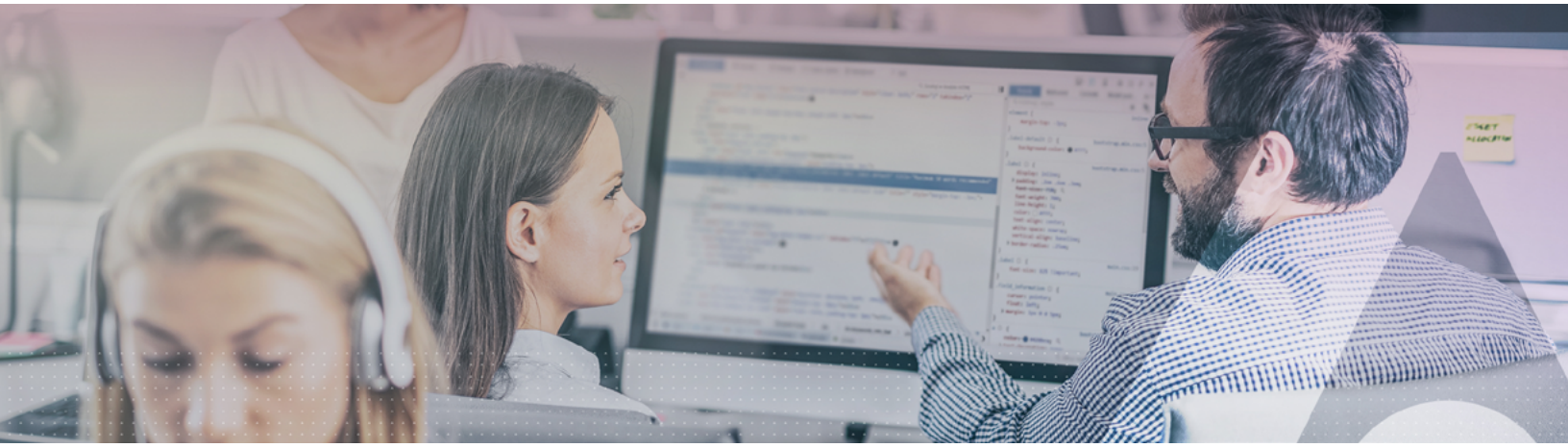
cpl.thalesgroup.com

THALES
Building a future we can all trust

Reduce risk, optimize cost, and accelerate digital transformation for financial services in India



The financial services industry is going through massive digital transformation driven by changing consumer habits, competitive pressures, and technological advances. The trend towards a new all-digital customer experience is causing a rapid adoption of new technology to support better capabilities and scalability. However, the combined challenges of cybersecurity threats and a stricter regulatory environment heighten the risks and increase the costs of digital transformation. Thales can help financial service providers mitigate risks, control costs and accelerate digital transformation by optimizing and automating data-centric protection throughout their hybrid IT environments.

The drive towards innovation and transformation

The growth of the digital economy has completely changed consumer habits. Consumers have come to expect a hyper-personalized experience that is fast, convenient and secure. It is no different in banking, where digital-only banks are growing rapidly, with several of them already attracting millions of customers per month with an all-digital, low cost experience.

This is driving innovation across the financial services industry. Banks have been quickly adopting technologies to enable secure, remote, multi-device banking transactions; secure digital payments leveraging biometrics, tokens, and context-based security; and even the full digitization of contracts, subscriptions and consumption of services.

Meanwhile under the Digital India mission, the Government of India has formulated 'Policy on Open APIs, that promotes software interoperability for all e-Governance applications & systems and provide access to data and services to citizens through multiple channels, such as web, mobile and common service delivery outlets.

Banks are leading with open banking initiatives driven by innovations from Fintechs that includes sharing of financial transactions through APIs.

Finally, the pandemic has forced an once unthinkable shift towards remote work and a mostly cashless and contactless payment society. This has resulted in the adaptation of systems for remote access, or a complete migration to the cloud for multiple bank systems.

Banks adapt through massive digital transformation

These trends have led banks to adopt modern electronic bank account management (eBAM) systems to open, maintain, and close accounts and to generate reports required by regulations. Consequently, banks are in the midst of a massive digital transformation. They have:

- Created secure mobile applications and end to end integration with core banking systems such as eBAM and Customer relationship management (CRM) for on boarding, mobile banking, and mobile payments.

- Put in place contextual transaction risk analysis (TRA) systems that integrate machine learning and artificial intelligence with strong customer authentication.
- Adopted hybrid and cloud-based workloads for core banking applications, which enables scalability and flexibility and supports employee remote access.
- Employed modern automated digital certificates and blockchain-based networks for financial, inter-bank, and foreign exchange transactions to create a non-repudiatable transaction record.
- Responded to open banking mandates by:
  - Adding capabilities for secure communications with third parties to core offerings.
  - Employing big data analytics to gather insights and capitalize on consumer behavior and preference data.
  - Making the multi-factor authentication process as easy as possible for customers.

Cybersecurity and regulatory risks escalate transformation costs

The process of digitalization has forced financial institutions to capture ever-increasing amounts of sensitive customer data to make banking easier and to create new desirable financial services for customers. But the dramatic rise in cyberattacks together with the dissolution of the security perimeter caused by the adoption of hybrid IT, generate the need for ever more security solutions. With multiple solutions protecting different platforms and different environments, the costs and complexity of protecting the new hybrid IT infrastructure grows exponentially.

Today organizations & financial institutions are facing more and more compliance and regulatory measures to protect the confidential & sensitive data wherever it is stored or used (data at rest/data in transit protection)

A very important measure to be adopted is: **decouple keys from data** - encryption keys should always be segregated and separately managed from application owners in a certified key management solution (FIPS 140-2 Level 3)

Some of the below compliance mandates have necessitated for having defense in depth data security controls

ISO 27001 Requirements: A.12.3 Cryptographic controls & Key Management

- PCI DSS (Payment Card Industry Data Security Standard)
- RBI Guidelines on Information Security/Cybersecurity Framework/Digital Payments Guidelines
- SEBI for CyberSecurity & Resilience Framework
- IRDA – Guidelines on Information & CyberSecurity
- IDRBT guidelines for Cloud Security
- UIDAI guidelines for Aadhar Vault
- NPCI DEM Mandate/Message Authentication Code
- GDPR (General Data Protection Regulation)
  - enforced from 25 May 2018
- Data Protection Bill (Coming soon)
  - Privacy by design principle to be incorporated

Financial institutions find themselves in a difficult situation. The digital customer experience, openness of modern banking and flexibility of hybrid IT are essential to their business. Nevertheless, they create a vulnerability when it comes to privacy and data protection.

How Thales can help: A cybersecurity approach for risk reduction and cost optimization

Challenge 1: Protection of the cloud transformation

While cloud platforms may be secure, the shared responsibility model dictates that, the organization that owns the data and grants access to this data is ultimately responsible for its security. It is important to choose a data security framework that works across multiple cloud providers, since 81% of organizations use more than 2 cloud service providers.

Solution: Streamlined Data and Identity Protection across Hybrid IT

Thales solutions streamlines data and identity protection in the cloud, implementing solutions that can scale across multi-cloud environments and allows customers to reduce the number of security solutions used, reducing cost, complexity and points of failure.

Thales Data Protection solutions protect sensitive data at rest with the CipherTrust Data Security Platform, using obfuscation technologies, such as encryption and tokenization, so that even if the data is stolen, it is unusable to cyber criminals. Thales Hardware Security Modules (HSMs) safeguard digital identities, applications and sensitive key materials that are used to protect applications and new initiatives based on blockchain or IoT technology. Thales network encryption solutions protect network traffic between data centers and the headquarters to backup and secure disaster recovery sites — whether on premises or in the cloud.

Thales Identity and Access Management solutions simplify user access to cloud services, streamline cloud identity management, and help eliminate password difficulties for IT and users. The solution maintains both security and a frictionless user experience by requiring an additional authentication in high-risk situations.

Challenge 2: Complexity of privacy compliance and data protection

The complexity of compliance with the myriad of global regulations and the challenge of protecting data across multiple environments is a major challenge for financial service providers. Data security and privacy compliance need to be automated with policy-based protection for all sensitive data.

Protect your sensitive data, regardless of where it flows or resides.

Determine where your most sensitive assets are located across your on-premises, cloud, and virtual environments. Search your file servers, applications, databases, and virtual machines for data at rest that must to be protected.

Solution: Simplified compliance with centralized data and identity security

The Thales CipherTrust Data Security Platform unifies data discovery, classification, data protection, and unprecedented granular access controls with centralized key management – all on a single platform. This results in less resources dedicated to data security operations, ubiquitous compliance controls, and significantly reduced risk across your business. SafeNet Trusted Access provides a single pane view of access events across your app estate to ensure that the right user has access to the right application at the right level of trust. Thales' access management and single-sign-on solutions add granular control over the access policies.

Challenge 3: Protection for omnichannel digital payments

Payment processing is the lifeblood of all financial service providers and merchants. Ensuring the security of consumer data is essential to the integrity of intra-bank network payments, ACH transfers, check clearing, mobile payments, credit card and "instant" payments peer-to-peer systems.

Solution: Globally Deployed Payment Security Solutions

Thales payment solutions secure 80% of payment card transactions worldwide. Thales Payment HSMs are used by issuers, acquirers, processors and payment networks to secure all manner of financial transactions and emerging payment models globally. Our CipherTrust Tokenization solution dramatically reduces the cost to comply with mandates like PCI DSS by replacing sensitive personal data with valueless tokens.

Thales helps more than 3,000 financial institutions secure their banking and payment services around the world. Thales solutions help organizations simplify financial services compliance, facilitate security auditing, protect their customers, and avoid data breaches, ultimately reducing the cost and risk of adopting new technologies and achieving competitive advantage.

Challenge 4 : Breaking the Security Silos & Adopting a Platform Strategy

Some data might require encryption, while other data may need to be tokenized, masked, deleted or left as is. Using single purpose tools can only secure specific type of data, system or environments.

Implementing disjoint technology products to apply data-level protection can create data silos and security gaps, defeating the purpose of an integrated data protection strategy across the organization.

Solution

Effective data protection controls & measures have to address the organization's unique data security requirements, while keeping it flexible and scalable to accommodate the new requirements over time.

Rather than purchasing multiple products from multiple vendors, organizations are better served by implementing a comprehensive data security platform.

The major advantage of The Thales CipherTrust Data Security Platform is that protection is applied to data itself, independent of the data's location.

It becomes more effective as it happens automatically—sensitive data gets identified as soon as it enters an organization's IT ecosystem, and get secured with policy-based protection that lasts throughout the data lifecycle

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us