Leading Private Sector Bank's Digital Transformation with Accops Platform

CASE STUDY

About the Client

The client is a leading private sector bank known for its robust financial services and commitment to digital transformation.

With a diverse user base, including third-party vendors, IT administrators, and business users, the bank has consistently focused on enhancing security and operational efficiency. As remote work became the norm, the bank sought a scalable and secure solution to enable seamless remote access while ensuring compliance with stringent security standards.

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

Challenges Faced

A leading private sector bank was facing challenges in securely enabling remote access for its users, which included third-party vendors, IT administrators, and business users.

Previously, the bank relied on traditional VPN and VDI platform with only around 500 users. However, with the shift to remote work, the bank needed a scalable and secure solution to support a significantly larger user base.

Implementation of Accops Platform

To address these challenges, the bank adopted Accops' solutions, which enabled secure access for 30,000 users to their business applications at peak during Covid years. The users ranged from IT admins and business users to external vendors who required access to internal portals. Accops' Zero Trust Network Access (ZTNA), virtual desktop infrastructure (VDI), and remote browser solutions played a crucial role in facilitating this transition.

Optimization and Expansion

Over time, the bank optimized its VDI usage, reducing the number of VDI users to 10,000. This ensured that only IT administrators, Infosec teams, developers, and vendors accessing critical servers leveraged VDI, improving efficiency and resource utilization.

Furthermore, the bank expanded its use of Accops' ZTNA solution by integrating new use cases, such as enabling developers to connect securely to test environments. This included mobile app developers requiring Layer 3 (L3)

connectivity to test applications without needing physical office access. Accops' turbo protocol facilitated this secure L3 connectivity for mobile app developers.

VDI Use Cases

- **Core Users:** The majority of VDI users include developers, network teams, information security teams, and back-end operations teams who access critical applications.
- **Critical Application Isolation:** For regulatory compliance, certain critical applications such as SWIFT require isolation from the rest of the IT network. Accops' VDI ensures complete application isolation to meet these regulatory requirements.
- **Intern Support:** Short-term interns working with the bank can securely access necessary applications via VDI with BYOD support, without direct integration into the core IT network.
- **Internal IT & Call Centers:** The bank's internal IT helpdesk users, who use VoIP services, as well as customer-facing call center functions, rely on a combination of Accops ZTNA for secure voice traffic and VDI for business application access.
- **Developer Access to Test and Dev Environments:** Developers, including both internal teams and outsourced development teams, use VDI to securely access test and development environments. For outsourced development teams, BYOD support ensures secure access without requiring corporate-owned devices, maintaining a controlled and secure environment for application development and testing.

Biometric Authentication Implementation

In addition to remote access solutions, the bank deployed Accops for biometric authentication, supporting 90,000 users. Previously, the bank used a biometric authentication system that required proprietary scanners, leading to high costs and complex integrations with multiple applications. Integrating biometrics into 15 additional applications would have required extensive API development and ongoing maintenance.

Accops provided a seamless biometric authentication solution integrated with Active Directory (AD), allowing any AD-integrated application, including login to user desktops, to be made biometric-enabled within minutes. This eliminated the need for costly API integrations and ensured compatibility with various biometric devices from different vendors. Additionally, Accops facilitated the creation of a centralized biometric database, enhancing security and scalability.

Results & Benefits:

Scalability	Expanded secure remote access from 500 users to 30,000+ users.
Cost Savings	Reduced biometric authentication costs by eliminating the need for proprietary scanners and API integrations.
Efficiency	Optimized VDI access for critical users, reducing unnecessary resource consumption.
Security	Strengthened security with Zero Trust principles and seamless biometric authentication.
Flexibility	Enabled developers and remote workers to access test environments without physical office visits.
Managed Services	Provided dedicated on-site support, ensuring smooth operations and quick issue resolution.

Conclusion

By implementing Accops' secure access and biometric authentication solutions, the bank successfully enhanced its digital infrastructure, enabling secure, scalable, and cost-effective remote access for employees, vendors, and IT administrators. This transformation not only improved operational efficiency but also reinforced security, positioning the bank for future growth in a digital-first world.

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.