safous THINK YOUR ACCESS

CUSTOMER CASE STUDY

BANKING · PRIVILEGED ACCESS

How a National Bank Gained Full Control Over Privileged Access



300–400
Servers

INDUSTRY
Banking

SYSTEMS
Critical banking systems

USERS
Internal teams & third-party vendors

THE NEED

Secure and control privileged access to critical banking systems across internal teams and third-party vendors.

Top Challenges

Limited control
Little control over user access with VPN-based connectivity.

Poor traceability
Gaps in traceability created compliance risk.

Insider threat risk
No user-level accountability.

External access risk
External access significantly expanded the attack surface.

Business Outcomes

Application-level control
Network-level VPN access replaced with granular, application-level control.

Full session visibility
Full session monitoring and recording for audit and compliance.

No more password sharing
Password sharing eliminated with secure, brokered access.

Supervised vendors
Third-party vendor access is controlled and supervised.

SAFOUS CONTROLS IN THIS DEPLOYMENT

- Granular, application-level access control
- Brokered access without password sharing
- Session monitoring and recording
- Controlled, supervised vendor access

How It Works

Illustrative Safous access flow

Teams & vendors — Safous — Banking systems

About Safous — Provided by IIJ (Internet Initiative Japan), Japan's first ISP, listed on the Tokyo Stock Exchange Prime Market. ISO/IEC 27001 certified and SOC 2 attested. PoPs across Asia, plus North America and Europe. Customer name withheld for confidentiality.

safous THINK YOUR ACCESS

Request a demo or PoC: safous.com/get-started