accops

Enhancing Security with Multi-Factor Authentication at India's largest private bank

CASE STUDY

B

About the Client

India's largest private bank deployed a SASE solution for their employees using corporate laptops. These laptops had direct network access to business applications, with additional security layers like endpoint security software (e.g., Dell PC).

However, a new mandate from the Reserve Bank of India (RBI) required that any internet-facing application accessed by vendors be protected with multi-factor authentication (MFA).

INDUSTRY	**BANKING**
PRODUCTS DEPLOYED	**ACCOPS MFA, ACCOPS ZTNA**

Challenges Faced

While the bank's existing SASE (Secure Access Service Edge) solution was integrated with Azure Active Directory (Azure AD) and employees had Azure AD Premium P1 licenses (incurring no additional cost for MFA), their third-party vendors faced a different challenge. Vendors using the bank's core lending applications were not on Azure AD Premium P1. Instead, these users were created in local databases for each application. The lending applications were publicly accessible, making them vulnerable to brute force attacks and identity theft.

The regulator mandated that all critical applications—especially lending applications generating significant revenue—must be protected against cyber threats. However, implementing MFA was complicated because:

- The applications were over a decade old and highly customized, making upgrades to a modern version that supports SAML authentication unfeasible.
- Each application had its own local database, requiring individual user credentials.
- The bank wanted seamless role-based access management for vendors.
- SASE-based MFA required vendors to have Azure AD P1 licenses, adding cost.
- The SASE solution's cloud-based control plane could not integrate with the bank's Identity and Access Management (IDAM) system, which was a critical concern as the business team wanted to avoid any friction in the manual user onboarding processes.

Solution

To address these challenges, India's largest private bank evaluated and implemented an Accops solution. The key features of this solution included:

- **On-Premise Deployment:** Accops was deployed as an application proxy gateway to avoid changes to existing applications.
- **Passwordless Authentication:** Users entered a username and received a one-time password (OTP) for login.
- **Centralized Access Portal:** Upon logging into Accops, users accessed only the applications permitted to them.
- **Identity Continuity:** The correct username was auto-filled for each application to prevent credential misuse.
- **Seamless Integration with IDAM:** Accops customized APIs to align with the bank's onboarding and offboarding process.
- **No Additional Application Changes:** The existing applications remained untouched, ensuring minimal disruption.

Implementations and Outcomes

The Accops solution was deployed for 20,000+ users, including employees and third-party vendors. The key benefits included:

- **Stronger Security Controls:** MFA was implemented without changing legacy applications.
- **Improved Compliance:** The bank adhered to RBI's security mandate.
- **Seamless User Experience:** Role-based access ensured users accessed only their assigned applications.
- **Streamlined Vendor Management:** The automated IDAM integration simplified onboarding and offboarding for vendors with high attrition rates.
- **Device Tracking:** While enforcement wasn't strict, the bank could now track devices used by vendors.

Future Scope

The bank aims to enhance security further by:

- **Implementing Device Binding:** Restricting vendors to specific devices for improved control.
- **Preventing Data Leakage:** Introducing restrictions like disabling copy-paste and print screen operations.
- **Strengthening Identity Security:** Enhancing measures to prevent unauthorized device switching.

Conclusion

India's largest private bank successfully tackled a complex security challenge by implementing the Accops solution, ensuring compliance with regulatory requirements while maintaining operational efficiency. The project's success sets the foundation for further security enhancements and a more robust identity management framework in the future.

Accops enables secure and instant remote access to business applications from any device and network, ensuring compliant enterprise mobility for business users while keeping governance with the organization.

Discover how Accops can transform your remote and hybrid work strategies.
Reach us today at contact@accops.com for a free consultation.