SailPoint

SOLUTION BRIEF

Extending Identity Governance **to Highly Privileged Accounts**

Organizations have long known the value of identity governance and privileged account management programs; they are foundational elements of any modern security strategy. Even as the maturity of these programs progress, they are often independent activities. Yet security silos increase risk while decreasing productivity, and can ultimately result in noncompliance with regulations. Organizations are now realizing the security and productivity benefits of integrating identity governance and privileged account management programs together.

Increased Security Risk

When privileged account management is independent of identity governance, these uniquely sensitive accounts suffer from typical problems associated with a lack of governance. The number of orphaned or unused privileged accounts rises. Privileged entitlement creeps into non-administrative accounts. Privileged access is mistakenly granted to people who do not need or should not have it. A lack of governance leads to these effects and elevates risk to the business as a result.

Decreased Productivity

Productivity is also negatively affected by a dividing wall between identity governance and privileged account management. Employees requiring access to privileged accounts find themselves having to wait to gain access due to manual administration being used in place of the integrated and automated provisioning identity governance processes provide.

The combination of elevated risk and reduced productivity can be avoided through a modern unified security strategy that includes the integration of identity governance and privileged account management.

80%

of security breaches involve privileged credentials, according to Forrester[1]

[1] The Forrester Wave™: Privileged Identity Management, Q3 2016

Integrating Identity Governance and Privileged Access

By integrating privileged access and identity governance solutions, organizations can holistically manage access to privileged and non-privileged accounts. The SailPoint IdentityIQ Privileged Account Management (PAM) integration module extends identity governance process and control to highly privileged accounts, allowing enterprises to break down management silos and enforce consistent business processes and policies for better oversight and risk mitigation.

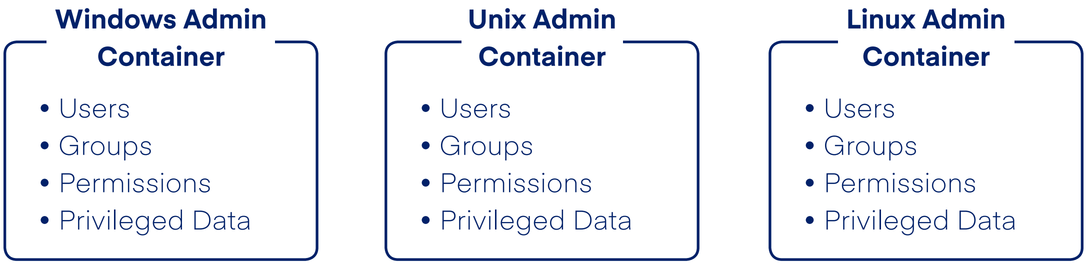
The IdentityIQ Privileged Account Management (PAM) integration module extends the value of SailPoint's open identity platform by allowing organizations to:

1

Establish Complete 360-degree Visibility and Governance Over Privileged Accounts

Identity governance processes can now encompass privileged accounts and access. Accounts with elevated or advanced access are subject to the full spectrum of identity governance – lifecycle management, certification, access request, and higher-order security policies such as separation of duties. Organizations may now apply the full spectrum of security controls over privileged accounts from a single pane of glass.

Additionally, identity governance now understands key privileged access management concepts such as containers or vaults. These containers hold privileged data (often privileged account credentials), the users and groups allowed to access this data, and the access control lists that describe the exact permissions of each user or group. This allows for context around permissions granted to users or groups on these containers, ensuring that only the proper access to privileged accounts is granted as needed.



Windows Admin Container

- Users
- Groups
- Permissions
- Privileged Data

Unix Admin Container

- Users
- Groups
- Permissions
- Privileged Data

Linux Admin Container

- Users
- Groups
- Permissions
- Privileged Data

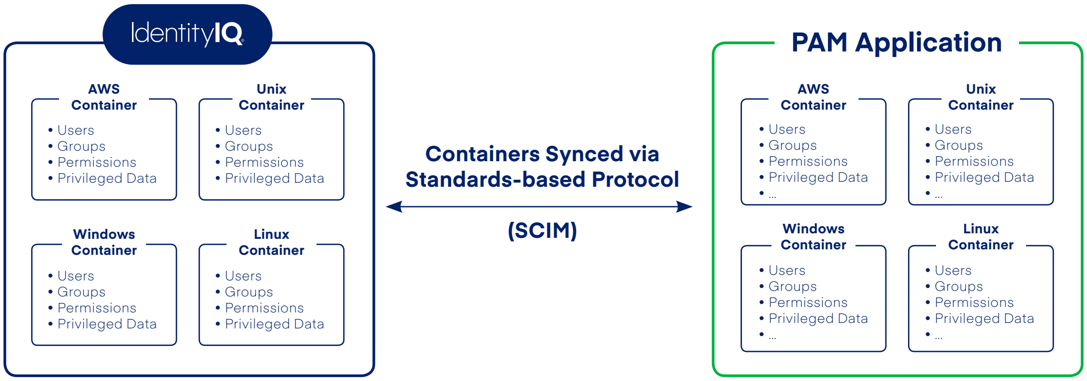
2 Simplify and Centralize Administration of Privileged Accounts

Administration of privileged account management is also simplified. A single point of administration allows business staff to request, approve, grant, and certify access to privileged accounts just as they do with other identity-related activities. The familiar business-oriented interface provided by IdentityIQ ensures streamlined governance of these sensitive accounts.

Rather than contacting disparate parties to discuss access needs and communicating across different parts of the organization to gain access to needed resources, employees now only need to leverage existing, centralized identity governance processes. IdentityIQ is already optimized to quickly handle provisioning or any life cycle processes, gathering approvals, and performing other security policy checks rapidly and efficiently.

3 Integrate with Leading Third-party PAM Solutions

Rather than integrating on a vendor-by-vendor basis, SailPoint worked with leading privileged account management vendors to establish a PAM extension to the widely adopted System for Cross-domain Identity Management (SCIM) standard protocol. This ensures that businesses can utilize whatever PAM vendor they choose. SailPoint Identity+ Alliance PAM Vendors such as BeyondTrust, CyberArk, and Thycotic are a few examples of vendors leveraging the benefits of the integration with SailPoint IdentityIQ.



Since the integration relies on the extended SCIM standard, it follows the same direct logical path regardless of the PAM vendor. Rapid deployment is possible by integrating with any PAM vendors implemented in the enterprise, and migrating from one PAM vendor to another will not harm the integration with SailPoint's IdentityIQ. Additionally, the use of standards ensures that the integration is free from product version conflicts and upgrades will not need to be made in unison. The use of open standards and industry-driven cooperation provides a stable foundation for a deep integration between the two programs.

Enhance Security and Productivity by Extending Identity Governance to Privileged Accounts

Organizations in today's accelerating business environment must wield the security and productivity benefits from expanding identity governance to include privileged accounts. Thanks to SailPoint's IdentityIQ Privileged Account Management (PAM) integration module, businesses can gain visibility into these special accounts, govern them from a centralized location, rapidly grant access to ensure productivity, and do all of this through the use of accepted industry standards which reduce implementation time and cost.

Additionally, organizations can improve security and administration efforts with out-of-the-box credential cycling that enables privileged account management solutions to store and manage IdentityIQ service account credentials, retrieving them only when performing identity tasks. Enterprises can eliminate the silos of operation within their organization, extend identity governance to encompass privileged account management and bring the full power of identity to reduce security risk and boost productivity.