BUSINESS CONTEXT

- Customer’s IT assets are managed by internal teams as well as many third party vendors.
- Multiple users have privileged access to the confidential information, which includes sensitive data.
- Need to secure, control & monitor access of privileged users to IT infrastructure and ensure compliance to their security policy. The main business drivers are -
  - Control & monitor privileged access to IT assets (Servers, network & security Devices)
  - Comply to group security policy
APPROACH AND SOLUTION

Tech Mahindra catered to the client problem as follows:
- Designed & implemented centralized PIM solution integrated with IT infra
- Implemented CyberArk / PUAM solution to control privilege access to Servers, DBs, Network Security devices and Web Applications
- Implement Role Base Access Control, 2FA for Vault and Safe Admins, SSO, video & command logging
- Implemented Password management for all privileged accounts
- Integrated around 5000 devices
- Assessment of internal applications and privilege ID monitoring needs.

IMPACT & HIGHLIGHTS

Control and manage insider threats to sensitive data leakage, disruption of services
Defend outsider threat more effectively by protecting the privileged and service accounts
Enabling audit for privileged accounts