

The Business Value of CyberArk Endpoint Privilege Manager



Frank Dickson
Group Vice President,
Security and Trust, IDC



Megan Szurley
Business Value Manager,
Business Value Strategy Practice, IDC

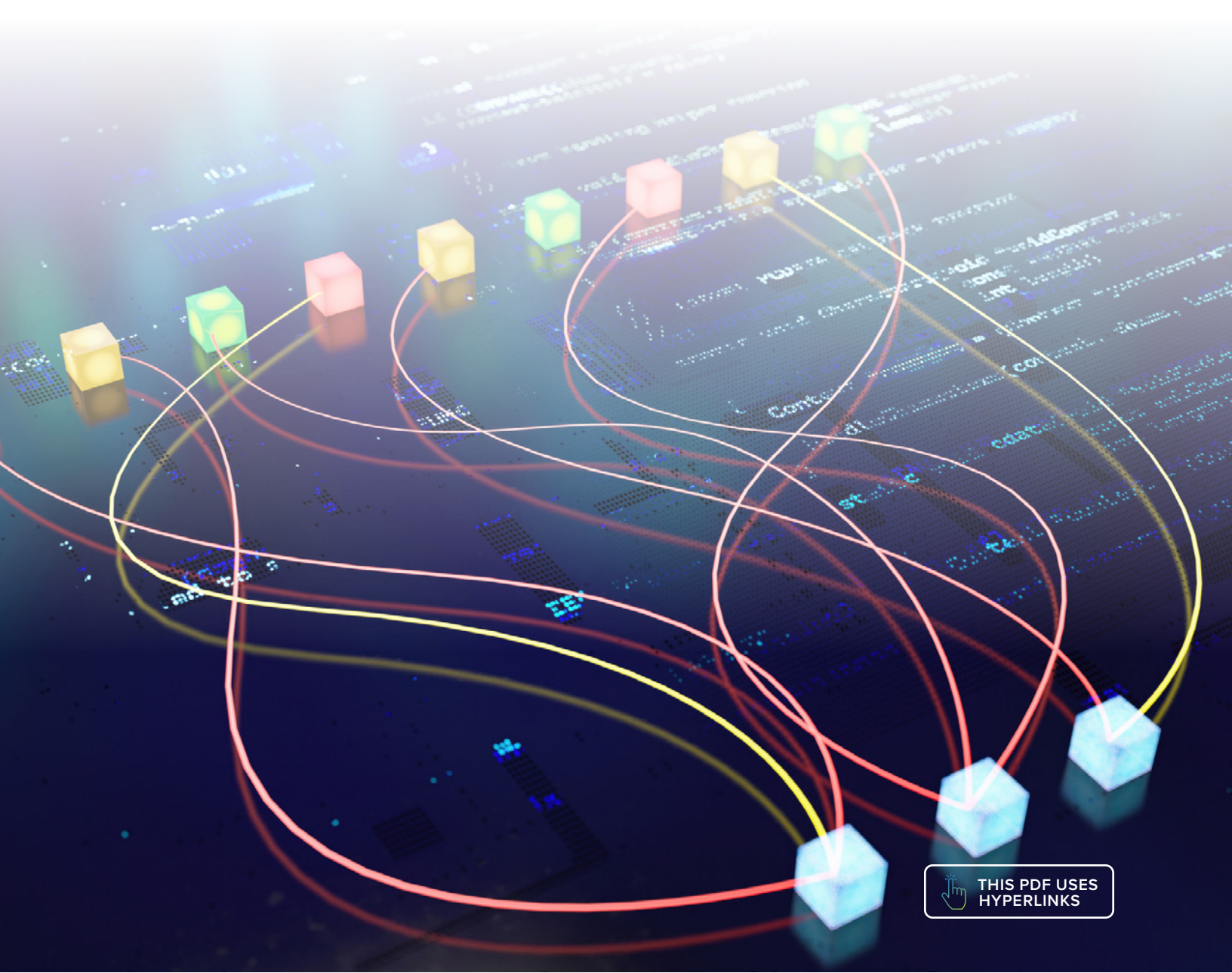


Table of Contents

Business Value Highlights	3
Executive Summary	3
Situation Overview	4
CyberArk EPM Overview	5
The Business Value of CyberArk EPM	6
Study Firmographics	6
Choice and Use of CyberArk EPM	7
Business Value and Quantified Benefits	9
Security and Compliance Benefits	14
Business Enablement Benefits	18
ROI Summary	19
Challenges/Opportunities	20
Conclusion	21
Appendix 1: Supplemental Data	22
Appendix 2: Methodology	23
About the IDC Analysts	24
Message from the Sponsor	25

BUSINESS VALUE HIGHLIGHTS

Click any link and look for the ► symbol on the corresponding page. Use the Return to Highlights button to return this page.

274%

three-year ROI

\$3 million

in average annual benefits

48%

more efficient identity
access management teams

26%

more productive
compliance teams

74%

reduction in
over-privileged accounts

57%

reduction in account
takeover attacks

49%

reduction in malware
spread risk

49%

better protection of
mission-critical resources
and services

46%

greater cyber-resiliency

27%

more efficient IT
infrastructure team

\$24,167

reduction in annual
third-party software
subscription costs

43%

reduction in help desk
calls/tickets related
to malware

40%

reduction in help desk
calls/tickets related
to privilege elevation
requests

Executive Summary

This document explores how organizations improved their cybersecurity posture and operational efficiency by adopting CyberArk Endpoint Privilege Manager (EPM). By shifting to CyberArk EPM, businesses were able to reduce the risks associated with excessive user privileges, streamline IT and help desk operations, and enhance compliance readiness. The solution enabled the management of privileges for users and applications through centralized policy enforcement, automated credential management, and seamless integration with existing infrastructure. These capabilities helped organizations strengthen endpoint security, support regulatory requirements, and empower users with secure, frictionless access to the tools they need.

Through a series of in-depth interviews, IDC conducted research that explored the value and benefits for organizations using CyberArk EPM to decrease the risk to workstations and servers.

Based on this data set and employing Business Value methodology, IDC calculates that these customers will achieve benefits worth an annual average of \$3 million (\$56,000 per 1,000 managed endpoints) and a three-year ROI of 274% through the following:

- **IT benefits:**

CyberArk EPM streamlined endpoint administration by enabling privilege management through centralized policy enforcement, simplifying credential management and security, improving visibility across devices, and allowing IT teams to operate more efficiently and focus on strategic initiatives.

- **Security and compliance:**

The platform enhanced security posture by enforcing least-privilege access, automating credential rotation, and providing detailed audit logs, which supported proactive threat response and simplified compliance with regulatory standards. In addition to logs, CyberArk EPM satisfies specific and crucial compliance requirements, such as removing local admin rights, enforcing least privilege, and maintaining software inventory.

- **Business enablement:**

CyberArk EPM improved workforce productivity by enabling seamless access to approved tools, reducing downtime, and minimizing reliance on IT support, all while maintaining a secure and user-friendly experience.

Situation Overview

Early personal computing operating systems were defined by a high degree of openness that significantly contributed to the growth and dominance of the Microsoft software ecosystem. The system architecture was designed to be accessible and extensible. Developers could interact directly with system resources, hardware, and memory.

A key aspect of this openness was the freedom granted to end users. By default, users had administrative privileges, which meant they could install applications, modify system settings, and even alter core components of the operating system without restriction. This open environment fostered a vibrant third-party software market and encouraged hardware manufacturers to develop drivers and utilities for the platform. Microsoft's decision to keep its operating systems open and user-configurable — combined with administrative access, a permissive installation model, and strong developer support — was instrumental in creating a rich, diverse, and resilient software ecosystem that thrived.

Unlimited freedom is great until it isn't. Enter the modern era of cybersecurity, beginning on December 18, 2013, when news broke that Target was investigating a major data breach

“potentially involving millions of customer credit and debit card records.” The Target data breach was certainly not the first data breach, but it marks the modern era of cybersecurity because the event moved the impact and awareness of data breaches from Pennsylvania Avenue and Wall Street to Main Street. Cybersecurity will never be the same.

In life, good people sometimes do bad things. Likewise, in cybersecurity, seemingly good files or applications do bad things. These types of attacks are given the moniker “exploit.” Taking advantage of a vulnerability in a browser or in Microsoft Word to launch PowerShell commands on a remote endpoint to take control of the device would be representative of an exploit. The resulting ease of leveraging an exploit kit on a PC with unlimited local administrative privilege became the enabler of cybermiscreants and their illicit financial cybergains; the term “ransomware” may even apply.

So, the great enabler of computing platforms’ openness became the greatest source of threat. The privileges that users have to maximize their productivity are the same privileges that cybermiscreants use to compromise the endpoint and then the organization. Thus, a challenge is presented to organizations: Enable end-user productivity, which is the life of computing, while protecting the user from attacks that take advantage of excessive local administrative privileges.

CyberArk EPM Overview

CyberArk EPM plays a crucial role in reducing cyber-risk by limiting what users can do once they’re logged into a system. Traditional security tools, such as antivirus and Endpoint Detection and Response (EDR), are designed to detect known and suspected threats based on behaviors and indicators, but they often miss the risks that excessive user privileges pose. EPM addresses this gap by proactively enforcing access-based controls, reducing the attack surface, and preventing potential misuse before it occurs.

This approach is especially effective against attacks that exploit elevated access — such as ransomware or credential theft — where attackers use legitimate accounts to move laterally or disable defenses. By applying the principle of least privilege, CyberArk EPM helps stop threats before attackers execute or leverage privilege elevation.

Importantly, CyberArk EPM doesn’t disrupt productivity. Modern solutions allow users to perform necessary tasks without full admin rights, striking a balance between security and usability. In short, EPM is a practical safeguard against the all-too-common scenario of users having more access than they should.

Effective endpoint privilege management centers on two core principles: removing local administrative rights and enforcing least privilege. Most users don’t need full admin access

to do their jobs, yet many still have it, creating unnecessary risk. By revoking local admin rights, organizations reduce the chance of malware or attackers gaining elevated control. Least privilege ensures users and services only access what's essential for their tasks. This minimizes the impact of compromised accounts and prevents privilege creep over time. Together, these practices form a strong foundation for securing endpoints without sacrificing usability or productivity.

Appropriately, CyberArk EPM is designed to help organizations enforce least privilege and remove unnecessary local administrator rights across endpoints. It supports Windows, macOS, and Linux environments and extends protection to physical machines, virtual desktops, and cloud workloads. CyberArk EPM enables granular control over user and application privileges, allowing organizations to tailor access policies without disrupting productivity.

One of its strengths is its ability to manage application behavior through policy-based controls. This includes just-in-time elevation, credential protection, and the blocking of unauthorized software. CyberArk EPM also integrates with identity platforms and IT service management tools, streamlining workflows and automating privilege requests.

Security features include protection against ransomware and credential theft, with capabilities such as fake “honeypot” accounts to detect malicious activity. CyberArk EPM also supports compliance efforts by maintaining audit trails and enforcing separation between privileged and non-privileged actions.

CyberArk's QuickStart framework allows organizations to begin reducing risk immediately, offering out-of-the-box policies that simplify deployment. While no solution is a magic bullet, CyberArk EPM provides a practical and flexible approach to privilege management, helping organizations strike a balance between security and usability. It's like giving users the keys to the right doors — without handing them the master key to the whole building.

The Business Value of CyberArk EPM

Study Firmographics

IDC conducted seven in-depth interviews with organizations using CyberArk EPM to reduce cyber-risks and manage endpoint privileges. Study participants had robust knowledge about the impact and use of CyberArk on their organization. They were asked a wide variety of quantitative and qualitative questions about the cost and benefit impact of CyberArk EPM on their IT, security, and risk operations.

The interviewed organizations were all based in the United States and represented a diverse set of industries — including healthcare, manufacturing, professional services, transportation, travel, and consumer packaged goods. On average, these organizations had approximately 51,000 employees and 994 IT staff and managed nearly 49,000 endpoints, with annual revenues averaging \$22.8 billion (Table 1).

TABLE 1
Firmographics of Interviewed Organizations

Firmographics	Average	Median	Minimum	Maximum
Number of employees	50,857	53,000	3,600	100,000
Number of IT staff	994	1,050	45	2,000
Number of endpoints (workstations, laptops, desktops)	48,786	30,000	3,500	100,000
Annual revenue	\$22.8B	\$16.0B	\$2.4B	\$61.4B
Countries	United States (7)			
Industries	Consumer Packaged Goods, Healthcare (2), Manufacturing, Professional Services, Transportation, Travel			

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Choice and Use of CyberArk EPM

Across the interviews, consistent themes emerged when the interviewees were asked about the reasons they chose CyberArk EPM. The solution was selected as a strategic investment to reduce risk by addressing the problem of overprivileged users across the entire enterprise. Participants also emphasized the platform’s ability to support compliance and audit readiness, helping organizations meet regulatory obligations with confidence. CyberArk’s seamless integration with existing IT infrastructure and its scalability across hybrid and cloud environments were also critical factors. Additionally, customers valued the ability to enforce granular and just-in-time access controls and the strengthened endpoint security posture through least privilege enforcement.

Collectively, these capabilities positioned CyberArk EPM as a foundational element of the participants' broader cybersecurity and governance strategies. Study participants elaborated on these factors:

Tool consolidation (healthcare):

"My organization used CyberArk in other forms and realized that we did not have a single source for endpoint privilege management, which was complicated. We decided to add CyberArk EPM to our CyberArk suite to address this challenge."

Better access and administration control (manufacturing):

"My organization selected CyberArk EPM because we did not have the ability to implement just-in-time access and lacked the granular control of administrative access that we needed. We also lacked any form of auditing to track who had access, what they had access to, and why."

Endpoint security control (travel):

"Prior to adopting CyberArk EPM, my organization was faced with challenges related to endpoint security. Users with development roles and responsibilities did not have good security control on their elevated privileges on laptops, desktops, and workstations. Most of them had local admin rights on their machines, which was a big red flag."

Scalability and extensibility (transportation):

"My company has been partners with CyberArk for a long time. When we looked for an endpoint management tool, we knew that CyberArk would help us meet our overall information security control standards and regulations at scale. We viewed CyberArk as a best-of-breed partner that would provide us extensibility across our entire enterprise."

Constant evolution of tools (professional services):

"There were two reasons why my organization chose CyberArk EPM: security posture and IT help desk efficiency. With CyberArk, our company has always been rock solid, so we added EPM. As they've grown over the years that we have been using them, they've done a great job of following the threat model. Whenever something pivoted, they had a solution, or they acquired a solution and did a great job of integrating all the tools to work together, which is rare."

Strengthened cybersecurity (travel):

"A big benefit of CyberArk EPM is in the area of audit and compliance. We have audit logs and documentation of the access developers have. It's a very controlled and secured environment. The type of software that is available to the developers, because of this EPM solution, is very controlled; they just can't download anything from the internet. We also no longer have tons of vulnerabilities coming up every month."

Table 2 illustrates that organizations using CyberArk EPM reported that they were supporting an average of 34,729 internal staff and managing 2,361 business applications through the platform. The solution was deployed across a wide range of endpoints, with an average of 38,671 Windows endpoints and 7,300 macOS endpoints. This table reflects CyberArk EPM’s ability to support large, complex environments with diverse endpoint needs.

TABLE 2
Organizational Usage of CyberArk EPM

CyberArk EPM Environment	Average	Median
Internal staff supported	34,729	30,000
Business applications	2,361	513
Window endpoints	38,671	27,000
MacOS endpoints	7,300	500

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Business Value and Quantified Benefits

Participants consistently reported significant improvements in security posture, compliance readiness, and IT productivity resulting from their use of CyberArk EPM. Importantly, the solution enabled centralized, policy-based management of users’ privileges on endpoints, automated credential rotation, and reduced over-privileged accounts. These capabilities helped organizations prevent credential compromise, streamlined help desk operations, and enhanced audit and incident response processes. The platform’s scalability and seamless integration with existing infrastructure were also highlighted as key benefits of adoption.

Study participants made these comments about the most significant benefits resulting from their use of the solution:

Increased security and centralization (healthcare):

“The largest benefit of CyberArk EPM is increased security and ransomware protection. Having central, policy-based management has been big; we no longer have to manage privilege accounts on a per-device basis.”

Single point of truth (healthcare):

“It has been a huge benefit for my organization that CyberArk EPM is our single source of truth for privilege management to enforce within endpoints.”

Scalability from one tool (transportation):

“The biggest operational benefit from using CyberArk EPM for our company is the scalability to meet a myriad of different use cases with one tool of control.”

Easy scalability (travel):

“My organization was going through some mergers and acquisitions while rolling out CyberArk EPM, and the timing couldn’t have been better. It was very easy to scale CyberArk EPM during all that change — it was simple to deploy and move across different endpoints and workstations. Being able to handle that right from the start of integration made a big difference.”

Prevention of credential compromise (manufacturing):

“A significant benefit of CyberArk EPM is that it provides my organization with better prevention of compromised credentials and ensures that we have an additional layer of protection on each endpoint. There is peace of mind knowing that if a device is lost or stolen that it cannot be compromised.”

Automated password rotation (CPG):

“My organization has about 100,000 user-facing endpoints, each with an admin account and [unique] password. With CyberArk EPM, those passwords get automatically rotated within five hours of being used. It’s all automated, which saves a ton of time and effort compared to doing it manually.”

Figure 1 (next page) presents IDC’s calculation of the cumulative benefits participants achieved from adopting CyberArk EPM. Factoring in deployment time, organizations realized \$3 million in average annual benefits (\$56,000 per 1,000 managed endpoints), with gains distributed across security and compliance, IT efficiency, and business enablement.

Common Areas of Value Achieved by Study Participants:

Security and compliance:

Organizations reported that CyberArk EPM reduced the risk of compromised endpoints by supporting key tasks such as continuous authentication, step-up authentication, multi-factor authentication (MFA), and audit readiness.

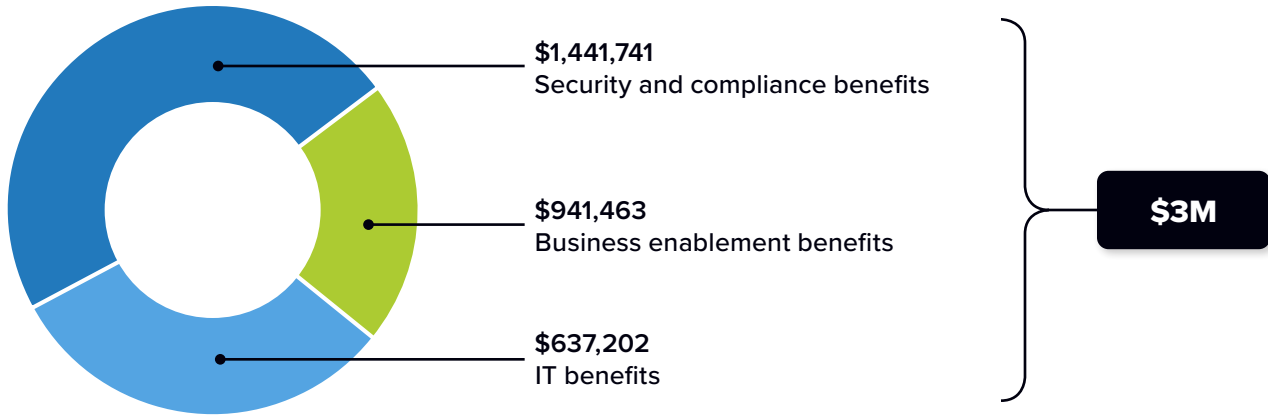
IT efficiency:

The solution eased the burden of discovery and access for cloud, infrastructure, and asset managers by increasing visibility and automation and lowering IT costs.

Business enablement:

End-user productivity was enhanced through seamless privilege management and reduced downtime.

FIGURE 1
Average Annual Benefits per Organization
 (\$ per interviewed organization)



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Interviewed organizations found that CyberArk EPM helped IT cloud, infrastructure, and asset management teams streamline operations by centralizing control and simplifying policy enforcement across diverse environments. The solution made it easier to manage credentials, deploy updates, and maintain visibility into endpoint activity. These capabilities often helped IT make strategic decisions regarding devices and subscriptions and reduced manual labor. Additionally, participants reported that CyberArk EPM also improved IT help desk operations. The solution reduced dependency on IT intervention because there were fewer escalations and more efficient workflows as a result of functions such as just-in-time privilege elevation.

Study participants elaborated with these supporting comments:

Self-service capabilities (professional services):

“From the IT standpoint, CyberArk EPM gives end users the ability to install, uninstall, and change network connection settings without having to go through the IT department to get it done.”

Decreased software costs (manufacturing):

“My organization is saving about \$50,000 a year with CyberArk EPM. It helps us identify machines that are not being used and, as a result, not pay for that software anymore.”

Easier asset management (transportation):

“My organization has derived the most value from CyberArk’s EPM’s scalability across the entire organization; it is easier to manage [local administrator] passwords and deploy updates to endpoints. Additionally, CyberArk provides more insights into our privilege access space. It helps IT and asset managers make decisions more clearly.”

Help desk impact (professional services):

“My organization considers CyberArk EPM one of our crucial pillars of defense. We have changed a lot of layers of defense, and, as a result, we have seen less impact on the help desk because there has been a decrease in malware.”

Reduced help desk escalations (healthcare):

“There has been a reduction in help desk escalations.”

Table 3 highlights the annual IT cost savings that organizations achieved using CyberArk EPM. These savings were attributed to CyberArk EPM’s ability to identify unused machines and software, allowing companies to eliminate unnecessary licensing and subscription costs. Specifically, the interviewed organizations reported an average of \$24,167 in annual third-party software subscription savings.

► **TABLE 3**
IT Cost Savings

IT Cost Savings	With CyberArk EPM
Annual third-party software subscription savings	\$24,167

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IDC next quantified the impact of CyberArk EPM on cloud, infrastructure, and asset management roles. Participants found that the solution provided a number of enhancements for the teams, including visibility improvement, simplified discovery, stronger control over endpoint privileges, automated local administrator credentials rotation, secure access, and policy-based management. These capabilities enabled IT teams to operate more effectively and focus on strategic business initiatives. The accompanying quote from a manufacturing organization reinforces this impact: *“With the free time provided by CyberArk EPM, our IT staff can focus more on digital transformation from on prem to the public cloud and application modernization.”*

Table 4 quantifies these anecdotal observations in terms of efficiency. After adoption, interviewed companies found that IT recognized a 27% efficiency gain, in that this team needed 6.8 fewer FTEs with CyberArk EPM to manage their IT environment — including cloud, assets, and infrastructure. This further illustrates that these highly skilled individuals have had their time freed to scale to support organizational growth and otherwise drive innovation. This efficiency gain was valued at \$682,053 in staff time per year.

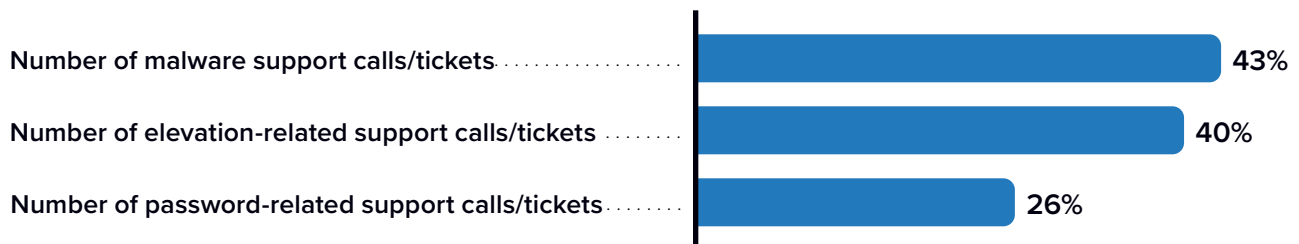
► **TABLE 4**
IT Infrastructure Team — Efficiency Gain

IT Infrastructure Team	Before CyberArk EPM	With CyberArk EPM	Difference	Benefit
Total FTE count	25.0	18.2	6.8	27%
Value of staff time per year	\$2,498,720	\$1,816,667	\$682,053	27%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Figure 2 focuses on the impact of CyberArk EPM on help desk operations, emphasizing its role in reducing endpoint-related support issues. Organizations reported that the solution significantly decreased the risk of malware and streamlined privilege management through features such as just-in-time privilege elevation. These capabilities helped reduce the number of escalations and support tickets, allowing help desk teams to operate more efficiently and focus on higher-value tasks.

► **FIGURE 2**
Help Desk Operations Impact
 (Percentage reduced)



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Security and Compliance Benefits

IDC next focused its analysis on the impact of CyberArk EPM on security, risk, and compliance. Study participants reported that the solution strengthened security and compliance efforts by enabling organizations to enforce privilege access across endpoints and eliminating the risk of users holding standing administrative rights. This removal of local admin rights — often a requirement in many regulations and compliance frameworks — was a key benefit that the participants cited. Organizations also benefited from the detailed audit logs, enforcement of least privilege, and process-level visibility. These functions allowed security teams to monitor activity and respond to threats with greater precision. Additionally, the platform reduced risk by simplifying privilege elevation and access control when the team was supporting incident response or proactive threat hunting. Compliance teams also benefited from standardized documentation and automated reporting, making it easier to demonstrate adherence to regulatory policies without manual effort or fragmented data sources.

Study participants detailed their security and compliance benefits below:

Detailed log activity (professional services):

“Our security staff gets a tremendous amount of log activity out of the CyberArk EPM agent because it’s looking at every single process. We have the benefit of not needing administrative rights on the endpoint, which prevents a lot of cyberattacks. Also, they can use the logs that are coming out of EPM in a lot of incident response and threat model or threat hunting activities. It is a huge benefit and a plus for the security team.”

Robust reporting (manufacturing):

“CyberArk EPM helps our security people not have to manually elevate privileges and then take them away. It also provides robust reporting on logins, which cuts down on the amount of time they spend auditing and providing documentation.”

Automated password management (CPG):

“CyberArk EPM fully audits access to any server with admin rights. The password is never known by the end user. Every password is different on every machine, and they are automatically managed. It’s a huge reduction in security risk. It’s also just easy for the users. They just log into CyberArk and can connect to what they need.”

Better over-privilege account management (healthcare):

“We got rid of all of our over-privileged accounts with CyberArk EPM!”

Significant risk decrease (healthcare):

“Risk has been reduced pretty significantly with CyberArk EPM, probably by about 50%. It has solved issues where people have more privileges than needed in the past, and, as a result, have accidentally compromised our company.”

IDC validated these statements by first studying the impact of CyberArk EPM on identity and access management (IAM) teams. Organizations reported that features such as passwordless MFA, continuous authentication, privilege elevation, and step-up authentication significantly improved operational effectiveness. The solution and features helped enforce tighter access controls and streamline workflows for the team. Additionally, CyberArk EPM helped the team reduce unmanaged endpoints, such as laptops, desktops, or tablets, which were previously outside the scope of security control. These endpoints often had local administrative rights, lacked consistent policy enforcement, and were not integrated into privileged access workflows or monitoring systems.

As a result, **Table 5** shows that companies interviewed reported that IAM teams had a substantial efficiency gain of 48%. This means that CyberArk freed up the time of 6.8 FTEs that was once spent on very manual and time-consuming work, helping them focus on other security-related initiatives. This efficiency gain was valued at \$678,431 in staff time per year.

While the 48% efficiency gain in IAM teams reflects operational improvements, these gains directly support stronger security outcomes, such as tighter access controls, reduced unmanaged endpoints, and improved audit readiness, making them a critical component of the organization’s overall security and compliance posture.

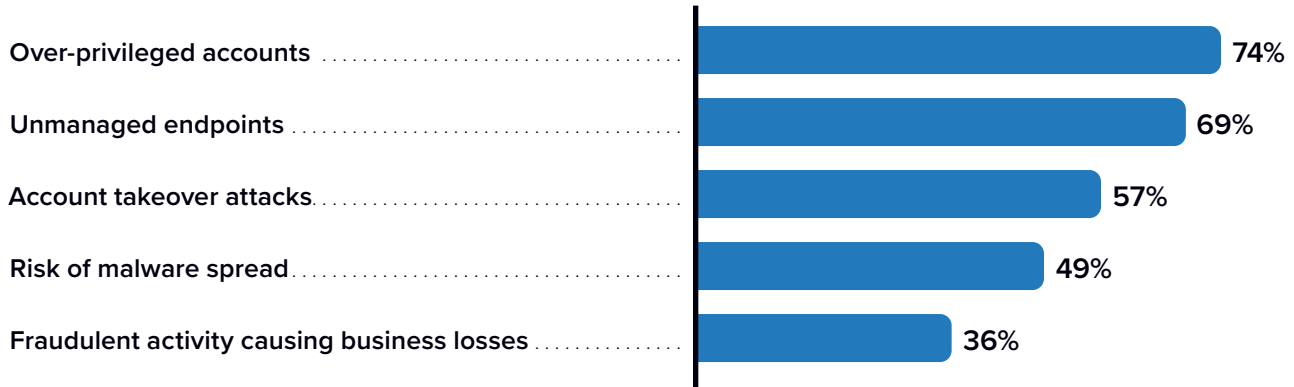
► **TABLE 5**
Identity Access Management Team Efficiency Gain

Efficiency Gain	Before CyberArk EPM	With CyberArk EPM	Difference	Benefit
Total FTE count	14.1	7.3	6.8	48%
Value of staff time per year	\$1,411,765	\$733,333	\$678,431	48%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Figure 3 (next page) presents the security impact of CyberArk EPM, emphasizing its effectiveness in reducing critical risks across endpoints. Organizations reported substantial decreases in over-privileged accounts (74%), unmanaged endpoints (69%), and account takeovers (57%). These metrics highlight CyberArk EPM’s ability to proactively mitigate threats and enforce least-privilege policies across the enterprise, resulting in organizations strengthening their cybersecurity posture and reducing exposure to common attack vectors.

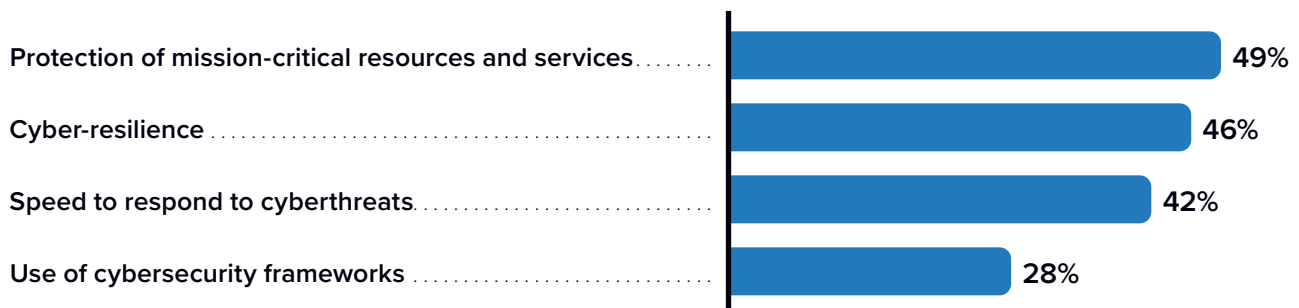
► **FIGURE 3**
Security Impact of CyberArk EPM
 (Percentage reduce)



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

IDC next noted that CyberArk EPM impacted the overall cyber-resiliency of study participants by providing the necessary endpoint frameworks and protections. In fact, **Figure 4** shows that participants reported that the solution increased the protection of mission-critical resources and services by 49%, improved cyber-resiliency by 46%, and increased their speed to respond to cyberthreats by 42%. These improvements stem from the platform’s ability to automate security processes, enforce consistent policies, and provide visibility across endpoints. These metrics underscore the value of CyberArk EPM in not only reducing risk but also in enabling organizations to operate with greater confidence and agility in the face of evolving cyberthreats.

► **FIGURE 4**
Resiliency Impact of CyberArk EPM
 (Percentage increased)



n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

CyberArk EPM significantly enhanced compliance team productivity across interviewed organizations by delivering robust endpoint protection, detailed audit logs, standardized documentation, and compliance-ready security frameworks. The solution helped organizations better adhere to regulatory policies and streamline compliance-related tasks. This ultimately reduced the burden on internal teams. A compelling quote from a travel industry participant underscores the impact: *“Compliance was a major factor when deciding to deploy CyberArk EPM. Without the solution, we would not be able to prove to the auditors that we abide by the relevant policy. We would not be compliant.”* These improvements translated into compliance teams recognizing a 26% productivity gain (Table 6). This gain resulted in 6.3 FTEs being able to work with the equivalent productivity level of having 1.7 additional FTEs on staff. IDC valued this productivity gain at \$115,625 annually.

► **TABLE 6**
Compliance Team Productivity Gain

Compliance Team Productivity Gain	Before CyberArk EPM	With CyberArk EPM	Difference	Benefit
Equivalent productivity level, FTEs	6.3	7.9	1.7	26%
Value of staff time per year	\$437,500	\$553,125	\$115,625	26%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

CyberArk EPM’s ability to automate security processes and mitigate risks also reduced the financial burden associated with compliance and incident response. Organizations reported noteworthy savings through reduced insurance premiums, fewer regulatory fines, and generally less administrative overhead. Customer testimonials reinforce the financial impact. A manufacturing organization noted that *“Using CyberArk EPM ensures a level of security and compliance for my business. Without it, our insurance premiums would be higher, and we would have to pay more for regulatory compliance.”* As shown in Table 7 (next page), this resulted in participants saving \$810,000 per year.

TABLE 7
Annual Operational Cost Savings

Annual Operational Cost Savings	With CyberArk EPM
Annual operational cost savings	\$810,000

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Business Enablement Benefits

Finally, IDC found that CyberArk EPM enabled higher levels of end-user productivity and operational efficiency across the interviewed organizations. The solution enabled end users to work more efficiently by removing friction from everyday tasks that previously required IT intervention. With policy-based access and just-in-time privilege elevation, users gained self-service capabilities to install approved applications, adjust system settings, and connect to networks. Generally, because of the seamless design of CyberArk EPM, most end users were unaware of the underlying security controls, allowing them to focus on their work without disruption. This intuitive approach not only improved access to tools but also minimized downtime and delays. As a result, IDC found that the organizations were more agile and responsive.

Study participants offered these comments about business enablement:

End-user efficiency (professional services):

“A big benefit of CyberArk is that our endpoint users do not know that we are even doing anything to protect their devices. The only time they are aware of CyberArk is if a net new application is being installed from the internet, they will get a CyberArk pop-up that asks for a business justification. It prompts my team to go look at it, evaluate it, and make sure it’s something that we want in the environment. If all those are true, a policy is created that allows others to install as if they were an administrator. It creates a lot of efficiency.”

Seamless end-user security (CPG):

“We get a huge security value from using CyberArk EPM. It is seamless, and the end user doesn’t even know they’re being secure because it is so easy to use.”

Less downtime impact (healthcare):

“CyberArk EPM has reduced the impact of downtime at my organization, which has helped improve productivity of our end users.”

In **Table 8**, IDC quantified end-user productivity gains that resulted from CyberArk EPM’s self-service capabilities, user-friendly nature, and seamless integration. Interviewed organizations reported that end users were able to work with three percent greater productivity, meaning they were working with the equivalent productivity level of having 99.8 additional FTEs on staff. Using standard IDC methodology that factors in a 15% operating margin, it was calculated that end users were able to work with the equivalent productivity level of having a net of 15 additional FTEs on staff, which was valued at \$1,047,455 per year.

TABLE 8
Business Enablement — End-User Productivity

End-User Productivity Gain	Before CyberArk EPM	With CyberArk EPM	Difference	Benefit
Equivalent productivity level, FTEs	3,536	3,635	99.8	3%
Equivalent productivity level, FTEs net	3,536	3,551	15.0	0.42%
Value of staff time per year	\$247,500,000	\$248,547,455	\$1,047,455	0.42%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

ROI Summary

Summing up the financial and business-related benefits from participant usage of CyberArk EPM, IDC calculated an average three-year ROI. As shown in **Table 9** (next page), IDC projects that these companies achieved three-year discounted benefits worth an average of \$7,161,200 per organization through increased staff effectiveness, cost reductions, and business enablement. These benefits compare with the total three-year discounted costs of \$1,912,600 per organization. These levels of benefits and investment costs resulted in an average three-year ROI of 274% and a payback period of seven months.

► **TABLE 9**
Three-Year ROI Analysis

Three-Year ROI Analysis	Per Organization	Per 1,000 Managed Endpoints
Discounted benefits	\$7,161,200	\$133,521
Discounted investment	\$1,912,600	\$35,661
Net present value (NPV)	\$5,248,600	\$97,861
ROI	274%	274%
Payback	7 months	7 months
Discount factor	12%	12%

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Challenges/Opportunities

While CyberArk’s Endpoint Privilege Manager is a mature and feature-rich solution, there are factors that may inhibit broader market adoption. One key challenge is the perceived complexity of deployment and policy configuration. Organizations with limited IT resources may perceive the initial setup — particularly the removal of local admin rights and enforcement of least privilege — as disruptive to user workflows. This can lead to resistance from both end users and IT teams, especially in environments where local administrative flexibility has historically been the norm. This challenge is certainly not unique to CyberArk: Any security offering that requires modification of people and processes faces a similar issue.

From a competitive standpoint, CyberArk faces pressure from vendors offering integrated endpoint security suites that bundle privilege management with EDR, antivirus, and threat detection. These all-in-one platforms may appeal to organizations willing to make compromises as they seek simplicity and agent consolidation. Furthermore, open source and lower-cost alternatives — while less comprehensive — can be attractive to organizations prioritizing cost over value. As the market matures, CyberArk will need to continue demonstrating the unique value of its depth and specialization in privilege security to maintain its leadership position.

Conclusion

Organizations today face mounting challenges in securing endpoints due to excessive user privileges, fragmented access controls, and increasing threats, such as ransomware and credential theft. To help address these issues, CyberArk offers Endpoint Privilege Manager, a solution designed to enforce least-privilege access to applications, automate credential rotation, and streamline policy-based management across diverse endpoint and server environments. IDC's research found that CyberArk EPM delivers both qualitative and quantitative benefits, including improved security posture, enhanced IT and compliance team efficiency, and greater end-user productivity. The solution also reduces operational costs and simplifies audit readiness. For every dollar invested, organizations realized substantial returns, achieving a 274% three-year ROI and recouping their investment within just seven months.

Appendix 1: Supplemental Data

Table 10 presents a summary of IDC’s Business Value calculations as fully described in the previous sections, with total average annual benefits of \$3 million per organization accruing annually.

TABLE 10
Specific Calculations: Benefits from Use of CyberArk EPM

Category of Value	Average Quantitative Benefit	15% Margin Applied	Calculated Average Annual Value
IT cost savings	\$24,167 in annual cost reductions	No	\$24,167
IT infrastructure team — admin and mgmt. efficiency gains	27% higher efficiency worth 6.8 FTEs, \$100,000 salary	No	\$613,036
IAM efficiency gain	48% higher efficiency worth 6.8 FTEs, \$100,000 salary	No	\$609,781
Compliance team productivity gain	26% higher productivity worth 1.7 FTEs, \$70,000 salary	No	\$103,925
Annual operational cost savings	\$810,000 in annual operational cost savings	No	\$728,036
Business enablement — end-user productivity gains	3% higher productivity worth 99.8 FTEs, \$70,000 salary	Yes	\$941,463
Total average annual benefits	\$3M per organization per year		

n = 7; Source: IDC Business Value In-Depth Interviews, July 2025

Appendix 2: Methodology

IDC utilized its standard ROI methodology for this project. This methodology is based on gathering data from current users of CyberArk EPM as the foundation for the model.

Based on interviews with organizations using the platform, IDC performed a three-step process to calculate the ROI and payback period:

- 1. Gathered quantitative benefit information during the interviews using before-and-after assessment of the impact of CyberArk EPM.** In this study, the benefits included IT cost reductions and avoidances, staff time savings and productivity benefits, and revenue gains.
- 2. Created a complete investment (three-year total cost analysis) profile based on the interviews.** Investments go beyond the initial and annual costs of using CyberArk EPM and can include additional costs related to migrations, planning, consulting, and staff or user training.
- 3. Calculated the ROI and payback period.** IDC conducted a depreciated cash flow analysis of the benefits and investments for the organizations' use of CyberArk EPM over a three-year period. ROI is the ratio of the NPV and the discounted investment. The payback period is the point at which cumulative benefits equal the initial investment.

IDC bases the payback period and ROI calculations on a number of assumptions, which are summarized as follows:

- Time values are multiplied by burdened salary (salary + 28% for benefits and overhead) to quantify efficiency and productivity savings. For the purposes of this analysis, IDC has used assumptions of an average fully loaded \$100,000 per year salary for IT staff members and an average fully loaded salary of \$70,000 for non-IT staff members. IDC assumes that employees work 1,880 hours per year (47 weeks x 40 hours).
- The net present value of the three-year savings is calculated by subtracting the amount that would have been realized by investing the original sum in an instrument yielding a 12% return to allow for the missed opportunity cost. This accounts for both the assumed cost of money and the assumed rate of return.
- Further, because CyberArk EPM requires a deployment period, the full benefits of the solution are not available during deployment. To capture this reality, IDC pro rates the benefits on a monthly basis and then subtracts the deployment time from the first-year savings.

Note: All numbers in this document may not be exact due to rounding.

About the IDC Analysts



Frank Dickson

Group Vice President, Security and Trust, IDC

Frank Dickson is the group vice president for IDC's Security and Trust research practice. In this role, he leads the team that delivers compelling research in the areas of AI security; cybersecurity services; information and data security; endpoint security; trust; governance, risk, and compliance; identity and digital trust; network security; privacy and legal tech; and application security and fraud. Typically, he provides thought leadership and guidance for clients on a wide range of security topics, including ransomware and emerging products designed to protect transforming architectures and business models.

[More about Frank Dickson](#)



Megan Szurley

Business Value Manager, Business Value Strategy Practice, IDC

Megan Szurley is manager for the Business Value Strategy practice, responsible for creating custom business value research that determines the ROI and cost savings for enterprise technology products. Szurley's research focuses on the financial and operational impact of these products for organizations once deployed and in production. Prior to joining the Business Value Strategy practice, Szurley was a consulting manager within IDC's Custom Solutions division, delivering consultative support across every stage of the business life cycle: business planning and budgeting, sales and marketing, and performance measurement. In her position, Szurley partners with IDC analyst teams to support deliverables that focus on thought leadership, business value, custom analytics, buyer behavior, and content marketing. These customized deliverables are often derived from primary research and yield content marketing, market models, and customer insights.

[More about Megan Szurley](#)

Message from the Sponsor



Securing Every Identity with the Right Level of Privilege Controls.

CyberArk is proud to support this IDC research, which quantifies the business value of CyberArk Endpoint Privilege Manager (EPM) as part of a broader identity security strategy.

As organizations face increasing pressure to reduce risk while improving operational efficiency, EPM helps enforce least privilege at scale—without disrupting user productivity.

We extend our sincere thanks to the customers who generously shared their time, insights, and experiences. Their contributions were instrumental in shaping this study and validating the real-world impact of EPM.

The findings reflect what we hear from customers every day: that proactive endpoint privilege management is a critical enabler of both security and agility. Our support for this research underscores CyberArk's vision of securing every identity with the right level of privilege controls. We hope this report provides useful insights as you evaluate how to protect your endpoints and empower your teams.

[Take the CyberArk EPM interactive product tour](#)

IDC Custom Solutions

IDC Custom Solutions produced this publication. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis that IDC independently conducted and published, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. This IDC material is licensed for external use and in no way does the use or publication of IDC research indicate IDC's endorsement of the sponsor's or licensee's products or strategies.



IDC Research, Inc.
140 Kendrick Street, Building B, Needham, MA 02494, USA
T +1 508 872 8200

[idc.com](https://www.idc.com)

[in @idc](https://www.linkedin.com/company/idc)

[X @idc](https://twitter.com/idc)

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. With more than 1,300 analysts worldwide, IDC offers global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries. IDC's analysis and insight helps IT professionals, business executives, and the investment community to make fact-based technology decisions and to achieve their key business objectives.

©2025 IDC. Reproduction is forbidden unless authorized. All rights reserved. [CCPA](#)