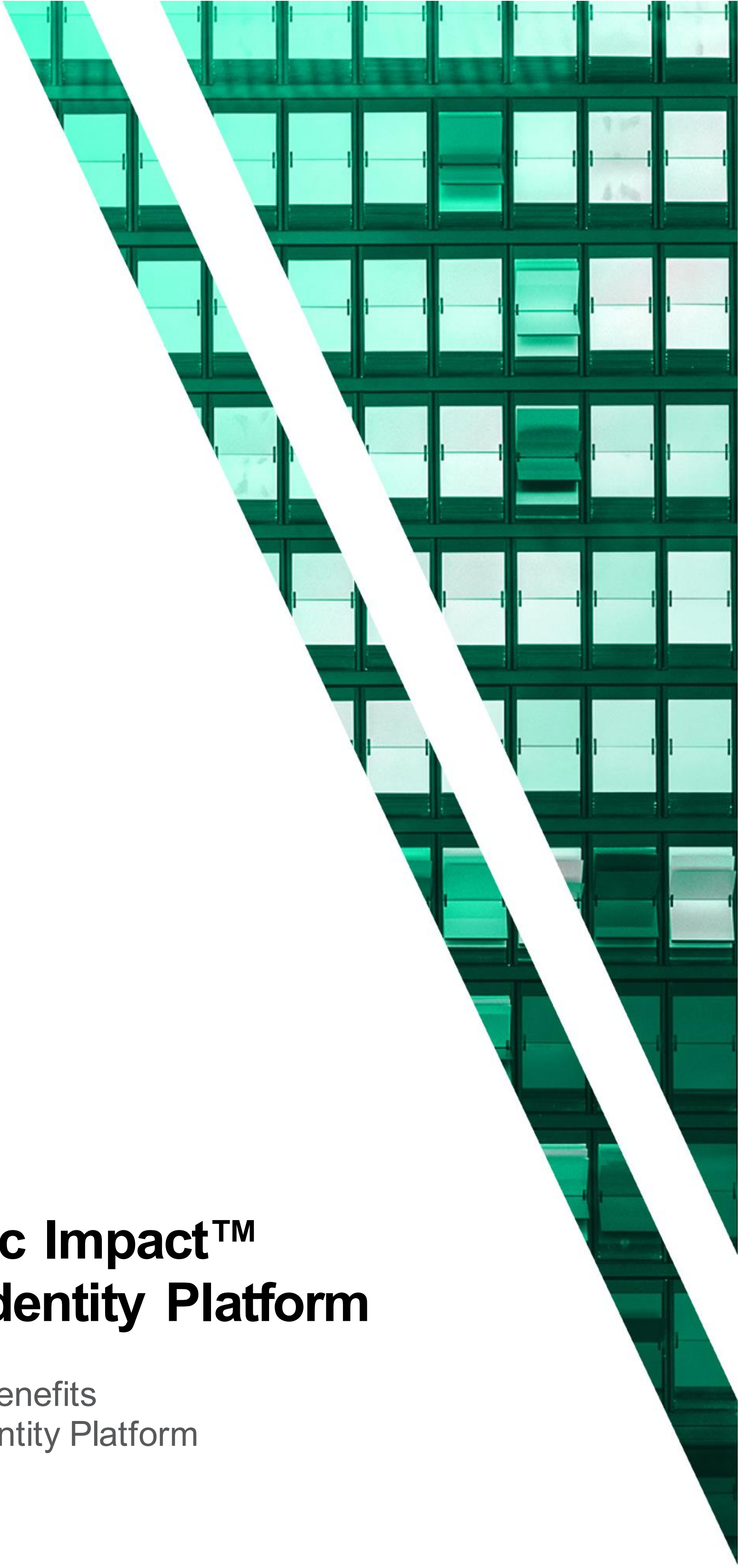
FORRESTER®



The Total Economic Impact™ Of Google Cloud Identity Platform

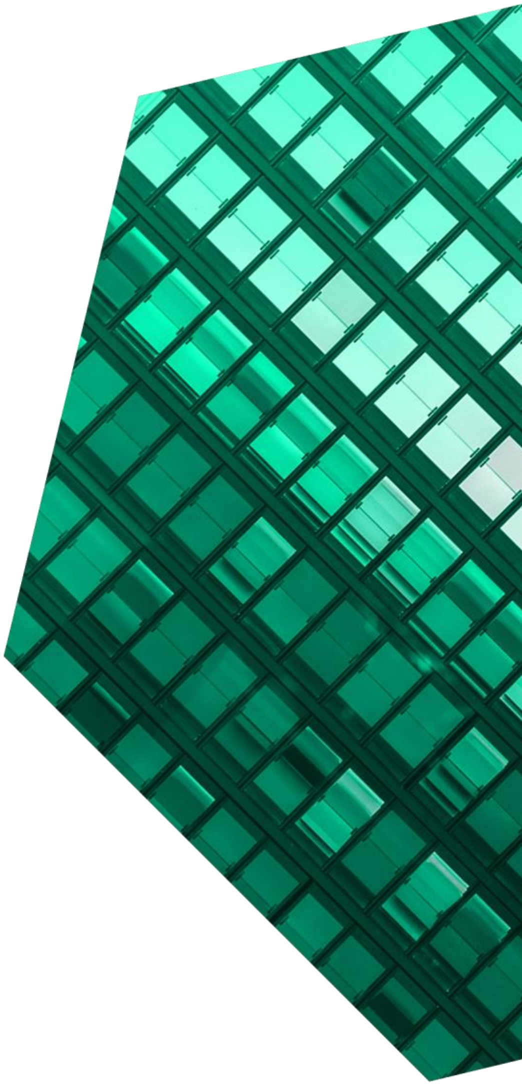
Cost Savings And Business Benefits
Enabled By Google Cloud Identity Platform

SEPTEMBER 2022

A FORRESTER TOTAL ECONOMIC IMPACT™ STUDY COMMISSIONED BY GOOGLE

Table Of Contents

Consulting Team: Adi Sarosa
Isabel Carey



ABOUT FORRESTER CONSULTING

Forrester provides independent and objective research-based consulting to help leaders deliver key transformation outcomes. Fueled by our customer-obsessed research, Forrester's seasoned consultants partner with leaders to execute on their priorities using a unique engagement model that tailors to diverse needs and ensures lasting impact. For more information, visit forrester.com/consulting.

Executive Summary

In an increasingly digital world, organizations face very complex and changing customer identity and access management (CIAM) requirements. They have to connect and implement enrollment, authentication, authorization, and self-services use cases to the varied landscape of existing connected business applications and legacy CIAM solutions. Having the right tool is critical to protect customers from account takeover, identity theft, and privacy abuses.

Google Cloud Identity Platform helps organizations add identity and access management functionality to their applications. The platform is a managed service by Google that introduces security and scalability to the application.

KEY STATISTICS

Return on investment (ROI)
83%

Net present value (NPV)
$492K

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

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed seven respondents at four organizations with experience using Google Cloud Identity Platform. Forrester also conducted an online survey of 351 cybersecurity leaders who were responsible for cybersecurity decision-making, operations, and reporting at global enterprises in Australia, Canada, Germany, the UK, and the US. For the purposes of this study, Forrester aggregated the experiences of the interviewees and survey respondents and combined the results into a single composite organization with $5 million in annual revenue, 200 employees, 30 engineers, and 800,000 users to be authenticated per month.

Between 2018 and 2020, the number of stolen identity cases increased by

300%

Prior to using Google Cloud Identity Platform, some interviewees noted their organizations would use a user authentication platform from another vendor, while others did not use any. Interviewees who used a different vendor cited functionality and the lack of scalability as the main reasons for switching. Meanwhile, interviewees at organizations where Google Cloud Identity Platform was their first authentication platform started to realize the need for an authentication tool as their organization grew, and more users were accessing their applications. More users meant more data was being collected, which increased their vulnerability to cyberattacks.

After the investment in Google Cloud Identity Platform, interviewees noted their ability to grow their businesses without worrying about the scalability of their authentication platform, or their data security. Key results from the investment include cost avoidance from not having to build and maintain their authentication tool, business growth from being able to target larger customers, and risk reduction from enhanced security in their application environment.

Passwordless authentication adoption trend

Percentage of employees that use today	Percentage of employees expected to use in one year
41%	**70%**

KEY FINDINGS

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

- **Cost avoidance from using a managed service.** By adopting and implementing Google Cloud Identity Platform, the composite organization avoid having to dedicate engineering resources to build and manage the platform. It is more economical for their engineers to work on the core value of their business and have others handle technical work, such as authenticating users. A managed service helps the composite organization avoid more than $760,000 in costs.
- **Incremental profit growth due to reliability and scalability of the platform.** For the composite organization, having a reliable and easily scalable authentication platform as part of their application offers their customers confidence in working with them and using their applications. This is particularly important when working with enterprise-level and larger customers. The scalability and reliability of the tool contributed to $124,000 in additional revenue per year to the composite organization.
- **Risk reduction of potential cyberattacks and data breaches.** Having Google Cloud Identity Platform as part of their security technology stack better protects the composite organization from potential cyberattacks and data breach events. This reduces the chances of the composite organization potentially getting fined or losing brand equity and customer trust. With this, the composite organization realized $192,000 in cost savings.

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

- **Ease of setup and implementation.** Setting up and implementing Google Cloud Identity Platform was relatively easy for the composite organization with the help of various resources and materials Google provided.
- **Developer satisfaction.** The engineers and developers of the composite organization appreciates not having to be pulled into other engineering work, especially those outside the core competency. This helps them truly focus on creating value for their organization and not be distracted by feature updates and basic infrastructure.

- **Customer satisfaction.** The customers of the composite organization exhibit greater trust and satisfaction when they know Google Cloud Identity Platform is used as the authentication service. The combination of the Google brand, their trust of the different features, and the overall security of the platform eases potential concerns from clients, which allows the organization to fully focus on presenting their core offerings.

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

- **Annual licensing cost.** The annual cost of the Google Cloud Identity Platform is driven by the number of users that need to be authenticated monthly, and the complexity of the authentication process (i.e., SMS, email authentication, MFA). Over three years, the composite organization pays close to $431,000 for its Google Cloud Identity Platform licensing.
- **Internal costs for setup and user training.** The composite organization spends time and resources to set up Google Cloud Identity Platform. This mostly included configuration and integration work with other tools in their organization's IT environment. They also needed time to train users, specifically those who would be in charge of the ongoing support and maintenance of the tool. Over three years, the composite organization spends about $97,000 related to time for setup and user training.
- **Internal costs for ongoing support and management.** Upon implementation, the composite organization had members of the IT organization take time to manage, work, or develop the tool. They also have a support team involved to help with any questions. Over three years, the composite organization spends about $63,000 related to ongoing support.

The financial analysis which is based on the interviews and survey found that a composite organization experiences benefits of $1.08 million over three years versus costs of $591 thousand, adding up to a net present value (NPV) of $492 thousand and an ROI of 83%.

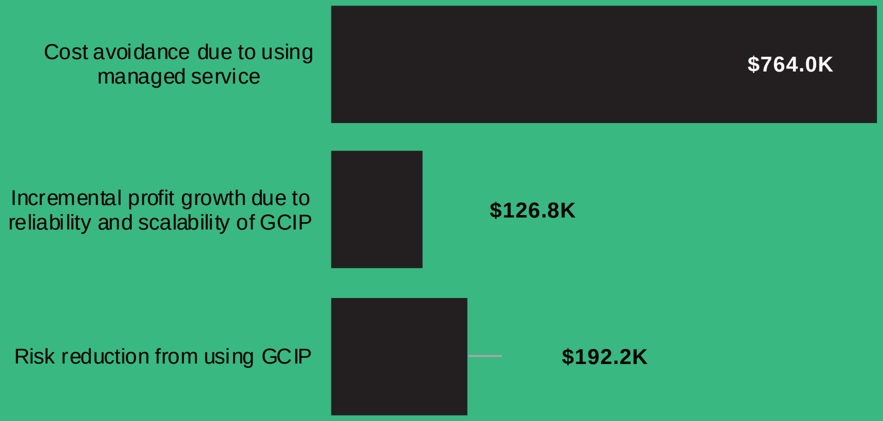
ROI
83%

BENEFITS PV
$1.08M

NPV
$492K

TOTAL COSTS
$591K

Benefits (Three-Year)



> **“Our clients are Fortune 100 companies. They would not use our tool if our authentication can be a point of weakness for them. The fact that they recognize the Google brand and I can integrate [it] with other tools in a matter of minutes dramatically reduces any possible concerns they have for us.”**
>
> — CTO, automation software

TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews and survey, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in Google Cloud 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 Google Cloud Identity Platform can have on an organization.

DUE DILIGENCE

Interviewed Google stakeholders and Forrester analysts to gather data relative to Google Cloud Identity Platform.

INTERVIEWS

Interviewed seven representatives at four organizations using Google Cloud Identity Platform to obtain data with respect to costs, benefits, and risks.

COMPOSITE ORGANIZATION

Designed a composite organization based on characteristics of the interviewees and survey respondents.

FINANCIAL MODEL FRAMEWORK

Constructed a financial model representative of the interviews and survey using the TEI methodology and risk-adjusted the financial model based on issues and concerns of the interviewees and survey respondents.

CASE STUDY

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

DISCLOSURES

Readers should be aware of the following:

This study is commissioned by Google and delivered by Forrester Consulting. It is not meant to be used as a competitive analysis.

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the study to determine the appropriateness of an investment in Google Cloud Identity Platform.

Google 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.

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

Forrester fielded the double-blind survey using a third-party survey partner.

The Google Cloud Identity Platform Customer Journey

Drivers leading to the Google Cloud Identity Platform investment

Interviews

Role	Industry	Revenue	Number of users authenticated
Software Engineer	Digital Healthcare	$1 to 5 million	1.5 million
Security Engineer	Digital Healthcare	$1 to 5 million	1.5 million
COO	Digital Healthcare	$1 million	2.5 million
CTO	Digital Healthcare	$1 million	2.5 million
Product Manager	Automation Software	$163 million	110,000
Software Engineer	Automation Software	$163 million	110,000
CTO	Automation Software	$1 to 5 million	13,000

KEY CHALLENGES

Prior to their investment in Google Cloud Identity Platform, most interviewees were not using an authentication solution, while one was using a competitor solution. Regardless, the interviewees experienced common challenges which included: a growing user base, increased security risks associated with sensitive customer data, and challenges with resource allocation and prioritization. The interviewees emphasized that their organizations were growing — they recognized the need for an authentication solution but lacked the expertise or resources to construct their own.

Both interviewees and survey respondents noted their organizations struggled with common challenges, including:

- **Increased need with growth in user base.** Interviewees recognized that a quickly growing user base required an authentication tool to manage platform access. Homegrown solutions were possible with a small user base but became difficult to manage as the organization grew. A software engineer at a digital healthcare company affirmed that, “As our userbase grew, we needed to establish an authentication mechanism.”

> **“We were operating in a fast-changing world. Thus, we didn’t want to spend engineering resources recreating something that is outside our core competency.”**
>
> *Product manager, automation software*

- **Increased risk without an authentication platform.** Having an authentication tool ensures only permitted users have access to secure networks and protected resources, preventing costly data breaches or leaks. According to the

COO of a digital healthcare firm, their organization needed to increase security as they "started collecting more personal health data and sensitive information."

- **Increased need for resource allocation and prioritization.** Interviewees recognized the need for an authentication tool but lacked the resources to build a homegrown solution. Although necessary, it was often not within the core capabilities of the organizations. Building one would take engineers away from business tasks of higher value. In many cases, organizations did not even possess the resources or engineers to set up their own authentication platform."

SOLUTION REQUIREMENTS

The interviewees and survey respondents searched for a solution that could:

- **Scale in relation to performance and cost.** Interviewees were looking for an authentication tool that could scale along with their business growth. With the increase in the number of users to be authenticated, interviewees did not want their authentication tool to hinder performance or affect costs. The COO at a digital healthcare company said, "As the size of our clients that use our service grew, we needed to find a solution that can assist with big scale implementation in a fast and secure manner."

- **Offer security.** Interviewees found that security was a major consideration in both deciding to invest in an authentication tool, and when comparing between which to implement. The CTO at an automation software firm highlighted the importance of having data security from both internal and external threats as it was a customer priority.

- **Provide managed service.** Interviewees had never considered building their own authentication tool as it was not their main competency, and would rather deploy precious, limited resources elsewhere. The COO at a digital healthcare company shared, "We want our engineers to focus on what we're best at. We will use best-of-breed solutions around us on things that we are not good at."

- **Offer vendor familiarity.** The Google brand was another differentiator for some interviewees when comparing between authentication tools to implement. Some organizations were already using other Google products, and thus it made sense to implement Google Cloud Identity Platform for seamless integration and compatibility. The software engineer at a digital healthcare firm said: "Our company was already a big user of Google products."

Forrester's Perspective: Why You Need A Roadmap For Cloud Identity Governance (CIG)

Creating a strategy roadmap to deploy cloud identity governance solutions is critical for successful cloud migration, cloud refactoring, and cloud operations projects. This is critical firstly because too many people have access to cloud consoles, cloud infrastructure is changing continuously, and all workloads are on the internet by default. CIG solutions form a formidable and systemic line of defense against these attacks.

COMPOSITE ORGANIZATION

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

Description of composite. The composite is an organization with 200 employees and $5 million in annual revenue. Their IT organization consists of 30 engineers. They also have about 800,000 users on average that need to be authenticated every month.

Deployment characteristics. To set up Google Cloud Identity Platform, the composite organization is deploying three engineers from their IT organization. Two of them will go through user training and will be involved in the ongoing management of the tool.

Key Assumptions

- **$5 million annual revenue**
- **200 employees**
- **30 engineers**
- **800,000 users to be authenticated per month**

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 avoidance from using a managed service	$307,218	$307,218	$307,218	$921,653	$764,005
Btr	Incremental profit growth due to reliability and scalability of the platform	$51,000	$51,000	$51,000	$153,000	$126,829
Ctr	Risk reduction of potential cyberattacks and data breaches	$77,286	$77,286	$77,286	$231,858	$192,199
	Total benefits (risk-adjusted)	$435,504	$435,504	$435,504	$1,306,512	$1,083,033

COST AVOIDANCE FROM USING A MANAGED SERVICE

Evidence and data. The interviewees experienced significant savings from using a managed service solution instead of creating and maintaining their own authentication tool. Creating their own tool would be costly and requires a steep time and personnel investment. Many engineering teams also lacked the depth and experience, particularly in stack developers, that are necessary to build a tool that met the same security requirements offered within the Google Cloud Identity Platform.

Ongoing maintenance of their own tool would also require additional resources. The interviewees recognized the necessity of an authentication platform but also recognized that it took focus and resources away from their core applications and business. Adopting Google Cloud Identity Platform allowed the composite organization to effectively allocate resources with a focus on delivering their core competencies.

- The CTO at a digital healthcare company stated, “We were operating in a fast-changing world. Thus, we didn’t want to spend engineering resources recreating something that is outside our core competency.”

> **“Providing high security in an authentication tool is difficult to implement properly on your own. It is very costly. Thus, Google Cloud Identity Platform provides you the ease of mind to focus on building your application, product, and business.”**
>
> *Software engineer, digital healthcare*

- A managed service solution also offered significant time savings. The CTO at an automation software firm said, “The more complex aspect of managing your own platform would be around adding users, deleting users, disabling users, having all those API endpoints to manage. There is definitely huge time savings here by using Google Cloud Identity Platform"

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

- Building an authentication platform takes 3,000 hours.
- The average fully burdened hourly salary of the engineers is $56.[2]
- The average fully burdened annual salary of the engineers is $115,569.
- Tool maintenance requires 10% of the 30-person engineering team to be involved.
- The engineers involved will need to dedicate 50% of their time to platform maintenance.

Risks. Benefits from cost avoidance due to using a managed service may vary, and specific considerations include:

- The size of the engineering team and their specific skills and experience.
- The complexity of the authentication platform and its security requirements.
- The geography and industry the organization is competing in, which would impact the salary of its engineering team.

Results. To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $764,000.

Cost Avoidance From Using A Managed Service

Ref.	Metric	Source	Year 1	Year 2	Year 3
A1	Total hours needed to build the platform	Composite	3,000	3,000	3,000
A2	Fully burdened hourly salary	TEI standard	$56	$56	$56
A3	Total cost to build	A1*A2	$168,000	$168,000	$168,000
A4	Size of engineering team	Composite	30	30	30
A5	Assumed percentage of engineering team involved in user authentication maintenance	Interview	10%	10%	10%
A6	Percentage of time dedicated to maintenance	Interview	50%	50%	50%
A7	Annual fully burdened salary	TEI standard	$115,569	$115,569	$115,569
A8	Total cost to maintain	A4*A5*A6*A7	$173,353	$173,353	$173,353
At	Cost avoidance from using a managed service	A3+A8	$341,353	$341,353	$341,353
	Risk adjustment	↓10%			
Atr	Cost avoidance from using a managed service (risk-adjusted)		$307,218	$307,218	$307,218
	Three-year total: $921,653		**Three-year present value: $764,005**		

INCREMENTAL PROFIT GROWTH DUE TO RELIABILITY AND SCALABILITY OF GOOGLE CLOUD IDENTITY PLATFORM

Evidence and data. Interviewees reported incremental profit growth due to their use of Google Cloud Identity Platform. The reliability and performance of Google Cloud Identity Platform improved customer satisfaction and trust. The high availability and security of the platform retained customers and gave them confidence that their data would be protected, which helped interviewees with sales and customer retention.

In addition, the scalability of Google Cloud Identity Platform was attractive to organizations. Interviewees were hesitant to build and maintain their own authentication tool, considering the time and effort required to grow the platform to meet higher demand.

- The security engineer at a digital healthcare company shared, "Authentication helps get users stay on the product. Without Google Cloud Identity Platform, we might have a much more difficult time to get people to use the product."
- The COO of a digital healthcare company said, "Without Google Cloud Identity Platform, we would not be able to target our enterprise clients, which would amount to over 50% of our business."
- The product manager at an automation software firm said: "The cost of authenticating users with our previous solution would have been 40% of our total cost. By switching to Google Cloud Identity Platform, we saved 95% of that cost."
- The CTO at an automation software first said: "I've never seen an outage with Google Cloud Identity Platform in the 7 to 8 years we've been working on this. Google Cloud Identity Platform has at least a 99.99% availability, while other tools in the market are probably more in the 99.9% or 99% availability. If we had a breach, we would have lost our top 10 customers, and that would be 95% of our business."

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

- The organization has a yearly revenue of $5 million.
- The composite organization realized 12% in additional revenue each year, attributed to the scalability and reliability of the tool, which allows them to target larger customers and larger deals.
- The net margin of the composite organization is 10%.

Risks. Incremental profit growth due to Google Cloud Identity Platform's reliability and scalability may vary, and specific considerations include:

- The significance of the applications that use Google Cloud Identity Platform to authenticate users to the overall business (i.e., percentage of revenue).
- The competitive landscape that the organization is participating in.
- The specific industry and geography the organization is located in.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $127,000.

Incremental Profit Growth Due To Reliability And Scalability Of Google Cloud Identity Platform

Ref.	Metric	Source	Year 1	Year 2	Year 3
B1	Annual revenue	Composite	$5,000,000	$5,000,000	$5,000,000
B2	Percentage of additional revenue attributed to reliability and scalability of tool	Interview	12%	12%	12%
B3	Net margin	Forrester Assumption	10%	10%	10%
Bt	Incremental profit growth due to reliability and scalability of Google Cloud Identity Platform	B1*B2*B3	$60,000	$60,000	$60,000
	Risk adjustment	↓15%			
Btr	Incremental profit growth due to reliability and scalability of Google Cloud Identity Platform (risk-adjusted)		$51,000	$51,000	$51,000
	Three-year total: $153,000		**Three-year present value: $126,829**		

Forrester's Perspective: IAM Must Be A Central Component Of Your Technology Portfolio

Great customer experiences lead to higher revenue growth for your company. To provide great experiences, you must invest in the technology, systems, and processes that help win, serve, and retain customers. IAM is one such technology. Although focused on security, IAM has evolved into a tool to help build and sustain long-term relationships with customers.

RISK REDUCTION FROM USING GOOGLE CLOUD IDENTITY PLATFORM

Evidence and data. Authentication tools deal with sensitive data and serve as entryways to interviewee products and platforms. Security and risk were top of mind for the interviewees. If the tool fails, users would be locked out of a business's platforms. As a product manager at a marketing automation firm noted, "user authentication is the beginning of the journey for the end user." If the authentication platform fails, end users would be unable to access the interviewee's products, which would greatly reduce their effectiveness.

Security of their customer's sensitive data was another major risk for organizations. A security breach to the authentication platform would be costly to fix and could cause irreparable damage to a brand's reputation and negatively impact consumer perception and sales.

- The security engineer at a digital healthcare company said: "As a healthcare company, we care about the security of our data. Worst case scenario, we can shut down our services if we have a lot of leaks"
- The CTO at a digital healthcare company told Forrester: "Logging in and accessing our platform is a critical function of the platform. If our SSO breaks or doesn't work, we have 2.5 million users that cannot access the platform"
- The software engineer at an automation software company said: "If we do get breached, the damage would be irreversible. Our image would be damaged for life, and that's something we take seriously."

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

- The composite organization experiences 1.8 material breaches annually.[3]
- The average cost per data breach event is $252,569.[4]
- The percentage reduction of risk by using Google Cloud Identity Platform is in line with the spend for authentication platform as a percentage of overall security spend, which is 20%.
- **Risks.** Risk reduction due to using Google Cloud Identity Platform may vary, and specific considerations include: The industry and market position of the organization, which affects their likelihood of being targeted for a cyberattack.
- Other hardware and software tools that make up the IT infrastructure security technology stack.

Results. To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year, risk-adjusted total PV of $192,000.

> **"User authentication is probably 80% of our security posture. All access control to data in the infrastructure is through authentication."**
>
> *CTO, automation software*

Risk Reduction From Using Google Cloud Identity Platform

Ref.	Metric	Source	Year 1	Year 2	Year 3
C1	Number of material breaches experienced annually	Forrester research	1.8	1.8	1.8
C2	Average cost per data breach event	Forrester research	$252,569	$252,569	$252,569
C3	Percentage attribution to Google Cloud Identity Platform as reflected by percentage of overall security spend	Interview	20%	20%	20%
Ct	Risk reduction from using Google Cloud Identity Platform	C1*C2*C3	$90,925	$90,925	$90,925
	Risk adjustment	↓15%			
Ctr	Risk reduction from using Google Cloud Identity Platform (risk-adjusted)		$77,286	$77,286	$77,286
	Three-year total: $231,858		Three-year present value: $192,199		

Forrester's Perspective: CIG Solutions Control Access Rights Between Users And Resources

CIG solutions provide an important, single-pane-of-glass vantage point to activities of identities in the cloud console. Key steps to integrating CIG solutions with their cloud platforms include: 1) integrating data sources, 2) discovering, importing, and tracking cloud identities and resources; 3) analyzing and exposing users' overlapping, shadow, and transitive access rights; 4) setting and tracking baseline based on activity and custom roles; 5) tracking activity and further identifying excessive permissions; 6) performing continuous, automatic, and manual Zero Trust attestation, and 7) producing textual and graphical reports.

UNQUANTIFIED BENEFITS

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

- **Ease of setup and implementation.** Interviewees emphasized how easy and quick it was to set up Google Cloud Identity Platform. Google provides ample resources to support implementation, and interviewees reported an excellent user experience requiring little user training.
  - **Google provides support and resources.** A software engineer at a digital healthcare company describes, "setting up Google Cloud Identity Platform is easy because Google provides SDKs, developer guides, individual blogs, and all the tools developers need if they need help."
  - **Easy user experience.** A product manager at an automation software company outlined: "Google Cloud Identity Platform has a really good user experience, and the console is really helpful. I don't think we've ever faced an issue or bug that was not documented."
- **Developer satisfaction.** With a managed service like Google Cloud Identity Platform, developers can focus on building specific features and functionality without having to do more tedious basic platform and infrastructure work. Developers could focus their time on higher value and higher interest work, increasing satisfaction. The CTO at a digital healthcare company emphasized this, saying, "By using manager service, our developers can focus on building the features instead of having to think about the infrastructure and basic functionality."
- **Customer satisfaction.** Interviewees shared that some features (e.g., SSO capabilities) offered by Google Cloud Identity Platform differentiated it from other authentication tools. The CTO at an automation software firm shared, "The number one most frustrating thing for customers is not being able to log in. Having an SSO capability means users don't need to have another username and password that they have to memorize and manage."

FLEXIBILITY

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

- **Baseline investment for future security infrastructure development.** With Google likely adding new features or new products that can be integrated into Google Cloud in general, interviewees see their investment in Google Cloud Identity Platform as an enabler to better position themselves in the future. A CTO at a digital healthcare company said: "This is a base on which Google will likely add features on top of in the future. There will likely be new types of authentication methods in the future, and Google will likely adapt those changes into the product. By investing today, we can reap the benefits in the future."
- **Agility for future integrations.** The ease of integrating other tools with Google Cloud Identity Platform enables future opportunities for organizations in terms of improving their technology stack or partnering with others. A CTO at an automation software company added: "I can authenticate any OAuth or SAML third-party partner in literally minutes now because we already have Google Cloud Identity Platform set up. I can integrate partners in a matter of minutes versus days or months, so that opens up a lot of opportunities."

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

Analysis Of Costs

Quantified cost data as applied to the composite

Total Costs

Ref.	Cost	Initial	Year 1	Year 2	Year 3	Total	Present Value
Dtr	Annual licensing cost	$0	$173,250	$173,250	$173,250	$519,750	$430,847
Etr	Internal costs related to setup	$97,328	$0	$0	$0	$97,328	$97,328
Ftr	Internal costs related to ongoing support	$0	$25,425	$25,425	$25,425	$76,275	$63,228
	Total costs (risk-adjusted)	$97,328	$198,675	$198,675	$198,675	$693,353	$591,403

ANNUAL LICENSING COST

Evidence and data. Google Cloud Identity Platform charges a monthly active user fee for most of its sign-in methods. Any user that has signed in within a given month is considered an active user. Inactive users are stored at no cost. Certain elements are charged per successful verification.

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

- 800,000 users are active and authenticated each month.
- Pricing may vary. Contact Google for additional details.

Risks. The exact licensing costs incurred by an organization will depend on:

- The number active users to be authenticated each month.
- The verification method used by different users.

Results. To account for these risks, Forrester adjusted this cost upward by 5%, yielding a three-year, risk-adjusted total PV of $431,000.

Google Cloud Identity Platform Annual Licensing Cost

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
D1	Cost per month	Google		$165,000	$165,000	$165,000
Dt	Google Cloud Identity Platform annual licensing cost	D1*12	$0	$165,000	$165,000	$165,000
	Risk adjustment	↑5%				
Dtr	Google Cloud Identity Platform annual licensing cost (risk-adjusted)		$0	$173,250	$173,250	$173,250
	Three-year total: $519,750			**Three-year present value: $430,847**		

INTERNAL COSTS RELATED TO SETUP

Evidence and data. Interviewees shared that setting up Google Cloud Identity Platform at their organization required some involvement from their IT team. Additionally, a few users had to go through user training to ensure they could answer any questions from internal stakeholders.

- Some interviewees shared that setting up Google Cloud Identity Platform was a quick and easy process. A software engineer at a digital healthcare company said it only took them an hour, done by one employee.
- Others noted the process took slightly longer, but still simple enough to be completed by one person. The CTO at a digital healthcare company said: "Setup took us 20 hours of developer time, which was mostly configuration. This was done by one person."
- Some interviewees elaborated the full end-to-end need to set up Google Cloud Identity Platform. A software engineer at an automation software firm said: "Setting up the basics took us 3 months. This was to completely migrate the user data, the applications that access the data, [and] changing the applications to talk with the other services."
- The CTO at an automation software company added: "Setting up Google Cloud Identity Platform took us 15 minutes, but integrating them with enterprise clients, [and] with our other services was a 3-week project to get us up and running."
- In terms of training, a software engineer at an automation software company told Forrester:" "We rely on Google's resources because they are plentiful. We had five engineers spend one week in the sandbox [for user training]."

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

- They need 500 engineering hours for a full setup across all applications, including design, implementation, testing, and QA.
- Three engineers are involved in this process.
- The fully burdened hourly salary of the involved engineers is $56.[5]
- Two engineers go through user training, spending 40 hours (i.e., 1 week).

Risks. The exact costs incurred by an organization related to setup will depend on:

- The complexity of the IT environment and the integration work that needs to be completed.
- The skills and capabilities of the IT organization, which would impact the number of people who will be involved in setup, training, and the training duration.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $97,000.

Internal Costs Related To Setup

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
E1	Time to setup (hours)	Composite	500	0	0	0
E2	Number of people involved	Interview	3	0	0	0
E3	Fully burdened annual salary (hourly)	TEI standard	$56	0	0	0
E4	Number of users trained	Interview	2	0	0	0
E5	Duration of user training	1 week	40	0	0	0
Et	Internal costs related to setup	E1*E2*E3+E3*E4*E5	$88,480	$0	$0	$0
	Risk adjustment	↑10%				
Etr	Internal cost related to setup (risk-adjusted)		$97,328	$0	$0	$0
	Three-year total: $97,328			Three-year present value: $97,328		

INTERNAL COST RELATED TO ONGOING SUPPORT

Evidence and data. Interviewees noted that in terms of ongoing support and management, Google Cloud Identity Platform is relatively a light lift that does not require constant monitoring.

- A software engineer at a digital healthcare company said: “It is mostly a set and forget tool. We have one person check the platform from time to time, spending 15 to 30 minutes.”
- A product manager at an automation software company shared: “We have six people that interact with Google Cloud Identity Platform on an ongoing basis to manage, work, and develop it. They spend 4 hours per week to check that everything is OK.”
- A CTO at an automation software firm said: “In terms of ongoing management, we spend maybe one hour per month.”

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

- Two engineers are involved in ongoing support and maintenance.
- They spend 10% of their time.
- The average fully burdened annual salary is $115,569.

Risks. The exact costs incurred by an organization related to ongoing support will depend on:

- The complexity of the IT environment and the integration work that needs to be completed on an ongoing basis.
- The skills and capabilities of the IT organization, which will impact the number of people involved, and the average time spent.

Results. To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $63,000.

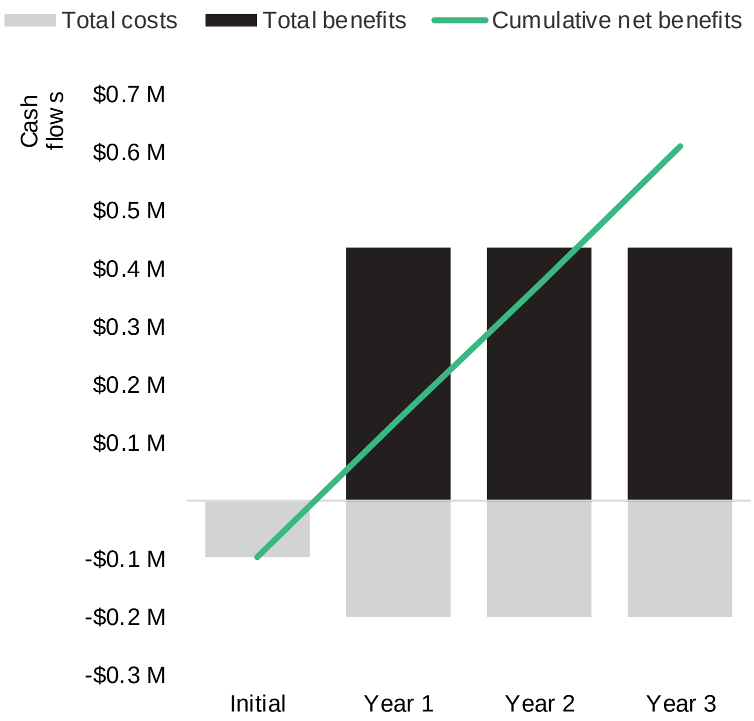
Internal Costs Related To Ongoing Support

Ref.	Metric	Source	Initial	Year 1	Year 2	Year 3
F1	Number of people needed for maintenance	Composite		2	2	2
F2	Percentage of time dedicated	Interview		10%	10%	10%
F3	Average annual fully burdened salary	TEI standard		$115,569	$115,569	$115,569
Ft	Internal cost related to ongoing support	F1*F2*F3	$0	$23,114	$23,114	$23,114
	Risk adjustment	↑10%				
Ftr	Internal cost related to ongoing support (risk-adjusted)		$0	$25,425	$25,425	$25,425
	Three-year total: $76,275			Three-year present value: $63,228		

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	($97,328)	($198,675)	($198,675)	($198,675)	($693,353)	($591,403)
Total benefits	$0	$435,504	$435,504	$435,504	$1,306,512	$1,083,033
Net benefits	($97,328)	$236,829	$236,829	$236,829	$613,158	$491,630
ROI						83%
Payback period (months)						<6

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%.

Appendix B: Supplemental Information

Related Forrester Research

“Why CX: Proof That Investing In Experience Improves Revenue, Cost, And Resilience,” Forrester Research, Inc., June 7, 2022.

“Identity Orchestration: Decision Tool,” Forrester Research, Inc., March 28, 2022.

“The Current State Of Enterprise Passwordless Adoption,” Forrester Research, Inc., January 19, 2022.

"The Roadmap To Deploy And Use Cloud Identity Governance,” Forrester Research, Inc., December 9, 2021.

“How Cloud Identity Governance Can Help Mitigate Access And Entitlement Risks.”, Forrester Research, Inc., September 29, 2020.

Appendix C: Endnotes

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

[2] Fully burdened salary includes both the direct wages and indirect costs of employment beyond direct compensation, including, but not limited to: hiring costs, training costs, financial services, paid time off, sick leave, expenses, retirement contributions, payroll taxes, and incremental technology and workplace costs for the employee.

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

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

[5] Fully burdened salary includes both the direct wages and indirect costs of employment beyond direct compensation, including, but not limited to: hiring costs, training costs, financial services, paid time off, sick leave, expenses, retirement contributions, payroll taxes, and incremental technology and workplace costs for the employee

FORRESTER®