efficiency from reduced password resets	$101,250	$101,250	$101,250	$303,750	$251,794
Ftr	End-user productivity improvement	$1,280,000	$1,600,000	$2,080,000	$4,960,000	$4,048,685
	Total benefits (risk-adjusted)	$3,427,630	$5,168,896	$6,328,396	$14,924,922	$12,142,459

VENDOR CONSOLIDATION AND IDENTITY MODERNIZATION

Evidence and data. Interviewees' organizations looked to reduce the cost and complexity of their IAM infrastructures, which (in the prior states) typically included a legacy on-premises presence and SaaS-based point solutions. With Microsoft Entra, interviewees' organizations could sunset their legacy IAM infrastructures including the physical and proxy servers as well as previous identity-as-a-service (IDaaS) solutions because Azure AD now manages and secures authentication for all applications including non-Microsoft apps. Moving from a point-solution-integration approach to Microsoft Entra lowered license costs for interviewees' organizations. For those that already had Microsoft 365 E5 licenses, the savings were often significant if considered a sunk cost for the business case. Interviewees shared the following examples of how their organizations reduced license costs:

- The identity and access team lead at a software company told Forrester that after their organization replaced its legacy on-premises IAM solution, it saved $200,000 to $250,000 annually in human capital costs from managing the associated infrastructure.
- The principal IT engineer at a semiconductor organization said that before using Microsoft Entra, their company relied on a third-party MFA solution that cost more than $1 million dollars a year. The organization also relied on a separate point solution for onboarding new external accounts, which proved costly as well. Once the organization implemented Azure AD, it sunset both tools. The interviewee said: "Again, just like MFA, Microsoft is offering this [as a part of the Microsoft 365 E5 license] up to a point. So, there's a strong financial driver for switching."
- Similarly, the director of solutions architecture at an insurance company said that prior to using Microsoft Entra, their organization previously bought multiple tools to manage employee identities and authentication. With Azure AD, the organization reevaluated its approach and made

a “replace list” of identity tools that it is replacing with Microsoft Entra products. The interviewee said, “We can definitely [save] millions of dollars per year [as] we get rid of prior tools and leverage Azure AD.” At the time of the interview, the organization was also going through the process of closing down its legacy on-premises environment, which decision-makers expected to deliver significant savings in infrastructure and operational costs.

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

- Microsoft Entra license costs are at parity with the license cost of its prior point solution.
- The legacy IAM solution leveraged seven physical servers, five of which were due for replacement in Year 1 and two of which were due for replacement in Year 2. Moving to Azure AD eliminates the need to replace these servers.
- The composite organization reassigns one full-time employee (FTE) responsible for managing IAM-related, on-premises infrastructure.

Risks. The following factors may affect the magnitude of this benefit and are reflected in the risk-adjustment percentage:

- The number of servers associated with the legacy on-premises infrastructure.
- Annual costs related to legacy IAM software and solutions.
- The speed at which the organization is able to sunset legacy infrastructure.
- Whether or not the company already has Microsoft 365 E5 licenses and considers that to be a sunk cost, which would affect the savings associated with prior-license spend.

“We wanted to centralize all of our IAM tools, and we decided to use Microsoft Entra because of what Microsoft offered in terms of its security and enterprise relationships, and also [because of] the fact that our CISO felt comfortable about having our identity managed by Microsoft.”

Identity and access team lead, software

“With the migration from AD FS to Azure AD, we looked to reduce our dependence on on-prem infrastructure [and] the … burden and liability around owning that infrastructure, making sure that it’s patched, and moving to something that can operate at scale — especially as it relates to identity. We wanted to get the benefits of cloud-based heuristics for risky sign-ins [and] things that Azure AD offers that AD FS did not.”

Identity and access team lead, software

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

Vendor Consolidation And Identity Modernization					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
A1	License fees for legacy IAM tools	Interviews	$750,000	$750,000	$750,000
A2	Number of IAM machines sunset as a result of Azure AD investment	Interviews	5	2	0
A3	Cost per machine	Composite	$12,500	$12,500	$12,500
A4	Number of FTEs who manage IAM-related infrastructure	Composite	1	1	1
A5	Fully burdened annual salary of an IAM FTE	Composite	$150,000	$150,000	$150,000
At	Vendor consolidation and identity modernization	A1+A2*A3+ A4*A5	$962,500	$925,000	$900,000
	Risk adjustment	↓10%			
Atr	Vendor consolidation and identity modernization (risk-adjusted)		$866,250	$832,500	$810,000
	Three-year total: $2,508,750			**Three-year present value: $2,084,082**	

IDENTITY TEAM EFFICIENCY GAINS

Evidence and data. Interviewees said their organizations spent a significant amount of resources on management and maintenance of their previous IAM solutions, and that this left little time for projects that could further strengthen security postures or improve user experiences. In addition to managing IAM solutions, the organizations also struggled to manage permissions for their multicloud environments. The head of enterprise security architecture at an insurance company said, "Previously it was a dump of who was using what permissions, and it was up to the manager to decide whether it was good or bad."

By migrating to Azure AD, the organizations were able to leverage the benefits of a modern and comprehensive cloud solution, which freed time for their dedicated IAM teams to focus on adding value to the businesses, and even reallocating some workers to other teams that needed additional resources.

- Interviewees' organizations reduced the number of FTEs required to manage their respective environments. Because the organizations eliminated on-premises infrastructures and reduced the number of point solutions, they no longer needed to dedicate as much talent to IAM solutions management and could dedicate these FTEs to more strategic IAM initiatives and to improving employee experiences.
- A senior security engineer in the software industry said their organization revamped its provisioning model with Azure AD. They said: "During the [COVID-19] pandemic, it became vitally important that we implement self-provisioning. We sent people laptops and they could sign into them, and that was a great win." This change allowed the organization to free three FTEs per region from provisioning devices

on behalf of the users. It also meant end users could get their devices sooner and did not lose productive time waiting for their devices to be provisioned.

- The identity and access team lead at another software company said their organization had several compliance regimens that required gathering evidence for audits at least four times per year. This collection was a cumbersome process both for the tech-compliance team and for the people who collected that evidence. With Azure AD, all of the identities and access management approval workflows became accessible in one system. The team lead said: "There were five operational teams spread across the company that were responsible for various identity workflows. Now, we have been able to centralize almost all of it to a single ops team."
- The head of enterprise security architecture in the insurance industry said that before using Microsoft Entra, their company was overwhelmed with managing permissions and had to hire outside consultants to supplement its IAM team. Although the organization spent millions of dollars investing in consultant labor, it still lacked full visibility into permissions, automation, and true multicloud expertise. After adopting Microsoft Entra Permissions Management and over the course of six months to one year, the company terminated all external contracts and hired internal employees. The interviewee said: "Overall, about 70-plus consultants [were] replaced by 11 full-time employees and the tooling we have. Eventually, we saved $6 million to $7 million dollars [in] the process over the course of two and a half years."

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

- Before the Azure AD investment, the IAM team consisted of 10 FTEs.
- Three FTEs who previously focused on onboarding, offboarding, and provisioning are reallocated to other, value-add tasks.
- One FTE who previously performed general maintenance activities in the legacy IAM environment is reallocated to other, value-add tasks.
- One FTE who previously performed compliance activities is reassigned.
- The composite organization adopts Permissions Management in Year 1. As a result, in Year 2, the composite organization eliminates 50% of contractor resources and fully terminates them in Year 3.

Risks. The following factors may affect the magnitude of this benefit and are reflected in the risk-adjustment percentage:

- The size of the organization's IAM team before investing in Azure AD.
- The organization's commitment to reevaluate current systems and workflows and adopt Azure AD.
- The need for external resources to manage permissions in the multicloud environment.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $3.3 million.

Identity Team Efficiency Gains					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
B1	IAM team members with previous IAM solution	Composite	10	10	10
B2	Reduction in effort for onboarding/ offboarding and provisioning (FTEs)	Interviews	3	3	3
B3	Reduction in effort for managing previous IAM solution (FTEs)	Interviews	1	1	1
B4	Reduction in compliance effort with previous IAM solution (FTEs)	Interviews	1	1	1
B5	Total reduction in effort for IAM team	(B2+B3+B4)/B1	50%	50%	50%
B6	Fully burdened annual salary of an IAM FTE	Composite	$150,000	$150,000	$150,000
B7	Subtotal: Identity team efficiency gains	B1*B5*B6	$750,000	$750,000	$750,000
B8	External contractors required to run identity provisioning and permissions management	Composite	5	5	5
B9	Contractor hourly rate	TEI standard	$150	$150	$150
B10	Contractor labor cost attributed to identity provisioning and permissions management	B8*B9*2,080	$1,560,000	$1,560,000	$1,560,000
B11	Reduction to contractor labor with Microsoft Permissions Management	Interviews	0%	50%	100%
B12	Subtotal: Labor efficiency in identity provisioning and permissions management	B10*B11	$0	$780,000	$1,560,000
Bt	Identity team efficiency gains	B7+B12	$750,000	$1,530,000	$2,310,000
	Risk adjustment	↓10%			
Btr	Identity team efficiency gains (risk-adjusted)		$675,000	$1,377,000	$2,079,000
	Three-year total: $4,131,000			**Three-year present value: $3,313,636**	

IMPROVED SECURITY POSTURE

Evidence and data. Interviewees told Forrester that improving security posture was among the top drivers for their organizations' investments in Microsoft Entra. According to Forrester research, 20% of external attacks are carried out with the use of weak or stolen credentials.[3] Additionally, Microsoft research says it sees 1,287 password attacks every second (i.e., more than 111 million per day), and that in 2022, it saw 5.8 billion password breach replay attacks per month, 31 million phishing attacks per month, and 5 million password spray attacks per month.[4]

Interviewees said that by securing all applications with Azure AD, their organizations were able to improve visibility, implement granular risk-based policies to ensure that employees only had access to the applications that they need, and — through MFA — proactively protect against phishing, credential stuffing, and other techniques that exploit compromised user credentials.

Interviewees shared the following examples of how their organizations' security postures improved:

- The director of solutions architecture at an insurance company told Forrester that, with Azure AD, their organization is more secure. Before using Azure AD, security logs from the legacy IAM solutions were either nonexistent or ineffectual regarding any real impact to organizational security. The director said: "Now we have all the guardrails in place [so] that people can't do what I'll say [are] silly things. We're definitely more secure now as far as breaches go. Where it's helped is the logging and understanding of what's happening in the tenant. The visibility is way better than anything we've ever had with on-prem."
- The principal IT engineer at a semiconductor company described how Conditional Access was an important component to protect organizational assets. They said: "Today, we use phishing-resistant credentials, and they are extremely attractive to the security-minded folks like me because they provide a good user experience but also deliver high-level security for us. We also heavily rely on Conditional Access. And I would put that at the top of the list."

"Azure AD gives us the ability to be a bit more granular about what folks can do and not give them [the] keys to the castle. So, that's a big benefit."

Director of solutions architecture, insurance

"For us, stronger security posture was [the] number-one reason for starting the adoption of passwordless [authentication]."

Director of solutions architecture, insurance

- Some interviewees said that beyond SSO and MFA, their organizations had started on their journeys to passwordless authentication. More than two-thirds of security decision-makers in a Forrester survey reported that their organizations are currently adopting passwordless authentication for the workforce.[5] While security professionals try to minimize security risks by encouraging employees to use strong passwords, this approach does not seem sufficient to prevent current cybersecurity threats. According to a 2022 report, more than 80% of web-application breaches are attributed to stolen credentials.[6] By no longer requiring users to enter passwords, organizations can reduce the risk of a security incident.
- Microsoft Entra Permissions Management enabled interviewees' organizations to rightsize permissions and manage identities across multiple clouds, which also contributed to improved security. The multicloud visibility enabled by Permissions Management helped IAM teams see how many permissions employees were granted and whether this access was necessary for their roles across Microsoft Azure, Amazon Web Services (AWS), and Google Cloud. The head of enterprise security architecture at an insurance company said: "Before, developers asked for super user access

so that they could do their job and … didn't have to come back to the security team again, but that introduced a lot of risk. They were doing it with good intent, but it caused security challenges." With Microsoft Entra Permissions Management, the organization restricted developers' privileges and automated an on-demand, time-bound permission request that would allow users to get access and troubleshoot an issue if there is an emergency.

The same interviewee also said that using Microsoft Entra Permissions Management in conjunction with Azure AD allowed their organization to become more secure while dedicating fewer resources to the IAM activities due to automations available in the tool. They said: "Without Microsoft Entra Permissions Management, the security was a nightmare for us. Security is never a done deal, but now we can focus on many other areas [such as] enhancing our DNS security, web posture, and all. Previously, all our time was spent on identity, access, [and] provisioning. Now, we [can] get out of it and focus on other weak links where we can invest."

"For us, the main benefit of Microsoft Entra [Permissions Management] is visibility and a possibility to rightsize permissions based on findings [and] based on analytics."

Senior IT system engineer, manufacturing

"If you do want to remove someone's permissions, you need to defend why you're doing it and why they don't need it or [say] the reason you think they don't need it or [share] where your information is coming from. That was quite hard to do without Microsoft Entra Permissions Management."

Senior IT system engineer, manufacturing

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

- Before using Microsoft Entra, the composite organization experienced an annual average of 3.1 material security breaches at an average per-breach cost of $750,000.[7]
- After completing the Microsoft Entra deployment, the composite organization reduces its likelihood of a breach by 15% in Year 1 and by 20% in Years 2 and 3, compared to the prior state.
- Breaches negatively impact 33% of the composite's 10,000 total employees at a time, and the average breach-related downtime is four hours.
- The average employee's fully burdened hourly rate (i.e., including salary, benefits, and payroll taxes) is $40.

Risks. The size of the benefit can vary based on:

- The prior frequency of breaches and the total cost of a breach.

- The Microsoft Entra products implemented and the organization's maturity as it relates to threat detection and remediation.
- The number of employees affected by a breach and their average fully burdened rates.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $1.5 million.

Improved Security Posture

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Average annual number of material breaches before using Microsoft Entra	Forrester research	3.1	3.1	3.1
C2	Average cost of a breach	Interviews	$750,000	$750,000	$750,000
C3	Reduced likelihood of a breach with Microsoft Entra	Interviews	15%	20%	20%
C4	Subtotal: Reduced risk of a major security breach	C1*C2*C3	$348,750	$465,000	$465,000
C5	Total employees	Composite	10,000	10,000	10,000
C6	Average percent of employees impacted	Forrester research	33%	33%	33%
C7	Average downtime per employee per breach (hours)	Forrester research	4	4	4
C8	Average fully burdened hourly rate of an employee	TEI standard	$40	$40	$40
C9	Subtotal: Reduced employee downtime during a breach	C1*C3*C5*C6*C7*C8	$245,520	$327,360	$327,360
Ct	Improved security posture	C4+C9	$594,270	$792,360	$792,360
	Risk adjustment	↓15%			
Ctr	Improved security posture (risk-adjusted)		$505,130	$673,506	$673,506
	Three-year total: $1,852,142			**Three-year present value: $1,521,840**	

IMPROVED DEVELOPMENT VELOCITY

Evidence and data. Developer experience as well as the balance between security and inefficiencies in the development process were top of mind for interviewees. They said that when their organizations tightened security components and obligated developers to request permissions every time they needed new access, this tended to have a negative impact on product-development speed. A developer's work on a project could get interrupted by up to several days while the developer was waiting for access, and any project as a whole could get delayed by weeks or even months as those interruptions added up.

Security teams have a difficult task and are often viewed as a department that sets obstacles for the rest of the business, and changing this perception can be challenging. According to the interviewees, enabling Microsoft Entra Permissions Management was an "aha" moment because it produced a tangible improvement in security team members' experiences as well.

- The head of enterprise security architecture at an insurance organization said: “Every three weeks, a developer probably made a request two to three times and had to wait on average 48 hours to get permission. With hundreds of developers, it added up, and product development could get delayed by even a quarter or so.”

  The company relied on Microsoft Entra Permissions Management with its permission on-demand feature, which allows users to request just-in-time and just-enough access for cloud resources without accumulating standing privileges to automate the on-demand permissions requests. The interviewee said, “What previously took two to three days is right now handled in a couple of hours at most.”
- Interviewees said another aspect that benefits developers is that Azure AD is built around well-defined standards, and that allowed developers to integrate with Azure AD without having to worry about proprietary APIs or protocols. The principal IT engineer at a semiconductor company said: “With our legacy on-premises IAM solution, we had all sorts of proprietary protocols that were less documented and were hard to work with, whereas Azure AD is very much documented. So, if you want to build something that integrates with Azure AD, it’s not hard to find documentation out there to help you through that.”

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

- The composite organization has 1,000 developers, and 70% of them build for the cloud.
- A developer makes one access request per two-week sprint, and before Microsoft Entra Permissions Management set up automations, it took two business days to receive permissions.

> **“Permissions Management made three significant things [happen]. Number one: Developers are happy. Number two: From a security [standpoint], … the cloud security organization [is] happy. Number three: From the metrics standpoint, our CISO and the CISO organization [are] looking much better in front of the board.”**
>
> *Head of enterprise security architecture, insurance*

- With Microsoft Entra Permissions Management, wait time is reduced by 90% for permissions on demand requests.
- The composite organization takes advantage of Permissions Management capabilities in Year 2 and continues to use the product in Year 3.
- While developers wait for necessary access, they pivot to work on other tasks and projects, but they lose 10% of productivity because their workflows are disrupted.
- Developers do not take advantage of all the time that is saved via faster permissions, so Forrester applied a 50% productivity recapture. This means employees leverage 50% of the total time saved for productive work.

Risks. The size of this benefit can vary based on:

- The organization’s previous approach to granting permissions to developers.

- The organization's commitment to building automations to simplify the process for granting access.
- The average fully burdened rate of developers.

Results. To account for these risks and because developer productivity may be viewed as a softer benefit, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $922,400.

Improved Development Velocity					
Ref.	**Metric**	**Source**	**Year 1**	**Year 2**	**Year 3**
D1	Number of developers	Composite	1,000	1,000	1,000
D2	Percent of developers building for the cloud	Composite	70%	70%	70%
D3	Number of times a developer makes a permission request	Composite	25	25	25
D4	Time needed to receive a permission with former permissions processes (hours)	Interviews	16	16	16
D5	Wait time eliminated with Microsoft Entra	Interviews	0%	90%	90%
D6	Percent of developers' productivity wasted by waiting for permission	Assumption	10%	10%	10%
D7	Productivity recapture with Microsoft Entra	TEI standard	50%	50%	50%
D8	Average fully burdened hourly rate of a developer	TEI standard	$58	$58	$58
Dt	Improved development velocity	D1*D2*D3*D4*D5*D6*D7*D8	$0	$730,800	$730,800
	Risk adjustment	↓20%			
Dtr	Improved development velocity (risk-adjusted)		$0	$584,640	$584,640
	Three-year total: $1,169,280			**Three-year present value: $922,422**	

IMPROVED HELP DESK EFFICIENCY FROM REDUCED PASSWORD RESETS

Evidence and data. Interviewees said their organizations' previous IAM solutions were not set up to support self-service password resets. Because of this, the organizations received thousands of requests per month to assist with password resets, and each of them was routed through the help desk. Each ticket represented a set amount of time for the help desk worker to resolve the issue, but it also meant that an end user was locked out of certain applications while the ticket was being resolved.

After deploying Azure AD, interviewees' organizations could take advantage of the self-service capabilities for password resets and significantly reduced the number of password reset requests that made it to the help desk. This self-service capability also aligned better with end users' expectations because self-service password resets are so prevalent in consumer-facing websites and applications.

- The director of solutions architecture at an insurance company said: "Generally, if your passwords [were] locked out, you could not do anything. Now, you just go to the portal and reset

it yourself and [the] job [is] done. With Azure AD, the number of requests the help desk gets has [been] significantly reduced."

- Several interviewees' organizations started to work on transitioning to passwordless authentication and, in time, they expect to eliminate the majority of password-reset requests.

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

- The help desk receives an average of 500 password reset requests per month before investing in Azure AD.
- In Year 1, the number of requests decreases by 75%, and this remains stable for the subsequent years.
- The average cost for a password reset request is $25.

Risks. The size of this benefit could vary based on:

- The number of password reset requests the organization received with its previous IAM solution.
- The average cost per password reset request.
- The adoption and use of the self-service tool.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $251,800.

Improved Help Desk Efficiency From Reduced Password Resets

Ref.	Metric	Source	Year 1	Year 2	Year 3
E1	Average number of password reset requests per month with previous IAM solution	Composite	500	500	500
E2	Reduction in password reset requests with Azure AD	Interviews	75%	75%	75%
E3	Cost per request	Composite	$25	$25	$25
Et	Improved help desk efficiency from reduced password resets	E1*E2*E3*12 months	$112,500	$112,500	$112,500
	Risk adjustment	↓10%			
Etr	Improved help desk efficiency from reduced password resets (risk-adjusted)		$101,250	$101,250	$101,250
	Three-year total: $303,750			**Three-year present value: $251,794**	

END-USER PRODUCTIVITY IMPROVEMENT

Evidence and data. In addition to enhancing security, all of the interviewees' organizations were looking to improve their employee experiences. According to Forrester research from 2022, 60% of business and technology professionals indicated that improving the experience of employees was a key IT objective during the next 12 months.[8] Relatedly, interviewees said that a primary goal for their organizations was to improve user experience (UX) by enabling SSO for all applications and from any device or location. Interviewees recognized that users who did not have to enter their credentials at every step were more productive and that a poor sign-on experience is not only frustrating for end users but also negatively impacts how the organizations perceive their IT and identity teams.

- The principal IT engineer at a semiconductor company said their organization used SSO to improve UX. They said: "Anytime I access anything through single sign-on, I don't have to put in a password again. Now, if it's with Windows Hello for Business and I have a camera, I can use facial recognition to log me in, which means I don't have to really do anything."
- The director of solutions architecture at an insurance company said: "We want to reduce the complexity of people needing to know passwords. So, the goal is to lessen their cognitive loads so that people do not have to worry about what their passwords are anymore."
- The principal IT engineer at a semiconductor company said: "To give [employees] the ability to log into things without a password would impact everybody across the company. That is huge, especially when you look at how often people need to type in a password throughout the day."

"When we have discussions with [our users], I challenge [a lot of] them [by saying], 'Pick a day. Boot up your laptop fresh and count how many times you put in this password.' Because we do it so much, we don't think about it. … Some people [enter their password] 30 [times or] 40 times [or] sometimes … 50 times a day."

Principal IT engineer, semiconductor

"If you have your applications integrated with Azure AD, you can have a really, really sweet user experience, and security model, and simple administration."

Senior security engineer, software

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

- SSO and MFA are enabled for all 10,000 employees in the organization.
- Each employee saves an average of 10 minutes per week in Year 1 from having a single password and single login to access all critical applications. As more applications are added to SSO over time, employees experience greater weekly time savings of 12 minutes and 15 minutes in Years 2 and 3, respectively.

- The average, fully burdened hourly rate for an employee across the organization is $40.
- End users do not take advantage of all the time saved by this solution, so Forrester applied a 50% productivity recapture. This means employees leverage 50% of the total time saved for productive work.

Risks. The size of this benefit could vary based on:

- The time that employees save with Microsoft Entra relative to their previous authentication and access experiences.
- The type of employees and the nature of their work.
- The average fully burdened cost of employees.

Results. To account for these risks, Forrester adjusted this benefit downward by 20%, yielding a three-year, risk-adjusted total PV of $4.0 million.

End-User Productivity Improvement

Ref.	Metric	Source	Year 1	Year 2	Year 3
F1	Total employees	Composite	10,000	10,000	10,000
F2	Time saved per week using Azure AD (minutes)	Interviews	10	12	15
F3	Hours saved per user per year (rounded)	F2*50 weeks/60 minutes	8	10	13
F4	Average hourly salary for a user (rounded)	TEI standard	$40	$40	$40
F5	Productivity capture	TEI standard	50%	50%	50%
Ft	End-user productivity improvement	F1*F3*F4*F5	$1,600,000	$2,000,000	$2,600,000
	Risk adjustment	↓20%			
Ftr	End-user productivity improvement (risk-adjusted)		$1,280,000	$1,600,000	$2,080,000
	Three-year total: $4,960,000			**Three-year present value: $4,048,685**	

UNQUANTIFIED BENEFITS

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

- **Working with Microsoft as a trusted IAM partner.** All interviewees said that working with fewer vendors was easier and that Microsoft provided very good customer service and support. This included co-engineering and support on new security-related initiatives.
- **Ensuring compliance with regulatory standards.** Several interviewees' organizations operate in highly regulated markets, and moving to the cloud with Microsoft Entra helped them adhere to their industries' requirements. The director of solutions architecture at an insurance company said: "First, being compliant protects us from incurring penalties. Second, with Microsoft Entra, we no longer have to do it the old-school way of using other point solutions."
- **Using External Identities in Microsoft Entra to streamline secure access for partners.** Several of the interviewees' organizations started using the External Identities capabilities in combination with other Microsoft Entra products such as Azure AD to help secure and manage customers and partners.

  The identity and access team lead at a software company said that during the pandemic, their organization was able to quickly and securely onboard various partners. They said: "[Without Microsoft Entra,] we would have had to create nearly 2,000 identities and then figure out a way of relaying the credentials to them. But we did not have to do that because we could simply take their existing work [identities] powered by Azure AD and give them access to stuff that they needed access to."

  The principal IT engineer at a semiconductor company said that beyond the cost of resources and the ease of integrating third-party resources, using External Identities contributed to improved security. They said: "The nice thing about guest access or external identity management is that when the account gets terminated on their side, it just stops working on our side. Putting on my security hat for a minute, this represents a way to close a security gap. That's a huge advantage from a security perspective."

"A major reason why we work with Microsoft is the support structure. [Microsoft is] so engaged with us. [Representatives are] going to have really intelligent conversations with you. I think the sheer size of Microsoft and how many people are working on this product [means] it's just too big to fail."

Senior security engineer, software

FLEXIBILITY AND INNOVATION: SAVINGS FROM REDUCTION IN BACKGROUND CHECKS

Evidence and data. Forrester research says the use of verified digital identity is one of the top trends shaping identity and access management in 2022.[9] Interviewees said their organizations have started to see the potential in relying on trusted digital identity for onboarding new employees, managing certifications, licenses, and password replacement or recovery for existing personnel, and even for managing software licenses for customers.

A co-founder and chief technology officer at a security organization told Forrester that recruiters carry a lot of liability. First, during hiring processes,

employers incur the risk of trusting that new hires are indeed who they say they are. Then, there is a risk of storing their data in a way that is or is not compliant. And, finally, employers must ensure that an employee's personal data is no longer stored at the end of their employment.

Microsoft Entra Verified ID partners with background check providers to verify a user's identity once so they can use it anywhere. This reduces the need for employers to store user data. The co-founder and chief technology officer at the security organization elaborated on this benefit: "If you leave my organization, you get to keep your wallet, and the employer or the recruiter does not have to worry about any of the liability."

A senior solutions architect in the identity and access management space at a software organization said their company tested Microsoft Entra Verified ID for onboarding new hires. They said: "We spend a lot of time and money working with different third parties for background checks. Once that process is done, we manually onboard new hires. The way [new hires] are providing their passports, their visas, and their work authorizations happens outside of Azure AD because [they're] not onboarded yet, and that is not as robust and secure as [we] would want it to be."

The same interviewee elaborated that relying on Microsoft Entra Verified ID in the future would allow their organization to significantly reduce the costs of working with third parties for background checks, and also reassign several FTEs dedicated to managing background checks and vendors.

Moreover, their organization projected shortening the hiring and onboarding processes and making employees available and ready for work sooner and at scale, if needed. The senior manager for productivity services and networking automations at the company said: "Adding more people manually is inefficient, may leave room for errors, and [may] cause some unwanted security incidents. Verified ID is helping us do this right and at scale."

> **"From the prehire [process] to the hiring process itself, all the identity, employment, work-authorization, and verification processes — which take a lot of time — could be easily resolved with Microsoft Entra Verified ID because the person [would] get validated digitally, and we [could] rely on their ID."**
>
> *Senior solutions architect, software*

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

- Two FTEs are dedicated to managing background checks and supporting vendors.
- As the change management efforts and general comfort with digital identity progress, the composite organization sees a 15% to 90% reduction in the effort needed to manage background checks.
- The fully burdened annual salary of a human resource specialist is $78,000.
- The composite organization sees a 30% churn rate and therefore needs to hire 3,000 new employees each year.
- A background check costs $50 per hire on average.
- The composite organization expects to replace 10% to 20% of traditional background checks with digital identity verification in Year 1, 50% to 70% in Year 2, and 90% to 95% in Year 3.

Results. This yields a three-year projected PV ranging from $321,500 (low) to $369,300 (high).

Savings From Reduction In Background Checks

Ref.	Metric	Source	Year 1	Year 2	Year 3
P1	Number of FTEs managing background checks	Composite	2	2	2
P2	Reduction in effort managing background checks with Microsoft Entra Verified ID	Composite	15%	60%	90%
P3	HR FTE fully burdened annual salary	Composite	$78,000	$78,000	$78,000
P4	Productivity recapture	TEI standard	50%	50%	50%
P5	Subtotal: Reduction in background check management	P1*P2*P3*P4	$11,700	$46,800	$70,200
P6	Total employees	Composite	10,000	10,000	10,000
P7	Average turnover rate	Composite	30%	30%	30%
P8	Number of employees hired to compensate for turnover	P6*P7	3,000	3,000	3,000
P9	Average background check cost (fee paid to an external vendor)	Composite	$50	$50	$50
$P10_{LOW}$	Percent of background checks eliminated with Microsoft Entra Verified ID	Interviews	10%	50%	90%
$P10_{MID}$			15%	60%	92%
$P10_{HIGH}$			20%	70%	95%
$P11_{LOW}$	Subtotal: Vendor cost savings from reduction in background checks with Microsoft Entra Verified ID	P8*P9*P10	$15,000	$75,000	$135,000
$P11_{MID}$			$22,500	$90,000	$138,000
$P11_{HIGH}$			$30,000	$105,000	$142,500
Pt_{LOW}	Savings from reduction in background checks	P5+P11	**$26,700**	**$121,800**	**$205,200**
Pt_{MID}			**$34,200**	**$136,800**	**$208,200**
Pt_{HIGH}			**$41,700**	**$151,800**	**$212,700**
Three-year projected total: $353,700 to $406,200			**Three-year projected present value: $321,545 to $369,273**		

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**
Gtr	Microsoft Entra license fees	$0	$772,275	$811,650	$890,400	$2,474,325	$2,041,824
Htr	Internal effort	$428,340	$496,584	$414,084	$414,084	$1,753,092	$1,533,106
	Total costs (risk-adjusted)	$428,340	$1,268,859	$1,225,734	$1,304,484	$4,227,417	$3,574,930

MICROSOFT ENTRA LICENSE FEES

Evidence and data. Most interviewees' organizations already held an enterprise license for Microsoft M365 E5 that included access to Azure AD Premium P2, and Microsoft Entra Verified ID is currently available for free. Additional charges apply for Microsoft Entra Permissions Management and are defined by the number of connected cloud resources. Even though interviewees said that Azure AD came at no extra cost to their organizations, Forrester assigned a per-year licensing for the purposes of cost and benefit analysis.

"Microsoft M365 E5 is like the Mercedes plan. … You get everything."

Principal IT engineer, semiconductor

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

- With 10,000 employees, the annual cost of Azure AD Premium P2 license is $648,000 for the composite organization.
- The organization connects 700 cloud resources in Year 1 and increases the number to 1,600 by Year 3.
- Pricing may vary. Contact Microsoft for additional details.

Risks. The size of this cost could vary based on:

- The overall size of the organization and its need for different products within the Entra portfolio.
- Any negotiated discounts on licenses.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $2.0 million.

Microsoft Entra License Fees						
Ref.	**Metric**	**Source**	**Initial**	**Year 1**	**Year 2**	**Year 3**
G1	Subtotal: Azure AD P2 cost with M365 E5 license	Microsoft	$0	$648,000	$648,000	$648,000
G2	Number of resources for Microsoft Entra Permissions Management	Composite	0	700	1,000	1,600
G3	Microsoft Entra Permissions Management cost per resource per year	Microsoft	$0	$125	$125	$125
G4	Subtotal: Microsoft Entra Permissions Management subscription (per resource)	G2*G3	$0	$87,500	$125,000	$200,000
Gt	Microsoft Entra license fees	G1+G4	$0	$735,500	$773,000	$848,000
	Risk adjustment	↑5%				
Gtr	Microsoft Entra license fees (risk-adjusted)		$0	$772,275	$811,650	$890,400
	Three-year total: $2,474,325			**Three-year present value: $2,041,824**		

INTERNAL EFFORT

Evidence and data. Interviewees' organizations took a staggered approach to the rollout of Azure AD by incrementally onboarding more applications and users. Following the initial implementations, the organizations focused on building automations and defining new workflows. When Microsoft Entra Permissions Management became available, several of the organizations dedicated additional resources to testing and implementing the new product.

"We are adding more users, but we're not necessarily adding more identity engineers because of the APIs that Microsoft Entra provides to manage these identities at scale."

Identity and access team lead, software

Interviewees said the transition to Microsoft Entra was smooth for end users and that their organizations did not need to provide significant training or change management to ensure adoption. The director of solutions architecture for an insurance company said, "For end users, we just sent an email and some how-to [guidance that explained] what was coming."

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

- Three dedicated project managers oversee the initial six-month migration effort covering the majority of core business applications.
- Two project managers spend three months handling the additional effort of implementing Microsoft Entra Permissions Management in Year 1.
- As a part of the initial implementation, a team of two FTEs spend 50% of their time integrating the existing applications with Azure AD.
- The composite organization continues to migrate applications in subsequent years with support from one dedicated FTE.

- The average, fully burdened annual salary for an IAM team member is $150,000.
- The composite organization dedicates two FTEs to manage the Entra product family and associated ongoing projects.
- Each of the 10 IAM employees who interact with the Microsoft Entra solutions receives 20 hours of training during implementation and another two hours of training in each subsequent year.

Risks. The size of this cost could vary based on:

- The size of the deployment, which may vary based on the solutions being added, the overall size of the organization, and the prior solutions replaced.
- The average fully burdened salary of resources involved.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $1.5 million.

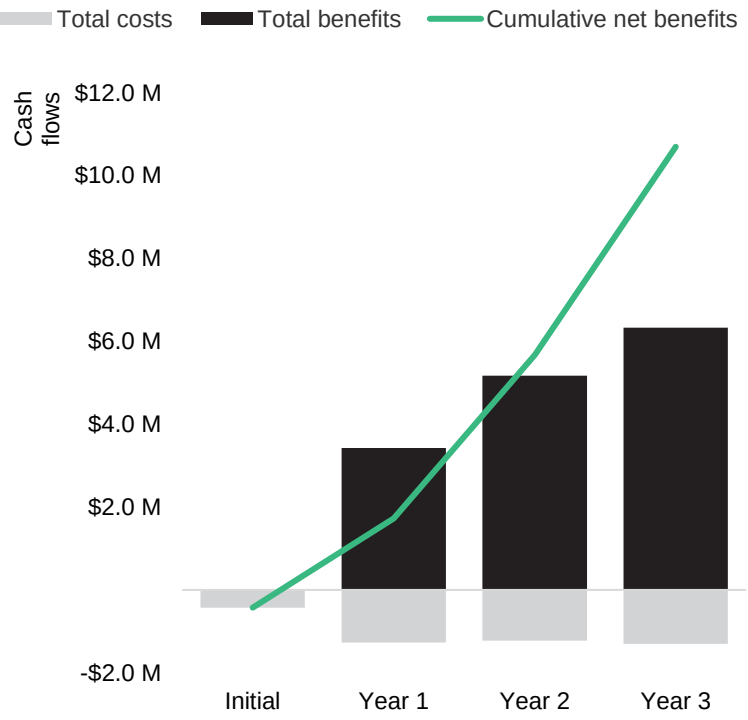
Internal Effort

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
H1	Number of FTEs involved in testing and deployment of Microsoft Entra	Composite	3	2	0	0
H2	Implementation time (months)	Composite	6	3	0	0
H3	Number of FTEs involved in app integration during implementation	Composite	2	0	0	0
H4	Number of FTEs involved in app integration	Composite	0	1	1	1
H5	Percent of time dedicated to app integrations	Composite	0%	50%	50%	50%
H6	Fully burdened IAM team salary	TEI standard	$150,000	$150,000	$150,000	$150,000
H7	Subtotal: Implementation and app integration cost	H1*H2*(H6/12)+ H3*H2*(H6/12)+ H4*H5*H6	$375,000	$150,000	$75,000	$75,000
H8	Ongoing solution management	2 FTEs*H6	$0	$300,000	$300,000	$300,000
H9	Training	Initial: 10 FTEs* 20 hours*$72 Years 1 to 3: 10 FTEs*2 hours* $72	$14,400	$1,440	$1,440	$1,440
Ht	Internal effort	H7+H8+H9	$389,400	$451,440	$376,440	$376,440
	Risk adjustment	↑10%				
Htr	Internal effort (risk-adjusted)		$428,340	$496,584	$414,084	$414,084
	Three-year total: $1,753,092			**Three-year present value: $1,533,106**		

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	($428,340)	($1,268,859)	($1,225,734)	($1,304,484)	($4,227,417)	($3,574,930)
Total benefits	$0	$3,427,630	$5,168,896	$6,328,396	$14,924,922	$12,142,459
Net benefits	($428,340)	$2,158,771	$3,943,162	$5,023,912	$10,697,505	$8,567,529
ROI						240%
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: Endnotes

[1] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

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

[3] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[4] Source: Joy Chik, "Microsoft Entra: 5 identity priorities for 2023," Microsoft, January 9, 2023.

[5] Source: "The Current State Of Enterprise Passwordless Adoption," Forrester Research, Inc., January 19, 2022.

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

[7] Source: Forrester Consulting Cost Of A Cybersecurity Breach Survey, Q1 2021.

[8] Source: Forrester's Priorities Survey, 2022.

[9] Source: "The Top Trends Shaping Identity And Access Management In 2022," Forrester Research, Inc., October 17, 2022.


FORRESTER®