Securden

Privileged Access Security Use Cases for Banks

Privileged Access Security Use Cases for Banks

How Securden Unified PAM Supports Banking IT & Infrastructure Teams

Modern banks operate large, complex IT and infrastructure environments spanning data centers, endpoints, and cloud platforms. Routine operations such as system maintenance, incident response, configuration changes, and emergency recovery require IT and infrastructure teams to access critical systems with elevated privileges.

When this access is permanent, broadly assigned, or insufficiently governed, it creates significant security and compliance risks, ranging from credential misuse and insider threats to audit gaps and regulatory exposure. These risks cannot be effectively addressed by traditional IAM controls, which are not designed to manage privileged access.

Securden Unified PAM provides centralized control over privileged access across banking IT environments, enabling Just-In-Time access, removal of standing administrative privileges, and complete visibility into privileged activity. This allows banks to maintain operational efficiency while strengthening security posture and meeting regulatory expectations.

1. Securing Privileged Access to Core Banking & Payment Infrastructure

(IT Operations + Security)

Banking Challenge

Core banking systems, SWIFT environments, payment gateways, and treasury platforms require privileged access for maintenance and operations. Static credentials and shared admin accounts increase breach risk.

How Securden Helps

Securden Feature	How It Applies in Banking
Privileged Account Discovery & Vaulting	Discovers and secures admin/service accounts across core banking servers, databases, and payment infrastructure
DevOps Secrets Management	Replaces hardcoded application credentials with API-based dynamic secrets fetched securely from an encrypted vault.
Just- In-Time Access (JIT)	IT Teams can access systems without ever viewing credentials, using approval-based, time-bound access.
Session Launch (RDP, SSH, SQL)	Secure, controlled access to critical banking systems

Outcome: Secure operations without exposing credentials or disrupting uptime.

2. Eliminating Standing Privileges for Bank Employees (EPM – Mandatory)

(Zero Standing Privilege Use Case)

Banking Challenge

Employees and IT staff often have permanent local admin rights, increasing ransomware and insider threat exposure.

How Securden Helps

Securden Feature	How It Applies in Banking
Endpoint Privilege Manager (EPM)	Removes permanent local admin rights from employee endpoints
Application-based Elevation Policies	Allows users to run approved apps/scripts with admin rights
Just-in-Time Privilege Elevation	Temporary admin access only when required
Full Audit Logs for Elevations	Tracks who elevated what, when, and why

Outcome: Eliminates permanent admin rights by enforcing just-in-time, restricted admin access, reducing endpoint attack surface and insider risk.

3. Controlled Privileged Access for IT & Infrastructure Teams

(Infra, Data Center, Cloud Ops)

Banking Challenge

Admins need elevated access for patching, upgrades, and incident response. Without controlled, on-demand privilege elevation, users get stuck waiting for permissions which results in frequent helpdesk tickets, operational delays, and eventually broad or standing access being granted to keep systems running.

How Securden Helps

Securden Feature	How It Applies in Banking
Role-Based Access Control (RBAC)	Access based on job role and system criticality
Approval Workflows	Dual control for sensitive systems
Just-in-Time Privileged Access	Access expires automatically after task completion
Centralized Admin Console	Unified visibility across on-prem and cloud

Outcome: Operational agility through role-based, just-in-time privileged access, reducing helpdesk dependency while enforcing least-privilege security across infrastructure environments.

4. Privileged Session Monitoring & Audit Readiness

(Security, Audit & Compliance Teams)

Banking Challenge

Security and IT teams lack real-time visibility into privileged sessions, making it difficult to know who accessed critical systems (Core banking, mainframe/z-OS, SWIFT & payment rails, databases, network/security devices), what actions were performed, and when those actions occurred.

How Securden Helps

Securden Feature	How It Applies in Banking
Privileged Session Monitoring (PSM)	Monitors live privileged sessions
Session Recording & Playback	Enables forensic review and investigations
Tamper-proof Audit Logs	Centralized, immutable logs for audits
Compliance Reports	Ready-made reports for banking regulators

Outcome: Complete visibility on privileged activity, answering ‘who’ did ‘what’, ‘when’, across all critical systems.

5. Meeting Banking Regulatory & IT Compliance Requirements

(Risk, GRC & Compliance Teams)

Banking Challenge

Banks must comply with FFIEC, GLBA, Basel III, and regional IT security mandates requiring strong privileged access controls.

How Securden Helps

Securden Feature	How It Applies in Banking
Policy-based Access Controls	Enforces regulatory access requirements
Automated Password Rotation	Meets credential hygiene mandates
Access Reviews & Certifications	Periodic validation of privileged access
Central Compliance Dashboard	Single view of compliance posture

Outcome: Continuous compliance instead of audit-driven firefighting.

6. Secure Third-Party & Vendor Access to Banking Systems

(Vendor Risk Management)

Banking Challenge

Vendors require access for support, but long-term access to credentials increases third-party risk. Banks must demonstrate governed vendor access with documented approvals, least-privilege enforcement, and audit evidence of who accessed what, when, and what actions were performed. Session trails and timely revocation support third-party risk, outsourcing governance, and audit requirements.

How Securden Helps

Securden Feature	How It Applies in Banking
Time-bound Vendor Access	Access is time-bound and expires automatically after the approved window
Password-less Remote Sessions	Vendors access systems without direct access to credentials.
Session Monitoring & Recording	Full visibility into vendor activity
Approval-based Access Requests	Controlled onboarding of vendors

Outcome: Reduced third-party risk with no direct credential exposure to vendors, plus audit-ready evidence through approvals, session monitoring/recordings, and time-bound access enforcement.

7. Privileged Access Across Hybrid & Cloud Banking Environments

(Cloud & Platform Teams)

Banking Challenge

Hybrid IT environments increase complexity in managing privileged access consistently.

How Securden Helps

Securden Feature	How It Applies in Banking
Unified PAM Platform	Single solution across on-prem and cloud
Cloud Account Privilege Management	Secures admin access to cloud workloads
CIEM (Cloud Infrastructure Entitlement Management)	Identifies excessive cloud permissions
Least-Privilege Enforcement	Rightsizing of cloud access

Outcome: Consistent privileged access controls across hybrid banking infrastructure.

8. Supporting SOC & Security Operations with Privileged Access Visibility

(SOC & Security Operations Teams)

Banking Challenge

Security teams often lack real-time visibility into privileged activities, making it difficult to investigate incidents involving admin accounts, lateral movement, or misuse of elevated access.

How Securden Helps (Verified Feature Mapping)

Securden Capability	How It Applies in Banking DevOps
Secrets Management	Secure storage of API keys, tokens, certificates, and service account credentials
Dynamic Secret Injection	Secrets are injected at runtime into CI/CD pipelines without hardcoding
Automated Credential Rotation	Regular rotation of DevOps secrets to reduce exposure
Access Policies for Non-Human Identities	Restricts which pipelines and tools can access specific secrets
Audit Trails for Secret Access	Full visibility into when, where, and how secrets are used

9. Secure Password Self-Service for Banking IT Users (SSPR)

(IT Support & Operations)

Banking Challenge

Manual password resets for internal users increase helpdesk load and delay operations.

How Securden Helps

Securden Feature	How it Applies in Banking
Password Self-Service Reset (SSPR)	Secure self-reset for internal IT users
Identity Verification (MFA-based)	Prevents unauthorized resets
Audit Trails for Resets	Full compliance visibility
Policy Enforcement	Aligns with bank password policies

Outcome: Reduced IT workload without compromising security.

10. Securing Privileged Access in Banking DevOps Environments

(DevOps, Platform Engineering & Security Teams)

Banking Challenge

Modern banks rely on DevOps pipelines, automation tools, and infrastructure-as-code to accelerate application development and system updates. These environments depend heavily on non-human identities such as service accounts, API keys, tokens, and secrets. When these credentials are hardcoded, shared, or poorly governed, they become high-value targets for sophisticated cyber-attacks and lateral movement.

Traditional IAM controls are not designed to secure non-human identities or manage privileged access within automated workflows.

How Securden Helps

Securden Capability	How It Applies in Banking DevOps
Secrets Management	Secure storage of API keys, tokens, certificates, and service account credentials
Dynamic Secret Injection	Secrets are injected at runtime into CI/CD pipelines without hardcoding
Automated Credential Rotation	Regular rotation of DevOps secrets to reduce exposure
Audit Trails for Secret Access	Full visibility into when, where, and how secrets are used
Integration with CI/CD Tools	Supports secure automation without disrupting DevOps workflows

Outcome: Banks can secure privileged access across DevOps pipelines and automation tools while preserving development velocity. This reduces the risk of credential leakage, supply-chain attacks, and unauthorized access without sacrificing agility or innovation.

To conclude, reliable banking operations depend on secure, controlled access to critical systems. When privileged access is simplified, governed, and visible, IT teams can focus on availability, performance, and innovation instead of manual access management.

Securden Unified PAM: Banks can secure privileged access across DevOps pipelines and automation tools while preserving development velocity. This reduces the risk of credential leakage, supply-chain attacks, and unauthorized access without sacrificing agility or innovation.

To conclude, reliable banking operations depend on secure, controlled access to critical systems. When privileged access is simplified, governed, and visible, IT teams can focus on availability, performance, and innovation instead of manual access management.