A Forrester Total Economic Impact™
Study Commissioned By Microsoft
August 2020

The Total Economic Impact™ Of Securing Apps With Microsoft Azure Active Directory

Cost Savings And Business Benefits Enabled By Microsoft Azure Active Directory For Applications

FORRESTER®

Table Of Contents

Project Team:
Nicholas Ferrif
Jasper Narvil

ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. Ranging in scope from a short strategy session to custom projects, Forrester's Consulting services connect you directly with research analysts who apply expert insight to your specific business challenges. For more information, visit forrester.com/consulting.

© 2020, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. For additional information, go to forrester.com.

FORRESTER®

Highlights From The Case Study

Improved user productivity:
$7.1 million

Efficiency gains for IT and Identity teams:
$3 million

Cost savings from previous IAM solution:
$1.9 million

Executive Summary

Advancements in identity and access management (IAM) technology as well as a similar advancements in the sophistication of security threats mean that many organizations that have relied on older or stitched-together identity solutions now find themselves at a greater risk of a data breach with limited capabilities for understanding how users are accessing resources and apps and improving user experience (UX). IT and Identity teams need to provide secure access to thousands of applications scattered across on-premises, public cloud, and private cloud environments, leveraging a variety of authentication protocols. To be successful, these teams require a simple solution that can cut through these complexities and apply consistent security and access policies to all applications and users.

Microsoft Azure Active Directory (Azure AD) is a cloud-based identity and access management solution that provides secure and seamless access to all types of applications — from software-as-a-service (SaaS) apps to on-premises apps to custom-built apps — to employees, partners, and customers from anywhere. 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 Azure AD to manage and secure all of their applications. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Azure AD for apps investment on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed several customers with years of experience using Azure AD to manage and secure all of their applications, from Microsoft apps to third-party SaaS and on-prem-based apps. Through the investment in Azure AD, organizations could consolidate their IAM infrastructure, reduce their on-premises footprint, eliminate the complexity and expense of managing multiple overlapping IAM solutions, improve UX by implementing single sign-on (SSO) and self-service password reset, improve security through granular conditional access policies and multifactor authentication (MFA) for all apps, and enable secure remote access to all apps for their remote and firstline workers.

Prior to using Azure AD to manage and secure all of their applications, the interviewed organizations used a combination of different IAM solutions to manage SaaS-based, on-premises, and custom-built apps. Customers used on-premises Active Directory and various identity federation systems for legacy applications, in addition to several different cloud-based identity solutions for SaaS and line-of-business apps, often remnants of old mergers and acquisitions or previous attempts to modernize their identity infrastructure. Finally, all customers had access to Azure AD and some were already using it to manage Microsoft applications and services such as Office 365 or Azure. This complex environment was difficult and time-consuming to manage and even more difficult to secure for the IT and identity teams. It also provided little benefit to end users, who struggled with inconsistent user experiences across the different apps, had to juggle multiple locations to access the different apps and resources they needed, and lacked clarity and control on how to manage their accounts and credentials.

ROI
123%

Benefits PV
$15.9 million

NPV
$8.8million

Payback
6 months

Key Findings

Quantified benefits. The following risk-adjusted present value (PV) quantified benefits are representative of those experienced by the companies interviewed:

- **Organizations reduced costs related to legacy on-premises infrastructure and eliminated costs associated with previous cloud-based IAM solutions, saving on average $1.9 million over three years.** Organizations could remove a significant number of servers from their on-premises environments and sunset licenses related to their previous IAM infrastructure and SSO licenses, saving money and reducing the size and complexity of their environments.
- **Users have a seamless single sign-on experience and can access applications from anywhere, saving users 10-minutes per week and the organization $2.9 million per year.** SSO and MFA are enabled for every employee at the interviewed organizations, providing enhanced security and a unified single sign-on experience to access all applications. Users no longer have to remember multiple sets of credentials to access the apps they need, and now view the IT team as productivity and business enablers.
- **The organizations reduced password reset requests by 75% by enabling self-service, saving $684k per year.** By enabling self-service password resets, the organizations empowered users to reset their own passwords, aligning the experience to user expectations and significantly reducing the number of password reset requests submitted to the help-desk.
- **Azure AD reduced risk of a data breach, amounting to more than $2.1 million over three years in reduced risk.** Azure AD has a number of features that enhance organizational security and improve organizations' ability to identify, investigate, and remediate threats in their environments. Interviewees cited granular conditional access policies, detailed and integrated security logs, multifactor authentication, and the overall security of Azure as ways to reduce exposure and enhance security capabilities.
- **The effort required by the IAM teams significantly decreased, resulting in an average of $1.2 million in annual savings and the ability to reallocate headcount to critical, value-adding areas.** Connecting all apps to Azure AD significantly reduced the amount of effort needed by the IAM teams to manage their day-to-day tasks. Interviewees cited automated user provisioning for onboarding/offboarding, reduced policy management, reduced vendor management, and eliminating the need to patch and maintain on-premises servers as areas of improved efficiency.

Unquantified benefits. The interviewed organizations experienced the following benefits, which are not quantified for this study:

- **Efficiency gains for internal developers.** Enterprise developers no longer need to expend time and energy on authentication because the Microsoft Authentication Library (MSAL) makes it easy for developers to add identity capabilities to their applications, and Microsoft Graph API offers a single endpoint for developers to access Azure AD APIs.

Costs. The interviewed organizations experienced the following risk-adjusted PV costs:

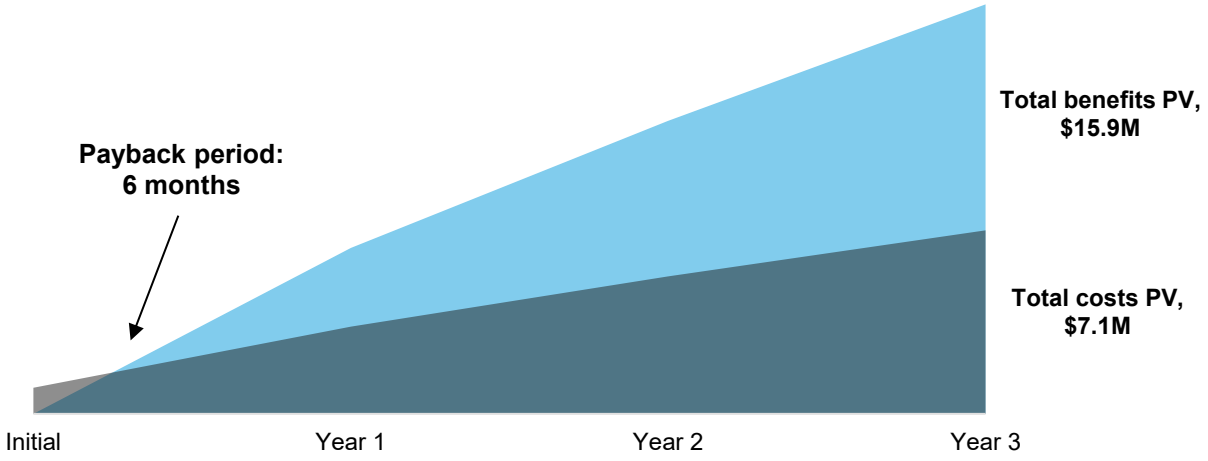
- **License costs.** While Azure AD was included in the interviewed organizations' existing licensing agreements, Forrester assessed an

additional cost of $2 million per year to extend the service to all employees in all locations including firstline and remote workers.

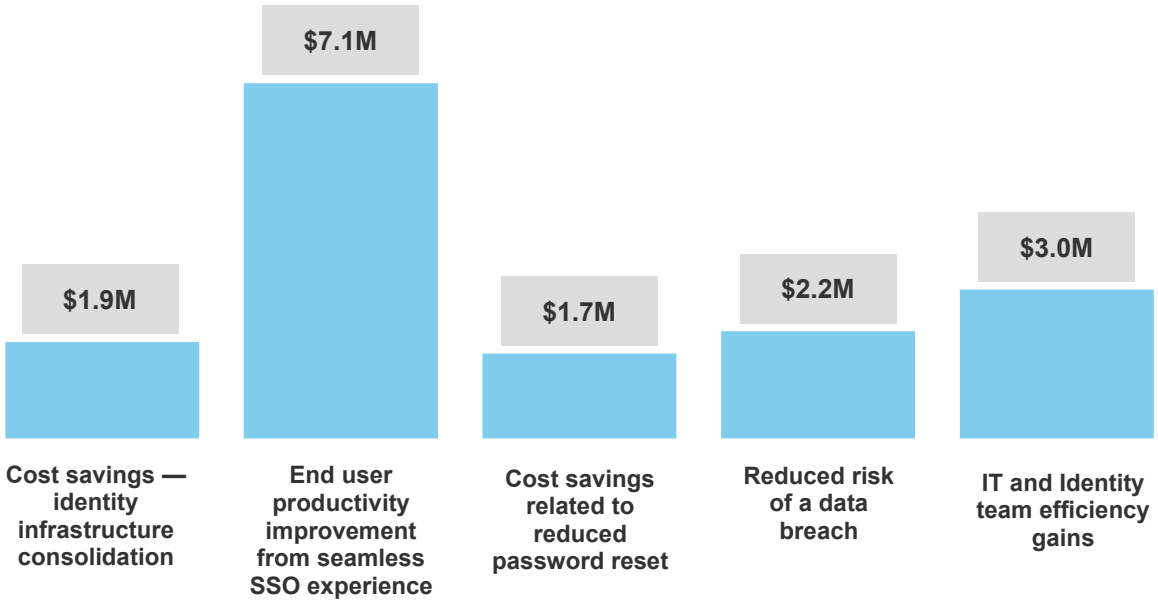
› **Deploying Azure AD to all applications.** Organizations spent time testing and migrating their core applications so that when they turned on Azure AD SSO for their users, users felt an immediate impact. After this initial migration, organizations focused on moving their other, less used applications to Azure AD, a process that continued over two years on average as certain applications reached the end of their service agreements or were more challenging to migrate.

Forrester's interviews with four existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experiences benefits of $15.9 million over three years versus costs of $7.1 million, adding up to a net present value (NPV) of $8.8 million and an ROI of 123%.

Financial Summary



(Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering implementing Microsoft Azure AD for identity and access management.

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 Azure AD for identity and access management can have on an organization:

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

DUE DILIGENCE
Interviewed Microsoft stakeholders and Forrester analysts to gather data relative to Azure AD for identity and access management.

CUSTOMER INTERVIEWS
Interviewed four organizations using Azure AD for identity and access management to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION
Designed a composite organization based on characteristics of the interviewed 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 interviewed organizations.

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

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by 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 report to determine the appropriateness of an investment in Microsoft Azure AD for identity and access management.

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.

The Azure Active Directory Customer Journey

BEFORE AND AFTER THE AZURE AD FOR IDENTITY AND ACCESS MANAGEMENT INVESTMENT

Interviewed Organizations

For this study, Forrester conducted four interviews with Microsoft Azure AD customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE	NUMBER OF EMPLOYEES	NUMBER OF APPLICATIONS
IT services	US, UK, EMEA, India	Global IT solutions architect	150,000	2,000 total apps
Manufacturing	Global	Information security services group	65,000	3,000 total apps
Building and industrial services	Global	Global security engineer —— identity	120,000	1,500 total apps
Electronics	Global	Sr. IT manager — public cloud Director of workplace technology	24,000	1,500 total apps

Key Challenges

Interviewed organizations faced common challenges before integrating all apps with Azure AD.

- **Complex infrastructure coupled with multiple, disjointed IAM solutions was difficult to manage and did not meet current security requirements.** Interviewed organizations had a wide range of previous environments and IAM solutions that they ultimately replaced with Azure AD. The commonalities across interviewees included: a legacy on-premises solution to connect on-premises applications; proxy servers or a VPN agent to connect modern applications; a SaaS-based SSO solution for cloud applications; and a legacy SSO for on-premises applications. These complex environments led to a number of challenges for interviewed organizations as highlighted by the customers below.

  The global security engineer for identity in the building and industrial services industry said: "Back in the day, if anything went down, it was always blamed on our legacy IAM solution because users were not able to log in, whether or not the IAM solution was actually causing the issue. Today, with Azure AD, when something goes down, I can say with 100% confidence that there is nothing wrong with Azure AD because Microsoft is managing that infrastructure."

  The information security services group professional in the manufacturing industry said: "We had some dated infrastructure. There were a lot of stranded costs from previous mergers and acquisitions; there was a lot of application rationalization that needed to be done. The goal was to collapse some of those costs into one and, in doing so, create a better user experience and a better service altogether."

> "We had some dated infrastructure. There were a lot of stranded costs from previous mergers and acquisitions, there was a lot of application rationalization that needed to be done. The goal was to collapse some of those costs into one and in doing so, create a better user experience and a better service altogether."
>
> *Information security services, manufacturing*

The global IT solutions architect in the IT services industry explained, "Keeping track of the compliance certificates necessary for the on-prem applications was a major challenge with our previous solution."

- **Improving security posture.** Interviewed organizations were all looking for ways to improve their security posture and ability to identify and remediate security incidents. Organizations felt increased pressure from the marketplace and leaders wanted to ensure that the next name that appeared in the headlines about a data breach was not theirs.

  The global security engineer for identity in the building and industrial services industry said: "We wanted to improve visibility because we didn't know what was going on in our legacy environment. Had we been attacked? Were we getting attacked? We were not really sure. So that is when we started looking for a solution that would provide multi-factor authentication and provide security for both our on-prem apps and those that are not on-prem and accessible externally."

  The senior IT manager for public cloud in the electronics industry told Forrester: "We saw all these different incidents in the news and knew that there was a growing threat. We knew that we needed multi-factor authentication and Azure AD Conditional Access to help address those threats."

  Additionally, organizations wanted to remove as much sensitive information from their on-site infrastructure as possible to reduce their risk exposure to potential attacks. The global security engineer for identity in the building and industrial services industry said "A big challenge with our previous solution was that we were storing all the user IDs for partners in our infrastructure. It was a huge pain because we were constantly worried about moving and managing those IDs and it made it difficult to scale-up our infrastructure."

> "We saw all these different incidents in the news and knew that there was a growing threat. We knew that we needed multi-factor authentication and Azure AD Conditional Access to help address those threats."
>
> *Senior IT manager for public cloud, electronics*

- **Improving UX and support capabilities around IAM.** Other on-prem and cloud-based identity solutions did not meet employee expectations for a seamless, modern experience and lacked the convenient support capabilities like SSO, passwordless, and automated user provisioning.

  The director of workplace technology in the electronics industry stated: "Our CIO really didn't like that anybody onboarding with our company was receiving — and this is not an exaggeration — two dozen credentials. In the executive branch, they took up to two weeks to get a new hire on their feet." The global security engineer in the building and industrial services industry elaborated: "Every time someone opened a new browser, they had to reenter their user ID and password on the login page. It was not seamless, and users complained and often had issues."

  In addition to a poor UX, legacy solutions did not offer a self-service solution to password reset requests, requiring users to connect directly with the help desk to resolve password-related issues. The sheer volume of password reset requests was enough to motivate organizations to look for a solution to alleviate some of the pressure and let employees reset their own passwords without IT intervention.

> "Our CIO really didn't like that anybody onboarding with our company was receiving – and this is not an exaggeration – two dozen credentials. In the executive branch, they took up to two weeks to get a new hire on their feet."
>
> *Director of workplace technology, electronics*

Why Azure Active Directory?

The interviewed organizations cited the following as reasons for ultimately choosing Azure AD to secure and manage their applications:

- **Conditional Access.** Interviewed organizations stressed that Azure AD was the only solution that offered robust adaptive risk-based access control with Conditional Access, and since deployment, interviewees reported that the capabilities have only become more advanced. The information security services group leader in the manufacturing industry explained: "Conditional Access was nonnegotiable as we moved to the cloud. We had to be able to apply policies that scoped applications, users, devices, and risk states. You can't let a compromised user walk into a cloud app anymore. It's unacceptable."
- **Microsoft's ability to offer a "best-in-suite" approach while providing "best-in-breed" solutions.** Interviewed organizations were looking to reduce the number of vendors and solutions in their ecosystems to reduce complexity and make things easier to manage. The information security services professional in the manufacturing industry said: "Our enterprise architects initially floated the idea of separating from the 'best-in-class' model to the 'best-in-suite' model. Instead of having 10 different vendors who are all the best in their fields and stitching them together, we wanted to invest in Microsoft and Azure AD to get the best integrated suite."

  In addition to the management efficiency gained by this best-in-suite approach, interviewed organizations also noted that Microsoft is a leader in the IAM industry, and there are significant security benefits associated with Microsoft automatically pushing updates to Azure AD (and the rest of their Microsoft applications) with no extra effort or downtime. The global security engineer in the building and industrial services industry said: "The best part is, if something is not available, you can put in a request, and as long as Microsoft feels that it will benefit their other customers, they will seamlessly push the update to everyone with no downtime or effort. We log in the next day, and the new capability is there."
- **Microsoft's reliability and efficacy with security.** Interviewed organizations were confident that Azure AD would be able to address their needs for an IAM solution. The global IT solutions architect in the IT services industry said: "The three things that we definitely needed were improved security posture, improved UX, and, maybe most importantly, improved predictability of the system. We couldn't have downtime. And Microsoft delivered on all three."

  The global security engineer in the building and industrial services industry explained: "I think this is the next big thing from Microsoft. Windows was a big thing that swept the market everywhere, and Azure AD will be the next big thing for sure; it'll be everywhere."

"Conditional access was non-negotiable as we moved to the cloud. We had to be able to apply policies that scoped applications, users, devices, and risk states. You can't let a compromised user walk into a cloud app anymore. It's unacceptable."

Information security services, manufacturing

"The best part is, if something is not available, you can put in a request, and as long as Microsoft feels that it will benefit their other customers, they will seamlessly push the update to everyone with no downtime or effort. We log in the next day and the new capability is there."

Global security engineer, building and industrial services

"I think this is the next big thing from Microsoft. Windows was a big thing that swept the market everywhere, and this Azure AD will be the next big thing for sure, it'll be everywhere."

Global security engineer, building and industrial services

Key Results

The interviews revealed that key results from the Azure AD investment include:

- **Consolidation and simplification of the IAM environment**. Interviewees discussed the benefits of having a single, fully integrated IAM solution for both end users and for internal IT and identity teams. Previously, organizations needed multiple employees with unique skill sets to manage their IAM solutions. The global IT solutions architect in the IT services industry said, "We had to leverage three different types of skill sets to do the same thing we can now do on Azure AD with one person." Additionally, Azure AD allowed organizations to reduce the

burden on their remaining on-premises infrastructure by authenticating all applications in the cloud. The global IT solutions architect in the IT services industry remarked: "Anything and everything is being authenticated with Azure AD. All applications — could be cloud, could be on-premises — are getting authorized via Azure AD rather than coming all the way to the on-prem Active Directory solution."

- **Improved UX by authenticating all applications, regardless of type and location, with Azure AD**. Interviewed organizations can connect all of their applications, whether legacy on-premises, cloud-hosted, or SaaS, to Azure AD for SSO and multifactor authentication for all of their users, reducing the number of credentials that users need to keep track of to one and enabling self-service for password reset requests to allow for even greater flexibility. The global IT solutions architect in the IT services industry said: "All users are getting authenticated via Azure AD. We have 1,000+ apps registered and enabled with MFA, and we're seeing over 150,000 authentication requests per day." The director of workplace technology in the electronics industry added, "We have two primary benefits for our users: The user experience is far better, and users have far fewer passwords to keep track of."

  In addition to the seamless login experience, organizations were also able to improve mobile access for firstline and remote workers, reducing the reliance on solutions like VPNs and improving the ability to work autonomously and access what they need, when they need it, on the device that they are most comfortable with.

> "Using Azure AD, we were able to deploy critical applications for our field reps on their mobiles. Now, they can access and authenticate using their mobile, and are less reliant on our office workers to troubleshoot or access and send critical data. That was a big plus for us."
>
> *Global security engineer for identity, building and industrial services*

- **Complete mitigation of legacy authentication attacks with Conditional Access and multifactor authentication.** Interviewed organizations noted that by deploying Azure AD, they were able to completely mitigate legacy authentication attacks in their environments. Attackers often exploit legacy authentication credentials to bypass modern security methods, like MFA, and gain access into an organizations network. The global IT solutions architect in the manufacturing industry said: "We had plenty of attackers who would compromise credentials via phishing, and immediately try to use legacy auth to get into a mailbox and either spam internally or externally for more phishing. We saw that all the time. We have seen Conditional Access policies basically 100% mitigate that which was huge for us."

  MFA also played an important role in preventing these legacy auth attacks for the manufacturer. "MFA's ability to help determine the health and compliance of a device that is trying to access our applications is huge for us. It has had an absolutely amazing impact from a security perspective. We implemented the policies, and where an attacker used to get through with the legacy auth, we can now see that stuff getting blocked in real time and say 'Yep, there's a compromised account. The attacker tried to get in. The attacker was denied. Let's go reset that user's password.'"

> "We had plenty of attackers who would compromise credentials via phishing, and immediately try to use legacy auth to get into a mailbox and either spam internally or externally for more phishing. We saw that all the time. We have seen conditional access policies basically 100% mitigate that which was huge for us."
>
> *Global IT solutions architect, manufacturing*

- **Improved security posture and visibility.** In addition to preventing attacks as highlighted above, Azure AD also helped organizations improve their overall security posture. The improvements in management efficiencies and the reduction in help desk password reset requests allowed organizations to focus more resources on security and take the time to investigate and mitigate security incidents that were slipping through the cracks before. The global security engineer for identity in the building and industrial services industry told Forrester: "Now, we have everything available to us so we can dig deeper into those smaller details. We have been able to increase our

security footprint by making sure that we are not impacted by even the small events that were typically not investigated before."

Capabilities such as password strength enforcement rules can help security teams ensure that their users are complying with the policies they set and can even add "restricted" passwords to prevent users from skirting rules or trying to leverage common, easily guessable passwords or passwords that have been previously compromised and are available on the dark web.

Composite Organization

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

The global conglomerate has $28 billion in annual revenue and 85,000 employees located at over 150 locations around the world, about 1,000 total applications in its ecosystem, and a Microsoft M365 E3 enterprise license agreement that includes the Azure AD Premium P1 plan. In addition to office locations, the organization manages distribution centers and supports a group of firstline workers, who include field sales reps and distribution center workers. The organization has a US-based headquarters and has centralized its IT management to operate from that location.

Before investing in Azure AD as its exclusive IAM solution, the organization had a number of IAM solutions in place, including a cloud-based identity solution to manage some of its SaaS apps, as well as an on-prem identity and federation solution that supported a core set of applications based on non-modern authentication methods. The organization was leveraging Azure AD but only to authenticate cloud-based Microsoft applications. Users were required to remember multiple credentials, IT had very little visibility into who was accessing applications, and there were no self-service capabilities enabled for IAM issues. Firstline and remote workers needed a VPN to access business-critical applications and access from mobile devices was not possible for certain applications.

The organization enables SSO, requires MFA for all applications and all users, and allows employees to access applications through a managed mobile device, desktop or laptop. 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

85,000 employees

1,000 total applications

Enabled 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	Cost savings — identity infrastructure consolidation	$1,572,250	$350,075	$290,700	$2,213,025	$1,937,044
Btr	End user productivity improvement from seamless SSO experience	$2,869,683	$2,869,683	$2,869,683	$8,609,050	$7,136,478
Ctr	Cost savings related to reduced password reset requests	$684,000	$684,000	$684,000	$2,052,000	$1,701,007
Dtr	Reduced risk of a data breach	$763,480	$872,549	$981,617	$2,617,646	$2,152,691
Etr	IT and Identity team efficiency gains	$1,202,850	$1,202,850	$1,202,850	$3,608,550	$2,991,310
	Total benefits (risk-adjusted)	**$7,092,264**	**$5,979,157**	**$6,028,851**	**$19,100,271**	**$15,918,530**

The table above shows the total of all benefits across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total benefits to be a PV of more than $15.9 million.

Cost Savings — Identity Infrastructure Consolidation

Organizations investing in Azure AD were aiming to reduce the cost and complexity of their existing IAM infrastructure that typically included a legacy on-premises presence and SaaS-based solutions managing modern cloud applications. After migrating to Azure AD for identity and access management, interviewed organizations could sunset their legacy IAM infrastructure, including the physical and proxy servers, previous identity-as-a-service solutions, and all of the licensing and auxiliary costs associated with managing the legacy solution because authentication for all applications, including non-Microsoft apps, was now managed and secured with Azure AD.

Organizations were often leveraging a perpetual license model for their legacy on-premises SSO solutions. By adopting Azure AD, they now avoid upgrading that license to stay current with security and new feature updates.

In addition to reducing costs, organizations also recognized that their previous identity solutions (legacy and cloud-based) were not offering the kind of visibility or control necessary to guarantee the security of their app ecosystems. The global IT solutions architect in the IT services industry said, “It was very difficult to make sure that those applications were not being compromised at any given point in time.” The senior IT manager for public cloud in the electronics industry elaborated, “We put a really big focus on standards so we could simplify the environment and reduce complexity with the intent of making things more simple and repeatable for our IAM team.”

Based on the customer interviews, Forrester estimates for the composite organization:

- The legacy IAM solution leveraged 15 physical servers, 10 of which were due for replacement in Year 1 and an additional five in Year 2. Moving to Azure AD eliminates the need to replace these servers.

Removes 15 servers from the on-premises environment and eliminates SSO- and IAM-related licenses.

“We probably had 50 or more significant on-premise apps, some production, some non-production to migrate. Then we had a similar number that we were able to sunset.”

Sr. IT manager for public cloud, electronics

- The legacy SSO solution was a perpetual license (one-time payment) that required occasional updates to get new capabilities and security updates. The composite organization avoids an upgrade to the legacy SSO solution in Year 1.
- In addition to the legacy SSO, the organization experienced annual costs related to other IAM solution licenses (from mergers and acquisitions), VPN services, and license costs associated with running the on-premises servers. These costs are estimated at 20% of the total legacy IAM license agreement annually.

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 organizations are able to sunset legacy infrastructure.

To account for these risks, Forrester adjusted this benefit downward by 5%, yielding a three-year risk-adjusted total PV of $1.9 million.

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

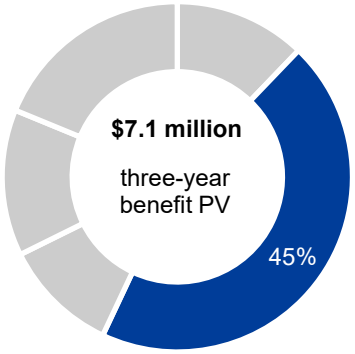
Cost Savings — Identity Infrastructure Consolidation: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
A1	Number of IAM machines that were sunset as a result of Azure AD investment	Composite	10	5	0
A2	Cost per machine	Composite	$12,500	$12,500	$12,500
A3	Avoided license costs — previous IAM solution	Composite	$1,530,000	$306,000	$306,000
At	Cost savings — identity infrastructure consolidation	(A1*A2)+A3	$1,655,000	$368,500	$306,000
	Risk adjustment	↓5%			
Atr	**Cost savings — identity infrastructure consolidation solution (risk-adjusted)**		**$1,572,250**	**$350,075**	**$290,700**

End User Productivity Improvement From Seamless SSO Experience

A primary goal for the interviewed organizations was to improve UX by enabling SSO for all applications, from any device or location. Organizations recognized that happy users are more productive, and a poor sign-on experience was not only frustrating for end users but also created significantly more work for IT teams and help desks and negatively impacted how the IT (and identity) teams were perceived by the organizations.

According to Forrester, the most important ingredient in an employee's experience at work is the ability to succeed and make daily progress toward the work they believe is most important. To this end, when employees are not able to easily access the applications and services that they need to be successful, they can easily become frustrated.[1] The global IT solutions architect in the IT services industry said, "When we started this project, the very first thing our CIO said was that even if we can only enable single sign-on, that is a huge win because enabling SSO is going to change the way that end users think about IT."



End user productivity improvement from seamless SSO experience: 45% of total benefits

FORRESTER®

- **Impact to organizational culture and perception of IT.** IT teams have a difficult task and are often viewed as a cost center or as the team that always says no. Changing this perception can be challenging, and for the interviewed organizations, enabling SSO was an "aha" moment for users because it represented a tangible improvement in their experience — enabled by the IT team. The global IT solutions architect in the IT services industry explained: "Even though most users were only saving a couple minutes per day, from an experience perspective, this was huge. They started to realize that IT isn't just all about restricting and imposing rules, but IT can enable changes that actually improve their day-to-day experience. And just because of this seamless single sign-on thing, users started listening to us, and adoption of new policies like MFA happened much faster and with less pushback."

  Another feature that impacted the UX was the newly released administrator consent workflow that allows users to request access to restricted applications directly from the sign-in window and lets administrators grant or deny that request in real time, rather than users hitting a brick wall and admins processing ad hoc requests.
- **Larger impact for some users.** While enabling SSO and MFA for all users improved the experience for everyone, firstline and remote workers experienced even more benefits because they received secure access to applications and data that previously needed a VPN or were inaccessible with the previous solutions. The global security engineer for identity in the building and industrial services industry explained: "Using Azure AD, we were able to deploy critical applications for our field reps on their mobiles. Now, they can access and authenticate using their mobile and are less reliant on our office workers to troubleshoot or access and send critical data. That was a big plus for us."

  Interviewees noted that as users grew more comfortable with the new SSO experience and the My Apps portal, team leads and department heads started creating curated app collection pages for specific teams and groups so users could easily see and access the specific apps that were critical to their roles without searching or asking for help. The IAM team efficiency gains from this are discussed in IT Efficiency Gains section.
- **Continual improvement with telemetry data, real-time logs, and reporting.** IAM teams have immediate access to telemetry data, security logs, and other administration tools from the moment they turn on Azure AD. This data allows IAM teams to better understand how users are accessing applications and where any issues may lie; it also informs roadmap decisions that can further improve the UX. The senior IT manager for public cloud in the electronics industry said: "It was configured. It was enabled. We started seeing telemetry immediately. This was data that we did not have access to before."

For the composite organization, Forrester assumes that:

- SSO is enabled for all 85,000 employees in Year 1.
- Employees save, on average, 10-minutes per week from having a single password and single login to access all critical applications. Some employees, especially remote and firstline workers, experience a bigger impact because they now have access to applications that previously needed additional technology (VPN) or were simply not accessible from a remote location or mobile device.

"Even though most users were only saving a couple minutes per day, from an experience perspective, this was huge. They started to realize that IT isn't just all about restricting and imposing rules, but IT can enable changes that actually improve their day-to-day experience. And just because of this seamless single sign-on thing, user started listening to us, and adoption of new policies like MFA happened much faster and with less pushback."

Global IT solutions architect, manufacturing

Users can access all critical applications and data from one place with one set of credentials.

- The average, fully burdened salary across the organization is $67,000 per year or $32.45 per hour.
- End users will not take advantage of every single minute that is saved by this solution, so Forrester has applied a 20% productivity capture — meaning that Forrester expects employees to leverage 20% of the total time saved for productive work.

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

- The number of employees leveraging the SSO solution.
- The time that employees save relative to their previous SSO solution experience.
- The average fully loaded compensation for the organization.
- The amount of time saved that employees leverage for productive work.

To account for these risks, Forrester adjusted this benefit downward by 40%, yielding a three-year risk-adjusted total PV of $7.1 million.

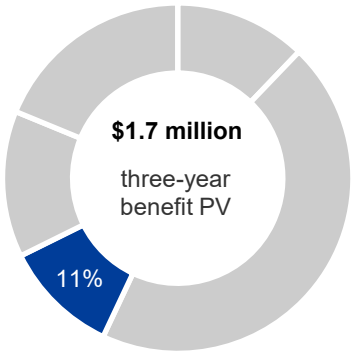
End User Productivity Improvement From Seamless SSO Experience: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
B1	Number of users	Composite	85,000	85,000	85,000
B2	Time saved per week using Azure AD SSO (minutes)	Composite	10	10	10
B3	Hours saved per user per year	C1*(C2/60*52)	8.67	8.67	8.67
B4	Average hourly salary for users (rounded)	$50k*1.35/2,080	$32.45	$32.45	$32.45
B5	Productivity capture	Composite	20%	20%	20%
Bt	End user productivity improvement from seamless SSO experience	B2*B3*B4*B5	$4,782,806	$4,782,806	$4,782,806
	Risk adjustment	↓40%			
Btr	**End user productivity improvement from seamless SSO experience (risk-adjusted)**		**$2,869,683**	**$2,869,683**	**$2,869,683**

Cost Savings Related To Reduced Password Reset Requests

Previous IAM solutions were not set up to support self-service password resets, and interviewed organizations' ecosystems were too complicated to support an elegant self-service solution. Organizations were receiving thousands of requests per month, all routed through the help desk, to assist with password resets. 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. The information security services professional in the manufacturing industry said, "Before we did self-service password management, we were looking somewhere between $500,000 and $700,000 a year in password reset costs."

Interviewed organizations said that with their previous IAM solutions, certain regions or groups would experience lock-out issues where a group of users was unable to access critical applications. The information security services professional in the manufacturing industry explained: "It's been hugely beneficial for people to be able to unlock their accounts when they're getting into some chronic lockout issues



Cost savings related to reduced PW reset requests: 11% of total benefits

FORRESTER®

from various regions. It was common with our previous solution, every year we'd have a pocket of users, 10 or 20 of them, that would have some rogue app that was locking them out, and it took forever to troubleshoot. Now, instead of 300 help desk calls, they can go out to the portal and unlock the account themselves."

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

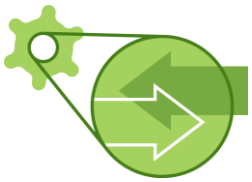
For the composite organization, Forrester assumes that:

- An average of 4,000 password reset requests were hitting the help desk each month before investing in Azure AD.
- Within two months of deploying, the number of requests decreases to 1,000 per month and remains stable — a 75% reduction.
- The average cost for a password reset request call is $20.

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

- The number of password reset requests received with the previous IAM solution.
- The extent of automated or self-services password reset request capabilities with the previous IAM solution.
- The average cost per password reset request.
- The adoption and use of the self-service tool.

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



75% reduction in password reset requests at the help desk through enabling self-service.

Cost Savings Related To Reduced Password Reset Requests: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
C1	Average number of password reset requests per month — previous IAM solution	Composite	4,000	4,000	4,000
C2	Reduction in password reset requests with Azure AD	Interviews	75%	75%	75%
C3	Cost per request	Composite	$20	$20	$20
Ct	Cost savings related to reduced password reset requests	C1*C2*C3*12	$720,000	$720,000	$720,000
	Risk adjustment	↓5%			
Ctr	**Cost savings related to reduced password reset requests (risk-adjusted)**		**$684,000**	**$684,000**	**$684,000**

Reduced Risk Of A Data Breach

All of the interviewed organizations expressed the need to improve organizational security posture through the investment in Azure AD by improving the visibility and reducing the complexity of their IAM solutions. Many hackers rely on compromised accounts to exfiltrate data from their targets; according to the Ponemon Institute, 51% of data breaches are caused by malicious or criminal actors.[2] By securing all applications with Azure AD, organizations were able to improve visibility, implement password strength rules, implement granular risk-based policies to ensure that employees only had access to the applications that they

needed, and, through MFA, prevent specific types of attacks from penetrating the network, even if a user's account was compromised.

- Azure AD Conditional Access and MFA significantly improved organizations' ability to prevent, detect, and quickly remediate specific types of attacks. Interviewed organizations referenced specific attacks, like legacy authentication, that they were able to prevent through the use of Azure AD's MFA and real-time security logs. Previously, these attacks would have been much more difficult to notice and ultimately remediate, so this represents a significant improvement in overall security posture and capabilities for the organizations.
- IAM teams leveraged Microsoft's password enforcement tool to ensure that all users had strong, secure passwords. This includes the ability to block specific passwords from being used (e.g., Password123) and can also exclude passwords that Microsoft has found to be exposed on the dark web or in leaked data breach materials.
- Security logs, and the easy integration with enterprise SIEM, represent new capabilities and visibility for the security team. Before Azure AD, security logs from the legacy IAM solutions were either nonexistent or inadequate to have any real impact to organizational security. The global security engineer for identity in the building and industrial services industry said: "The logs, the amount of data that we collect from Azure AD, is tremendous. We feed all the logs into our SEIM tool so we can see how much usage each application gets, what each user is doing, and which applications they access, and if we notice anything strange, we can immediately investigate."

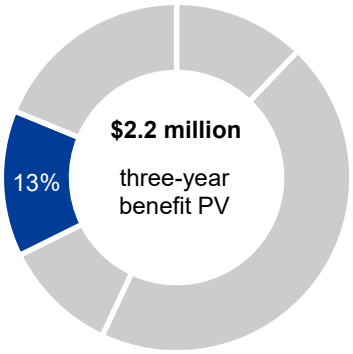
For the composite organization, Forrester assumes that:

- The average cost of a data breach for an organization of 85,000 employees is $17,340,000, or $204 per employee, based on the Ponemon Institute's assessment of breach costs relative to organizational size.[3]
- The average likelihood of a data breach of 10,000 records or more is 29.6% over two years, or 14.8% per year.[4]
- By deploying Azure AD for IAM and enabling SSO and MFA, the composite organization significantly improves its IAM maturity and reduces its risk exposure. This benefit ramps up over time as the organization integrates more applications and builds up security capabilities around Azure AD.

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

- The average cost of a data breach for the organization.
- The inherent risk of a data breach.
- The extent to which the organization is able to improve security posture and capabilities through the investment in Azure AD.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $2.2 million.



Reduced risk of data breach: 13% of total benefits

Reduce the likelihood of a data breach by 45% with Azure AD.

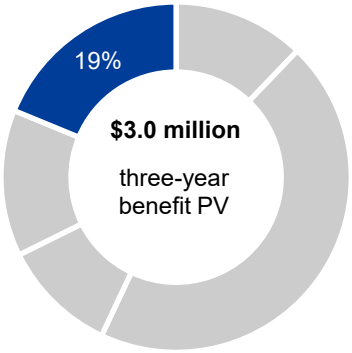
FORRESTER®

Reduced Risk Of A Data Breach: Calculation Table					
REF.	**METRIC**	**CALCULATION**	**YEAR 1**	**YEAR 2**	**YEAR 3**
D1	Average potential cost of data-breach ($204/employee)	Ponemon Institute	$17,340,000	$17,340,000	$17,340,000
D2	Average likelihood of a data breach (10,000+ records)	Ponemon Institute	14.80%	14.80%	14.80%
D3	Reduced likelihood of a breach	Composite	35%	40%	45%
Dt	Reduced risk of a data breach	D1*D2*D3	$898,212	$1,026,528	$1,154,844
	Risk adjustment	↓15%			
Dtr	**Reduced risk of a data breach (risk-adjusted)**		**$763,480**	**$872,549**	**$981,617**

IT Efficiency Gains

Interviewed organizations were spending a significant amount of resources to manage and maintain their previous IAM solutions, leaving little time for projects that could improve security posture, improve UX, or solve pressing issues with the legacy solutions. By migrating to Azure AD for their IAM solution, organizations could leverage the benefits of a cloud solution, freeing up time for their dedicated IAM team to focus on adding value to the business and reallocating some workers to other teams that needed additional resources. Areas where organizations experienced efficiencies related to their IT and identity teams include: reduced time and effort related to provisioning/deprovisioning; reduced effort to integrate a new application into Azure AD; reduced system downtime and issues blamed on the IAM infrastructure; reduced management effort related to patching and updates compared to the previous solution; reduced policy management effort for the IAM team; and reduced vendor management efforts.

- Interviewed organizations were able to automate device provisioning for onboarding new employees, partners, or customers and managing transfers. The information security services professional in the manufacturing industry said: “It is a lot easier now. We don’t have to go provision those services one at a time and create a file share form and things of that nature. When a new hire’s account gets rolled out and synced to Azure AD, they get a license automatically assigned, and those services are automatically provisioned for us.”
- In addition to onboarding, organizations noted the benefits of being able to quickly and effectively offboard an employee who leaves the company or is terminated, representing an improvement in organizational security posture. With Azure AD, as soon as an employee is terminated in the system, Azure AD will push that status and remove access to all applications and services immediately.
- Interviewed organizations could reduce the size of their dedicated IAM management teams and reduce the number of requisite skill sets needed to manage the environment. Because organizations eliminated on-premises infrastructure and reduced the number of license and vendors, workers did not need to be familiar with as many systems and could support a greater number of applications and services. The global IT solutions architect in the IT services industry said, “The four people who were just managing AD FS [Active Directory Federation Services] in the past have now moved into a bigger role and are part of the larger team that manages four critical pieces of our environment.”



IT efficiency gains: 19% of total benefits

> “It is a lot easier now. We don’t have to go provision those services one at a time and create a file share form and things of that nature. When a new hire’s account gets rolled out and synced to Azure AD, they get a license automatically assigned and those services are automatically provisioned for us.”
>
> *Information security services, manufacturing*

FORRESTER®

- Reallocated employees added value to the business. In each of the scenarios above, organizations were able to reduce the size of their IAM teams and reallocate employees to other, higher-value tasks around the organization.

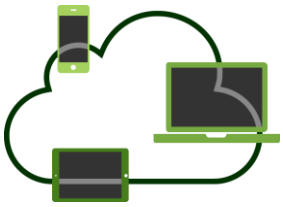
  The global IT solutions architect in the IT services industry explained: "We started focusing on upgrading the skill sets of those analysts who were previously handling help desk tickets. When we saw a reduction in the number of tickets, we reallocated them to other areas like supporting the data center, supporting end users, IT logistics, all those types of things. We trained them for the modern management world that we now live in."

  A senior IT manager for public cloud in the electronics industry said: "The automations allowed the IAM team to reduce headcount and focus on adding value to other areas of the business. One member of the provisioning team moved and is now full-time on the IT risk and compliance team."

> "The automations allowed the IAM team to reduce headcount and focus on adding value to other areas of the business. One member of the provisioning team moved and is now full-time on the IT risk and compliance team."
>
> *Sr. IT manager for public cloud, Electronics*

For the composite organization, Forrester assumes that:

- The IAM team consisted of 18 FTEs before the Azure AD investment.
- Two FTEs who previously focused on onboarding and provisioning are reallocated to other, value-added tasks.
- Four FTEs who previously performed general maintenance activities in the legacy IAM environment are reallocated to other, value-added teams.
- Three additional FTEs who previously performed activities, like vendor access management, application migration/integration into IAM solution, and policy management, are reallocated.



Reduce overall management effort for the IAM team by 50%.

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

- The size of the IAM team before investing in Azure AD.
- The number of FTEs who can be reallocated based on reduced effort required to manage and maintain Azure AD compared to the previous solution.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $3.0 million.

IT and Identity team Efficiency Gains: Calculation Table

REF.	METRIC	CALCULATION	YEAR 1	YEAR 2	YEAR 3
E1	IAM management team — previous IAM solution	Composite	18	18	18
E2	Reduction in effort — onboarding/offboarding and provisioning	Interviews	2.0	2.0	2.0
E3	Reduction in effort — maintenance of previous IAM solution	Interviews	4.0	4.0	4.0
E4	Reduction in effort — remaining IAM team	Interviews	3.0	3.0	3.0
E5	Total reduction in effort for IAM team	(E2+E3+E4)/E1	50%	50%	50%
E6	Fully burdened IAM team salary	Composite	$148,500	$148,500	$148,500
Et	IT and Identity team efficiency gains	E1*E5*E6	$1,336,500	$1,336,500	$1,336,500
	Risk adjustment	↓10%			
Etr	**IT efficiency gains (risk-adjusted)**		**$1,202,850**	**$1,202,850**	**$1,202,850**

Unquantified Benefits

In addition to the benefits outlined above, the interviewed organizations described other benefits of integrating all apps with Azure AD that were not specifically quantified in the study.

- **Efficiency gains for internal developers and faster time-to-value for new releases.** Interviewed organizations noted that because they leveraged Azure AD, and specifically MSAL and Microsoft Graph API, their developers no longer needed to spend time or energy on IAM-related development. The senior IT manager for public cloud in the electronics industry said: “It has definitely helped our middleware team. When they develop new solutions, they no longer need to focus on that authentication overhead because they know that they can leverage Azure AD to get it done.” The information security services professional in the manufacturing industry explained: “They are able to get an MVP version of those smaller, net-new apps out the door faster and more efficiently now. We’re talking a difference between six months of development, testing, and coding to one or two weeks.”

Internal development teams work more efficiently and reduce time-to-value for releases.

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are multiple scenarios in which a customer might choose to implement Azure AD for identity and access management and later realize additional uses and business opportunities, including:

- **Improving security and efficiency gains for the cybersecurity team.** Because Azure AD integrates security logs with leading enterprise SIEM solutions, cybersecurity teams can leverage this new data to improve their capabilities around identifying and remediating incidents, as well as reduce the time and effort involved with threat hunting. The information security services professional in the manufacturing industry said, “The cybersecurity team is certainly operating more efficiently and with better data now.”
- **Enabling a bring-your-own-device (BYOD) policy and improving mobility**. Before deploying Azure AD for all apps, interviewed organizations did not have or had very limited BYOD policies for employees. By leveraging Azure AD and Microsoft Endpoint Management (MEM, formerly Intune), organizations can push the Conditional Access policies to users’ personal devices, allowing them to access their core network in a secure way from anywhere.
- **Delegating entitlement management.** With the rapid adoption of SaaS apps and cloud services by business units, many central IT teams don’t know which access rights which users should have. Organizations were able to give app and data owners the ability to create groups and delegate management of access approvals and reviews. The information security services professional in the manufacturing industry explained: “The application owner or the data owner is able to grant users entitlements via a group or by adding the user to the app they own. They don’t have to work through IT; they don’t have to submit forms and wait for approvals; they can do it themselves. It delegates that entitlement management. We were very, very obsessed with groups on-premises and Active Directory. We used to see probably 4,000 to 5,000 requests a year for things of that nature that are now self-service.”

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

Note: Organizations need an Azure AD Premium P2 license to take advantage of delegated entitlement management.

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

Better Prepared For COVID-19

As highlighted above, one of the key flexibility benefits of using Azure AD to authenticate all apps is that it helps organizations enable BYOD policies and improves remote access to business-critical applications, regardless of where the application is hosted and what device the end user is using. Organizations that were managing all of their apps with Azure AD before COVID-19 found it much easier to expand their BYOD policies and rapidly adapt to enable an entirely remote workforce. These organizations are now effectively managing their newly remote workforces and are set up for success regardless of where and how users will need to access applications in the future. The global IT solutions architect in the IT services industry said: “The deployment of Azure AD and MEM (Intune) has enabled our organization to implement a BYOD policy so people can access our core network from personal devices securely, without any data loss. This has been especially beneficial recently when 97% of our users were suddenly working from home or in remote locations so the overall impact to user access has been minimal.”

Analysis Of Costs

QUANTIFIED COST DATA AS APPLIED TO THE COMPOSITE

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ftr	Licensing costs	$0	$2,142,000	$2,142,000	$2,142,000	$6,426,000	$5,326,837
Gtr	Integration costs	$1,013,513	$467,775	$233,888	$233,888	$1,949,063	$1,807,781
	Total costs (risk-adjusted)	**$1,013,513**	**$2,609,775**	**$2,375,888**	**$2,375,888**	**$8,375,063**	**$7,134,618**

Licensing Costs

Each interviewed organization held an enterprise license for Microsoft M365 E3 that included access to Azure AD Premium P1 for all users in the overall license cost. Even though Azure AD came at no extra cost to these organizations, Forrester assigned a per-year licensing cost to cover any additional licenses or upgrades necessary to roll Azure AD out to all 85,000 employees. Forrester made this assessment based on information gathered in the interviews, pricing and cost data provided by Microsoft for the most common suites for the types of organizations interviewed, and Forrester Analytics data.

One common misperception among interviewees before moving to Azure AD was that Azure AD only worked for Microsoft applications when, in fact, Azure AD integrates with thousands of non-Microsoft applications and is continuously adding integrations.

For reference, please find pricing details for the various Microsoft licensing agreements that include Azure AD, along with a description of the other products and services included:

- Microsoft 365 Enterprise, the most popular enterprise productivity and security suite that include Office apps, intelligent cloud services, and world-class security.
- Microsoft Enterprise Mobility + Security suite, an intelligent mobility management and security platform.
- Standalone Azure Active Directory Premium.

For the composite organization, Forrester assumes that:

- There is an additional cost of $2.0 million per year covering any additional license or upgrade costs so all 85,000 FTEs have access to Azure AD.

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

- The mix of firstline vs. information workers.
- The terms of an existing licensing agreement with Microsoft.
- The number of licenses needed.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $5.3 million.

Total Cost — Implementing Azure AD For All Apps: Calculation Table						
REF.	**METRIC**	**CALCULATION**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
F1	Microsoft license cost associated with Azure AD (estimated)*	Composite		$2,040,000	$2,040,000	$2,040,000
Ft	Licensing costs		$0	$2,040,000	$2,040,000	$2,040,000
	Risk adjustment	↑5%				
Ftr	**Licensing costs Azure AD (risk-adjusted)**		**$0**	**$2,142,000**	**$2,142,000**	**$2,142,000**

Integration Costs

Interviewed organizations outlined the costs associated with testing, migrating, deploying, and updating internal policies and workflows. Organizations described an initial effort to migrate the most heavily used, core applications to Azure AD first, to give the biggest impact to end users, and performed subsequent migrations in batches in the following years for less-used applications.

For the composite organization, Forrester assumes that:

- Two dedicated product managers oversee the initial nine-month migration effort covering the majority of core business applications.
- Initially, a team of 10 FTEs spend 50% of their time integrating the existing applications with Azure AD.
- Two project managers spend 50% of their time managing the ongoing migration efforts and also manage any net-new application integrations in Year 1, moving to a single project manager in subsequent years.
- The organization continues to migrate and rationalize its less used applications with a team of four FTEs in Year 1 and two FTEs in Years 2 and 3.
- The average, fully burdened salary for an IAM team member is $148,500 (a base salary of $110K per year).

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

- The number of applications that need to be integrated with Azure AD and the amount of effort required for each integration.
- The average fully burdened salary of the IAM team.

To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year risk-adjusted total PV of $1.8 million.

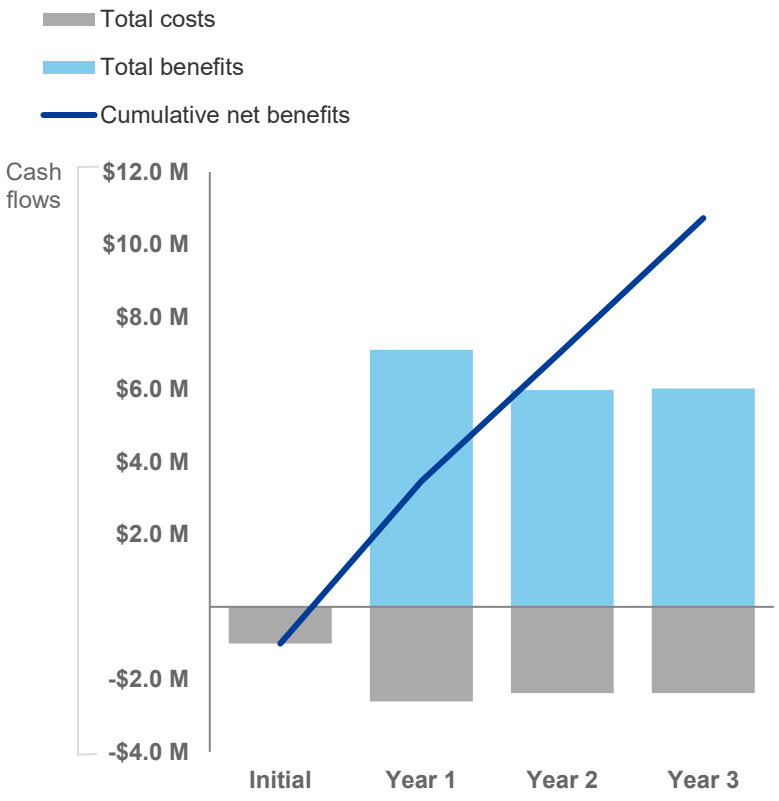
Implementation risk is the risk that a proposed investment may deviate from the original or expected requirements, resulting in higher costs than anticipated. The greater the uncertainty, the wider the potential range of outcomes for cost estimates.

Integration Costs: Calculation Table						
REF.	**METRIC**	**CALCULATION**	**INITIAL**	**YEAR 1**	**YEAR 2**	**YEAR 3**
G1	FTEs working in testing and deployment of Azure AD	Composite	2	2	1	1
G2	Time dedicated to migrating apps to Azure AD	Composite	75%	50%	50%	50%
G3	Average salary — IAM team	0	$148,500	$148,500	$148,500	$148,500
G4	Subtotal		$222,750	$148,500	$74,250	$74,250
G5	App integration team — FTE	Composite	10	4	2	2
G6	Percent of time dedicated to app integrations	Composite	50%	50%	50%	50%
G7	Subtotal: App integration costs		$742,500	$297,000	$148,500	$148,500
Gt	Integration costs		$965,250	$445,500	$222,750	$222,750
	Risk adjustment	↑5%				
Gtr	**Integration costs (risk-adjusted)**		**$1,013,513**	**$467,775**	**$233,888**	**$233,888**

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	($1,013,513)	($2,609,775)	($2,375,888)	($2,375,888)	($8,375,063)	**($7,134,618)**
Total benefits	$0	$7,092,264	$5,979,157	$6,028,851	$19,100,271	**$15,918,530**
Net benefits	($1,013,513)	$4,482,489	$3,603,270	$3,652,963	$10,725,209	**$8,783,912**
ROI						**123%**
Payback period (months)						**6.0**

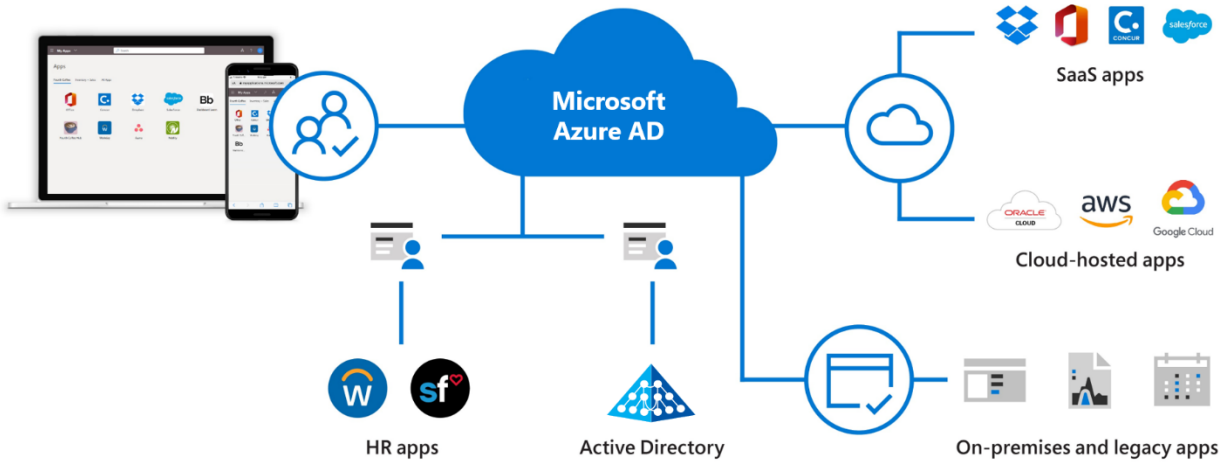
FORRESTER®

Microsoft Azure AD: Overview

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

Microsoft Azure Active Directory is a complete identity and access management solution with integrated security to manage and protect all users and data.

Azure AD offers industry-leading secure adaptive access through configurable Conditional Access policies, Identity Protection, and MFA. It provides secure, user-friendly sign-in experiences with one set of credentials to access all applications and convenient end user self-service options. It enables organizations to unify identity management in the cloud for all applications and users and integrates with on-premises Active Directory. Finally, it controls access with built-in identity governance and privileged identity management from one cloud IAM solution.



Azure AD is recognized as a leader in identity and access management and is used by over 200,000 organizations worldwide.

For more information, visit [aka.ms/aad](aka.ms/aad).

FORRESTER®

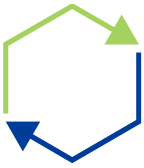
Appendix A: Total Economic Impact

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

"Build Your Identity And Access Management Strategy," Forrester Research, Inc., March 25, 2019

"Forrester's Identity And Access Management Maturity Assessment," Forrester Research, Inc., September 12, 2019

"Understand The State Of Identity And Access Management, 2020," Forrester Research, Inc., April 21, 2020

"The Employee Experience Technology Ecosystem," Forrester Research, Inc., February 14, 2019

Appendix C: Endnotes

---

[1] Sources: "The Employee Experience Technology Ecosystem," Forrester Research, Inc., February 14, 2019, and "Forrester's Identity And Access Management Maturity Assessment," Forrester Research, Inc., September 12, 2019.
[2] Source: "2019 Cost of a Data Breach Report," Ponemon Institute, 2019 (https://www.ibm.com/security/data-breach).
[3] Source: "2019 Cost of a Data Breach Report," Ponemon Institute, 2019 (https://www.ibm.com/security/data-breach).
[4] Source: "2019 Cost of a Data Breach Report," Ponemon Institute, 2019 (https://www.ibm.com/security/data-breach).