



Keeper Security Insight Report
Privileged Access Management Survey
User Insights on Cost & Complexity

Research finds PAM solutions are too complex with 68% of organizations paying for “wasted features” that are rarely used

*A global survey of 400 IT and security executives conducted in January 2023, by Keeper Security in partnership with TrendCandy Research, reveals an overwhelming industry desire for Privileged Access Management (PAM) solutions that are easy to deploy and maintain. The findings show that traditional PAM solutions are falling far short, largely because they are too complex to implement and use. An overwhelming **84% of IT leaders** said they want to simplify their PAM solution in 2023.*

In the current high-risk security climate, it is imperative that all organizations secure their privileged credentials, privileged accounts and privileged sessions to protect their crown jewels. However, many traditional PAM solutions are failing to provide their intended value outside of these core use cases, because deployment is either too complex, too cost-prohibitive, or both. In the era of remote work, organizations need agile identity security solutions that can protect against cybersecurity threat vectors by monitoring, detecting, and preventing unauthorized privileged access to critical resources.

Keeper Security, a leading innovator in privileged access management, wanted to better understand how IT leaders are thinking about PAM, deploying their PAM solutions, and streamlining their PAM implementations. Keeper commissioned an independent research firm to survey 400 IT and data security leaders in North America and Europe about their strategies and plans for PAM in 2023.



User feedback

PAM solutions fall short

Privileged access management solutions are primarily designed to protect IT staff, executive leadership, and research and development staff, however, the accelerated digital transformation and ceaseless barrage of cyberthreats is making it increasingly important to protect all end-users within an organization.

PAM adoption is widespread throughout businesses today, with 91% of survey respondents saying their organizations already use some type of PAM solution. Yet, the desire for simplicity is pervasive, with 87% of respondents saying they would prefer a “pared down” form of PAM that is easier to deploy and use. In addition, 58% of respondents said there is definitely or probably some waste in their PAM solution and 84% said they would definitely or probably want to simplify their PAM solution in 2023.




More than nine in ten IT leaders (91%) said their PAM solution has given them more control over privileged user activity. However, a large majority of organizations (85%) added that their PAM requires a dedicated staff to manage and maintain. Furthermore, these solutions often only protect a small portion of the organization’s user base, while additional solutions must still be purchased to protect non-privileged users. As a result of these expenses, nearly two-thirds of IT leaders (62%) say the downturn in economic conditions will likely cause them to scale back their current PAM solutions.

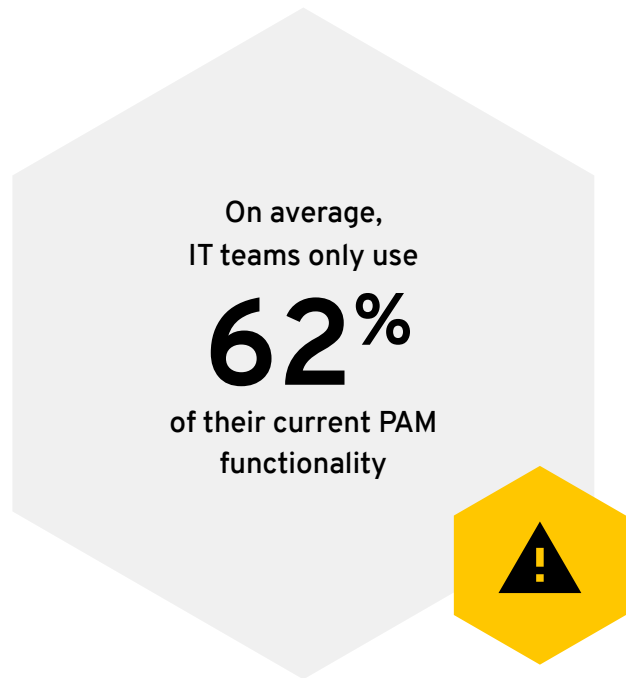


87%

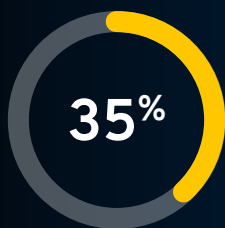
of respondents say they would prefer a “pared down” form of PAM that is easier to deploy and use

The survey found that more than half of all IT teams (56%) reported they had tried to deploy a PAM solution, but did not fully implement it. Of those, a staggering 92% said it was because their PAM solution was too complex to fully implement. This indicates a strong desire among respondents for the core functionality and benefits of PAM, but with simpler provisioning and more rapid deployment. Other notable highlights included:

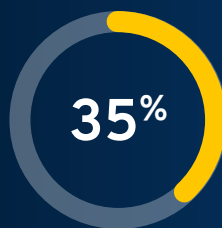
-  More than two-thirds of IT managers (68%) said their current PAM solution is too complicated or has too many features they don't need.
-  On average, IT teams only use 62% of their current PAM functionality.
-  Two-thirds of IT leaders (66%) said they need a better PAM solution, but 58% said they do not have one because it is too expensive.



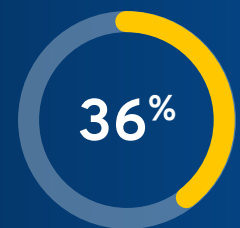
Roughly two-thirds of survey respondents also indicated that pricey and superfluous PAM features create too much complexity for users, reducing user satisfaction regardless of the organization's size



of IT leaders overall are highly satisfied with their current PAM solution



of IT leaders at large enterprises are highly satisfied with their current PAM solution








of IT leaders at mid-market organizations are highly satisfied with their current PAM solution

Organizations seek new solutions to meet operational challenges

In the post-pandemic workplace, the future of work will continue to be hybrid. And, as the network perimeter has expanded far beyond the confines of the office, IT professionals and, particularly, decision makers will need to recognize the critical importance of network monitoring and management for security purposes. Security leaders will have to develop IT strategies that streamline Software-as-a-Service (SaaS) applications, Wi-Fi connections and end-user experiences across their organizations.

To help get there, these survey results suggest that IT and security leaders have a strong interest in adopting a PAM solution that can protect their most sensitive systems, without the cost and complexity of traditional PAM products. Their top criteria included solutions that are quicker to deploy, more affordable, and simpler to understand and integrate. They also said they want smaller-scale PAM solutions that are easier to maintain and with fewer unnecessary features that drive up costs.

Based on the survey results, the top five benefits that IT leaders seek in a PAM solution include:

-  Managing and monitoring privileged user access
-  Preventing data breaches
-  Protecting against compromise of privileged credentials by external threat actors
-  Protecting against accidental or deliberate misuse of privileged access by company insiders
-  Ensuring privileged user access is updated to prevent “privilege creep”



In addition, respondents shared the top five benefits of a simplified PAM solution



Easier to deploy



Easier to integrate into other systems



Cost savings



Consolidated platform



Requires less staff

Conclusion

Companies should replace ‘traditional PAM’ with a unified solution

These survey findings illuminate why users have become so dissatisfied with traditional PAM products, which are becoming increasingly expensive and difficult to use. Traditional PAM solutions can require expensive on-premises management, are time-consuming to deploy and unable to monitor and protect every user, on every device, from every location. Respondents seek a unified PAM solution that provides complete visibility, security, control, compliance and reporting across the organization.

The concept of zero trust is foundational to an effective PAM solution, and a strict zero-knowledge approach is increasingly important as SaaS becomes the preferred deployment method for organizations. A zero-knowledge architecture protects user data from both attackers and vendors – everything is encrypted client side – ensuring that even vendor compromise or insider threats are mitigated. However, most traditional PAM solutions do not strictly adhere to zero-knowledge principles. Organizations are increasingly interested in protecting all users credentials – not just for privileged users. A zero-trust and zero-knowledge security platform provides organizations total visibility and control over all employee credential practices.

The digital landscape keeps evolving beyond the average IT professional’s control, and it will only continue to do so as technology advances and the workplace changes. The rapid digital transformation of organizations in response to the newly remote hybrid workforce has focused attention squarely on this central concern: You cannot secure what you cannot see. To maintain visibility and stay ahead of the next wave of cyberthreats, IT and security leaders will have to adapt, automate, and advance along with the ever-changing workplace.