BeyondTrust

SailPoint CERTIFIED

SAILPOINT IDENTITYIQ + BEYONDTRUST

INTEGRATED IDENTITY GOVERNANCE & PRIVILEGED ACCESS MANAGEMENT

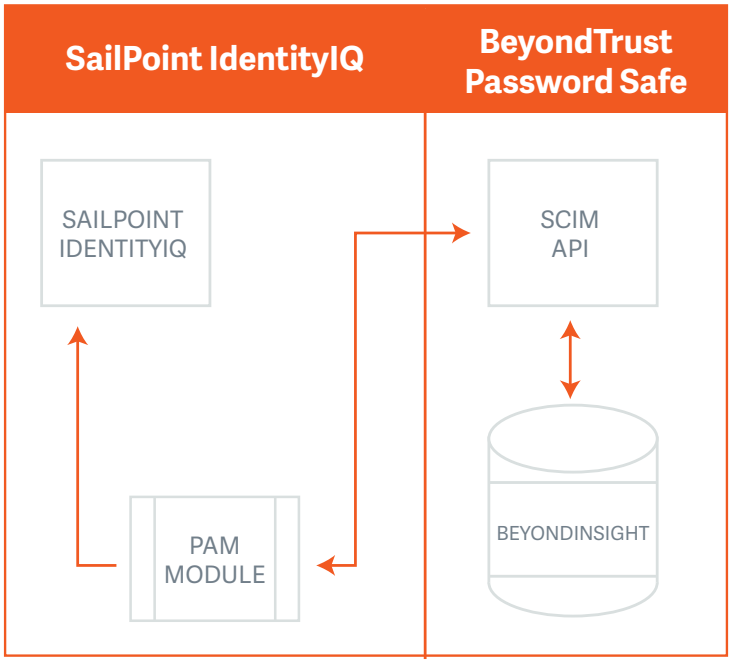
The BeyondTrust Privileged Access Management Platform integration with SailPoint IdentityIQ combines strong controls for privileged accounts with lifecycle management of identity governance. The integrated solution enables streamlined account and entitlement provisioning / deprovisioning, access request approvals and workflow. IT organizations get full visibility and enhanced security of users and accounts including access certification, separation of duties policy enforcement, privileged credential vaulting and rotation, privileged session monitoring and management, and more.

The SailPoint Certified capability leverages the System for Cross-domain Identity Management (SCIM) API built into the SailPoint IdentityIQ PAM Module, allowing privileged account vaults and associated entitlements to be visible and managed throughout the identity governance process. This allows the automated provisioning of privileged accounts to new end users who require them based on their job function, group membership, or business role, and allows managers to recertify or remove privileged accounts on a periodic and/or event-driven basis.

Automated Access
Empower IT admins, specialists and executives with the privileged access they need to do their job.

Centralized Management
Provide a complete, centralized view of each identity's access across all standard and privileged/shared/system accounts.

Reduced Risk
Continuously remove unnecessary privileged accounts as users switch jobs or leave the company.



Effectively Manage User Access for Both Privileged & Non-Privileged Accounts

Identity governance solutions help IT teams answer *"who has access to what?"* The integrated BeyondTrust and SailPoint solution allows organizations to answer *"is that access appropriate for privileged users?"* and *"is that privileged access being used appropriately?"*

SCIM-Based Integration ensures the automated exchange of user identity information between systems.

The SCIM API in the BeyondTrust PAM Platform enables organizations to automate the exchange of identity data, including:

- Add/remove users – admin or non-admin
- Add/remove users to/from groups
- View smart group permissions for a group
- View managed accounts

The API ensures that organizations can successfully track and manage identity changes in cloud environments.

FEATURES & CAPABILITIES

Complete Import

Importing a user provides direct access to the BeyondTrust Platform, providing controlled privileged access and audit activity. The account and its entitlement access data is fed back to IdentityIQ via API, providing visibility into user access.

Dynamic Entitlement Export & Reporting

All entitlements granted by the BeyondTrust Platform are delivered directly to SailPoint via API, providing complete support of out-of-station processes defined in IdentityIQ by including ad hoc reviews of user access.

Automated Safe API

Direct API-based integration provides immediate provisioning of and visibility into all privileged access. Depending on role membership, users may be granted immediate runtime access to request passwords or sessions for privileged accounts and be provided granular least privilege policies.

Dynamic Activity Audit & Reporting

The BeyondTrust Platform provides complete visibility and control of privileged access and extensive reporting, allowing organizations to effectively answer: Is that access being used appropriately?

BeyondTrust is the worldwide leader in Privileged Access Management, offering the most seamless approach to preventing privilege-related breaches. Our extensible platform empowers organizations to easily scale privilege security as threats evolve across endpoint, server, cloud, DevOps, and network device environments. We are trusted by 20,000 customers.

beyondtrust.com

V2019_04_ENG