Transforming Secure Access in India's Leading Banks with Accops

B

About the Clients

Two of India's top private sector banks—one being the largest private bank and the other ranked among the top three—faced significant challenges in securing remote access for employees, third-party vendors, IT administrators, and business users.

With regulatory mandates evolving and remote work becoming the norm, both banks required a scalable, secure, and efficient solution to protect their critical applications and data without disrupting business operations.

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

Challenges Faced

Bank 1: India's Largest Private Sector Bank

- Required Multi-Factor Authentication (MFA) for vendor access due to RBI's mandate.
- Vendors used personal devices to access business-critical lending applications, increasing security risks.
- Legacy applications, over a decade old, lacked modern authentication protocols like SAML or OAuth.
- The bank's existing Secure Access Service Edge (SASE) solution required vendors to have Azure AD P1 licenses, which would have significantly increased costs.
- The business team wanted a seamless onboarding and offboarding experience for vendors without manual intervention.

Bank 2: India's Third-Largest Private Sector Bank

- Initially supported only 500 remote users via traditional VPN and VDI.
- COVID-19 drove the need for a scalable remote work solution, increasing the user base to 30,000.
- Vendors, IT admins, developers, and business users needed secure remote access to internal portals, test environments, and critical applications.
- The bank required biometric authentication for 90,000 users but faced high costs and complex integrations with proprietary biometric systems.
- Compliance with security regulations necessitated application isolation for sensitive systems like SWIFT.

Accops' Solution & Implementation

Accops provided a comprehensive, scalable, and cost-effective solution addressing both banks' challenges:

1. Secure Remote Access for Employees and Vendors

- **ZTNA & VDI for 30,000+ Users:** Accops enabled secure remote access to business applications using Zero Trust Network Access (ZTNA), Virtual Desktop Infrastructure (VDI), and remote browser technology.
- **Role-Based Access Control:** Ensured that users could access only the applications relevant to their roles.
- **Passwordless Authentication:** Implemented an OTP-based login for vendors, eliminating weak password risks.
- **Secure BYOD Access for Vendors:** Provided full data protection, including copy-paste restrictions, keylogger protection, and prevention of screen capturing, ensuring secure vendor access while protecting sensitive banking data.

2. Multi-Factor Authentication for Legacy Applications

- **Application Proxy Gateway:** Enabled MFA without modifying legacy applications.
- **Identity Continuity:** Auto-filled application-specific usernames to prevent credential misuse.
- **Seamless IDAM Integration:** Automated vendor onboarding and offboarding, reducing operational overhead.

3. Biometric Authentication for Enhanced Security

- **90,000 Users Enabled:** Integrated biometric authentication with Active Directory (AD) for seamless access.
- **Cost Reduction:** Allowed the bank to use any biometric scanner, eliminating dependency on proprietary hardware.
- **Rapid Deployment:** Enabled biometric authentication for new applications without extensive API development.

4. Optimized IT & Developer Access

- **L3 Connectivity for Developers & Secure VoIP:** Provided secure access to test and development environments without requiring physical office visits. Additionally, ensured secure VoIP communication for internal IT and call center teams while business applications ran within the VDI environment, maintaining data security and compliance.
- **VDI for Critical Application Isolation:** Ensured secure, compliant access to high-risk applications like SWIFT.
- **Intern & Contractor Support:** Enabled temporary workers to securely access necessary applications with BYOD support.

Key Business Outcomes

Scalability	Expanded secure remote access from 500 users to 30,000+ users.
Cost Savings	Eliminated additional Azure AD P1 licensing costs, reduced biometric authentication expenses, and optimized IT infrastructure usage.
Operational Efficiency	Automated vendor lifecycle management, ensuring frictionless onboarding and offboarding.
Regulatory Compliance	Strengthened security posture in alignment with RBI mandates and internal risk management policies.
Improved User Experience	Passwordless authentication, role-based access, and biometric logins simplified access management.

Conclusion

By leveraging Accops' secure access, ZTNA, VDI, and biometric authentication solutions, India's largest and third-largest private banks successfully enhanced security, compliance, and efficiency in their IT operations. This transformation not only strengthened their cybersecurity posture but also set a benchmark for other financial institutions looking to adopt Zero Trust and MFA strategies without disrupting business continuity.

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.