As a financial institution dealing with monetary transactions, it chose SecureKi to secure its SWIFT environment and satisfy its compliance with the Customer Security Controls Framework.

The Company

A prominent banking group in Malaysia, which stands among the nation's largest, encompasses a spectrum of financial services including retail, wholesale, Islamic banking, and insurance.

The Challenges

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides financial messaging services to banks, financial institutions, and corporations worldwide. The technology is used to exchange sensitive information about financial transactions by more than 11,000 customers in over 200 countries. SWIFT provides a framework for customer security controls to fend off these attackers. The framework is designed for SWIFT members to secure their SWIFT environments and to limit access, detect, and respond to security threats. Realizing the framework's goals involves devising controls that cover issues of physical security, credentials, and user identities. As a result, SecureKi's Privileged Access Management (PAM) solution is critical to the framework's success.

The financial institution's challenges include:

1. 80% of SWIFT breaches are due to cybercriminals gaining privileged credentials of privileged accounts. In order to mitigate credential risks, the financial institution would need to protect and automate its access to its privileged accounts across both virtual and physical systems.

2. SWIFT has a Customer Security Controls Framework (SWIFT CSCF), a comprehensive list of security controls that all SWIFT customers must demonstrate compliance with. It recommends utilizing a Privileged Access Management (PAM) solution across privileged accounts, restricting access in accord with a principle of least privilege, implementing multi-factor authentication, and adopting a complex password standard.

3. Manage a large and intricate infrastructure with minimal human error and no unauthorized access.

Why the financial institution chose SecureKi

1 SecureKi PAM solution provides the financial institution’s IT security team with a centralized policy framework to authorize and govern their privileged users and accounts based on their roles and responsibilities with its granular access control. Fine-grained access control helps organizations protect their systems from unauthorized access and is able to custom-fit complex business operation access flow. It allows the restriction and control of privileged users through a rule and role-based centralized governing policy. The functionality provides the IT risk managers with command restricting and filtering capabilities to ensure least privilege access to target systems.

2 To assist the financial institution with adhering to the SWIFT CSCF framework and guidelines, SecureKi PAM solution's secure password vaulting, multi-factor authentication, and enforcing the principle of least privilege with granular controls ensure their privileged accounts and information are secure from unauthorized access. SecureKi PAM safeguards the financial institution’s SWIFT environment by seamlessly monitoring every single access to critical systems present in every layer of the SWIFT messaging network.

3 SecureKi’s PAM solution eased the IT team's workload with automated audit trails, custom reporting, session recording, and real-time monitoring, ensuring thorough oversight of privileged sessions.

SecureKi PAM offers the following benefits

Mitigate and reduce data security risks

Protect passwords and other credentials from unauthorized use and compromise. Limit the actions users can perform on systems and prevent the execution of unauthorized commands and prevent lateral movement within the network.

Increase accountability

Observe full attribution of user activity, even when using shared accounts. Comprehensive logging, session recording, and user warnings capture activity and provide a deterrent to unauthorized behavior.

Improve auditing and facilitate compliance

Simplify compliance by providing support for emerging authentication and access control requirements.

Reduce operations complexity with automation

Privileged single sign-on with MFA limits the risk of password-gathering malware attacks and optimizes the productivity of administrators with quick and secured access to their remote systems.