A Forrester Total Economic Impact™
Study Commissioned By CA
February 2018

The Total Economic Impact™ Of The CA Privileged Access Manager Solution

Cost Savings And Business Benefits Enabled By CA Privileged Access Manager

FORRESTER®

Table Of Contents

Project Director:
Bob Cormier
Vice President and Principal Consultant
Forrester Consulting

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®

Quantified Benefits

Compliance savings:
$613,009

Breach avoidance cost savings:
$1,268,295

Labor savings from ease of deployment and administration:
$71,574

(above are risk- and PV-adjusted)

Executive Summary

CA Privileged Access Manager protects an organization's business and empowers its people. The solution protects critical accounts and endpoints while providing a seamless user experience. CA commissioned Forrester Consulting to conduct a Total Economic Impact™ (TEI) study and objectively examine the potential return on investment (ROI) enterprises may realize by deploying its Privileged Access Manager solution. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of the CA Privileged Access Manager solution on their organizations.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed three CA Privileged Access Manager customers with between 75 and 1,150 privileged users, and an average of 15 months experience using the CA Privileged Access Manager solution. For this TEI study, Forrester has created a composite *Organization* to illustrate the quantifiable benefits and costs of investing in CA Privileged Access Manager.

Based on characteristics of the interviewed customers, the *Organization* is a global, midsize enterprise in the business of manufacturing, distribution, and services. It is headquartered in North America and Europe with multisite operations globally. It has been using CA Privileged Access Manager for three years to protect its critical accounts and endpoints. For more information, see the section titled Composite *Organization*.

Key Findings

Quantified benefits. The composite *Organization* experienced the following risk-adjusted present value (PV) quantified benefits totaling **$1,952,878** (see the Financial Analysis section for more details):

- **Compliance savings from CA Privileged Access Manager user session monitoring ($613,009).** Interviewed customers cited both internal labor savings and external audit savings. The average labor savings was one full-time equivalent (FTE) annually, and the average external audit savings was $150,000 annually due to recording of sessions and streamlined and automated remediation.
- **Breach avoidance cost savings ($1,268,295**). With breach avoidance, there's less time and effort involved in managing and mitigating breaches, thereby reducing the cost of activating the *Organization's* entire incident response team, saving $600,000 annually.
- **Labor savings from ease of deployment and ongoing administration ($71,574).** The *Organization* saved 400 hours in deployment and integration costs, compared to other privileged access management solutions. In addition, the *Organization* saved 520 hours per year in ongoing administration compared with alternative solutions.

Unquantified benefit. The composite *Organization* experienced the following benefit, which is not quantified in this study:

- **Session recordings — innocent log-on behavior.** In addition to tracking employees' keystrokes, the session recordings track incorrect (and mostly innocent) log-on behavior by users. The recordings make it much easier to identify the problem and creates a teaching exercise for the user in how to correctly log into the systems. Session recordings make IT administrators' jobs easier.

ROI: 107%

Benefits PV: $1.95 million

NPV: $1.0 million

Payback: Less than six months

Costs. The *Organization* experienced the following present value costs:

- **CA Privileged Access Manager fees ($943,894).** CA Privileged Access Manager fees include annual licenses, software maintenance, user session monitoring, training, and professional services.

Forrester's interviews and subsequent financial analysis found that the Organization experienced benefits of $1,952,878 over three years versus costs of $943,894, adding up to a net present value (NPV) of $1,008,984, with a **payback period of less than six months and an ROI of 107%.**

If risk-adjusted costs, benefits, and ROI still demonstrate a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. The risk-adjusted numbers should be taken as "realistic" expectations, as they represent the expected value considering risk. Assuming normal success at mitigating risk, the risk-adjusted numbers should more closely reflect the expected outcome of the investment.

Forrester Note: When we think corporate risk, we mostly think about cybersecurity and the growing risk from external threats — individual hackers, professional hacking organizations, and even nation-states. These high-profile risks have caught our attention and imagination.

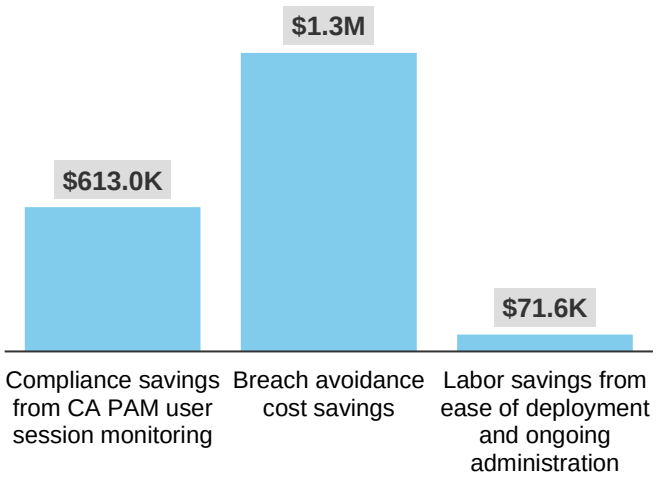
However, we also need to pay more attention to insider threats.

The release of confidential intellectual property (IP) or data can damage a firm's prestige and reputation or destroy customer relationships and financial results.

Companies are giving more tools, access, and trust to employees, consultants, freelancers, and partners at a time when data and IP have become the fundamental currency of business.

Organizations must address and control insider threats. Accidental and malicious misuse of company data threatens business performance and customer trust.

Benefits (Three-Year)



FORRESTER®

TEI Framework And Methodology

From the information provided in the interviews, Forrester has constructed a Total Economic Impact™ (TEI) framework for those organizations considering investing in the CA Privileged Access Manager solution.

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 CA Privileged Access Manager solution 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 CA stakeholders to gather data relative to the Privileged Access Manager solution.

CUSTOMER INTERVIEWS
Interviewed three organizations using CA's Privileged Access Manager solution 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 composite *Organization*.

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

DISCLOSURES

Readers should be aware of the following:

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

Forrester makes no assumptions as to the potential ROI that other organizations will receive. Forrester strongly advises that readers use their own estimates within the framework provided in the report to determine the appropriateness of an investment in the CA Privileged Access Manager solution.

CA 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.

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

The CA Privileged Access Manager Customer Journey

BEFORE AND AFTER THE PRIVILEGED ACCESS MANAGER (CA PRIVILEGED ACCESS MANAGER) SOLUTION INVESTMENT

For this study, Forrester conducted interviews with three CA Privileged Access Manager customers. Interviewed customers are described as follows (each requesting anonymity):

INDUSTRY	REGION	INTERVIEWEE	NUMBER OF DEVICES/ PRIVILEGED USERS
Retail bank	Headquartered in the UK	Sr. project manager	700/87
Transportation	Headquartered in the US	IT manager	3,000/1,150
Transportation	Headquartered in the US	Information security manager	1,500/75

Composite *Organization*

The *Organization* is a global, midsize enterprise in the business of manufacturing, distribution, and services. It has both business-to-consumer (B2C) and business-to-business (B2B) customers. The *Organization* has multisite operations globally and has been using CA Privileged Access Manager for three years to protect its critical accounts and endpoints.

This composite *Organization* currently has 5,000 addressable devices, up from 2,500 initially, and 1,000 users that have privileges.

The *Organization* and other customers have the option of deploying CA Privileged Access Manager as a hardened device or virtual machine to accelerate and automate the privileged access management life cycle. Our *Organization* has chosen the virtual machine version.

Before its investment in cloud-based CA Privileged Access Manager, the *Organization* had a manual process to manage passwords and used some automation tools to force policy changes of passwords. It also tried several homegrown solutions for privileged access on mainframes, and different solutions for Windows and Linux. Building and deploying these homegrown systems became very complicated. According to one interviewed customer, “A lot of hands had to be involved. It wasn’t just the security team; it was security and other teams that had to do pieces of it. It never really worked”.

> “I deal with other vendors, and CA is much more engaged in my business. It has to do with the CA people I’m fortunate enough to work with. The best thing that I found was their willingness upfront to work with us, to really understand what we wanted out of the product.”
>
> *Information security manager, transportation company*

Key Goals And Objectives

Security and risk (S&R) professionals responsible for access management must manage users’ access to sensitive applications and data without inhibiting business agility, compromising the digital experience for employees or customers, or violating compliance requirements — and they need to do so as effectively as possible.

The *Organization* had the following more specific goals and objectives, which were shared by the interviewed customers:

- Data breach prevention.

- Insider threat management.
- Ability to record sessions.
- Regulatory compliance and audit.
- Ability to cover hybrid IT infrastructure (expansion of available attack surface).

Operational Pain Points

The *Organization* was trying to avoid the following operational pain points with CA Privileged Access Manager:

- Insider modification or theft of confidential/sensitive information for personal gain.
- Theft of trade secrets or customer information to be used for business advantage or to give to a foreign government or organization.
- Sabotage of an organization's data, systems, or network.

Summary Of Key Results

The interviews revealed several key results attributed to the CA Privileged Access Manager solution investment as follows:

- **Compliance savings from CA Privileged Access Manager user session monitoring ($613,009).** Interviewed customers cited both internal labor savings and external audit savings. The average labor savings was one FTE annually, and the average external audit savings was $150,000 annually due to recording of sessions and streamlined and automated remediation.
- **Breach avoidance cost savings ($1,268,295**). With breach avoidance, there's less time and effort involved in managing and mitigating breaches, thereby reducing the cost of activating the *Organization's* entire incident response team, saving $600,000 annually.
- **Labor savings from ease of deployment and ongoing administration ($71,574).** The *Organization* saved 400 hours in deployment and integration costs, compared to other privileged access management solutions. In addition, the *Organization* saved 520 hours per year in ongoing administration compared with alternative solutions.

"Regulators are extending security and privacy mandates to cover the risks posed by privileged users and administrative accounts. CA Privileged Access Manager makes it much easier and less costly to comply with both security and privacy regulatory requirements."

Sr. project manager, retail bank

Financial Analysis

QUANTIFIED BENEFIT AND COST DATA

Total Benefits

REF.	BENEFIT	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Atr	Compliance savings from CA Privileged Access Manager user session monitoring	$246,500	$246,500	$246,500	$739,500	$613,009
Btr	Breach avoidance cost savings	$510,000	$510,000	$510,000	$1,530,000	$1,268,295
Ctr	Labor savings from ease of deployment and ongoing administration	$39,744	$22,464	$22,464	$84,672	$71,574
	Total benefits (risk-adjusted)	$796,244	$778,964	$778,964	$2,354,172	$1,952,878

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 $2 million.

Compliance Savings From CA Privileged Access Manager User Session Monitoring

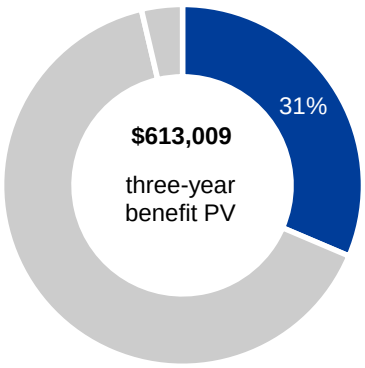
Auditors today want even more insight into how a firm grants access to sensitive and privileged credentials, such as for systems and database administrators, and what these administrators do with the system.

This CA Privileged Access Manager solution monitors user activity and provides real-time alerts to terminate potentially damaging sessions. Session recording and playback tracks all activities and events. All command line activity can be archived to meet audit and compliance mandates.

A single CA Privileged Access Manager appliance can support 2,000 (or more) recorded sessions. CA Privileged Access Manager ensures user accountability by auditing privileged activity and by recording videos of user sessions.

Before its investment in CA Privileged Access Manager, the *Organization* had a manual process to manage passwords and used some automation tools to force policy changes of passwords. The *Organization* also tried several homegrown solutions for privileged access on mainframes, and different solutions for Windows and Linux. Building and deploying these homegrown systems got very complicated. These inefficient and inaccurate approaches consumed precious administrator resources, increased potential risks, impeded employee productivity, and increased operational inefficiencies. These concerns were exacerbated by ongoing organizational changes and restructuring, which not only increased overall complexity but also made visibility into risks and interdependencies more challenging to assess.

Regulators are extending security and privacy mandates to cover the risks posed by privileged users and administrative accounts. Before the *Organization's* investment in CA Privileged Access Manager, the time and cost involved in proving compliance with regulatory mandates was excessively high. CA Privileged Access Manager helped reduce the time required to prove adequate protection and management of passwords and monitoring of privileged users and accounts. This reduced external auditor fees due to streamlined and automated remediation and helped



Compliance savings: 31% of total benefits

FORRESTER®

to achieve and maintain standards compliance (PCI, DSS, HIPAA, NERC-CIP, FISMA).

Modeling and assumptions. Interviewed customers cited both internal labor savings and external audit savings. The average labor savings was one FTE annually, and the average external audit savings was $150,000 annually due to recording of sessions and streamlined and automated remediation.

Risks. Forrester considered the following potential when assigning a risk adjustment:

- Other organizations may experience slower rollout and adoption of the benefits of CA Privileged Access Manager.
- There may be variations in the use of external auditors.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk-adjusted total PV of $613,009.

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.

Compliance Savings From CA Privileged Access Manager User Session Monitoring: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
A1	Internal labor savings — IT and audit	Interviews — one FTE	$140,000	$140,000	$140,000
A2	External audit fees — savings	Interviews	$150,000	$150,000	$150,000
At	Compliance savings from CA Privileged Access Manager user session monitoring	A1+A2	$290,000	$290,000	$290,000
	Risk adjustment	↓15%			
Atr	Compliance savings from CA Privileged Access Manager user session monitoring (risk-adjusted)		$246,500	$246,500	$246,500

Breach Avoidance Cost Savings

Organizations need business continuity (BC) or IT disaster recovery (DR) plans, and they also need to have a comprehensive incident response plan for breaches in general and breaches associated with privilege user issues. Organizations don't want to be developing an incident response plan in real time while employees are pilfering their intellectual property. A well-defined incident management program provides a script to follow when incidents occur.

CA Privileged Access Manager helps prevent security breaches by consistently protecting sensitive administration credentials, controlling privileged user access, enforcing security policies, and monitoring privileged user activity via user session recordings.

Here are the cross-functional roles, both internal and external, that should be included in an organization's incident response team, and where incident activation costs can be avoided.

- **Information security staff.** These individuals are responsible for handling the detailed investigation of the incident and possessing the capabilities for advanced forensics. Many organizations also hire external consultants to assist with incident response and forensics.

- **IT staff.** System and network administrators will help with incident investigations because of their advanced knowledge of the applications and systems they support.
- **Legal representatives.** It's essential to engage legal staff during the incident response to provide guidance on the legality of potential searches and the requirements of evidence collection, as they will likely have to defend the incident response plan.
- **Line-of-business representatives.** The information security team will need to partner with the business unit data owners to understand the data and its implications.
- **A data champion or chief data officer (CDO).** An individual who is responsible for the organization's use of data for business purposes is required. This individual has an incentive to ensure that the data is protected and used appropriately.
- **Corporate communications representatives.** These are the individuals who will speak for the company and provide the message that the company wants to deliver to its customers, investors, and business partners. Poor communication can increase customer frustration and irreparably damage an organization's reputation.
- **External investigators.** An external investigator with the necessary skills to properly respond to an incident can leverage a company's incident response team out of a difficult situation when it is overwhelmed.

The *Organization* recognized that the effects from privileged user breaches could be devastating, causing the company to lose revenue, market reputation, and market competitiveness.

The customers Forrester interviewed agreed that CA Privileged Access Manager helps avoid security breaches. With breach avoidance, there's less time and effort involved in managing and mitigating breaches, thereby reducing the cost of activating the *Organization's* entire incident response team.

Modeling and assumptions. Forrester's research supported an assumption that the *Organization* would incur a significant breach every year, and that several of the internal and external job roles listed above would have been activated to manage, mitigate, and control the breach. Interviewed customers estimated the cost of managing, mitigating, and controlling a breach to range between $400,000 to $800,000.

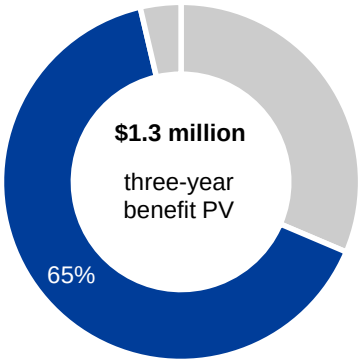
This amount does not account for an inadequate or unsuccessful incident response (or no response) that leads to financial, operational, and/or reputational losses. Readers should consider and assess the ability of their own organizations to respond to incidents and prevent significant financial and reputational losses.

Interviewed customers reported a wide range of cost avoidance benefits using CA Privileged Access Manager. Forrester will use an average of $600,000 per year before risks adjustments.

Risks. Forrester considered the following potential risks when assigning a risk adjustment:

- Since this is an estimate, it has been risk-adjusted.
- Readers of this study may have different savings outcomes.

To account for these risks, Forrester adjusted this benefit downward by 15%, yielding a three-year risk adjusted total PV of $1,268,295.



Breach avoidance cost savings: 65% of total

Forrester question: "What did your pre-CA Privileged Access Manager environment look like?"

Answer: "We tried several homegrown solutions for privilege access; different ones for mainframes, Windows and Linux. Building and deploying these homegrown systems got very complicated. A lot of hands had to be involved. It wasn't just the security team; it was security and other teams that had to do pieces of it. It never really worked".

Information security manager, transportation

FORRESTER®

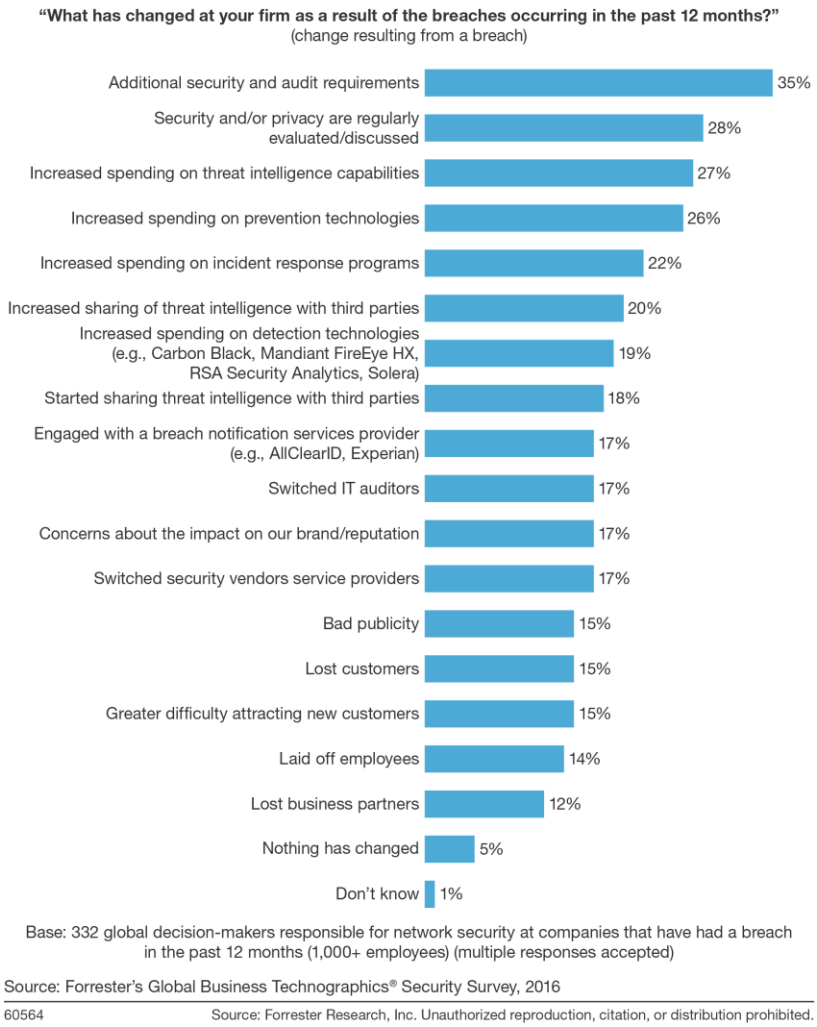
Breach Avoidance Cost Savings: Calculation Table					
REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
B1	Breach avoidance cost savings	Interviews	$600,000	$600,000	$600,000
Bt	Breach avoidance cost savings	B1	$600,000	$600,000	$600,000
	Risk adjustment	↓15%			
Btr	Breach avoidance cost savings (risk adjusted)		$510,000	$510,000	$510,000

The Forrester survey below asks the following question of companies that have experienced a breach in the past 12 months: “What has changed at your firm as a result of the breaches occurring in the past 12 months?” Note that most, if not all, of the responses involve some increased spending on technology or increased time and effort (labor expense) as a result of a breach.

FORRESTER RESEARCH | SECURITY & RISK PROFESSIONALS

Strategic Change Resulting From Breach

Planning For Failure: How To Survive A Breach



60564 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Labor Savings From Ease Of Deployment And Ongoing Administration

CA Privileged Access Manager is delivered as a single appliance that, according to interviewed customers, can be quickly deployed in only hours as a hardened device or a virtual machine. A single appliance protects thousands of resources and supports a larger number of concurrent sessions with fewer appliances, thus providing for a savings in IT labor costs.

When comparing CA Privileged Access Manager to other privileged access management solutions, interviewed customers reported savings of 400 hours in deployment and integration labor, and 0.25 FTEs or 520 hours annually for ongoing administration.

Modeling and assumptions. At the beginning of Year 1, the *Organization* saved 400 hours in deployment and integration costs, compared to other privileged access management solutions. In addition,

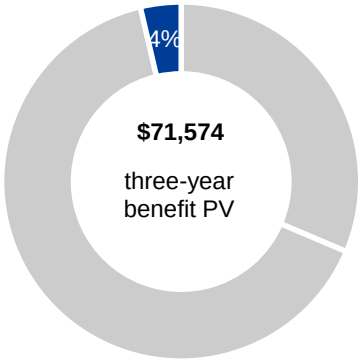
FORRESTER®

the *Organization* saved 520 hours per year, compared to other vendors. Forrester used an industry average cost (not fully loaded) of $48.00 per hour to calculate the benefits of ease of deployment and ongoing administration of CA Privileged Access Manager.

Risks. Forrester considered the following potential risks when assigning a risk adjustment:

- Since this is an estimate, it has been risk-adjusted.
- Readers of this study may have different savings outcomes.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year risk-adjusted total PV of $71,574.



Labor savings: 4% of total benefits

Labor Savings From Ease Of Deployment And Ongoing Administration: Calculation Table

REF.	METRIC	CALC./SOURCE	YEAR 1	YEAR 2	YEAR 3
C1	Hours saved — initial deployment and integration	Interviews	400	0	0
C2	Annual hours saved — ongoing administration	Interviews	520	520	520
C3	Labor cost per hour (not fully loaded)	Industry average	$48.00	$48.00	$48.00
Ct	Labor savings from ease of deployment and ongoing administration	(C1+C2)*C3	$44,160	$24,960	$24,960
	Risk adjustment	↓10%			
Ctr	Labor savings from ease of deployment and ongoing administration (risk-adjusted)		$39,744	$22,464	$22,464

Unquantified Benefit

Unquantified benefit. The composite *Organization* experienced the following benefit, which was not quantified for this study:

- **Session recordings — innocent log-on behavior.** In addition to tracking employees' keystrokes, the session recordings track incorrect (and mostly innocent) log-on behavior by users. The recordings make it much easier to identify the problem and create a teaching exercise for the user in how to correctly log into the systems. Session recordings make IT administrators' jobs easier.

Less than six months for payback

Time to recover the initial investment in CA Privileged Access Manager

FORRESTER®

Flexibility

The value of flexibility is clearly unique to each customer, and the measure of its value varies from organization to organization. There are scenarios in which a customer might choose to invest in the CA Privileged Access Manager solution and later realize additional uses and business opportunities. Here's a future flexibility option that the *Organization* is considering:

- CA Privileged Access Manager integrates well with other CA security products, including CA Advanced Authentication, CA Identity Suite, and CA Single Sign-On. In addition, CA also offers two optional components that enhance CA Privileged Access Manager. CA Threat Analytics for Privileged Access Manager continuously assesses risk and quickly detects anomalous behavior by analyzing privileged access and activities. CA Privileged Access Manager Server Control provides fine-grained controls over operating system-level access for mission-critical servers.

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

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.

Total Costs

REF.	COST	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
D1	Number of addressable devices	0	2,500	5,000	5,000	-	-
Dt	CA Privileged Access Manager fees	$193,000	$186,160	$368,660	$368,660	$1,116,480	$943,894
	Total costs	$193,000	$186,160	$368,660	$368,660	$1,116,480	$943,894

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 *Organization* expects risk-adjusted total costs to be a PV of $943,894.

CA Privileged Access Manager Fees

CA Privileged Access Manager is delivered as a single appliance that can be deployed in only hours as a hardened device or a virtual machine, protecting enterprise resources with one scalable, agentless solution.

The *Organization* incurred the following fees from CA: annual licenses based on addressable devices, software maintenance, user session monitoring, training, and professional services.

Modeling and assumptions. CA fees were based on 2,500 addressable devices in Year 1, and 5,000 devices in Years 2 and 3.

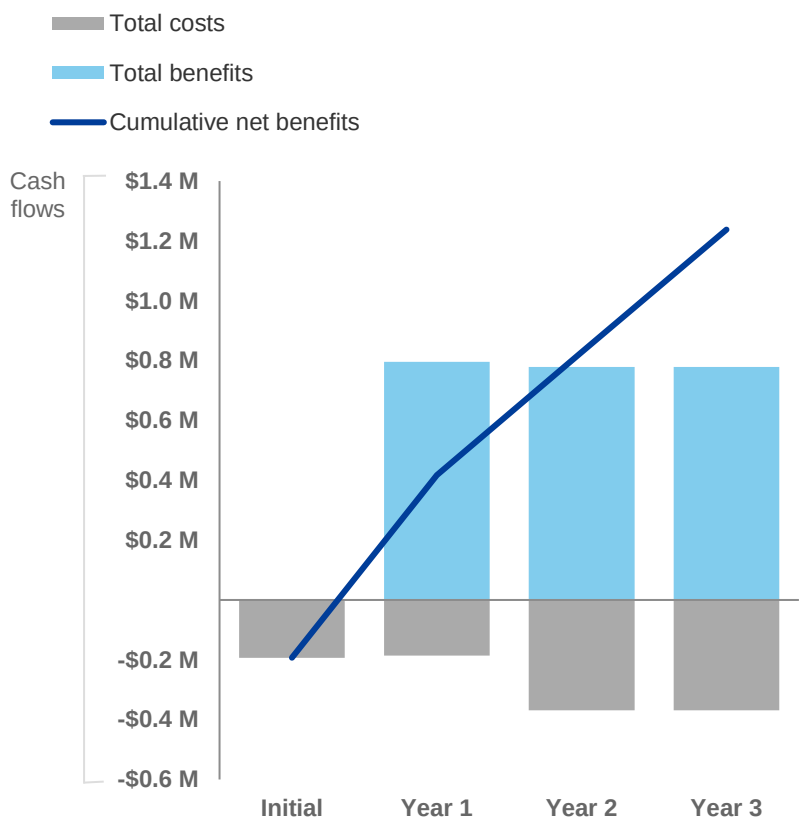
Risks. Forrester did not risk-adjust costs because the fees are actual quotes from CA.

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

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 Table (Risk-Adjusted)

	INITIAL	YEAR 1	YEAR 2	YEAR 3	TOTAL	PRESENT VALUE
Total costs	($193,000)	($186,160)	($368,660)	($368,660)	($1,116,480)	($943,894)
Total benefits	$0	$796,244	$778,964	$778,964	$2,354,172	$1,952,878
Net benefits	($193,000)	$610,084	$410,304	$410,304	$1,237,692	$1,008,984
ROI						**107%**
Payback period						**Less than six months**

If risk-adjusted costs, benefits, and ROI still demonstrate a compelling business case, it raises confidence that the investment is likely to succeed because the risks that threaten the project have been taken into consideration and quantified. Assuming normal success at mitigating risk, the risk-adjusted numbers should more closely reflect the expected outcome of the investment.

FORRESTER®

CA Privileged Access Manager Solution: Overview

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

CA Privileged Access Manager protects an organization's business and empowers its people.

Manage and control access to IT resources.

Centrally manage and unify privileged user policies across multiple physical and virtual environments. Users can securely access critical IT resources without gaining a footprint on the network — while you monitor all activity across your entire IT infrastructure.

Quickly protect the entire enterprise.

Deploy CA Privileged Access Manager as a hardened device or virtual machine to accelerate and automate privileged access management life cycle. Almost immediately, it will help proactively control user activity to prevent policy violations, exposures, and downtime.

Effectively monitor, react, and record.

This privileged access management solution enables organizations to monitor user activity and get real-time alerts to terminate potentially damaging sessions. Session recording and playback lets organizations track all activities and events. CA Privileged Access Manager easily archives all command line activity to meet audit and compliance mandates.

Protect hybrid-cloud consoles.

With Privileged Access Manager from CA, privileged users will gain access only to authorized hybrid cloud infrastructure — with all activity fully monitored and recorded.

Employ positive Privileged User Authentication.

With CA Privileged Access Manager, organizations can leverage its existing identity and access management infrastructure through integration with Active Directory, LDAP-compliant directories, RADIUS, TACACS+, smartcards, hardware tokens, and more.

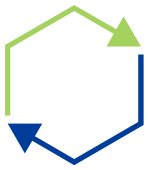
Appendix A: Total Economic Impact

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.

FORRESTER®