FORRESTER®



The Total Economic Impact™ Of CyberArk Privileged Access Management As A Service

Business Benefits And Cost Savings Enabled By CyberArk Privilege Cloud And Endpoint Privilege Manager

March 2021

Table Of Contents

Executive Summary 1

The CyberArk Privilege Cloud And EPM Customer Journey 6

Key Challenges 6

Composite Organization 7

Analysis Of Benefits 9

Operational Efficiency Savings For Privileged Access Management Administration 9

Compliance, Regulatory, And Audit Savings 11

CyberArk EPM Benefits 13

Reduced Risk Of Serious Security Breach 15

Unquantified Benefits 17

Flexibilty 17

Analysis Of Costs 19

Planning, Implementation, And Ongoing Labor Costs 19

Required Hardware 21

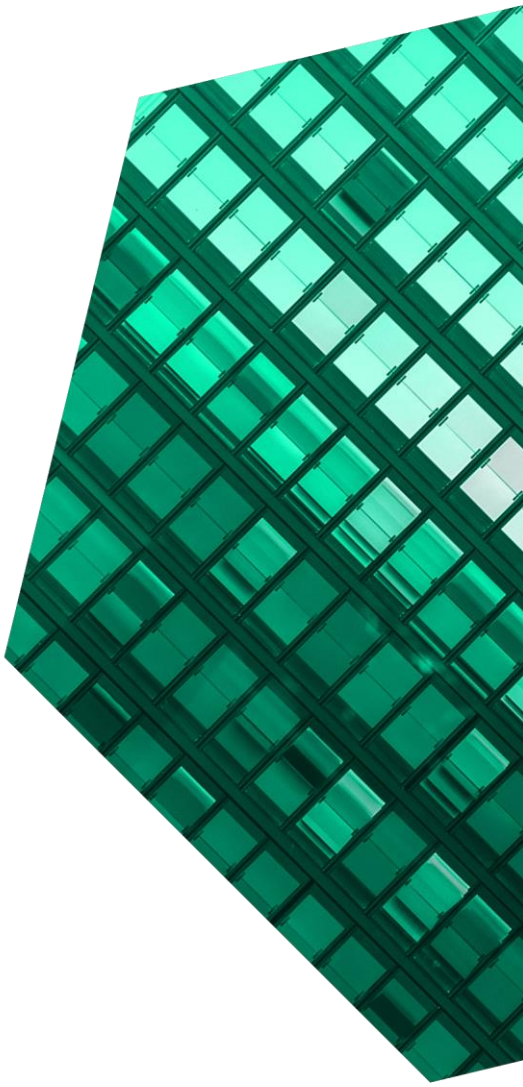
CyberArk Fees 22

Financial Summary 23

Appendix A: Total Economic Impact 24

Appendix C: Endnotes 25

Consulting Team: Bob Cormier, Vice President and Principal Consultant



ABOUT FORRESTER CONSULTING

Forrester Consulting provides independent and objective research-based consulting to help leaders succeed in their organizations. For more information, visit forrester.com/consulting.

© 2021, Forrester Research, Inc. All rights reserved. Unauthorized reproduction is strictly prohibited. Information is based on the best available resources. Opinions reflect judgment at the time and are subject to change. Forrester®, Technographics®, Forrester Wave, RoleView, TechRadar, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies.

Executive Summary

CyberArk's Privileged Access Management (PAM) software-as-a-service (SaaS) solutions Privilege Cloud and Endpoint Privilege Manager are part of CyberArk's identity security portfolio. Privilege Cloud offers credential vaulting and rotation and session management, and it is complemented by Endpoint Privilege Manager, which secures local admin rights on endpoints. Both solutions enable organizations to secure privileged access from endpoints to the cloud.

CyberArk 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 software-as-a-service (SaaS) version of CyberArk's Privileged Access Manager (PAM) solution called Privilege Cloud and CyberArk's Endpoint Privilege Manager (EPM) solution. The purpose of this study is to provide readers with a framework to evaluate the potential financial impact of deploying these two solutions at their organizations.

CyberArk PAM allows organizations to protect, control, and monitor privileged access to their most critical assets. CyberArk Privilege Cloud provides organizations with the ability to take a risk-based approach to credential and session management. CyberArk EPM helps to block and contain attacks at the endpoint by removing and managing local admin rights, blocking attempts to steal credentials, and implementing application controls. Both SaaS solutions enable organizations to enforce least-privilege principles and to defend against both internal and external threats.

To better understand the benefits, costs, and risks associated with this investment, Forrester interviewed five customers with experience using CyberArk Privilege Cloud and Endpoint Privilege Manager. For the purposes of this study, Forrester aggregated the experiences of the interviewed customers and combined the results into a single composite *Organization*.

KEY STATISTICS



Return on investment (ROI)
100%

Net present value (NPV)
$457,836

Prior to its investment in CyberArk, the composite *Organization* had a disparate set of environments and systems that made it difficult to manage privileged access for Windows and Linux, virtual machines and servers, networking devices, on-premises and SaaS databases and applications, and workloads in the public cloud.

This *Organization* had weak standards for managing privileged credentials (e.g., paper-based storage of passwords in sealed envelopes, manual rotation of passwords/credentials, pen/paper logbooks, physical safes, or password files in spreadsheets).

Passwords/credentials were seldom changed, there was no accountability, and employees shared passwords in plain text. Additionally, local admin rights on endpoints were not managed.

The composite *Organization* needed a centralized solution to better manage and store passwords and credentials used by human and machine identities.

The *Organization* needed to secure sessions in a way that would also meet audit and compliance requirements. The *Organization* also needed to reduce the risk of unmanaged local admin access on endpoints without increasing help-desk support costs. Decision-makers believe they found that solution in CyberArk.

KEY FINDINGS

Quantified benefits. Three-year risk-adjusted present value (PV) quantified benefits include:

- **Operational efficiency savings for privileged access management administration worth $104,914.** If the *Organization* had tried to match CyberArk's privileged access features and functionality manually, decision-makers would have had to hire more security and administrative staff, and the *Organization* still would have failed to achieve CyberArk's level of success, given that CyberArk has more than two decades of experience in securing privileged access for companies of all sizes — from large Fortune 500 enterprises to midsized organizations. Forrester estimates the composite *Organization* saves 780 hours annually when compared to hiring more staff. It also saves additional hours because CyberArk handles upgrades, patches, and infrastructure management.
- **Compliance, regulatory, and audit labor savings valued at $152,435.** Compared to its pre-CyberArk environment, the *Organization* saves 693 hours (or one-third of an FTE) in Year 1, and 1,387 hours in Years 2 and 3 as the learning curve progresses. It no longer incurs the significant time-based and financial costs associated with remediation of risks revealed in audit findings.
- **CyberArk EPM service desk benefits worth $70,502.** Each year, the *Organization* is able to save 780 IT help desk service requests at a cost savings of $40 per ticket. In addition, by removing a significant number of help desk tickets such as requests for application installation and privilege elevation, the *Organization* frees up staff to focus on higher-priority tasks. With CyberArk EPM in place, end users' productivity also increases without the need to wait for the tickets to be resolved.

Total Three-Year Risk Adjusted Benefits

$914,562

- **Reduced risk of a serious security breach valued at $586,711.** Forrester created a cost of breach model based on its "Cost Of A Security Breach" survey. There are two cost savings categories in this model: 1) cost avoidance savings for response and notification to affected parties, regulatory fines, customer compensation, customer lawsuits/punitive damages, additive audit and compliance costs, lost revenues/lost business due to system downtime, reduced revenues from customer loss, the cost to rebuild brand equity, and customer churn/cost to acquire new customers; and 2) the cost avoidance savings of internal employee productivity loss due to security breaches.

Unquantified benefits. Benefits that were reported but are not quantified in this study include:

- **Reduction of risk.** The successful use of CyberArk PAM and EPM protects company stakeholders' and shareholders' investments, providing security for an organization's most critical assets as well as maintaining a company's reputation.

- **Compliance with a broad set of regulations.** CyberArk PAM and EPM provide the ability to maintain ongoing compliance across a variety of regulations (e.g., General Data Protection Regulation [GDPR], Sarbanes-Oxley Act [SOX], Health Insurance Portability and Accountability Act (HIPAA), payment card industry data security standard [PCI DSS], and frameworks providing proof to auditors that secure controls have been implemented for privileged access. These include but are not limited to:
    - Enforcing effective privileged account and credential policies.
    - Restricting and controlling the allocation and usage of administrator-level operating system accounts.
    - Enforcing the security principles of need-to-know access, least-privilege, and segregation of duties.
    - Protecting the integrity of interactive operator sessions connecting to Tier 0 targets.
- **Better relationships with auditors and regulators.** Simplified and cost-effective audit reporting through a single, centralized repository of all audit data improves relationships with internal and external auditors and regulators.

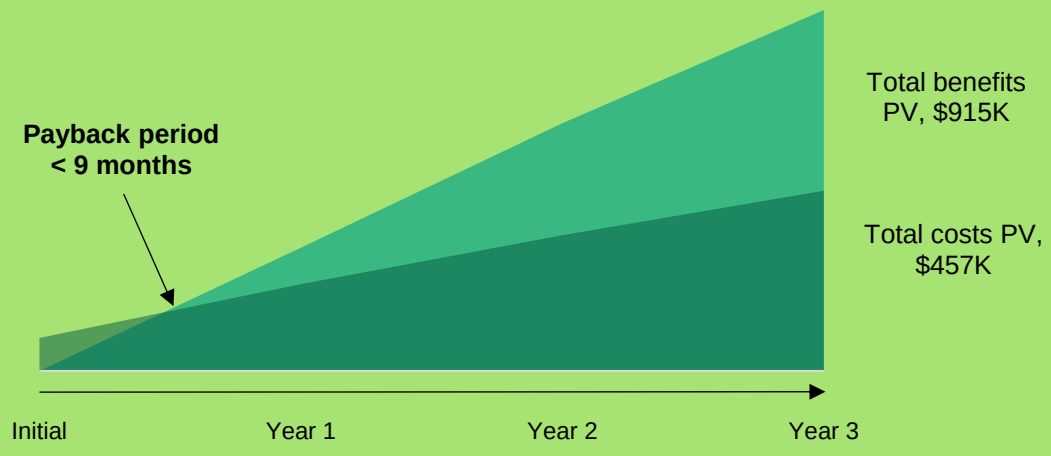
Costs. Three-year risk-adjusted PV costs include:

- **Planning, implementation, and ongoing labor costs of $162,137.** These costs are comprised of 780 hours of internal labor over an initial five-month period to plan the implementation, 520 hours annually of ongoing internal labor, and $16,400 for CyberArk EPM and Privilege Cloud Jump Start packages.
- **Required hardware of $3,000.** Interviewees said their organizations had to deploy lightweight connectors that host the secure tunnel to their IT assets, which is also leveraged for session management and credential rotation capabilities. This is a requirement for all industry-standard PAM SaaS solutions. As such, the composite *Organization* is required to install the connector.
- **Costs for CyberArk license fees of $290,989.** There are 50 CyberArk privileged users at the composite *Organization*, and the fee per user per month is $65. There are 4,500 workstations, and the EPM fee per workstation per month is $1.20. And one security engineer takes CyberArk PAM and EPM training courses for a cost of $6,400.

The customer interviews and financial analysis found that a composite *Organization* experiences benefits of $914,562 over three years versus costs of $456,726, adding up to a net present value (NPV) of $457,836 and an ROI of 100%.

ROI	BENEFITS PV	NPV	PAYBACK
100%	**$914,562**	**$457,836**	**< 9 months**

Financial Summary



TEI FRAMEWORK AND METHODOLOGY

From the information provided in the interviews, Forrester constructed a Total Economic Impact™ framework for those organizations considering an investment in CyberArk's PAM and EPM solutions.

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 CyberArk PAM and EPM can have on an organization.

DUE DILIGENCE

Interviewed CyberArk stakeholders to gather data relative to CyberArk's PAM and EPM solutions.

CUSTOMER INTERVIEWS

Interviewed five decision-makers at organizations using CyberArk's PAM and EPM solutions 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 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 CyberArk 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 CyberArk's PAM and EPM solutions.

CyberArk 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.

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

The CyberArk Privilege Cloud And EPM Customer Journey

Drivers leading to the CyberArk investment

Interviewed Organizations

Industry	Region	Interviewee	Total CyberArk users
Law firm	UK and global	Technology architect	300
Healthcare	US	Enterprise cybersecurity engineer	90
Insurance	US	Director of information security	65
Financial services	North America and global	Vice president of global identity access management	1,400
Financial services	US	VP of identity operations and engineering	500

KEY CHALLENGES

Before investing in CyberArk's Privilege Cloud and EPM SaaS solutions, the interviewees said their organizations were using an array of relatively ineffective tools.

Similar to the experiences of the interviewees' organizations, the composite *Organization* (see description below) struggles with the following common challenges:

- The *Organization* needed a solution to better manage and store credentials and secrets used by human and machine identities, and secure sessions while meeting audit and compliance requirements.
- The *Organization* had a disparate set of environments and systems that made it difficult to manage privileged access for Windows and Linux, virtual machines and servers, networking devices, on-premises and SaaS databases and applications, and workloads in the public cloud (e.g., Amazon Web Services, Azure).
- The *Organization* had poorly managed privileged credentials. For example, it used paper-based storage of passwords in sealed envelopes, manual rotation of passwords/credentials, pen/paper logbooks, physical safes, and password files in spreadsheets.
- Passwords and secrets (e.g., Secure Shell keys) were seldom changed, there was no accountability, and employees shared passwords.
- The *Organization* experienced high costs due to end users calling the help desk to install applications or to resolve problems on their workstations caused by downloading unauthorized applications.
- The *Organization* adopted security-as-a-service offerings so that the security team could spend more time deriving value from security

According to Forrester Research, the CyberArk PAM solution offers strong credentials and secrets vault management across a broad range of systems with many out-of-the-box integrations accessible via CyberArk Marketplace.

investments instead of spending time managing the infrastructure and other ongoing maintenance tasks.

- IT audits were becoming more costly in terms of time and effort required to respond to them as well as failed audits and fines for being out of compliance.
- There was exposure to a risk of breaches that could allow attackers to compromise privileged accounts that provide access to highly sensitive applications and systems. There was increased risk from cyberthreats (e.g., ransomware, phishing, insider threats) that could lead to data breaches, loss of company intellectual property, and reputational damage to the organization.

"I've been in cybersecurity for over 25 years now, and I've seen tons of vendors ignore their customers' inputs and experience downturns when they start to lose market share as a result. From my perspective, CyberArk is highly responsive and takes its customers' input seriously. I see the results in future enhancements to [CyberArk's] products."

VP of identity operations and engineering, financial services

COMPOSITE ORGANIZATION

Based on the interviews, Forrester constructed a TEI framework, a composite *Organization*, and an ROI analysis that illustrates the areas financially affected. The composite *Organization* is representative of the interviewees' companies, 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 *Organization* is a global enterprise with sales of around $1 billion, 5,000 employees, and 4,500 workstations. It has 50 privileged users including system, platform, and infrastructure administrators, cloud engineers, and developers whose privileged access is being onboarded into CyberArk. After a comprehensive vendor review process, decision-makers chose the CyberArk Privilege Cloud solution. The *Organization* also uses CyberArk Endpoint Privilege Manager to secure its Windows and Mac workstations.

Goals and objectives. The *Organization*'s decision-makers had the following goals and objectives they hoped to satisfy with Privilege Cloud and EPM. These included:

- Mitigating and reducing risk in managing and controlling privileged access and removing local admin rights from workstations.
- Reducing the time/effort spent on manually changing passwords and secrets used by human and machine identities.
- Decreasing the amount of time required to discover and onboard privileged accounts.
- Improving visibility from a compliance and governance perspective regarding credential management and activities undertaken by privileged users.
- Maintaining ongoing compliance across a variety of regulations and frameworks, providing proof to auditors that privileged access and least privilege enforcement are under control.
- Striking the balance of end-user productivity and maintaining strong security through managing local admin rights on the endpoint

- Reducing the high costs of end users calling the help desk to install applications or to resolve problems on their workstations caused by downloading unauthorized applications.
- Deploying a solution that aligned to the *Organization*'s strategy of using a security-as-a-service offering.

Key assumptions about the *Organization*

- **$1 billion in sales**
- **5,000 employees**
- **50 users of CyberArk Privilege Cloud**
- **4,500 workstations using CyberArk EPM**

Analysis Of Benefits

Quantified benefit data as applied to the composite *Organization*

Total Benefits						
Ref.	**Benefit**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Atr	Operational efficiency savings for privileged access management administration	$42,188	$42,188	$42,188	$126,563	$104,914
Btr	Compliance, regulatory and audit labor savings	$37,482	$75,018	$75,018	$187,518	$152,435
Ctr	CyberArk EPM service desk benefits	$28,350	$28,350	$28,350	$85,050	$70,502
Dtr	Reduced risk of a serious security breach	$235,925	$235,925	$235,925	$707,775	$586,711
	Total benefits (risk-adjusted)	$343,945	$381,480	$381,480	$1,106,905	$914,562

OPERATIONAL EFFICIENCY SAVINGS FOR PRIVILEGED ACCESS MANAGEMENT ADMINISTRATION

Evidence and data. The interviewees said their organizations experienced substantial time savings with their administration of CyberArk Privilege Cloud and EPM. The same is true of our composite *Organization*. Prior to investing in CyberArk, the *Organization* had a disparate set of environments and systems that made it difficult to manage privileged access. It had both Windows and Linux operating systems, multiple databases, hypervisors, and applications running on-premises and via SaaS, and many workloads running in multiple public clouds. Prior to using CyberArk, privileged credentials across these IT systems were poorly managed. For example, employees stored passwords on slips of paper in security envelopes or in pen/paper logbooks placed in physical safes, and some passwords were stored as files in (sometimes unprotected) spreadsheets. Employees seldom changed passwords and credentials, and if they did rotate them, they did so manually. There was no accountability for managing privileged credentials, and employees shared passwords without oversight or controls in place. Local admin rights on employee workstations were not managed, putting the *Organization* at additional risk. Additionally, the *Organization* experienced a high volume of help desk calls due to users downloading unauthorized applications to their workstations.

"At our company, CyberArk's solutions provide an additional level of value through risk reduction that's afforded to our shareholders and our customers by virtue of the security that we're implementing and the protection that they've come to expect."

Vice president of global identity access management, financial services company

Decision-makers needed to gain control over the *Organization*'s previously insecure processes by deploying CyberArk's solutions to add controls and benefitting from automated operational efficiencies for credential and session management and the removal of local admin rights on workstations.

Modeling and assumptions. If the *Organization* had tried to match CyberArk's privileged access features and functionality manually, decision-makers would have had to hire more security and administrative staff, and it would have still failed to achieve CyberArk's success. Forrester estimates the following for the composite *Organization*:

- It saves 780 hours annually with CyberArk compared to hiring more staff.
- The average fully loaded cost per hour for a security engineer is $60.10.
- The annual non-risk adjusted savings are $46,875. This leads to a total of $140,625 over three years.
- The annual risk-adjusted savings are $42,188. This leads to a total of $104,914 risk- and present value (PV) adjusted over three years.

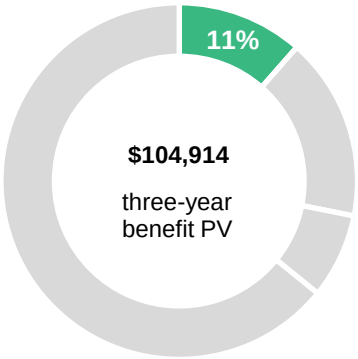
Risks. The actual improvement in operational efficiency may vary based on:

- The experience and competencies of existing security engineers.
- The fully loaded compensation of security engineers.
- The viability and maturity of the pre-CyberArk Privilege Cloud and EPM environments.

"CyberArk Privilege Cloud allows our organization to secure our infrastructure and applications and to run our privileged access management activities much more efficiently while maintaining the confidentiality of sensitive data."

Director of information security, insurance

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $104,914.



Operational efficiency savings for privileged access management administration
11% of total benefits

Operational Efficiency Savings For Privileged Access Administration					
Ref.	**Metric**	**Calc./Source**	**Year 1**	**Year 2**	**Year 3**
A1	Hours saved (privileged administration management)	Interviews	780	780	780
A2	Average fully loaded labor cost per hour (security engineer)	$125,000/2,080 hours	$60.10	$60.10	$60.10
A3	Total internal labor cost savings	A1*A2	$46,875	$46,875	$46,875
At	Operational efficiency savings for privileged access administration	A3	$46,875	$46,875	$46,875
	Risk adjustment	↓10%			
Atr	Operational efficiency savings for privileged access administration (risk-adjusted)		$42,188	$42,188	$42,188
	Risk-adjusted three-year total: $126,563		**Risk-adjusted three-year present value: $104,914**		

COMPLIANCE, REGULATORY, AND AUDIT SAVINGS

Evidence and data. Enterprises must continuously demonstrate that they can support and manage IT solutions in regulated environments and operate in a compliant manner. Privileged accounts, credentials, and secrets allow anyone who gains possession of them to control critical IT systems. They could potentially abuse that power by disabling security systems to steal, change, or destroy an organization's sensitive data. So, it's no surprise that internal auditors and regulatory compliance frameworks set specific controls and reporting requirements for the use of these credentials.

Interviewees said their organizations were challenged with improving and maintaining ongoing compliance across a variety of regulations and frameworks, as well as providing proof to auditors and regulators that privileged access was under control.

The same is true of our *Composite* organization. With its previous disparate systems and ineffective processes, meeting audit requirements was an arduous process. Internal and external auditors kept finding deficiences in privileged access controls for IT admins, cloud engineers, and developers with privileged access. These findings had to be analyzed and remediated, which proved difficult without an effective Privileged Access Management solution. Without CyberArk, it took more time and effort to

> **"There's nothing that annoys a regulator more than coming in and finding deficiencies that you as an organization didn't already identify. Because, to them, their perception is that they found something that you didn't know you had. So, CyberArk really does give you more credibility with the outside auditors and regulators by its ability to prove full compliance of regulations."**
>
> *Vice president of global identity access management, financial services company*

attempt to ensure compliance. With CyberArk, the *Organization* implements controls with the right level of governance and searchable audit logs, which reduces time spent by auditors looking for deficiencies. It also saves time and costs associated with remediation of findings.

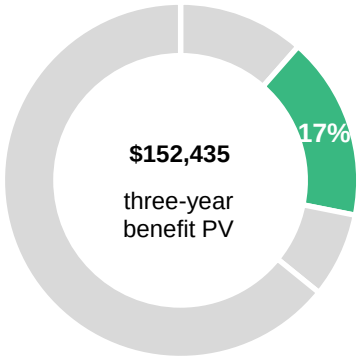
With a secure and central respository to store and rotate credentials making managing credentials easier and comprehensive session management, the *Organization* gains a solution in CyberArk that is flexible enough to support its growing needs in a secure and auditable way.

Modeling and assumptions. Compared to its pre-CyberArk environment, the *Organization* saves 693 hours or one-third of an FTE in Year 1 and 1,387 hours in Years 2 and 3 as the learning curve progresses. It no longer incurs the excessive time, effort, and costs associated with remediation of findings.

Risks. The actual improvement in operational efficiency may vary based on:

- The experience and competencies of existing security engineers.
- The fully loaded compensation of security engineers.
- The viability and maturity of the pre-CyberArk PAM environment.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV (discounted at 10%) of $152,435.



Compliance, regulatory, and audit savings
17% of total benefits

Compliance, Regulatory, And Audit Savings

Ref.	Metric	Calc./Source	Year 1	Year 2	Year 3
B1	Before CyberArk: hours spent on compliance, regulatory, and audit tasks	Interviews	693	1,387	1,387
B2	Average fully loaded labor cost per hour (security engineer)	$125,000/2,080 hours	$60.10	$60.10	$60.10
B3	Total internal labor cost savings	B1*B2	$41,647	$83,353	$83,353
Bt	Compliance, regulatory, and audit savings	B3	$41,647	$83,353	$83,353
	Risk adjustment	↓10%			
Btr	Compliance, regulatory, and audit savings (risk-adjusted)		$37,482	$75,018	$75,018
	Risk-adjusted three-year total: $187,518		**Risk-adjusted three-year present value: $152,435**		

CYBERARK EPM BENEFITS

Evidence and data. In addition to servers and IT infrastructure, workstations are attractive targets for attackers; all it takes is an unsuspecting user who clicks on a phishing email and malware is installed. From there, the attacker gains a foothold and moves laterally until they can access an organization's most sensitive applications and systems.

Removing local admin rights can significantly reduce risk, as users with local admin rights have the power to do virtually anything they want on the workstation — from downloading applications to removing or disabling security software. Local admin rights also allow employees to use any program, modify system configurations, and access powerful admin accounts. However, if local admin rights are stripped away and workstations only allow software install requests and configuration changes through the IT help desks, users experience decreased productivity while they wait for necessary access to systems and software.

Interviewees reported that CyberArk EPM provided a layered solution to secure privileges on endpoints, and it enforced the removal of local admin privileges while still allowing trusted applications to run. At the same time, the application control feature identifies, blocks, and contains malicious software at the end point including ransomware. Unknown applications can run in "restrict mode," preventing them from accessing corporate resources, sensitive data, or the internet. Credential theft protection detects and blocks attempted thefts of Windows credentials and those stored by popular applications, browsers, and file-cache credential stores.

> **"From a security perspective, CyberArk's Endpoint Privilege Manager allows us to rotate the local Windows credentials without using a third-party tool. From a compliance perspective, we now have full tracking for any of the applications that required privilege credentials or elevations on those devices."**
>
> *Director of information security, insurance*

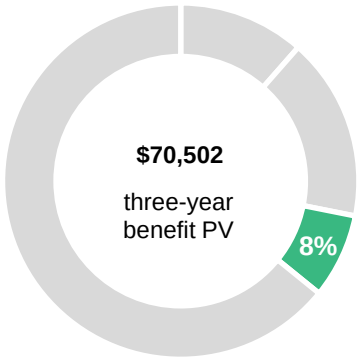
Modeling and assumptions. Prior to the composite *Organization*'s investment in CyberArk EPM, help desk costs were high due to end users calling for help installing applications or about problems on their workstations from the downloading unauthorized applications. Based on the interviews, Forrester estimates the *Organization* achieves a reduction of help desk service requests for software installations as follows:

- The *Organization* has 4,500 workstations and servers secured by EPM.
- Each year, it is able to save 788 IT help desk service requests at a cost savings of $40 per ticket.
- Annual savings equal $31,500 before risk adjustments. After risk-adjustments, annual savings equal $28,350.

Risks. The actual EPM benefits will vary based on:

- A company's average cost per help desk ticket for users requesting permission to install software or make other changes to their system.
- The overall technical expertise of the *Organization's* users.
- The relative expertise of the help desk staff.

To account for these risks, Forrester adjusted this benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $70,502.



CyberArk EPM benefits
8% of total benefits

CyberArk EPM Benefits

Ref.	Metric	Calc./Source	Year 1	Year 2	Year 3
C1	Number of workstations and servers secured by EPM (information only)	Composite *Organization*	4,500	4,500	4,500
C2	Number of help desk service requests for software installs before CyberArk EPM deployment	Interviews	3,150	3,150	3,150
C3	Number of help desk service requests for software installs after CyberArk EPM deployment	Interviews	2,363	2,363	2,363
C4	Number of service requests saved	C2-C3	788	788	788
C5	Cost per help desk service request	Industry average	$40.00	$40.00	$40.00
C6	Help desk service request savings	C4*C5	$31,500	$31,500	$31,500
Ct	CyberArk EPM benefits	C6	$31,500	$31,500	$31,500
	Risk adjustment	↓10%			
Ctr	CyberArk EPM benefits (risk-adjusted)		$28,350	$28,350	$28,350
	Risk-adjusted three-year total: $85,050			**Risk-adjusted three-year present value: $70,502**	

REDUCED RISK OF SERIOUS SECURITY BREACH

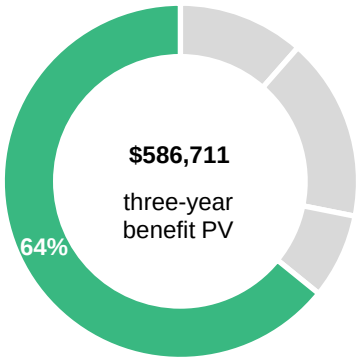
Evidence and data. The complex nature of managing privileged users and the environments they must integrate with and manage is greatly simplified by tools that provide low-friction security for privileged users. According to Forrester, CyberArk Privilege Cloud solution offers strong credentials and session management across a broad range of systems with many out-of-the-box integrations accessible via the CyberArk Marketplace. With more than 200 integrated solutions, the marketplace extends CyberArk's value into many other security technologies and provides immediate time-to-value. Many customers have proved the performance, scalability, and resilience of the offerings.

Modeling and assumptions. Forrester created a cost of breach model based on our "Cost Of A Security Breach" survey.[2] There are two cost avoidance calculations in this model (see below).

- Part 1: Row D3 includes a survey-based finding of $53 per employee costs. In Forrester's analysis, this relates to aggregated cost avoidance savings for the following: response and notification to affected parties, regulatory fines, customer compensation, customer lawsuits/punitive damages, additive audit and compliance costs, lost revenues/business due to system downtime, reduced revenues from customer loss, cost to rebuild brand equity, and customer churn/cost to acquire new customers.
- Part 2: Row D9 of this model includes the cost avoidance savings of internal employee productivity loss due to security breaches. Row Dtr calculates the reduced risk of a serious security breach and the resulting cost avoidance of having a solution such as CyberArk.

Risks. The actual breach avoidance benefits will vary based on security staffs' approaches for granting entitlements and authorizing privileged access to digital resources. This minimizes the risks of excessive entitlements and potential data breaches. Specific risk factors include overprivileged access, excessive permissions, orphaned accounts, and a lack of overall visibility and accountability.

To account for these risks, Forrester adjusted this breach avoidance benefit downward by 10%, yielding a three-year, risk-adjusted total PV of $586,711.



Reduced risk of serious security breach
64% of total benefits

Reduced Risk Of Serious Security Breach					
Ref.	**Metric**	**Calc./Source**	**Year 1**	**Year 2**	**Year 3**
D1	Average number of serious breaches per year	Forrester Research	2.1	2.1	2.1
D2	Number of internal employees	Composite *Organization*	5,000	5,000	5,000
D3	Average potential cost of breach ($53 per employee) exclusive of internal user downtime	Forrester research	$265,000	$265,000	$265,000
D4	Reduced likelihood of a breach	Interview data	22%	22%	22%
D5	Avoidance of breach costs per year	D1*D3*D4	$122,430	$122,430	$122,430
D6	Diminished/eliminated internal user productivity hours per breach	Forrester research	3.6	3.6	3.6
D7	Average hourly salary (business user)	$65K*1.35/2,080	$42.00	$42.00	$42.00
D8	Average percentage of employees affected per breach	Interview data	40%	40%	40%
D9	Avoidance of internal employee productivity loss due to security breaches	(D1*D2*D6*D7*D8)*D4	$139,709	$139,709	$139,709
Dt	Reduced risk of serious security breach	D5+D9	$262,139	$262,139	$262,139
	Risk adjustment	↓10%			
Dtr	Reduced risk of serious security breach (risk-adjusted)		$235,925	$235,925	$235,925
	Risk-adjusted three-year total: $707,775		**Risk-adjusted three-year present value: $586,711**		

UNQUANTIFIED BENEFITS

Additional benefits that customers experienced but were not able to quantify include:

- **Reduction of risk.** The successful use of CyberArk Privilege Cloud and EPM protects company stakeholders' and shareholders' investments, providing security for an organizations most critical assets, as well as maintaining a company's reputation.
- **Compliance with a broad set of regulations**. The ability to maintain ongoing compliance across a variety of regulations and frameworks providing proof to auditors that privileged access s under control. Readers may be able to relate to the following compliance regulations: PCI, PCI-DSS, SOX, GDPR, California Consumer Privacy Act (CCPR), American Institute of Certified Public Accountants Systems and Organization Controls (AICPA SOC), Health Insurance Portability and Accountability Act (HIPAA), Monetary Authority of Singapore Technology Risk Management (MAS TRM), Society of Worldwide Interbank Financial Telecommunication (SWIFT), European Network and Information Security Agency (ENISA), International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 27002 controls, and National Institute of Standards and Technology (NIST).
- **Better relationships with auditors and regulators.** Simplified and cost-effective audit reporting through a single, centralized repository of all audit data improves relationships with internal and external auditors and regulators.

> **"We have utilized more and more of CyberArk's auditing capabilities for compliance. What we are seeing with most auditors is that as soon as we say we have CyberArk, they say, 'Oh, great! Just send us this information from the CyberArk database.'"**
>
> *Director of information security, insurance*

FLEXIBILTY

Most of the interviewees said their organization used both CyberArk Privilege Cloud and EPM. The interviewees indicated their organizations will also add additional solutions in the future. These SaaS solutions include (note that descriptions below were provided by CyberArk):

- **CyberArk Remote Access (formerly Alero):** Enables secure privileged remote vendor and employee access to the most sensitive IT assets managed by CyberArk without the need for VPNs, agents, or passwords.
- **CyberArk Secrets Manager (formerly Application Access Manager):** Provides secrets management for applications, DevOps tools, and IT management and security solutions.
- **CyberArk Cloud Entitlements Manager:** Reduces excessive permissions risk and enforces least privilege across multicloud environments.
- **CyberArk Identity (formerly Idaptive):** Secure and manage identities with single sign-on (SSO), adaptive multi-factor authentication (MFA), and identity lifecycle management.

In 2018, CyberArk introduced a new consolidated PAM pricing and licensing model with a single offering for credential protection and session management. As of January 2021, CyberArk

incorporated additional capabilities with the addition of privileged remote access, SSO, and adaptive MFA for privileged users — all from one vendor. CyberArk also offers “success plans” that include strategically packaged resources, guidance, and expertise to help customers move their privileged access and identity security programs forward.

Flexibility might 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 *Organization*

Total Costs							
Ref.	**Cost**	**Initial**	**Year 1**	**Year 2**	**Year 3**	**Total**	**Present Value**
Etr	Planning, implementation, and ongoing labor costs	$72,766	$35,938	$35,938	$35,938	$180,579	$162,137
Ftr	Required hardware	$3,600	$0	$0	$0	$3,600	$3,600
Gtr	CyberArk fees	$7,040	$114,180	$114,180	$114,180	$349,580	$290,989
	Total costs (risk-adjusted)	$83,406	$150,118	$150,118	$150,118	$533,759	$456,726

PLANNING, IMPLEMENTATION, AND ONGOING LABOR COSTS

Evidence and data. Interviewees described using a phased approach to deploying CyberArk Privilege Cloud and EPM, with a goal of immediately improving their organizations' security postures while experiencing the least amount of pushback from end users. Here are the labor-intensive activity categories the composite *Organization* experienced:

> **"We were able to save 1.5 FTEs once CyberArk Privileged Access Management was up and running. We can now run CyberArk with one-half FTE including managing the excellent relationship we have with CyberArk."**
>
> *Technology architect, law firm*

1. The *Organization's* decision-makers identified servers that contain the most sensitive information (e.g., personally identifiable information [PII], credit card information, intellectual property), and they also identified which accounts have direct access to these servers. These can include operating system accounts, database accounts, application accounts, etc.
2. The *Organization*'s decision-makers identified and focused on securing built-in admin accounts (e.g., Windows administrators, UNIX root users, Oracle SYS users, Cisco Enable users). Hackers view these accounts as the highest-value targets. Initially focusing on these built-in admin accounts provides a significant improvement in the security posture without a lot of end-user pushback.
3. Next, the composite *Organization*'s security engineers loaded the credentials into the vault and set up an automated verification process to confirm the account credentials were accurate and that accounts were ready to start rotating credentials. End users are now able to connect directly to their target systems. Privileged sessions will then be connected, monitored and recorded via CyberArk session management capabilities.
4. On an ongoing basis, the composite *Organization*'s security engineers leverage automation to repeat these steps with new

systems (e.g., networking devices, databases, web applications). In addition, the *Organization* starts managing machine identities including application accounts, internet information services (IIS) application pools, registry keys, and any other hard-coded accounts.

5. The *Organization* deploys CyberArk EPM as part of a scheduled upgrade to its end-user workstations.

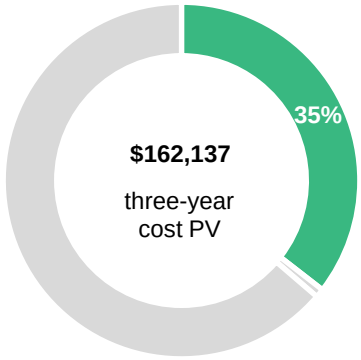
Modeling and assumptions. Forrester estimates for the composite *Organization* include:

- 780 hours of internal labor over an initial 5-month period to plan the implementation as described in steps 1-3.
- 520 hours annually of internal labor as described in steps 4 and 5.
- $16,400 for EPM and PAM Jump Start packages.

Risks. The planning, implementation, and ongoing labor costs will vary with:

- The competencies of existing security engineers.
- The fully loaded compensation of security engineers.
- The viability of the pre-CyberArk PAM and EPM environment.

To account for these risks, Forrester adjusted this breach avoidance benefit upward by 15%, yielding a three-year, risk-adjusted total PV of $162,137.



Planning, implementation, and ongoing labor costs 35% of total costs

Planning, Implementation, And Ongoing Labor Costs

Ref.	Metric	Calc./Source	Initial	Year 1	Year 2	Year 3
E1	Internal labor - vendor selection; implementation planning and deployment	Interviews - hours	780	0	0	0
E2	Ongoing labor to support CyberArk platform	Interviews - hours	0	520	520	520
E3	Average fully loaded labor cost per hour - security engineer	$125,000/2080 hours	$60.10	$60.10	$60.10	$60.10
E4	Total internal labor cost	(E1+E2)*E3	$46,875	$31,250	$31,250	$31,250
E5	EPM and PAM Jump Start packages	Interviews	$16,400	$0	$0	$0
Et	Planning, implementation, and ongoing labor costs	E4+E5	$63,275	$31,250	$31,250	$31,250
	Risk adjustment	↑15%				
Etr	Planning, implementation, and ongoing labor costs (risk-adjusted)		$72,766	$35,938	$35,938	$35,938
	Three-year risk adjusted total: $180,579			**Three-year risk-adjusted present value: $162,137**		

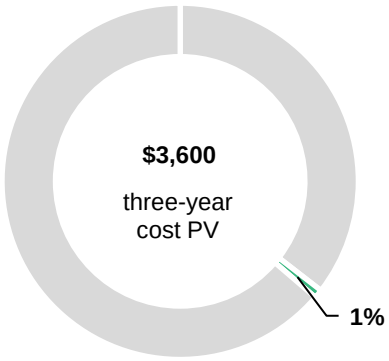
REQUIRED HARDWARE

Evidence and data. Some interviewees said their organizations needed to deploy lightweight connectors that host the secure tunnel to each organization's IT assets. This is also leveraged for the solution's session management and credential rotation capabilities. As such, the composite *Organization* is required to install the connector.

Modeling and assumptions. The average yearly cost of maintaining the connector (a server, operating system license, and associated storage) is $3,000.

Risks. Costs for connectors, servers, and storage will vary by the manufacturer, discounts, server size, etc.

To account for these risks, Forrester adjusted this cost upward by 20%, yielding a three-year, risk-adjusted total PV of $3,600.



Required hardware
1% of total costs

Required Hardware

Ref.	Metric	Calc./Source	Initial	Year 1	Year 2	Year 3
F1	On-premises server	Interviews	$3,000	$0	$0	$0
Ft	Required hardware	F1	$3,000	$0	$0	$0
	Risk adjustment	↑20%				
Ftr	Required hardware (risk-adjusted)		$3,600	$0	$0	$0
	Three-year total: $3,600			**Three-year present value: $3,600**		

CYBERARK LICENSE FEES

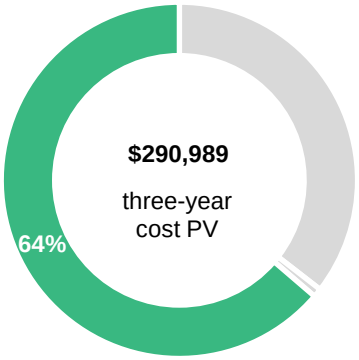
Evidence and data. The composite *Organization* has 50 CyberArk users.

Modeling and assumptions. CyberArk charges a Privilege Cloud license fee of $65 per 50 users per month for an annual total of $39,000. CyberArk charges an EPM license fee of $1.20 per 4,500 workstations per month for an annual total of $64,800. And one security engineer took CyberArk PAM and EPM training courses for a cost of $6,400.

Risks. CyberArk fees will vary with:

- Volume discounts negotiated by the customer with CyberArk.
- The number of CyberArk modules/products used by a customer.

To account for these risks, Forrester adjusted this cost upward by 10%, yielding a three-year, risk-adjusted total PV of $290,989.



CyberArk fees
64% of total costs

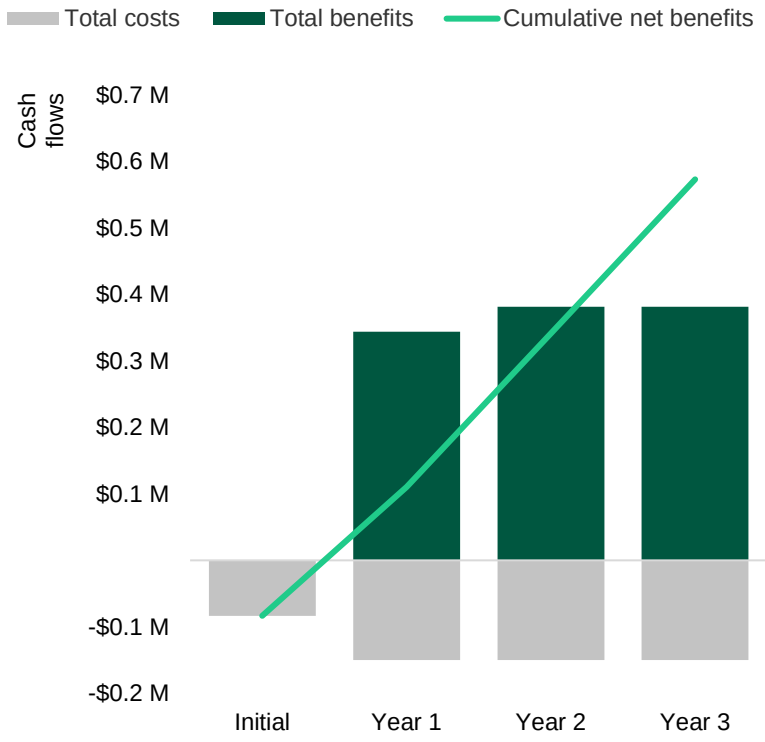
CyberArk Fees

Ref.	Metric	Calc./Source	Initial	Year 1	Year 2	Year 3
G1	Number of CyberArk users	Composite *Organization*	0	50	50	50
G2	CyberArk monthly fee per user	CyberArk quote	0	$65.00	$65.00	$65.00
G3	CyberArk annual user fees	(G1*G2)*12	0	$39,000	$39,000	$39,000
G4	Number of workstations for EPM	Composite *Organization*	0	4,500	4,500	4,500
G5	EPM monthly fee per workstation	CyberArk quote	0	$1.20	$1.20	$1.20
G6	EPM annual workstation fees	(G4*G5)*12	0	$64,800	$64,800	$64,800
G7	CyberArk platform training courses (two security engineers)	Interviews	$6,400	$0	$0	$0
Gtr	CyberArk fees	G3+G6+G7	$6,400	$103,800	$103,800	$103,800
	Risk adjustment	↑10%	□			
Gtr	CyberArk fees (risk-adjusted)		$7,040	$114,180	$114,180	$114,180
	Three-year total: $349,580			**Three-year present value: $290,989**		

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	($83,406)	($150,118)	($150,118)	($150,118)	($533,759)	($456,726)
Total benefits	$0	$343,945	$381,480	$381,480	$1,106,905	$914,562
Net benefits	($83,406)	$193,827	$231,363	$231,363	$573,147	$457,836
ROI						100%
Payback						<9 months

Appendix A: Total Economic Impact

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

TOTAL ECONOMIC IMPACT APPROACH

Benefits represent the value delivered to the business by the product. The TEI methodology places equal weight on the measure of benefits and the measure of costs, allowing for a full examination of the effect of the technology on the entire organization.

Costs consider all expenses necessary to deliver the proposed value, or benefits, of the product. The cost category within TEI captures incremental costs over the existing environment for ongoing costs associated with the solution.

Flexibility represents the strategic value that can be obtained for some future additional investment building on top of the initial investment already made. Having the ability to capture that benefit has a PV that can be estimated.

Risks measure the uncertainty of benefit and cost estimates given: 1) the likelihood that estimates will meet original projections and 2) the likelihood that estimates will be tracked over time. TEI risk factors are based on "triangular distribution."

PRESENT VALUE (PV)

The present or current value of (discounted) cost and benefit estimates given at an interest rate (the discount rate). The PV of costs and benefits feed into the total NPV of cash flows.

NET PRESENT VALUE (NPV)

The present or current value of (discounted) future net cash flows given an interest rate (the discount rate). A positive project NPV normally indicates that the investment should be made unless other projects have higher NPVs.

RETURN ON INVESTMENT (ROI)

A project's expected return in percentage terms. ROI is calculated by dividing net benefits (benefits less costs) by costs.

DISCOUNT RATE

The interest rate used in cash flow analysis to take into account the time value of money. Organizations typically use discount rates between 8% and 16%.

PAYBACK PERIOD

The breakeven point for an investment. This is the point in time at which net benefits (benefits minus costs) equal initial investment or cost.

Appendix C: Endnotes

[1] Source: “The Forrester Wave™: Privileged Identity Management (PIM), Q4 2020,” Forrester Research, Inc., November 18,2020.

[2] Source: “Cost Of A Security Breach,” Internal Forrester Survey Data, August 2020.


FORRESTER®