SailPoint

SOLUTION BRIEF

Secure Your Enterprise with the Powers of Identity and Privilege

Presented with

CYBERARK

Keeping organizations secure, while improving business and user productivity in today's accelerating threat environment, continues to be a challenge for today's IT leaders. As we have seen time and time again, cyber attacks such as the Equifax, WannaCry and NotPetya have demonstrated their ability to change the global business environment in an instant.

As organizations adopt cloud first, IoT and mobile strategies, their attack surface widens and provides new pathways for attackers to exploit unprotected businesses. Once the attackers get in, they seek access to the heart of the enterprise with the intent to cause costly harm that can include damaged reputations, financial losses and stolen intellectual property.

Forrester estimates that 80 percent of security breaches involve privileged credentials.

Organizations have long known the value of identity governance and privileged account management programs; they are foundational elements of any modern security strategy. However, these programs are often set up as independent activities, creating security silos that increase risk while decreasing productivity, and can ultimately result in noncompliance with regulations. Standalone solutions for both types of users lack the ability to enforce a unified access policy and consistent governance, provisioning and authorization processes. This can result in access violations and regulatory action.

To avoid these issues, organizations must have a single, automated, policy-based process for privileged and non-privileged users to effectively manage access requests, approvals, certifications, provisioning and remediation.

Secure Your Enterprise with the Powers of Identity and Privilege

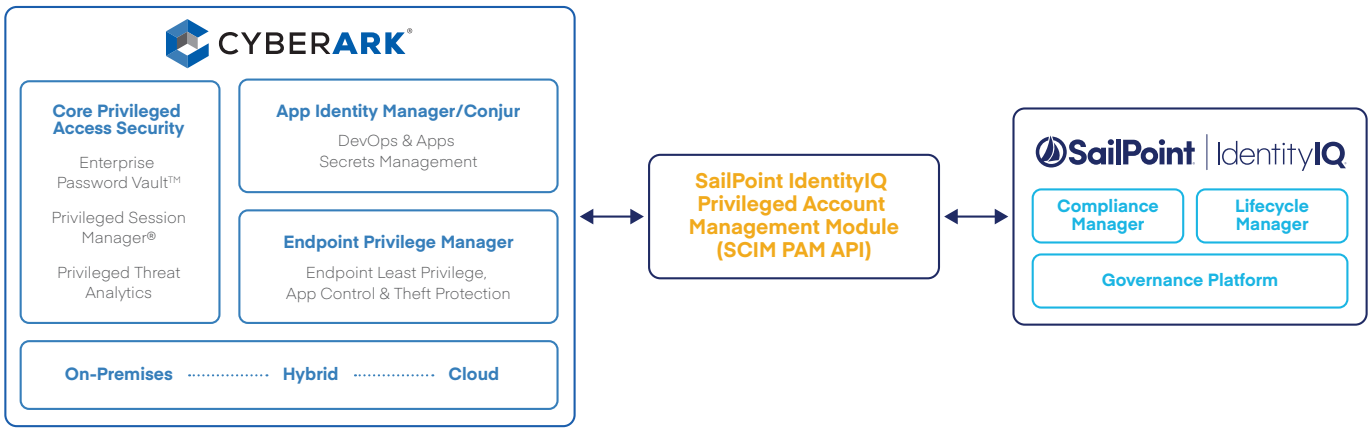
To address this siloed security challenge, SailPoint and CyberArk have partnered to provide an integrated, centrally-managed identity solution. The integration of SailPoint identity governance and CyberArk Privileged Access Security enables organizations to gain a unified, policy-driven approach to managing identity and access governance across non-privileged and privileged users alike. Organizations can now close security gaps, reduce risk, and eliminate redundant processes related to managing non-privileged and privileged access.

This combined solution provides organizations with increased control, visibility and governance over all user accounts in their environment, which helps reduce vulnerabilities such as an insider threat.

CyberArk Privileged Access Security integrates with SailPoint IdentityIQ to provide a unified, single pane of glass view of all identities, including privileged identities (individuals and applications) and access entitlements across the enterprise.

Out-of-the-box integration allows critical identity information to be shared between CyberArk Privileged Access Security and SailPoint IdentityIQ, establishing consistent controls over privileged and non-privileged access. The solution also offers:

- **Enhanced visibility:** Gain a complete view of an identity's access and its associated privileged and non-privileged accounts. Improve efficiency and control of privileged accounts and access data.
- **Automated governance controls:** Establish consistent governance controls to enforce user access policies and identify violations, such as separation-of-duty (SoD). Unify and centralize access certifications to mitigate risk of over-entitled users.
- **Streamlined secure delivery of access:** Centralize administration and control over all privileged and non-privileged accounts, enabling provisioning and de-provisioning of privileged access based on user role or lifecycle event changes.



The joint CyberArk and SailPoint solution is bi-directional, whereby user provisioning to CyberArk is performed directly from SailPoint IdentityIQ based on direct access, policies and an approval process defined within SailPoint IdentityIQ. In addition, CyberArk collects privileged user data, account information and access data, and sends it to SailPoint IdentityIQ.

With SailPoint's IdentityIQ Privileged Account Management (PAM) Integration module, organizations can gain visibility into these sensitive accounts, govern them from a centralized location, rapidly grant access to ensure productivity and establish consistent governance controls, all through accepted industry standards that reduce implementation time and cost.

Enterprises can now minimize security gaps that come from managing these otherwise siloed accounts, extend identity governance to encompass privileged account management, and bring the full power of identity to reduce security risks, enforce compliance and boost organizational efficiency.

Joint CyberArk and SailPoint Solution Capabilities and Benefits

By centralizing and unifying identity and access governance of privileged and nonprivileged users, organizations can:

Improve Visibility and Governance

- Enhance the visibility and control of privileged accounts and access data directly from IdentityIQ.
- Streamline governance and compliance processes by generating reports and auditing all identities and access permissions directly from IdentityIQ.
- Ensure privileged users are granted appropriate access permissions based on similar privileged users' attributes (e.g. roles, job functions) in accordance with the organization's access policy.

Simplify and Centralize Administration

- Unify account provisioning processes for both privileged and non-privileged users.
- Improve productivity and streamline delivery of privileged access.
- Fully manage privileged user (individuals/applications) lifecycles. Create, review and approve privileged user access permissions based on group affiliations, roles and other commonalities directly from IdentityIQ.
- Exclusive, out-of-the-box credential cycling enables privileged account management solutions to store and manage IdentityIQ service account credentials, retrieving them only when performing governance tasks.

Reduce Risk

- Reduce the attack surface and enhance regulatory compliance by limiting access privileges and deactivating stale/orphan privileged accounts.
- Apply consistent controls to privileged accounts for an improved security posture.

- Update user/group access privileges directly from IdentityIQ to avoid orphan privileged accounts, privileged entitlement creep and excess privileged permissions. Updated access permissions are automatically provisioned within the CyberArk Solution.
- Generate alerts and reports on privileged identities and access activities directly from IdentityIQ to detect unauthorized access changes or suspicious log-in activity to privileged accounts. Access reviews can be executed at the privileged user, group or system level.

The integration of CyberArk Privileged Access Security Solution and SailPoint Identity Governance enables organizations to gain a unified, policy-driven approach to identity and access governance across all users. Once deployed, the solution effectively arms organizations with the information they need to quickly identify and respond to security risks.

SAILPOINT: THE POWER OF IDENTITY™

sailpoint.com

SailPoint, the leader in enterprise identity management, brings the Power of Identity to customers around the world. SailPoint's open identity platform gives organizations the power to enter new markets, scale their workforces, embrace new technologies, innovate faster and compete on a global basis. As both an industry pioneer and market leader in identity governance, SailPoint delivers security, operational efficiency and compliance to enterprises with complex IT environments. SailPoint's customers are among the world's largest companies.

SB1213-1807