Banking & Financial Services

Leading International Bank deploys ARCON for Privileged Access Management

international bank

total assets

$ 103 Billion

employees

90,000+

no. of privileged IDs

20,000+

devices integrated

10,000+

concurrent users

400+

client brief

Bank has been an early adopter of technology, implementing world class IT systems to support its business operations. Bank has seen tremendous technology changes in the last few years, with the entry of new technology products and increasing expectations of customers bringing about sea changes in the way banks operate. Technology to banks is not just about backend operations, it is about customer satisfaction.

Data is critical to the operations of any financial institution. This bank was no different. This data is held on various critical server farms and sometimes even spread across locations. Bank was engaged in with its massive customer base of more than 3 million credit card customers & 20 million banking customers.

the challenge

Our client operates in multiple geographies with more than nearly 6600+Bank ATMs and 2500+ branches. Bank has dedicated IT team to manage data center and IT for managing the bank's core banking solution, infrastructure design, project management and services management. Technology has been key agenda for the bank over the years with impressive IT security. Banking Security team prides itself in being a market leader and as such not only adheres to industry regulations, but imposes strict security policies and procedures on itself to ensure sound security across all of its operations.

Bank faced a key issue for managing privilege identities across IT systems. Bank works in a shared data center environment for various group companies to support technology initiatives. To manage internal compliance and meet regulatory requirements, bank used highly manual and time consuming approach to managing privilege identities. Standard passwords applied to critical server environment which were stored in separate paper envelopes.

Growing concerns for the bank was to manage ever increasing privilege identities & compliance issues. Administrative concerns were added pain areas for administrative users.

Our team of consultants assessed such issues with series of discussions with system administrators, business users, application owners, support personnel and IT steering committee members of the bank. Based on responses from various IT Infrastructure teams we realized the fact that within 10 years of technology advancements the scale of server and the number of privilege users managing the same had almost quadrupled.

Banks Information Security Group and IT Compliance Group were under tremendous pressure from a resource and workflow perspective. This group has wide responsibilities including on-boarding and off-boarding users, enforcing security policies for managing privileged accounts and ensuring accountability to use of such highly critical accounts. Primary goals for investing in a privileged identity.

the solution

Bank choose ARCON Privileged Access Management Solution, which is a multitier life-cycle solution for securing, managing, password management and end-end monitoring of all activities associated with privileged accounts.

The initial phase of the project entailed rollout of Access Control Settings considering shared environment of the data center. This enabled approval for every access to sensitive data, improved productivity and access based on service tickets. Maintaining the log for each access request were added silver line to this solution.

Second phase of the project rollout focused on creation of enterprise level Password Vault which enabled bank to enforce an enterprise password policy across their most critical IT systems. This feature allowed ensuring accountability and access on need-to-know basis for data center, application and technology support teams.

ARCON PAM helped bank to establish a central management console for flexible operations of all actions associated with password management from requests to resets. Solution design provided better authentication and audit capabilities. All user accounts were integrated within the ARCON PAM (Privileged Access Management Solution) central repository – including

MSSQL, Oracle over toad, Windows admins, Unix Root and super admins, SSH based logins (for switches, routers, swift users, firewall and Cisco based user accounts).

Eventually, ARCON PAM helped the bank to store and monitors critical audit trails for audit, compliance and forensic purpose. ARCON PAM managed to provide highest satisfaction to Risk managers with mechanism for log review for critical sessions with collaborative integration with SIEM solution.

Significant benefits of the consultative approach to ARCON PAM deployment are highlighted below.

challenge	solution	benefit
Administrators need to remember multiple administrative passwords to login to different systems.	Single Sign On (SSO)	Significant reduction in managing account credentials & ability to admin-ister systems using individual identity
All personnel had equal privileges for usage of credentials.	Custom Access Control Settings	ARCON PAM allowed risk team to define custom access control based on requirement and job profile.
No accountability for usage of Privileged IDs	SMART* Audit Trails	Comprehensive audit trails generation for compliance and review
Inadequate enforcement of password policy & IS control for system users	Secure Password Management (SPM) . Change Control . Electronic Vault . Secured Printing	Seamless workflow & batch job oriented password management coupled with custom solution for storage ready secure envelopes.
Non accountability and trace for vendor activities	Vendor Access Controls	Comprehensive audit trails generation for compliance and review
Identity theft and sharing of critical system credentials.	Dual Factor Authentication (Soft Token based)	Minimize sharing of password.
Review of administrative user activities	Integration with Symantec Log Review Tool	Designing of interoperable work-flow allowed for seamless integration with Log review tool to ensure end-to-end monitoring.

*SMART refers to Specific, Meaningful, Aligned, Realistic, Time-based

about ARCON

ARCON is a leading Information Security solutions company specializing in Privileged Access Management and Continuous Risk Assessment solutions. With its roots strongly entrenched in identifying business risks across industries, it is in a unique position to comprehend and identify inherent security gaps in an organizations infrastructure framework and build and deploy innovative solutions/products to significantly mitigate potential risks.