The nationwide roll-out of SailPoint’s Predictive Identity Platform enables Police Forces to manage user access for privileged and non-privileged accounts, as well as gain extra visibility into user and session activity — all using industry standards to reduce implementation time and cost.

IT security teams within the Police Force need be able to answer:

1. **WHO**
   has access to what?

2. **SHOULD**
   they have that access?

3. **WHAT**
   are they doing with their access?

Identity governance solutions help IT teams within the Police Force to answer “who has access to what?” The integrated BeyondTrust and SailPoint solution allows organizations to answer “is that access appropriate for privileged users?” and “what are they doing with that level of access?” - giving more visibility and control.

**Features and Capabilities**

- **Automate Governance Controls**
  Provide a complete, centralised view of each identity’s access across all standard and privileged, shared, and system accounts.

- **Streamline Delivery Of Access**
  Establish centralised administration and control over all privileged and non-privileged accounts from within SailPoint enabling delivery of privileged access based on user role or lifecycle event changes.

- **Improved Security And Administration Efforts**
  Out-of-the-box credential cycling enables privileged account management solutions to store and manage SailPoint service account credentials, retrieving them only when performing identity tasks.
Effectively Manage User Access for Privileged & Non-Privileged Accounts

This bi-directional integration allows Police Forces across England and Wales to access the right information at the right time, wherever they are, by mapping identities over any given environment.

By enforcing least privilege through Endpoint Privilege Management, user access remains seamless but secure.

BUSINESS BENEFITS

Complete Import
- Importing a user provides direct access to the BeyondTrust PAM Platform, providing controlled privileged access and an activity audit. The account and its entitlement access data are fed back to the SailPoint Predictive Identity Platform via API, providing visibility into user access.

Dynamic Entitlement Export & Reporting
- All entitlements granted by the BeyondTrust PAM Platform are provided directly to SailPoint via API, providing complete support of out-of-station processes defined in the Predictive Identity Platform 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 run time access to request passwords or sessions for privileged accounts and be provided granular least privilege policies.

Dynamic Activity Audit & Reporting
- The BeyondTrust PAM Platform provides complete visibility and control of privileged access and extensive reporting, allowing Police Forces to effectively answer: Is that access being used appropriately?

Common Use Cases Police Forces Are Facing:

Lack of visibility over user access
- Accurate and up-to-date information is imperative to ensuring a successful policing operation. This process can be hindered by unmanaged privileges.

Validation of compliance requirements
- Unchecked user access makes compliance - such as Cyber Essentials Plus (and many more) - very challenging to meet.

A vulnerable, growing attack surface
- By not knowing which identities have access to what - and with no least privilege in place - there is a huge risk of ransomware/malware attacks.