CYBERSECURITY CASE STUDY

Simplifying Access and Strengthening Security

Client Overview

Our client is a nationwide conglomerate with a workforce of over 30,000 employees spread across diverse business units and locations.

Challenges

- The client faced challenges in managing secure access across various applications, including:
    - SAP
    - Office 365
    - Palo Alto VPN
    - Microsoft Windows with Azure AD, and
    - IT device administration.
- Previously, each application required a separate Multi-Factor Authentication (MFA), leading to confusion and inefficiency.
- Users struggled with multiple MFA apps, and administrators found it hard to maintain visibility and control over access.

Solutions

We proposed implementing RSA Secure ID, a unified solution offering Single Sign-On (SSO) and centralized MFA for all applications.

Our deployment included:

- Setting up RSA Auth managers/IDR with centralized management
- Connecting to RSA Cloud for seamless synchronization and AD credential validation
- Integrating applications using protocols like RADIUS, SAML, and OAuth

Implementation Results:

- User Simplicity: A single app to manage logins across applications
- Administrative Visibility: A unified dashboard allows full visibility into user access and activity
- Enhanced Security: Each login is verified, reducing the risk of account takeovers and breaches

Before & After Summary:

- Before: Multiple MFA systems, lack of visibility, and complex user experience
- After: Unified MFA and SSO with centralized management, seamless access, and strengthened security

Results

Our solution and implementation not only simplified secure access but also enabled the client to monitor and control access, preventing potential breaches.