Now Tech: Authentication Management Solutions, Q3 2018

Forrester's Overview Of 26 Authentication Management Providers

by Andras Cser and Merritt Maxim

August 7, 2018

Why Read This Report

You can use authentication management solutions to simplify and standardize credential processing for applications, reduce the operational costs of authentication, and improve the authentication experience by minimizing friction. But to access these benefits, you'll first have to select from a diverse set of vendors — vendors that vary by size, functionality, geography, and vertical market focus. S&R pros should use Forrester's Now Tech report to understand the value they can expect from an authentication solution provider and select vendors based on size and functionality.

Key Takeaways

Improve Security With Authentication Management Solutions

Authentication management solutions provide improved user security, reduced risk of data breaches, and better, consistent, enforceable password policies. They also reduce the cost of application security coding for login, as well as improve the user experience.

Select Vendors Based On Size And Functionality

Each vendor focuses on either employee-facing (B2E), business-partner-facing (B2P), or consumer-facing (B2C) authentication and access management. While some vendors offer more than one kind of authentication solution, their install base or revenue splits across the above modalities will speak volumes of their specialization.

Authentication Is Mission-Critical Infrastructure — Treat It As Such!

Authentication is mission-critical infrastructure. If it's down, your employees and customers won't be able to access your company's resources, causing downtime and reputation loss. Therefore, it's imperative to dedicate full-time employees to the implementation and operation of your authentication solution.

Now Tech: Authentication Management Solutions, Q3 2018

Forrester's Overview Of 26 Authentication Management Providers

by Andras Cser and Merritt Maxim
with Stephanie Balaouras, Bill Barringham, and Peggy Dostie

August 7, 2018

Table Of Contents

Related Research Documents

The Forrester Wave™: Customer Identity And Access Management, Q2 2017

The Forrester Wave™: Identity-As-A-Service, Q4 2017

The Forrester Wave™: Risk-Based Authentication, Q3 2017

Top Trends Shaping IAM In 2018

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Improve User Security With Authentication Management Solutions

Authentication management solutions provide the front door for users (employees, business partners, and consumers) accessing web and native mobile applications. Forrester defines this market in the following manner:

> *Authentication management solutions provide human and machine users with login, secure token service (STS) and validation, single sign-on (SSO), session management, identity federation, native two-factor authentication (2FA), and coarse-grained authorization to web and native mobile applications in a centralized policy management and auditing framework.*

In terms of business benefits, authentication management solutions:

- **Provide comprehensive and multilayered login credential processing.** These tools ensure that only people with the right credentials can access your or your business partner's applications at the right time.[1] Authentication management enforces password policies and provides risk-based, step-up, and knowledge-based authentication, to improve site security.[2] Centralized policy management and auditing help with keeping security costs down.
- **Reduce the operational support costs of identities and application coding.** Since authentication management solutions provide a single and standardized security coding framework for in-house-built applications, application developers don't have to worry about login logic and reinvent the wheel for creating disparate authentication routines in their apps; instead, they can use APIs and SDKs that authentication management solutions provide.[3]
- **Reduce end user friction.** Authentication management solutions allow end users to log in once and then roam freely across multiple apps, creating an easy-to-use, delightful app-access experience. This helps improve employee productivity (no time wasted when logging into corporate apps) as well as consumers (all features are available on the corporate portal after authentication).[4]

Select Vendors Based On Size And Functionality

We segmented the vendors in this market into three categories based on revenue: large established players ($140 million or more in annual revenue), midsize players ($30 million to less than $140 million in annual revenue), and smaller players (less than $30 million in annual revenue) (see Figure 1). We did not include vendors that we estimated to have less than $2 million in revenue.

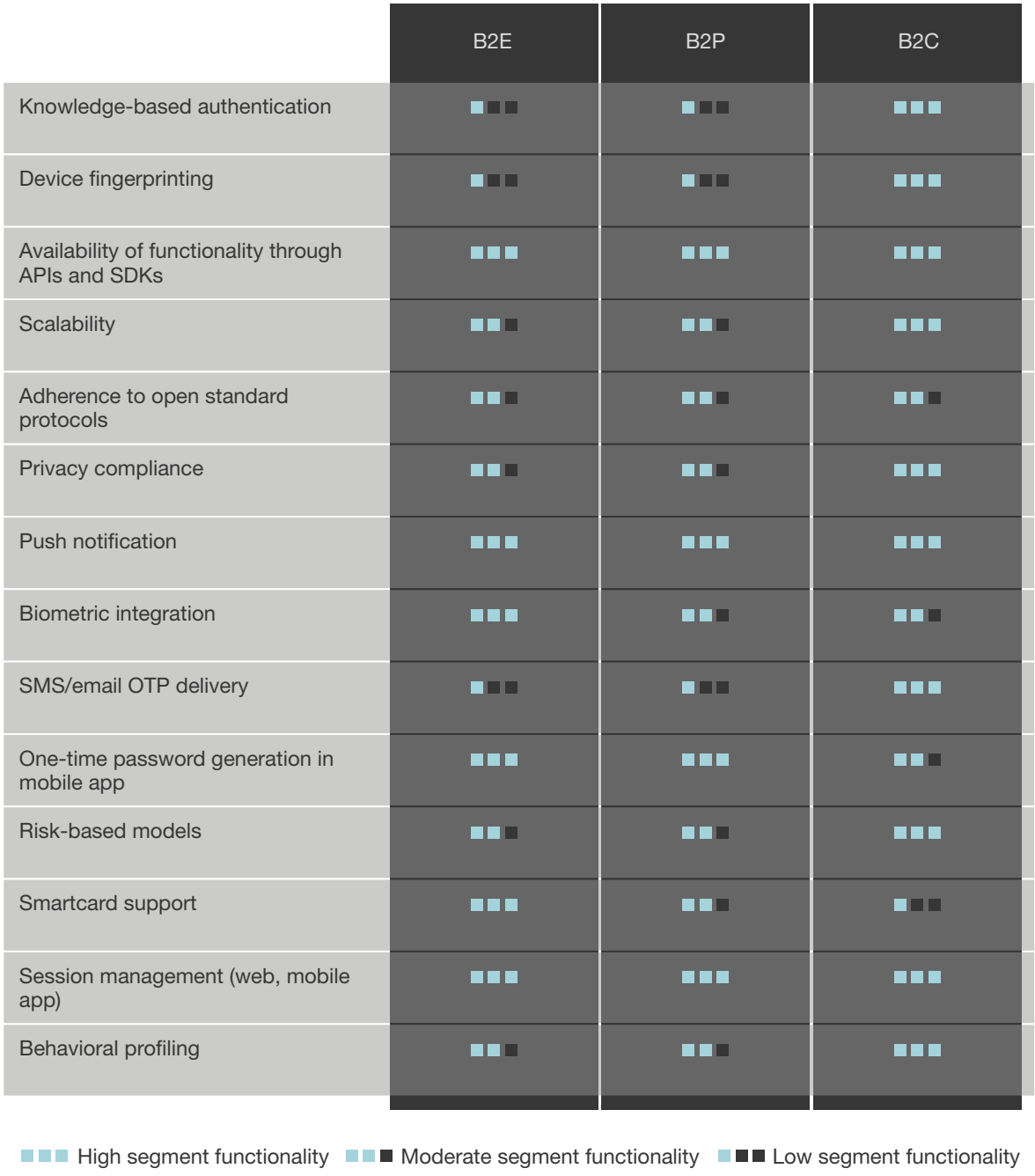
FIGURE 1 Now Tech Market Presence Segments: Authentication Management Solutions, Q3 2018

*Forrester estimate

Forrester spoke with our expert analysts and interviewed external subject matter experts in our search for the most important authentication management technologies. We identified the following segments, each with varying capabilities (see Figure 2):

- **B2E solutions provide employee authentication and usually SSO into web apps.** These solutions also offer employee-facing 2FA options, extensive centralized policy management, authorization, high availability, and auditing. Often, they offer simple self-service capabilities for users, such as forgotten user ID and password recovery/reset.[5]
- **B2P solutions primarily provide business-partner-facing authentication.** These solutions offer identity verification, strong, standards-based credentialing, as well as a broad spectrum of identity federation protocol support including SAML. These solutions allow employees of one organization to gain controlled access to applications of another organization.
- **B2C solutions offer customer or consumer access management.** These solutions usually provide risk-based authentication, 2FA options, and some level of self-service and consent management for users.

FIGURE 2 Now Tech Functionality Segments: Authentication Management Solutions, Q3 2018



Align Individual Vendor Solutions To Your Organizational Needs

The following tables provide an overview of vendors with details on functionality category, geography, and vertical market focus (see Figure 3, see Figure 4, and see Figure 5).

FIGURE 3 Now Tech Large Vendors: Authentication Management Solutions, Q3 2018

LARGE >$140M annual authentication revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top 3 by revenue %)	Sample customers
CA Technologies	B2E, B2C, B2P	NA: 50%; EMEA: 20%; AP: 20%; LATAM: 10%*	Financial services, healthcare, public sector*	JP Morgan Chase, SK Infosec, TIAA
IBM	B2E, B2P, B2C	NA: 32%; EMEA: 34%; AP: 28%; LATAM: 6%	Financial services, public sector, telco	POST Luxembourg
Microsoft	B2E, B2P, B2C	NA: 55%; EMEA: 35%; AP: 5%; LATAM: 5%*	Financial services, insurance, high-tech	Daimler, Insurwave, volparasolutions
Okta	B2E, B2P, B2C	NA: 85%; EMEA: 9%; AP: 6%*	Entertainment, media, and leisure; manufacturing; retail and wholesale	21st Century Fox, Allergan, Broadcom
Oracle	B2E, B2C, B2P	NA: 60%; EMEA: 30%; AP: 5%; LATAM: 5%*	Financial services, public sector, retail and wholesale*	Vendor did not disclose.
RSA	B2E, B2C, B2P	NA: 70%; EMEA: 16%; AP: 8%; LATAM: 6%*	Financial services, insurance, healthcare	Applied Materials, Intuit, Netflix

* The vendor did not provide information for this cell; this is Forrester's estimate.

FIGURE 4 Now Tech Midsize Vendors: Authentication Management Solutions, Q3 2018

MIDSIZE $30M to $140M annual authentication revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top 3 by revenue %)	Sample customers
Auth0	B2E, B2P, B2C	NA: 50%; EMEA: 30%; AP: 15%; LATAM: 5%	Financial services, media, high-tech	Atlassian, Dow Jones, Mass Mutual
Duo Security	B2E, B2P	NA: 75%; EMEA: 20%; AP: 3%; LATAM: 2%	High-tech, education, healthcare	Centura Health, Facebook, Stanford University
Entrust Datacard	B2E, B2P, B2C	NA: 40%; EMEA: 30%; AP: 30%	Financial services, public sector, high-tech	NASA JPL, Santander Santiago, Vipsnet
Exostar	B2P	NA: 90%; EMEA: 10%	Aerospace/defense, life sciences, healthcare	BAE Systems, Boeing, Merck
ForgeRock	B2E, B2C	NA: 45%; EMEA: 45%; AP: 5%; LATAM: 5%	Public sector, high-tech, financial services	Agfa, AutoZone, Pearson
Google	B2E, B2C	NA: 50%; EMEA: 20%; AP: 20%; LATAM: 10%*	Financial services, public sector, high-tech*	Vendor did not disclose.
OneIdentity	B2E	NA: 50%; EMEA: 35%; AP: 10%; LATAM: 5%*	Education, healthcare, financial services*	Bakersfield PD, City of Frankfurt
OneLogin	B2E, B2P, B2C	NA: 82%; EMEA: 11%; AP: 6%; LATAM: 1%*	High-tech, financial services, professional services	British Red Cross, Consort Medical, Kreditech

* The vendor did not provide information for this cell; this is Forrester's estimate.

FIGURE 4 Now Tech Midsize Vendors: Authentication Management Solutions, Q3 2018 (Cont.)

MIDSIZE $30M to $140M annual authentication revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top 3 by revenue %)	Sample customers
OneSpan (VASCO)	B2C, B2E, B2P	NA: 24%; EMEA: 48%; AP: 25%; LATAM: 3%*	Financial services, insurance, high-tech	Konami, Mizuho, Penn State University
OpenText (Covisint)	B2P	NA: 49%; EMEA: 18%; AP: 22%; LATAM: 11%	Manufacturing, insurance, energy	The Auto Club, Daimler, Shell
Ping Identity	B2E, B2C	NA: 65%; EMEA: 25%; AP: 7%; LATAM: 3%*	Finance, retail, software and internet	Applied Materials, GSK, Intuit
SAP	B2C, B2E, B2P	NA: 35%; EMEA: 45%; AP: 15%; LATAM: 5%*	Entertainment, media, and leisure; retail and wholesale; manufacturing	DC Thomson, Provident Financial Group, Softonic
SecureAuth + Core Security	B2E, B2P	NA: 72%; EMEA: 11%; AP: 16%; LATAM: 1%*	Financial services, healthcare, manufacturing	ESCO, Unisys, United Methodist
Symantec	B2E, B2C, B2P	NA: 65%; EMEA: 14%; AP: 16%; LATAM: 5%*	Financial services, healthcare, high-tech	Citrix, E-TRADE, USAA

* The vendor did not provide information for this cell; this is Forrester's estimate.

FIGURE 5 Now Tech Small Vendors: Authentication Management Solutions, Q3 2018

SMALL <$30M annual authentication revenue

	Primary functionality segments	Geographic presence (by revenue %)	Vertical market focus (top 3 by revenue %)	Sample customers
Entersekt	B2C, B2P	NA: 5%; EMEA: 95%	Financial services, insurance, high-tech	FirstBank of Colorado, Nedbank, Swisscard AECS
Janrain	B2C, B2P	NA: 64%; EMEA: 30%; AP: 6%	Consumer goods, pharma/healthcare, retail	Coca-Cola, McDonald's, Philips
Nok Nok	B2C	NA: 60%; EMEA: 9%; AP: 30%; LATAM: 1%*	Telco, financial services, professional services	ICBC, NTT DOCOMO, PayPal
Optimal IdM	B2E, B2P, B2C	NA: 70%; EMEA: 20%; AP: 5%; LATAM: 5%*	Financial services, high-tech, education*	Blue Cross Blue Shield of Montana, U.S. Bank, WestMonroe*
Uniken	B2E, B2C	NA: 14%; EMEA: 1%; AP: 84%; LATAM: 1%*	Financial services, healthcare, travel/hospitality	BOI, CDSL
Yubico	B2C	NA: 50%; EMEA: 20%; AP: 20%; LATAM: 10%*	Retail and wholesale, high-tech, professional services	Facebook, Google, Microsoft

*The vendor did not provide information for this cell; this is Forrester's estimate.

Recommendations

Treat Authentication As Mission-Critical Infrastructure

Authentication plays a vital role in maintaining a robust IAM framework for your firm. Forrester clients and interviewees identified the following as the most important items when implementing an authentication solution:

› **Dedicate headcount to supporting the authentication solution.** The most common mistake we see is that companies regard authentication management solutions as just another project or business application. In reality, authentication management solutions demand 24x7 support, since, if your authentication is down, neither your employees, your business partners, nor your customers

can access your site, invariably causing dissatisfaction, lost profits, and damaged reputation. Smooth integration and operation of authentication management solutions is of paramount importance and can only be achieved by dedicating employees to operations.

- **Involve application developers, network security, and middleware admins early on.** Most authentication management solutions will support at least a handful of internally developed applications. Integration makes most sense if application developers disable native, legacy authentication in their applications and switch to relying on the authentication solution's centralized authentication framework instead. This is no easy task, especially for a large number of in-house-developed apps: S&R pros must carefully plan scoping and phasing of centralized authentication implementation. Network security and middleware administrators must be providing active support for authentication implementation as single sign-on (SSO) platforms connect to Active Directory and LDAP. SSO platforms also often force changes to how web traffic is routed within and across the borders of the firm.
- **Use risk-based features in authentication.** To reduce user friction, seek out authentication management solutions that offer risk-based policies based on the user's device and location. These risk-based features allow an employee sitting at their office desk at 10 a.m. local time on a weekday access to all their apps just using simple (e.g., password) credentials but force riskier users accessing the firm's apps from a brand-new device from Asia during the middle of night on a weekend to perform 2FA.[6]
- **Favor solutions with canned desktop and biometric integration.** While most authentication management solutions don't provide native biometric modality support (e.g., finger, face, or voice, etc.), with accelerating weakening of the password, your firm will only be able to defend its assets using easy-to-use multi-factor authentication (MFA). Integration and testing of biometric sensors (especially for desktop) integration is no easy task. Demand that your authentication management solution vendor provide centralized and productized biometric and desktop login integration.[7]

Supplemental Material

Market Presence Methodology

We defined market presence in Figure 1 based on factors such as: 1) ability to provide listed capabilities and 2) the target user group to which the solution provides authentication.

To complete our review, Forrester requested information from vendors. If vendors did not share this information with us, we made estimates based on available secondary information. We've marked companies with an asterisk if we estimated revenues or information related to geography or industries. Forrester fact-checked this report with vendors before publishing.

Endnotes

[1] See the Forrester report "The Forrester Tech Tide™: Identity And Access Management, Q4 2017" and see the Forrester report "Mobile Application Authentication Trends And Best Practices."

[2] See the Forrester report "Forrester's Risk-Centric Identity And Access Management Process Framework."

[3] Forrester created a framework to quantify the costs and benefits for various IAM approaches to determine which one provides the best return on investment (ROI). See the Forrester report "Making The Business Case For Identity And Access Management."

[4] In our 2017, 20-criteria evaluation of customer IAM (CIAM) providers, we identified the eight most significant ones — Auth0, ForgeRock, Gigya, Janrain, LoginRadius, Microsoft, Ping Identity, and Salesforce — and researched, analyzed, and scored them. See the Forrester report "The Forrester Wave™: Customer Identity And Access Management, Q2 2017."

[5] Implementing 2FA is a top priority for security decision makers. For more on IAM priorities and 2FA adoption plans, see the Forrester report "Understand The State Of Identity And Access Management: 2017 To 2018."

[6] See the Forrester report "The Forrester Wave™: Risk-Based Authentication, Q3 2017" and see the Forrester report "TechRadar™: Biometric Authentication, Q1 2017."

[7] See the Forrester report "Top Trends Shaping IAM In 2018," see the Forrester report "Best Practices: Behavioral Biometrics," and see the Forrester report "The State Of Facial Recognition For Authentication And Verification."

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

141433

A Forrester Total Economic Impact™
Study Commissioned By Auth0
October 2017

The Total Economic Impact™ Of The Auth0 Identity Platform

Cost Savings And Business Benefits Enabled By Auth0

FORRESTER®

Table Of Contents

Project Director:
Liz Witherspoon
October 2017

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.

FORRESTER®

Key Benefits

Increased revenue from customer conversions and new feature releases:
$2 million

Faster time-to-market for integrations:
$2.7 million

Reduction in IAM-related management costs:
$3.7 million

Executive Summary

Auth0 provides an identity-as-a-service (IDaaS) platform that organizations use for consumer, business partner, and employee identity management. As a service, Auth0 helps organizations overcome the challenge of developing complex identity solutions for their web, mobile, internet-of-things (IoT), and internal applications by providing prebuilt, secure logins and APIs that can be used by developers in place of custom coding. Auth0 commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and examine the potential return on investment (ROI) enterprises may realize by deploying the Auth0 Identity Platform. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the Auth0 Identity Platform on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with a few years of experience using the Auth0 Identity Platform. These organizations, which rely on Auth0 to provide identity management for their external customers, trusted business partners, and employees, struggled to centralize and streamline the process. They lost time and potential business because it was cumbersome to secure access to their products, content, application program interfaces (APIs), and microservices within a complex ecosystem of partners, customers, and employees.

Prior to using the Auth0 Identity Platform, the customers relied on individual developers to create the code or custom integrations for secure login and single sign-on (SSO) and other identity needs. However, this led to inconsistencies in the user experience for identity, making it difficult for customers and business partners to access content and products. When innovating around identity, interviewed companies were not able to easily implement multifactor authentication and passwordless or social login; they also could not easily secure web and mobile applications before Auth0. They experienced lower conversion rates, lost partner business, and increased developer costs and costs related to password and registration issues.

Key Findings

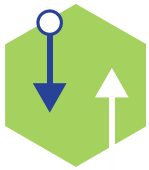
Quantified benefits. The following risk-adjusted quantified benefits are representative of those experienced by the companies interviewed:

- **Reduction in identity-related management, development, and maintenance hours.** Auth0 reduced developer hours because, instead of coding identity logic directly into each application, developers could access Auth0's software development kits (SDKs) with prebuilt logins and integrations. It also reduced the management and maintenance time associated with identity management.
- **Increased revenue from customer conversions.** Customers using Auth0 as the identity management platform for applications that directly face customers and generate revenue for the organization reported a 15% percent increase in customer registrations or online purchases due to Auth0's flexible and easy login options.
- **Faster time-to-market for integrations that require identity and access management (IAM).** Prior to Auth0, customers struggled to complete custom integrations with their business partners, resulting in a slower realization of the project's value or lost business.

ROI
548%

Benefits PV
$11.7 million

NPV
$9.9 million



Payback
< 6 months

- **Reduction in costs associated with password and customer registration issues.** Incorrect passwords account for a large volume of help desk traffic in general. Prior to Auth0, employees and customers of the organizations interviewed had inconsistent logins across their applications and services. Their support costs were reduced with Auth0.
- **Faster release of new application features and functionality for customer-facing features.** Because Auth0 takes the development of code related to identity out of the hands of the developer and provides Auth0 software development kits (SDKs) for use, developers can release applications faster. This speed of release of new functionality translated into customer revenue that can be recognized more quickly for the interviewed organizations.

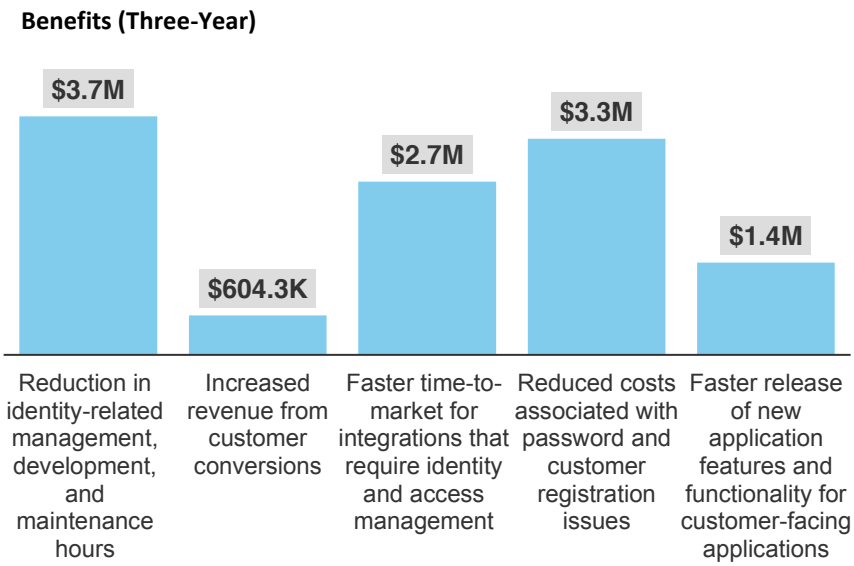
Unquantified benefits. The interviewed organizations experienced the following benefits, which were not quantified for this study:

- **Increased developer and end customer satisfaction**. Developers using Auth0 reported enjoying using it and felt that it was created by and for developers. They felt they could communicate with Auth0's engineering team freely.
- **High satisfaction with the Auth0 service and expertise.** Customers reported a high level of trust in the development expertise that went into the software development kit supplied by Auth0. They relied on Auth0's high level of service for updates and unexpected patches.
- **Reduced cost of handling security and audit issues**. Customers reported reduced time spent on audit-related requests. If they had experienced data breaches in the past related to login databases, they reduced that risk with Auth0.
- **Faster innovation around application development that requires authentication.** Customers reported that they could innovate more quickly while rolling out applications using multifactor authentication; passwordless and social connections; and other identity-related features. Auth0 made this innovation more turnkey for them.

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

- **Licensing and professional services costs.** Organizations paid a monthly recurring licensing and one-time professional services fee to Auth0.
- **Implementation and ongoing management.** Customers reported a short, up-front implementation period that lasted from a few days to a few months, depending on the complexity of the organization.

Forrester's interviews with five existing customers and subsequent financial analysis found that an organization based on these interviewed organizations experienced present value (PV) benefits of $11,670,195 over three years versus (PV) costs of $1,801,933, adding up to a net present value (NPV) of $9,868,262 and an ROI of 548%.


Benefits (Three-Year)
$3.7M
$604.3K
$2.7M
$3.3M
$1.4M
Reduction in identity-related management, development, and maintenance hours
Increased revenue from customer conversions
Faster time-to-market for integrations that require identity and access management
Reduced costs associated with password and customer registration issues
Faster release of new application features and functionality for customer-facing applications

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 the Auth0 Identity Platform.

The objective of the framework is to identify the cost, benefit, flexibility, and risk factors that affect the investment decision. Forrester took a multistep approach to evaluate the impact that the Auth0 Identity Platform 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 Auth0 stakeholders and Forrester analysts to gather data relative to the Auth0 Identity Platform.

CUSTOMER INTERVIEWS
Interviewed five organizations using the Auth0 Identity Platform 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 Auth0's Identity Platform'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.

The Auth0 Identity Platform Customer Journey

BEFORE AND AFTER THE AUTH0 IDENTITY PLATFORM INVESTMENT

Interviewed Organizations

For this study, Forrester conducted five interviews with Auth0 Identity Platform customers. Interviewed customers include the following:

INDUSTRY	REGION	INTERVIEWEE	DRIVERS FOR IMPLEMENTING AUTH0
Media	Headquartered in California	Engineering manager	+ Support SSO for large enterprise customers and those demanding OpenID authentication + Select one identity provider to broker applications + Enable authentication seamlessly, including on mobile apps + Scale up business more quickly because of ease of adding authentication + Avoid issues with compliance, encryption, or other data requirements for transferring identity information
Manufacturing	Headquartered in New Jersey	Senior enterprise architect	+ Provide authentication/access to standard API catalogue for internal and external consumption + Provide secure access to the API gateway that does all the policies, rules, regulations, and governance + Create a new digital workspace for IT + Create one profile for end user customers and employees + Implement the most current security technologies for applications and APIs, including OpenID Connect and OAuth2.0 + Secure components and interfaces for IoT platforms so that they can interface with older technology
Printing	Headquartered in the Netherlands	Director of API management	+ Standardize access to applications across business units + Avoid tying authentication to Active Directory + Avoid costs associated with acquisitions to give those users access to applications + Disconnect the microservices from the access to it + Avoid developers making insecure and incompatible choices for authentication + Expose APIs to third parties external to the company
Online sports platform	Headquartered in Canada	Cofounder	+ Reduce risk of a database leak/breach + Enable turnkey additions of third-party/social logins and reduce maintenance of those logins + Create ability to log in as a user to troubleshoot issues + Speed up time-to-market in different geographies and in different segments
Recycling and waste disposal	Headquartered in Arizona	Enterprise architect	+ Support replatforming of website and mobile apps + Combine authentication for all customer-facing apps under one platform + Improve stability of the website providing core services + Increase eCommerce part of the business

Key Challenges

Customers interviewed for this study shared a common goal of standardizing on one identity platform. In most cases, this supported a wider corporate effort to securely open boundaries between partners, customers, and the company to enable easier transfer of content,

products, APIs, microservices, or information provided between these entities. To open the boundaries of their organization, the companies realized that they needed a faster, efficient, secure, and developer-centric identity management solution. The solution needed to separate the development of the applications from the identity management process.

- **Avoid developers making insecure and incompatible choices for authentication.** Customers who chose Auth0 had, in the past, allowed individual developers of different business units to create the identity functionality for the applications developed. The companies had the goal of removing the decision making and coding behind identity from the developers' hands, freeing the developer to focus on creating core application functionality faster.
- **Enable business to grow more quickly.** In the past, customers had to create custom integrations related to identity and SSO. In some cases, they could not meet their customers' requirements around identity and lost potential business. Furthermore, they wanted to make it easier for customers, whether they were business-to-business (B2B) or consumers, to log in more easily, quickly, and securely so that they could transact more readily. Auth0 enabled them to do that.
- **Take advantage of innovative identity management approaches.** Customers wanted to provide advanced identity options to their customers and employees, including social login, multifactor authentication, passwordless login, and SSO to name a few. However, they didn't have the internal expertise to build and manage these connections. Using Auth0, customers could access a software development toolkit and immediately incorporate identity functionality into applications without having to maintain those connections. Because Auth0 is a service, the identity capabilities and code are updated on a regular basis in its code library. If social logins update their APIs or have third-party security issues, Auth0 immediately updates the code, which quickly updates within customers' applications.

"For us to do the digital transformation, the most critical aspect we wanted to solve first was the identity in a single profile. And that's the key benefit of Auth0."

Senior enterprise architect, manufacturing

"One of the reasons we chose Auth0 was the ease of implementation and developer-centric dashboard. A developer can have a self-service kind of scenario and download from there to kick-start the process. That's where we see the most value for our resources as well as the ease of integration to iPhone apps, Android apps, API gateways, and user authentication."

Senior enterprise architect, manufacturing

Solution Requirements

The interviewed organizations searched for a solution that could:

- Serve as a single platform for all their identity management needs.
- Support the most current advances in identity standards and methods.
- Be flexible enough to change with the social sites' identity approaches and other adjustments in requirements.
- Provide an easy solution that even nontechnical resources could use.

"One customer tells us that you need to send data in one way and the other customer says the exact opposite. With Auth0, they've already thought about all that and built it out."

Engineering manager, media company

Key Results

The interviews revealed that key results from the Auth0 Identity Platform investment include:

- **Improved consistency of identity management.** Auth0 streamlined the identity management process and centralized it within one platform. It removed the hard work of writing code related to identity from developers' tasks, enabling them to focus on developing core functionality for applications.
- **Increased conversions and integrations for new customers.** The move to Auth0 enabled organizations to convert consumers 15% more frequently. This was due to a better customer experience with identity, including social login. Also, for business-to-business integrations requiring identity management, customers could reduce the time to build those connections by 33%. This was because Auth0 offers extensive access to common identity integrations.
- **Improved security and quality of identity management.** Customers felt that their previous identity management systems were vulnerable to security issues. One customer described an instance of having a login database hacked that contained sensitive customer data. The breach nearly cost the startup company its investor. Other customers described unease around having developers not trained in security writing code for identity. They felt that it was managed in too many different locations among disparate development teams across the organization. With Auth0, this was no longer an issue because all code related to identity was now accessible through the Auth0 software development toolkit, written by engineers who are experts in secure identity.

> "Auth0 is part of our core platform functionality — we didn't want people to have to authenticate in five different ways. Our mantra is 'Let's not expose our org chart to our customers and to our partners. Let's not make somebody figure out the authentication calls across the organization.'"
>
> *Director of API management, printing*

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 five 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:

Description of composite. The multibillion dollar organization uses Auth0 as its identity platform for its thousands of external customers and hundreds of external business-to-business relationships that include contractors, business partners, and distributors. The partners and customers in this ecosystem need secure access to their content, APIs, and microservices. Furthermore, the organization has 10,000 internal employees, half of whom traverse through Auth0 with internal applications and mobile apps that have been built for them. The organization generates revenue through its business-to-business and business-to-consumer (B2C) customer bases; the faster, more seamless processes the organization provides to its customers for gaining access to APIs, content, and microservices, the more quickly the company can grow its business.

In the past, the organization had a less stable, less reliable approach to identity and authentication. Developers whose core expertise was not security had developed and maintained identity and authentication functionality for the organization's core commercial website and internal

Key assumptions

150K customer logins per month

5K internal employees who traverse through Auth0 for authentication

150 developers and administrators using Auth0

partner portal. In some cases, the organization relied on integration with existing directory services, which was problematic when the organization acquired new companies or extended authentication to external customers. This led to an inconsistent approach to authentications and SSO and a less stable environment with regular downtime caused by identity and authentication systems. This also increased the threat of a security breach for user information and led to a less optimal customer experience for the outside customer or partner. In the course of transacting with the company, they may have used multiple logins for access to different applications or areas of the company's IP or be taken to third-party sites to complete actions, such as making a purchase. Additionally, relying on integration with existing directory services decreased the level of centralization and control over access and use of corporate content and IP.

Key uses of Auth0. A key use of Auth0 for business-to-consumer, business-to-business, and business-to-enterprise (B2E) was to enable developers, external partners, employees, and customers to access content, APIs, and microservices securely without having to maintain a database of user ID and passwords or "hard code" authentication into the applications. Another key use was to enable authentication seamlessly, including with mobile and IoT applications, and meet the demands of enterprise business customers for the standard and security they expect for single sign-on.

> "We wanted to tackle two things when looking for an identity solution: website stability and controlling the user experience. Auth0 really shined as far as the out-of-the-box API support, especially for angular. It had a simple documentation page about how you integrate — 15 minutes and we were up and running with a proof of concept."
>
> *Enterprise architect, recycling and waste disposal*

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA AS APPLIED TO THE COMPOSITE

Total Benefits

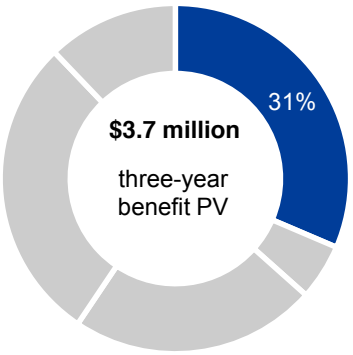
REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Reduction in identity-related management, development, and maintenance hours	$1,474,227	$1,474,227	$1,474,227	$4,422,681	$3,666,184
Btr	Increased revenue from customer conversions	$243,000	$243,000	$243,000	$729,000	$604,305
Ctr	Faster time-to-market for integrations that require identity and access management	$1,071,000	$1,071,000	$1,071,000	$3,213,000	$2,663,418
Dtr	Reduced costs associated with password and customer registration issues	$1,334,531	$1,334,531	$1,334,531	$4,003,594	$3,318,782
Etr	Faster release of new application features and functionality for customer-facing applications	$570,000	$570,000	$570,000	$1,710,000	$1,417,506
	Total benefits (risk-adjusted)	$4,692,758	$4,692,758	$4,692,758	$14,078,275	$11,670,195

Reduction In Identity-Related Management, Development, And Maintenance Hours

Auth0 customers reported several ways in which the platform reduced their development and maintenance hours related to identity management.

- Auth0 reduced developer hours because instead of coding identity logic directly into each application, developers can pull from a software development kit. Because coding identity logic can take hours of developer time, especially for those who are not experts in this area, the reduction is a significant one. It reduces the burden on an individual developer. Furthermore, it reduces maintenance time on those apps.
- Auth0 reduced the overall time to integrate, streamline, and secure identity administration. In the past, customers relied on a decentralized approach to identity management with the result of having inconsistency and reduced security around identity for employees and customers. To approximate the functionality of Auth0, customers estimated from three to 10 more full-time developers to build and run a comparable identity management platform. This model makes a conservative 20% reduction in administration time and effort due to Auth0.

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 nearly $11.7 million.



Reduction in development hours: **31%** of total benefits

FORRESTER®

- Auth0 reduced the time required to fix third-party security bugs that require unexpected patches. This is because Auth0 security experts continually update all of Auth0's software development toolkit as well as the core service in response to security bugs or other changes. For example, vulnerabilities such as HeartBleed were fixed by Auth0's engineering resources and made immediately available to customers.

Based on the composite organization, which has 150 developers and administrators working on many internal and customer-facing applications, the model estimates 50 developer hours saved for each new application and service created by developer teams across the organization. At a fully loaded hourly salary of $57, the development hours avoided total over $1.2 million annually. Pushing that savings further is the avoided maintenance time for those same applications, estimated at 10% of the original development hours. In addition, the composition organization avoided having to implement two unexpected security patches related to identity annually, saving more than $2,000 each year and avoiding the associated risks with those vulnerabilities. The final calculation contributing to this benefit is the 20% reduction in administrative time and effort for three full-time employees to manage secure identity administration. At an estimated $120,000 annual salary fully loaded, this reduction in workload equates to around $72,000 annually. In addition, Auth0 requires little training in comparison to previous platforms used or created, which saves 20 hours annually for all developers incorporating identity into their apps. In total, those administration and training savings equal $225,000 per year.

Customers have different identity management solutions in place prior to implementing Auth0. Some are replacing a combination of in-house tools and existing SSO and authentication solutions, such as Active Directory. Depending on the type of solution in place prior to Auth0, this benefit can vary. Furthermore, the number of unexpected vulnerabilities with third-party logins will vary depending on the organization.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $3,666,184.

"Auth0 answered the question of how we prove the identity of the caller of an API or a person logging into a UI. And they enable us to do it in a way that gives us the flexibility to grow our organization and plug into different identity providers so that we don't have to be limited by a technology purchase decision we made 15 years ago."

Director of API management, printing

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.

Reduction In Identity-Related Management, Development, And Maintenance Hours: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
A1	Number of developers securing internal and external applications		150	150	150
A2	Developer hours saved for each application developed		50	50	50
A3	Number of new services/applications developed annually by individual engineers annually that require login as part of the development process		3	3	3
A4	Hourly developer salary		$57	$57	$57
A5	Development hours avoided	A1*A2*A3*A4	$1,282,500	$1,282,500	$1,282,500
A6	Maintenance time saved	Estimated at 10% of original	$128,250	$128,250	$128,250
A7	Subtotal	A5+A6	$1,410,750	$1,410,750	$1,410,750
A8	Avoided time fixing third-party security bugs (unexpected patches)	20 dev hrs * $57 hrly salary * 2 times per year	$2,280	$2,280	$2,280
A9	Number of full-time equivalents required to manage secure identity administration to		3	3	3
A10	Annual salary fully loaded for IAM professional		$120,000	$120,000	$120,000
A11	Reduction in administrative time and effort for IAM due to Auth0		15%	15%	15%
A12	Training time avoided for developers using Auth0		150	150	150
A13	Hours avoided in training annually		20	20	20
A14	Hourly developer salary		$57	$57	$57
A15	Subtotal	A9*A10*A11+ A12*A13*A14	$225,000	$225,000	$225,000
At	Reduction in identity-related management, development, and maintenance hours	A7 + A8 + A15	$1,638,030	$1,638,030	$1,638,030
	Risk adjustment	↓10%			
Atr	Reduction in identity-related management, development and maintenance hours (risk-adjusted)		$1,474,227	$1,474,227	$1,474,227

Increased Revenue From Customer Conversions

Customers using Auth0 as the identity management platform for applications that directly face consumers and generate revenue for the organization reported a 15% percent increase in customer registrations or online sales due to Auth0's easier login process, optimized for conversion through its user experience design. In the past, customers who needed to log into an application to shop or complete a purchase may have been diverted due to a forgotten password or a difficult login process. With Auth0, organizations can add social login, email login,

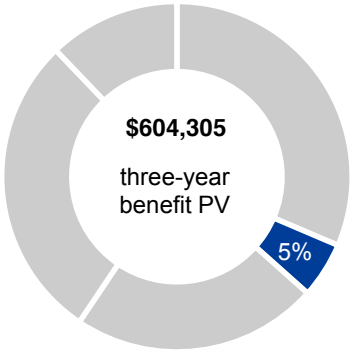
passwordless login, and other customer-friendly login types that ensure a smooth, easy conversion options for consumers. This translates to a revenue increase annually, even after accounting for a 20% operating margin.

The model assumes the following about the organization converting consumers at a higher rate:

- On average, 30,000 users sign in or register monthly.
- The average value of a customer transaction is $25.00.
- The percentage increase in customer registration or purchase due to Auth0's easier login is 15%.
- The average operating margin of the customers interviewed is 20%.

The average number of customers who register or sign in monthly varies widely among organizations. Also, the average value of a transaction is highly dependent on the type of organization along with the average operating margin for that organization.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $604,305.



Higher conversion rate for consumers: **5%** of total benefits

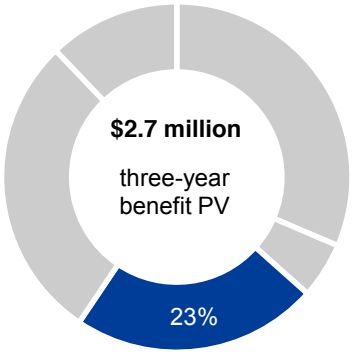
Higher Conversion Rate For Customers: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
B1	Average number of users/registration sign-ups monthly		30,000	30,000	30,000
B2	Percentage conversion increase due to Auth0's easier login	15%	15%	15%	15%
B3	Additional monthly conversions due to easier login	B1*B2	54,000	54,000	54,000
B4	Average value of a customer transaction		$25	$25	$25
B5	Operating margin	15%	20%	20%	20%
Bt	Higher conversion rate for customers	B3*B4*B5*12	$270,000	$270,000	$270,000
	Risk adjustment	↓10%			
Btr	Higher conversion rate for customers (risk-adjusted)		$243,000	$243,000	$243,000

Faster Time-To-Market For Integrations That Require Identity And Access Management

Customers of Auth0 generate business through integrations with their business-to-business partners. Prior to Auth0, they struggled to complete custom integrations with their business partners, resulting in a slower realization of the project's value. Furthermore, they estimated that about two projects per year were lost because their identity management platform could not support the requirements of their business partners and customers, such as SSO, multifactor authentication, and passwordless login. Using Auth0, those integrations can occur quickly and seamlessly, leading to a faster time-to-market and revenue recognition.

The model assumes that the composite organization integrated five new business partners or customers monthly at an average contract value of $500,000 because these are enterprise-wide, business-to-business



Faster time-to-market for integrations: **23%** of total benefits

FORRESTER®

relationships. The time to integrate the projects is 33% faster, which leads to almost $5 million in revenue recognized more quickly. Accounting for an average operating margin among the customers interviewed of 20%, the additional annual value due to Auth0 is $990,000. The number of lost deals before Auth0 due to having an insufficient and inefficient identity platform amounts to $150,000 in additional value.

The results can vary by the size and number of the contracts that are sold annually for an organization. Furthermore, every organization's operating margin varies depending on its operational strategy.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $2,663,418.

Faster Time-To-Market For Integrations That Require Identity And Access Management: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
C1	Faster integration of business-to-business customers				
C2	Number of new business partners or customers integrated monthly		5	5	5
C3	Annual value of new business or partner contracts		$500,000	$500,000	$500,000
C4	Monthly value of new business or partner contracts	C3/12	$41,667	$41,667	$41,667
C5	Average time to integrate new business or partner contract before Auth0	Months	6	6	6
C6	Percentage improvement in time to complete the integration	33%	33%	33%	33%
C7	Time improvement in integrating new contracts	Months	1.98	1.98	1.98
C8	Value of time improvement for integrating new business or partner contracts	C2*12*C4*C7	$4,950,000	$4,950,000	$4,950,000
C9	Operating margin	15%	20%	20%	20%
C10	Subtotal: Value of time improvement for integrating new contracts	C8*C9	$990,000	$990,000	$990,000
C11	Number of lost deals annually before Auth0 due to insufficient and inefficient identity platform		2	2	2
C12	Subtotal: Value of deals lost prior to Auth0	C3*C11*C9	$200,000	$200,000	$200,000
Ct	Faster time-to-market for integrations that require identity and access management	C3*C4	$1,190,000	$1,190,000	$1,190,000
	Risk adjustment	↓10%			
Ctr	Faster time-to-market for integrations that require identity and access management (risk-adjusted)		$1,071,000	$1,071,000	$1,071,000

Reduced Costs Associated With Password And Customer Registration Issues

Incorrect passwords account for a large volume of help desk traffic in general. Prior to Auth0, employees and customers of the organizations interviewed had no consistent identity experience across their applications and services. They did not have adequate social login capabilities, multifactor authentication, or passwordless login. This led to incorrect logins and password reset requests, especially for internal logins across the organization. Furthermore, external customers who registered to create accounts with an organization sometimes struggled with login due to the inconsistencies highlighted above.

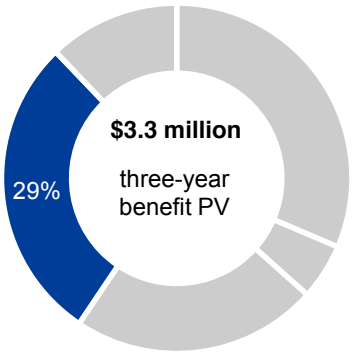
For the composite organization, Forrester assumes that:

- There are 1,250 internal logins per day for corporate applications and services.
- There are 5,000 external logins per day from customers and business partners accessing applications from outside the company.
- Three percent of those daily logins are incorrect; 50% of those lead to a password reset request.
- The average cost to reset a login or to complete a customer registration through customer support is $10.00.

Following these assumptions, the composite organization stands to save over $1 million annually in the costs associated with password and new registration assistance. The model assumes a three-month implementation time period in Year 1 before the benefits will be realized. The reduction in support costs will vary with:

- The number of users logging in or registering daily.
- The support costs associated with resolving password or registration issues.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $3,318,782.



Reduced costs associated with password resets: **29%** of total benefits

> "With our past solution, emails were not getting to users, the reset email didn't arrive, or it was in the spam folder. Since implementing Auth0, the volume of calls has gone down considerably — the reset is ready to use and works well."
>
> *Enterprise architect, recycling and waste disposal*

FORRESTER®

Reduced Costs Associated With Password And Customer Registration Issues: Calculation Table					
REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
D1	Number of internal logins per day	Source: composite	1,250	1,250	1,250
D2	Number of external logins per day	Source: composite	5,000	5,000	5,000
D3	Number of logins that are incorrect per day	3%	187.5	187.5	187.5
D4	Average cost to reset a login		$10	$10	$10
D5	Percentage of incorrect logins that lead to a password reset request		50%	50%	50%
D6	Cost savings from avoided manual registration of new customers	D3*D4*D5*365	$342,188	$342,188	$342,188
D7	Number of logins per day	D1+D2	6,250	6,250	6,250
D8	Percentage of customers who call the help desk to complete registration — before Auth0	3%	5%	5%	5%
D9	Average cost to complete the registration through customer support		$10	$10	$10
D10	Subtotal: Cost savings from avoided manual registration of new customers	(D1*5%)+(D2*5%)* D4*365	$1,140,625	$1,140,625	$1,140,625
Dt	Reduced costs associated with password and customer registration issues	D6+D10	$1,482,813	$1,482,813	$1,482,813
	Risk adjustment	↓10%			
Dtr	Reduced costs associated with password and customer registration issues (risk-adjusted)		$1,334,531	$1,334,531	$1,334,531

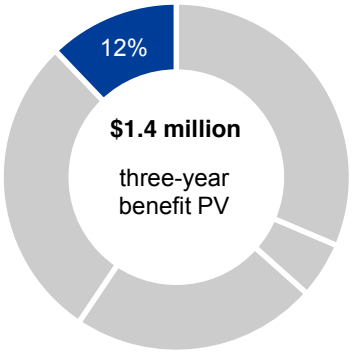
Faster Release Of New Application Features And Functionality For Customer-Facing Applications

Because Auth0 takes the development of code related to login out of the hands of the developer and provides an updated software development kit of multiple login types available for use, developers can release applications faster. This earlier release of new functionality translates into customer revenue that can be recognized more quickly. Customers estimated that they could improve the time-to-release new customer-facing features in apps by an average of 10 weeks because they can use Auth0's software development kits (SDKs).

The model assumes that the features released generate an additional $30,000 in revenue weekly because they are built for customer-facing applications that sell products or services. The composite organization released 10 new features, on average, to its customer base, which enabled the company to bring in revenue more quickly, totaling about $600,000 annually accounting for a 20% operating margin.

Customers have a wide range of applications and development timelines.

To account for these risks, Forrester adjusted this benefit downward by



Faster release of application features: **12%** of total benefits

FORRESTER®

5%, yielding a three-year risk-adjusted total PV of $1,417,506.

Faster Release Of New Application Features And Functionality For Customer-Facing Applications: Calculation Table					
REF.	**METRIC**	**CALC.**	**YEAR 1**	**YEAR 2**	**YEAR 3**
E1	Improvement in time-to-release new customer-facing features for apps in weeks		10	10	10
E2	Weekly value of new feature to business		$30,000	$30,000	$30,000
E3	Number of new features released annually		10	10	10
E4	Operating margin		20%	20%	20%
Et	Faster release of new application features and functionality for customer-facing applications	E1*E2*E3*E4	$600,000	$600,000	$600,000
	Risk adjustment	↓5%			
Etr	Faster release of new application features and functionality for customer-facing applications (risk-adjusted)		$570,000	$570,000	$570,000

Unquantified Benefits

Customers interviewed for this research expressed a wide range of benefits that could be quantified but were not within this study. They include:

- **Increased developer and end customer satisfaction**. Developers using Auth0 reported enjoying using it and felt that it was created by and for developers. Said one customer, "Auth0's integration into the developer tools that we use is very seamless." Other customers commented that Auth0 is user-friendly enough that nontechnical resources can assist in enabling authentication for external customers. End user customers who log in into applications using Auth0 are satisfied with seamless SSO that also works with mobile devices. Overall, there is no disruption to end users (internal or external) when getting access to new applications.
- **High satisfaction with the Auth0 service and expertise.** Customers reported a high level of trust in the development expertise that went into the making of Auth0. They felt that the responsiveness of the Auth0 team to customers' authentication needs and requirements was fast and thorough. And, when new regulations or other technology enhancements come out, Auth0's engineers are ahead of the game for the developers and have figured it out for the company. This benefit was not quantified, but it can result in additional developer time savings. Said one enterprise architect: "One of the things that may sound small but is huge to us — we use Slack internally for communication — we talk to Auth0 using it. That has been a wonderful experience interacting with the engineering team — we open a ticket and then immediately go to Slack and can just ask general questions."
- **Cost of handling security and audit issues**. One customer interviewed reported a database leak caused by its ineffective authentication system. It almost resulted in the loss of an investor in this early-stage company. The company chose Auth0 to lower its risk of future breaches. Other customers reported reduced time spent on audit-related requests. They had to respond to auditor requests on the applications they were monitoring. With Auth0, they could spend less time tracking down application usage by login.
- **Faster innovation around application development that requires authentication.** Customers reported that they could innovate more quickly while rolling out applications using multifactor authentication, passwordless login, and social connections. Auth0's turnkey solutions, which enable companies to do AB testing and roll out new application features and functionality more quickly, invigorate the innovation process.

"I think the biggest financial case I could make for Auth0 is the preposterously huge amount of money it would take for us to build and support something comparable. Because Auth0 is a SaaS vendor, we spend a tiny fraction of what it would cost for us to do it ourselves. And we know we need it."

Director of API management, printing

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 the Auth0 Identity Platform and later realize additional uses and business opportunities, including:

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.

- **Better identify behaviors and purchasing trends of customers to increase conversions, personalize engagement, and build brand loyalty.** Digital identity is an integral part of an organization's interaction with consumers. Auth0 can provide a unified view of the customer, consolidating data sources to deliver a consistent brand experience at each customer touchpoint. This can lead to higher personalization and conversion rates.
- **Build an omnichannel experience for customers.** Auth0 can become a "single source of truth" for digital identities and integrates with marketing and advertising networks. This allows consumer brand companies to better target campaigns and in-app advertising. As Auth0 customers centralize their identity platform, they have the potential to use the intelligence gained from understanding consumer behavior to inform future promotions. This can lead to increased revenue.
- **Quickly adapt to future login trends.** Identity management continues to evolve, and Auth0 continually updates and releases new code to the software development kits. That means that, in the future, customers already using Auth0 will have faster access to identity innovations and can incorporate them more quickly than those not using Auth0.

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

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Ftr	Licensing and professional services costs	$0	$600,000	$600,000	$600,000	$1,800,000	$1,492,111
Gtr	Implementation and ongoing management	$11,400	$120,000	$120,000	$120,000	$371,400	$309,822
	Total costs (risk-adjusted)	$11,400	$720,000	$720,000	$720,000	$2,171,400	$1,801,933

Licensing And Professional Services Costs

Organizations pay a monthly recurring licensing and professional services fee to Auth0. The composite organization pays $600,000 annually for the use of Auth0, which includes ongoing access to Auth0's software development kits (SDKs) and the expertise and skill sets of the authentication experts that Auth0 provides.

The table above shows the total of all costs across the areas listed below, as well as present values (PVs) discounted at 10%. Over three years, the composite organization expects risk-adjusted total costs to be a PV of more than $1.8 million.

Licensing And Professional Services Costs: Calculation Table

REF.	METRIC	CALC.	YEAR 1	YEAR 2	YEAR 3
F1	Monthly license costs		$50,000	$50,000	$50,000
F2	Months in year		12	12	12
Ft	Licensing and professional services costs	D2*D3	$600,000	$600,000	$600,000
	Risk adjustment	0%			
Ftr	Licensing and professional services costs (risk-adjusted)		$600,000	$600,000	$600,000

Implementation And Ongoing Management

Customers reported a short, up-front implementation period that lasted from a few days to a few months, depending on the complexity of the organization. For this model, the average initial implementation time used was one month of dedicated developer time at an average hourly rate of $57.00. The ongoing management of Auth0 by a dedicated administrator is estimated at $120,000 annual salary, fully loaded, and represents the dedicated administration time of that professional.

The three-year total PV for implementation and ongoing management was $309,822.

Implementation can vary from days to a few weeks, depending on the complexity of the organization

Implementation And Ongoing Management: Calculation Table

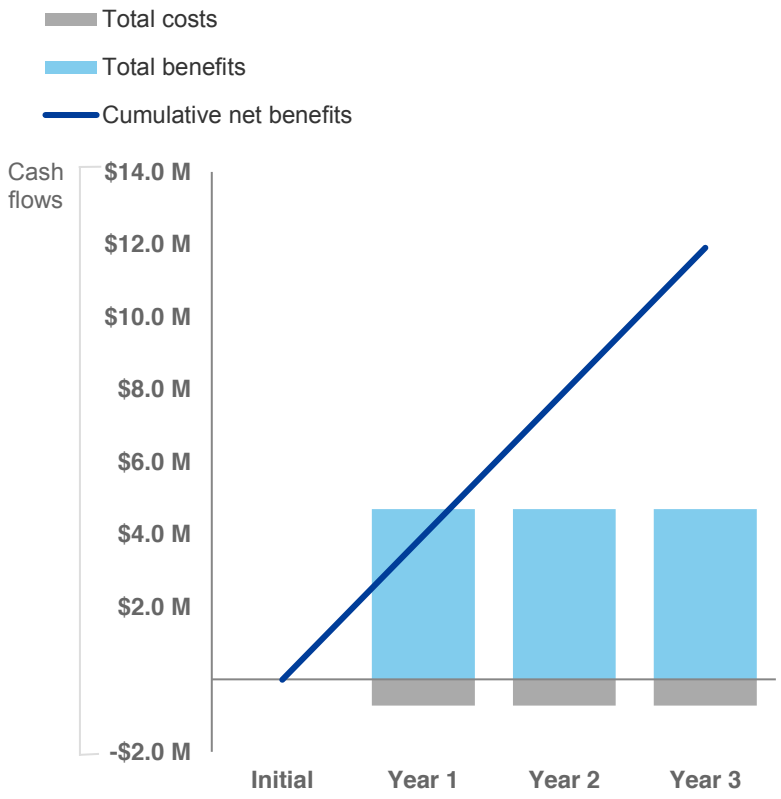
REF.	METRIC	CALC.	INITIAL	YEAR 1	YEAR 2	YEAR 3
G1	One month of dedicated developer time for implementation	In hours	200			
G2	Average hourly salary of developer		$57			
G3	Ongoing management by a dedicated administrator			1	1	1
G4	Average annual salary of developer			$120,000	$120,000	$120,000
Gt	Implementation and ongoing management	G1*G2+G3*G4	$11,400	$120,000	$120,000	$120,000
	Risk adjustment	0%				
Gtr	Implementation and ongoing management (risk-adjusted)		$11,400	$120,000	$120,000	$120,000

The financial results calculated in the Benefits and Costs sections can be used to determine the ROI and NPV for the composite organization's investment. Forrester assumes a yearly discount rate of 10% for this analysis.

Financial Summary

CONSOLIDATED THREE-YEAR RISK-ADJUSTED METRICS

Cash Flow Chart (Risk-Adjusted)



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

Cash Flow Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($11,400)	($720,000)	($720,000)	($720,000)	($2,171,400)	($1,801,933)
Total benefits	$0	$4,692,758	$4,692,758	$4,692,758	$14,078,275	$11,670,195
Net benefits	($11,400)	$3,972,758	$3,972,758	$3,972,758	$11,906,875	$9,868,262
ROI						548%
Payback period						< 6 months

FORRESTER®

Auth0 Identity Platform: Overview

The following information is provided by Auth0. Forrester has not validated any claims and does not endorse Auth0 or its offerings.

About Auth0

Auth0, a leader in identity-as-a-service (IDaaS), provides customers in every sector with the only identity solution they need for their web, mobile, IoT, and internal applications. Its extensible and secure platform seamlessly authenticates and secures more than 50 million logins per day, making it loved by developers and trusted by global enterprises.

With US headquarters in Bellevue, WA, and additional offices in Buenos Aires, London, and Sydney, Auth0 provides 24x7 support to its global customers who are located in 70+ countries, supporting billions of logins every year.

About the Auth0 Identity Platform

Adding IAM services to any platform has historically been a painful process, with long implementations and complex integrations. Auth0 takes all complexity out of the equation for custom and third-party applications with its developer-centric Identity Platform that is extensible, secure, and quick to integrate. With full-blown SDKs for 30+ languages, live documentation, and seamless GitHub integration, Auth0 empowers customers to achieve their authentication goals with minimal effort and enables them to dedicate their valuable internal resources to growth and product innovation.

Authentication is not easy. Whether it's a basic use case or a complex one that requires multifactor authentication (MFA), single sign-on (SSO), social logins, Enterprise Federation, API security, and more, Auth0 provides a feature-rich platform that caters to the demanding needs of today's B2B, B2C, B2E, and IoT use cases. In fact, most businesses today demand a hybrid use case, and Auth0 is perfectly suited for this scenario. Auth0's default configuration can be easily extended and customized for any business scenario using extensibility points that enable fine-tuned authentication and access control. Auth0 even extends its flexibility to deployment models with both on-premises and cloud options. Finally, Auth0 supports more than 30 social providers and 10 enterprise connections such as Azure Active Directory, ADFS, WS-Federation, and Google Apps that can be enabled instantly for ultimate flexibility.

From the start, Auth0 has been built on recognized identity standards including OpenID Connect, JWTs, OAuth, LDAP, SAML, and WS Federation, enabling easy user and device management. Auth0 has also built state-of-the-art security into its platform and supports stringent compliance standards including SOC2, HIPAA, and GDPR.

Auth0 Customers

Auth0's customers are located around the globe and represent a diverse array of industries and sectors. Thousands of brands rely on Auth0 for all their identity management needs and trust Auth0 to keep their internal and external customer data completely secure. A small sampling of Auth0's extensive customer base includes: Atlassian, Schneider Electric, Dow Jones, Mazda, Siemens, Financial Times, and AMD. For in-depth customer success stories, please visit: https://auth0.com/resources/case-studies.

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.