Securing your enterprise with Identity Governance and Privileged Access Management (PAM) integration

Introduction

A recent study by Forrester Research unveiled a direct correlation between data breaches and the immaturity of organizations' Identity and Access Management (IAM) systems. The study found that organizations with mature IAM functions experience half the number of breaches that less mature companies experienced.[1] A key marker of IAM maturity is the use of an integrated platform approach for IAM, specifically Identity Governance, along with Privileged Access Management (PAM) technologies to streamline operations in order to better develop consistent access control policies and achieve operational efficiency.

This white paper references findings from a 2019 survey of 209 organizations which were asked about Identity Governance and PAM integration[3]. It describes best practices for integrating both types of solutions and highlights the risks/ challenges faced by organizations that have not properly integrated Identity Governance and PAM solutions in order to provide a unified view of users'access.

pwc SailPoint CYBERARK

An overview of Identity Governance and PAM integration

Enterprises have become increasingly reliant on digital information to meet business objectives, effectively manage operations and compete in a digitally connected world. This includes tasks like migrating to the cloud, managing a growing internet of things, increasingly relying on developers and more. The ever-growing digital ecosystem demands that organizations transform their identity programs to protect and monitor critical data and systems from cybersecurity threats. Identity governance solutions enable organizations to securely perform business operations by granting users and applications access to digital assets which is reviewed periodically for appropriateness and ongoing use.

Certain users, such as IT systems administrators, require elevated or privileged rights to access critical yet sensitive systems, applications and data across the enterprise in order to do their jobs and maintain business continuity. However, this type of access can pose a serious threat if misused or compromised. Forrester Research estimates that 80 percent of security breaches involve theft of privileged credentials.[2] Adversaries often target these types of privileged accounts to gain a foothold within a corporate network and infiltrate systems across the enterprise. They typically do so through the use of phishing schemes designed to obtain user credentials from insiders such as employees and third-party business partners – including suppliers, consultants and contractors.

A staggering 80 percent of the survey's respondents said they had experienced cases of privileged access being incorrectly or over-assigned.[3] The risks of poorly managed privileged accounts are significant and can include unauthorized exposure to sensitive data, alteration of files, and downtime of critical systems and applications. Integrating Identity Governance and PAM solutions can help organizations to mitigate these risks.

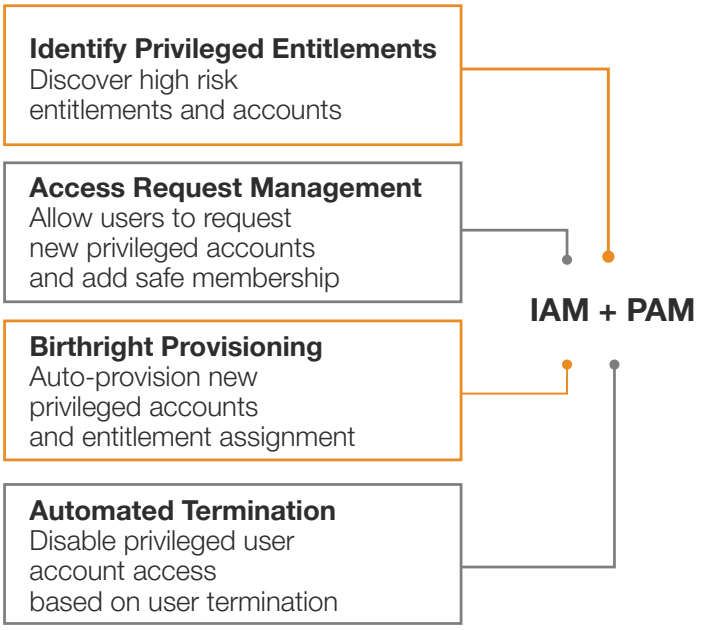
An integrated approach

Many organizations have invested heavily in identity technologies and processes to address risks, compliance and operational gaps associated with the management of digital identities and access. But as adversaries develop increasingly sophisticated attack techniques, businesses have been forced to reassess the capabilities of their identity solutions. While all components of IAM should be under consideration, a rash of breaches involving privileged credentials has increased the focus on securing the access rights of privileged users.

To protect data from internal and external threats, organizations will need to manage the entire lifecycle of privileged accounts and credentials. Despite the rising frequency of the compromise of privileged accounts, many organizations lack the mature capabilities needed to effectively manage privileged access. This has compounded the risk of compromise. Some organizations, for instance, have purchased solutions but haven't developed corresponding processes and governance to make them effective. Others may have good processes in place but lack the enabling technologies needed to address privileged access risks at an enterprise scale. Some organizations have implemented both Identity Governance and PAM solutions, but many have not integrated the two.

Of the survey respondents, 72 percent had implemented an IAM solution and 83 percent had implemented a PAM solution. However, over three quarters (77 percent) reported that they had not integrated the two solutions. This practice can result in inconsistent access processes and policies across silos of tools, leading to faulty reporting and failed audits.

Regardless of their IT maturity, organizations should integrate Identity Governance and PAM to effectively manage both privileged and non-privileged user access requests, approvals, certifications, provisioning and remediation.

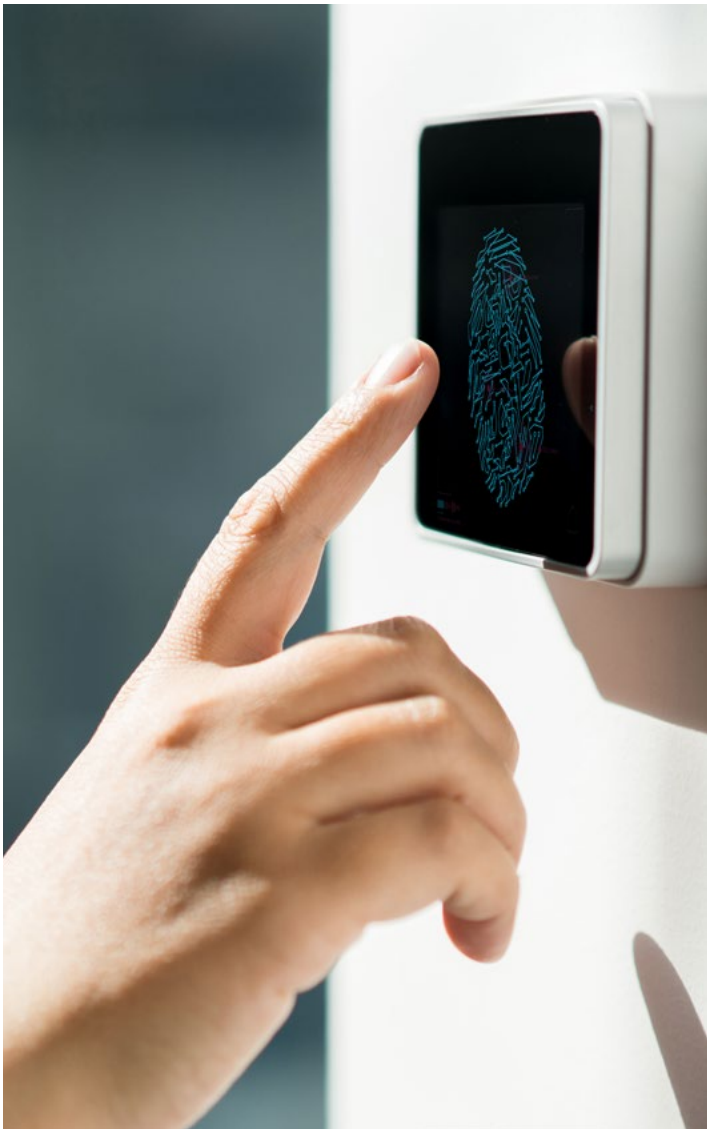


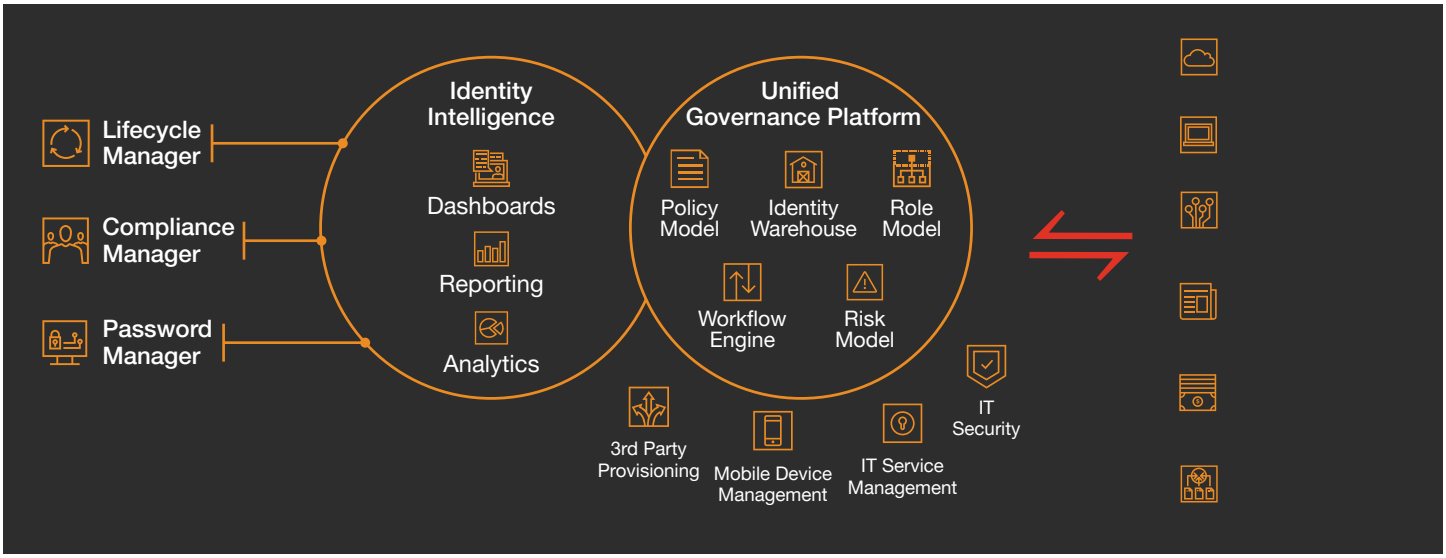
Enabling technologies

The SailPoint Identity Governance Solution

SailPoint, a global leader in Identity Governance, provides an open Identity Governance platform that helps organizations manage access across the enterprise, including on-premise and cloud-based systems and applications. The SailPoint platform comprises components catering to various Identity Governance needs, including:

- **Compliance Management**, for access certifications, access policy management, auditing and reporting.
- **Lifecycle Management**, for access request and provisioning, password management and lifecycle events processing.
- **Advanced PAM Integration**, which enables advanced governance controls such as auditing, approvals, and policy checking. Reviews of privileged access can also be viewed and centrally managed from the Identity Governance platform.





The CyberArk Privileged Access Security Solution

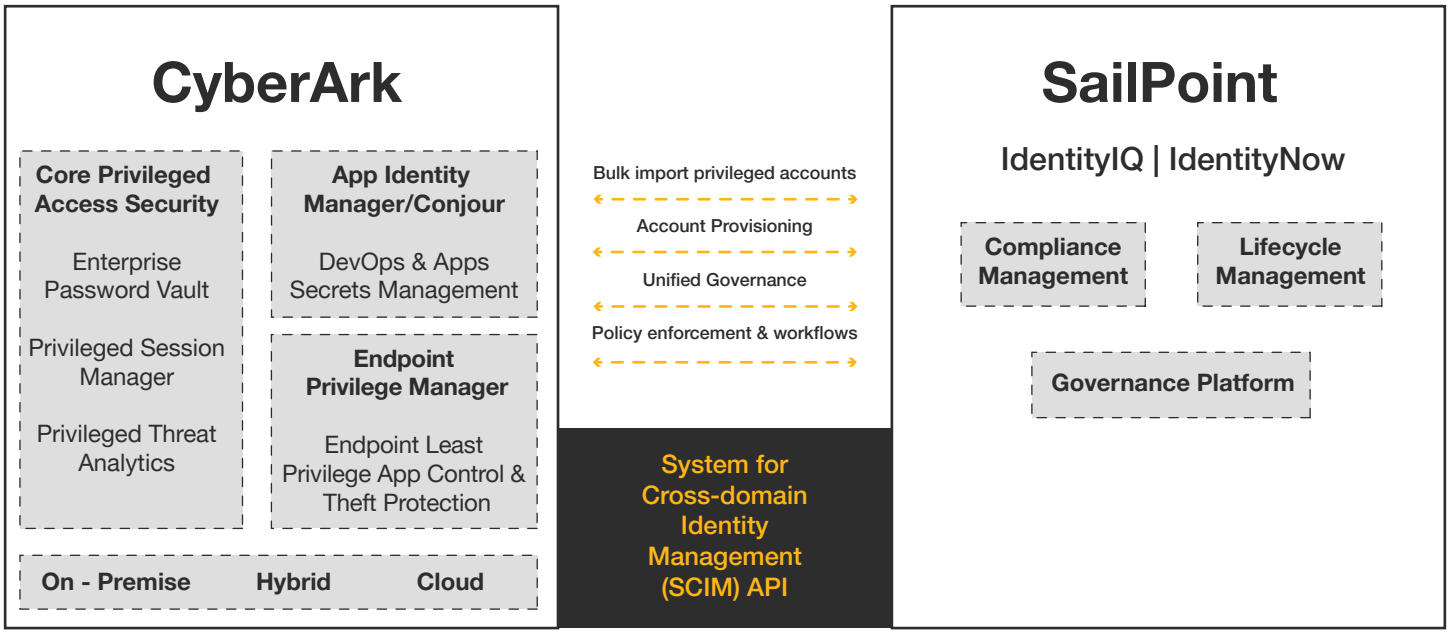
CyberArk, a global leader in Privileged Access Management, provides organizations with the ability to manage and secure privileged access for individuals and applications. The solution secures credentials like passwords, secrets and SSH keys, controls account access, and isolates, records and monitors privileged sessions for auditing and forensics analysis. The CyberArk Privileged Access Security Solution is based on the CyberArk Shared Technology Platform, which combines an isolated vault server, a unified policy engine and a discovery engine to help provide continuous scalability, reliability and security for privileged accounts.

CYBERARK PRIVILEGED ACCESS SECURITY SOLUTION

ENDPOINT PRIVILEGE MANAGER	CORE PRIVILEGED ACCESS SECURITY	APPLICATION ACCESS MANAGER
Least Privileged and Credential Theft Protection for Workstations	STANDARD Risk-based Credential Security and Session Management to Protect Against Attacks ALERO Remote Vendor Access to CyberArk ADVANCED Least Privileged Server and Domain Controller Protection	Secures Management for Applications, Tools, Containers and DevOps
ON - PREMISES	HYBRID	CLOUD

Integrating SailPoint and CyberArk

SailPoint and CyberArk have partnered to provide an integrated, centrally managed solution. This seamless integration with the CyberArk Privileged Access Security solution is done via a SCIM-based integration model. This allows critical identity information to be shared between the two solutions.



A much bigger risk than reward?

One of the key components of the SailPoint cloud open identity platform is the ability to integrate with and govern a host of enterprise applications and directories including Active Directory, database systems, HR systems, and more, regardless of whether they are in the cloud, on-premise or a hybrid of both. This integration usually requires creating a service account that will authenticate to each target application in order to read identity information.

Most of the time, these service accounts are given elevated privileges to create, modify and delete accounts in the target applications. However, as critical enterprise applications are increasingly onboarded into the IAM platform, these accounts make for high-value targets for threat actors.

One survey respondent mentioned a concern, saying, “Integration causes an issue related to segregation of duties; admins in IAM tool can provide themselves with access in the PAM tool.” The solution to this valid concern is to develop and apply IAM and PAM implementation best practices such as the following:

- Record and actively monitor all privileged sessions and/or commands.
- Conduct periodic access review for administrative and privileged users.
- Limit access for remote administrators, contractors and outsourced parties.
- Automatically deprovision privileged users' access as they terminate.
- Do not allow shared administrative accounts and limit administrative access.
- Implement least-privilege access for administrators.
- Automate role-based provisioning to apps and infrastructure.

In addition to the above, the CyberArk PAM platform provides credential cycling capability, a feature that allows applications which require credentials (such as username and password) to obtain that information directly from CyberArk. This feature can significantly reduce the risk that an admin will be able to provision rogue accounts on target applications.

Key drivers and benefits

Ninety percent of the survey's respondents said they were concerned that the lack of a unified access policy across all accounts was creating an inconsistent access experience for users3. An integrated IAM and PAM implementation can correct this issue and can enable businesses to securely manage identities, quickly respond to incidents and help facilitate regulatory compliance. It can also help automate real-world business use cases involving the management of privileged accounts. Some of these use cases include:

- Discovering privileged accounts and credentials configured in the PAM application which can be effectively managed through the IAM solution.
- Implementing a unified, policy-driven approach to IAM across all users.
- Automatically provisioning new privileged accounts by using role-based access provisioning or provisioning policies configured in the IAM solution.
- Leveraging user profile attributes such as title, business unit and job profile to grant appropriate access to privileged accounts.
- Automating periodic access reviews for privileged accounts.
- Automating and enforcing segregation of duties (SOD) policies across privileged and non-privileged accounts.
- Automating terminations of privileged accounts access based on user separation or termination events as processed by the IAM solution.

Implementation of these use cases can help businesses gain enhanced visibility into privileged accounts by accessing account data directly from the IAM solution.

Conclusion

In today's digital business ecosystem, organizations face increasingly sophisticated cybersecurity threats that often target insiders, including employees and third-party business partners. Many organizations are attempting to address these threats by implementing solutions to govern access for both privileged and non-privileged users. However, this approach is not as effective as it could be if the two technologies were integrated, providing a more holistic view of and approach to managing users and administrators who possess access across both realms. The integration of solutions such as CyberArk and SailPoint can enable an organization to further reduce such inherent risks through the use of automated controls.

References

1. A commissioned study conducted by Forrester Consulting on behalf of Centrify, December 2016
2. Cser, Andras, “The Forrester Wave™: Privileged Identity Management, Q3 2016”
3. Survey conducted by SailPoint and CyberArk, September 2019

Further information

For more information about successfully integrating IAM and PAM visit:

PwC - https://www.pwc.com/us/en/services/consulting/cybersecurity.html
SailPoint - https://www.SailPoint.com/
CyberArk - https://www.cyberark.com/

pwc.com