CyberArk Privileged Account Security Solution Integrated with SailPoint IdentityIQ

CyberArk has partnered with SailPoint to deliver an enhanced privileged identity and access governance solution. By integrating the CyberArk Privileged Account Security Solution with SailPoint IdentityIQ™, organizations can centrally manage and control all identities, including privileged identities and entitlements, to quickly detect and mitigate access risks of privileged users, while ensuring compliance.
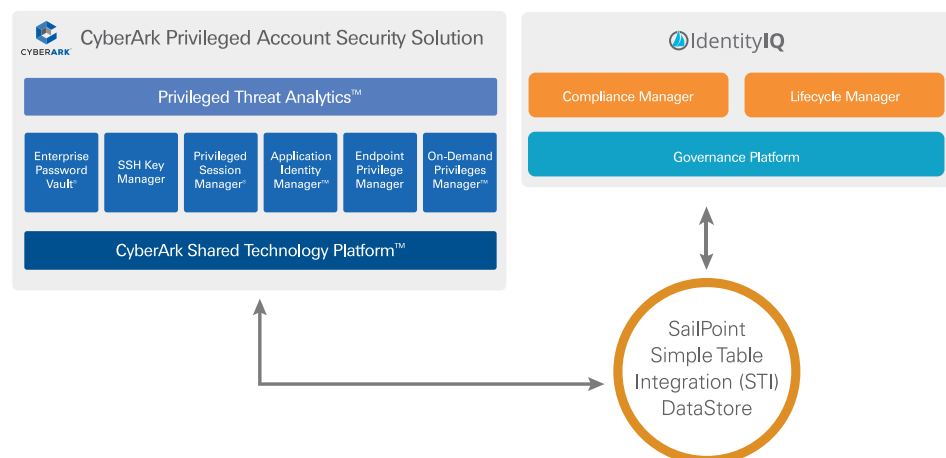
When it comes to managing users and their access entitlements, a majority of organizations have two separate solutions to manage the identity lifecycle and access policies for privileged and non-privileged users. Standalone solutions for both types of users lack the ability to enforce a unified access policy and consistent governance, provisioning and authorization process. This can result in access violations and regulatory action.

To avoid this issue, 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.

The CyberArk Privileged Account Security Solution integrated with SailPoint IdentityIQ provides a unified view with centralized policy-based identity management for all identities, including privileged identities (individuals and applications) and access entitlements to ensure access policy and regulatory compliance.

Highlights

- Gain visibility and control of privileged user data and access permissions directly from IdentityIQ.

- Quickly detect risks and amend access entitlement issues associated with privileged users.

- Automate the privileged user provisioning process based on groups, policies and approval workflows.

- Accelerate compliance efforts with unified top down governance processes for all users.

Joint CyberArk-SailPoint solution for unified visibility, management and control of all users, including privileged users and corresponding access entitlements

A single source for provisioning, authorizing and managing all user identities, including privileged identities and access entitlements

The CyberArk Privileged Account Security Solution is a unified enterprise-class solution that manages and secures all privileged accounts used by individuals and applications. The solution secures credentials including passwords and SSH keys, controls account access and isolates and records privileged sessions for auditing and forensics analysis. Built on a single platform, the solution centralizes all privileged user information and activities, providing a single source of privileged identity and access data directly into SailPoint IdentityIQ.

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

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

- 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. All privileged access requests are verified using an automated approval workflow. Once approved, data is automatically synchronized with the CyberArk Privileged Account Security Solution and a privileged user is added to the relevant privileged account(s).
  - 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.
- Execute periodic reviews and re-certification of privileged access directly from IdentityIQ
- Enforce application access permissions defined within IdentityIQ using CyberArk Application Identity Manager™ to ensure the application can only access authorized assets.
- 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.

Summary

The integration of CyberArk Privileged Account Security Solution and SailPoint IdentityIQ 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 involving the organization's most powerful identities – privileged users.

Connected **Partner**

Joint CyberArk and SailPoint Solution Benefits:

- Provides enhanced visibility and control of privileged accounts and access data directly from IdentityIQ.

- Unifies account provisioning processes for privileged and non-privileged users.

- Ensures privileged users are granted appropriate access permissions based on similar privileged users' attributes (e.g. roles, job functions), and in accordance with the organization's access policy.

- Reduces the attack surface and enhances regulatory compliance by limiting access privileges and deactivating stale/orphan privileged accounts.

- Streamlines governance and compliance processes by generating reports and auditing all identities and access permissions directly from IdentityIQ.

About CyberArk

CyberArk is the only security company that proactively stops the most advanced cyber threats – those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage. To learn more, visit us at www.cyberark.com

About SailPoint

As the leader in identity and access management (IAM), SailPoint helps hundreds of global organizations securely and effectively deliver and manage user access from any device to data and applications residing in the datacenter, on mobile devices, and in the cloud. The company's innovative product portfolio offers customers an integrated set of core services including identity governance, provisioning, and access management delivered on-premises or from the cloud (IAM-as-a-service).