CASE STUDY

A Defence Equipment Manufacturing Organisation under the Ministry of Defense

ProcessIT Global

Overview

The client is an Indian organisation engaged with production of Battlefield Equipment. It is the 37th-largest defence equipment manufacturer in the world, 2nd-largest in Asia, and the largest in India. The organization consists of a total 41 production units under the corporate headquarters located in Kolkata.

Possessing the unique distinction of over 200 years' experience in defence production. Mainly engaged in production, testing, logistics, research, development and marketing of a comprehensive product range in the area of land, sea and air systems, our client has received patronage both in India and abroad for its quality of products and services.

The organization engages a workforce of about 80,000 thus often called the "Fourth Arm of Defence", Its total sales engagement was at US$3 billion (₹22,389.22 crores) in the year 2020–2021.

Challenge

To maintain extremely high level of security and meet compliance requirements,

The organization needed to ensure that each of its employees can only access the systems relevant to their specific roles.

Fast access providence was needed for new bulk hired employees, to access the appropriate systems and resources, in order to avoid delays to the delivery of vital information to organizations and individuals.

To reduce the risk of highly confidential data being breached, our client also needed to revoke access for former staff as soon as their employment ends.

Managing access to all these systems and resources needed to be customised under one single umbrella, within a highly secure intranet environment.

Solution

Intranet implementation of Identity Manager and Access Manager was done by PITG to meet the client's needs.

Identity Manager was synchronized with identity information across multiple directories, creating a single master identity for each unique onboarded user and eliminating most of the manual tasks associated with user management.

Bulk user provisioning was configured through Identity Provisioning via Connectors.

After Successful creation of users in Identity manager, the same was provisioned to target applications. Which triggered one automated email to the user's supervisor email ID with a random password. Users can login to the unified portal and on first time login it would redirect to Identity manager Self-service password reset portal to setup user profile (set security question-answers, auto-change first time provided password etc.)

Access manager was integrated with the applications to ensure protection of the access while making them conveniently accessible only to authorized users.

With the capability of Single Sign On, Users were able to access all of the organizational resources i.e., email, central document manager etc. as per their authorities, from one unified intranet portal name “Comnet.2.0”.

Self Service Password was integrated maintaining company password policies to enable users to reset their own passwords.

Results

The successful implementation of the solution, and the launch of “Comnet 2.0” played a vital role in enabling the client to meet its identity management challenges efficiently and effectively

Enhanced Data security: The Identity Manager provides a unified, real-time view of account information and access rights across diverse applications and systems with a completely automated framework. Thus, highly confidential data remains secure even within the organization.

Unified user management: Supervisors are easily able to review their staffs' permission rights, a single-click 'revoke' triggers automated workflow that actions this without any further human intervention. All the user identities are easily governed over a single unified platform.

Accelerated administration: Automation accelerates user account administration, reduces the risk of human error, leveraged to provision users more quickly freeing up valuable IT resources, so that they have more time to dedicate to other value-added tasks.