THE BANKING HANDBOOK

Mastering Data Security And Compliance In The Digital Age

TABLE OF CONTENTS

Introduction

New-age enterprise banks have customers across different geographies, countries, and locations. With millions of transactions processed every minute across a global infrastructure, keeping track of sensitive information from falling into unauthorized hands is challenging.

So, what makes the banking sector a hacker's favorite playground? Is it because they have access to more sophisticated attack techniques? Or is the security infrastructure insufficient to protect data?
The answer is yes to both possibilities.

Banks undergo continuous digitization of infrastructure that creates new attack surfaces and vulnerabilities, which, most of the time, go undetected. Simultaneously, there are millions of bank transactions happening every minute. So how can banks protect their data as they expand globally in a highly operative network?

This eBook explains the evolving banking landscape affecting data security and current architecture limitations to protect data. It suggests how enterprise banks can benefit from Fortanix's unique approach to securing data. Fortanix recommends decoupling security from the infrastructure. It means that even if the firewall gets broken and a hacker finds their way into the network, the data is not a sitting duck.

Popular Trends

There is a visible transition in Banking with the 'brick and mortar' model shifting towards digital channels. Banks are increasingly moving to the cloud and delivering superior customer experiences through channels like internet banking, cards, and online trading platforms. On the flip side, this has also increased concerns around data security, explicitly preventing digital fraud, securing cross-border data transfers, and complying with changing banking regulations.

Adoption of Cloud, AI/ML, Blockchain

As the market for cloud security solutions in the banking sector is set to grow at a CAGR of 33.1% for the forecast period (2021 – 2026), securing data in the cloud is increasingly important. AI and ML are critical in new age banking from a data security perspective because they can help detect and prevent cyber-attacks by analyzing large amounts of data in real-time and identifying patterns and anomalies that may indicate a potential threat. Still, they also present security risks if not properly implemented.

Meanwhile, the growing blockchain ecosystem has raised concerns about data privacy and protecting sensitive information. Since blockchain is a decentralized system, once data is recorded on the blockchain; it can be accessed by anyone with permission to view the ledger, making it essential to manage the visibility and access to sensitive information. Blockchain security measures such as encryption, access controls, and network segmentation must be implemented to protect sensitive information and ensure data privacy.

Popular Trends

Merger and Acquisitions

The rapid growth of fintech institutions, neo banks, new digital banking platforms, and other digital marketing places presents a lucrative opportunity for growth for larger enterprise banks via mergers and acquisitions.

Integrating systems from the acquiring and acquired companies can result in data being stored in disparate systems, leading to complexities in securing the data.

Additionally, different security protocols and standards in place at the two companies can make it challenging to ensure consistent and effective data security measures are in place across the newly merged entity. From a security perspective, financial institutions must enforce uniform security controls across this ever-expanding ecosystem of newer branches, locations, and technologies.

Rise of Super Apps – Banking and Everything Else

Digital banking was primarily limited to paying bills, checking balances, and making transactions. However, because of fierce competition from magnanimous marketplaces such as Amazon, Google, Paypal, etc., enterprise banks are incorporating eCommerce and social media platforms. For example, banks facilitate extended marketplaces so customers can now shop and buy tickets for flights, meals, movies, and groceries and win real money as loyalty points.

This new banking phenomenon has given rise to partnerships with third-party vendors requiring banks to share their data pools with several other businesses. As a result, a vast amount of data floating in an open bank ecosystem is a hot target for cybercriminals.

Data Security Challenges

The challenge of securing data has become a top priority for banks, especially with the ongoing shift toward digitalization. Integrating cloud technology and interconnected systems has made managing data more intricate and ensuring its security a monumental task. When data is spread across multiple clouds, it becomes increasingly difficult to secure, especially for larger banks with multiple branches and locations. To address this challenge, banks must balance legacy security systems with modern infrastructure and expand their security measures to accommodate a growing network. They must also keep pace with evolving regulatory demands and prioritize protecting privacy.

Cut Down on Complexity

The primary challenge is fine-tuning interoperability between legacy data security systems and modern architecture. However, managing data residing in disparate systems is the bigger challenge.

In a multi-cloud environment, data is dispersed in several systems. Due to infrastructural complexity, misconfigurations, and vulnerabilities, ensuring data is fully secured becomes cumbersome. The complexity becomes multi-fold for larger banks with increased locations and branch offices to manage security for fragmented data.

Stay In Line with Emerging Regulatory Requirements

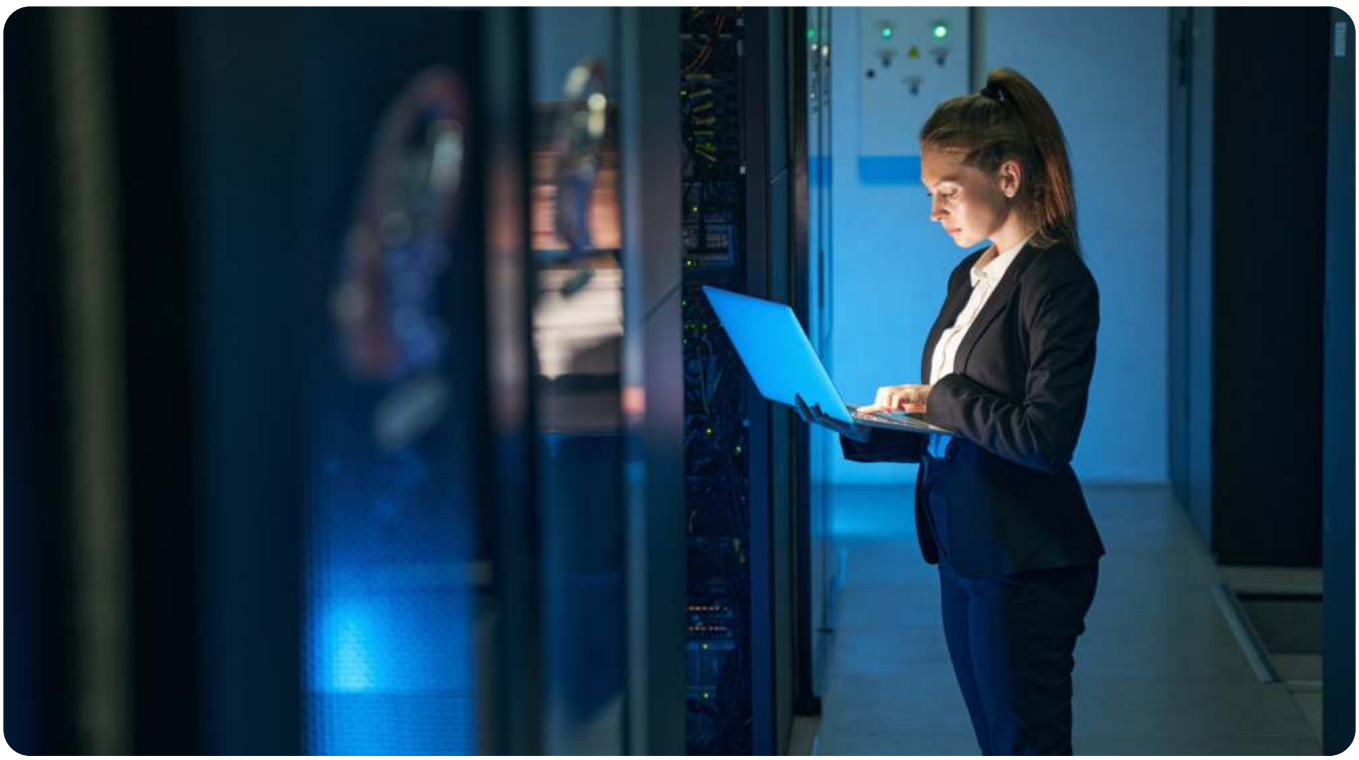
With the high volume of data flowing across borders and systems, banking is more regulated and scrutinized than ever. Data is constantly under regulatory scrutiny by regulatory bodies that strictly examine every stage of data handling, including data collection, processing, and storage. This has increased the challenge for banks to stay compliant and in line with some of these varied regulatory requirements.

Scale Security to The Expanded Ecosystem

Larger banks interconnected with partner banks and marketplaces have many partner institutions, online systems, locations, and branches. Their complex infrastructure and technology make data security management a herculean task.

For example, when a bank acquires a firm from a different geography, it must fine-tune its security setup to meet the region's compliance laws. Hackers are now adept at finding loopholes within the security apparatus of partner banks, less secure branch offices, and other connected systems.

So, banks need data security that can scale and controls that can be applied across this system. They need centralized audits, control, and reporting to assess and fix security gaps. Ensuring privacy at the core of an enterprise is also critical.



Current Architectural Limitations

Data Security is Siloed and Disparate

Enterprise banks rely on multiple vendors for their data security requirements, such as encryption and key management solutions. They need 2-3 legacy HSMs, multiple cloud-native key management systems, and other point solutions for secrets management and database encryption (TDE).

These disparate solutions solve only part of the problem at a premium price with costly maintenance and additional costs for every new application. And with no integration with public cloud/hybrid infrastructures, organizations must maintain separate solutions for on-premises applications and public cloud. This is inefficient and makes it very difficult to apply consistent policies and controls across the organization and to undertake compliance audits.

The solution is to replace this fragmented data security system with a single unified system for the entire enterprise. A centralized dashboard can help them track data moving within different networks.

Current Architectural Limitations

Not Suited for Hybrid Environments

Banks must manage a polarised world of legacy data security infrastructures and cloud-based applications to meet strict compliances and enable digitization.

The existing legacy systems often fall short when managing cloud environments. Existing HSM/KMS solutions have typically treated on-premises data security and cloud data protection as two problems, with two solutions delivered on two different technology stacks. Due to the lack of interoperability between systems, moving from one system to the other is difficult, making cloud deployments almost impossible.

Legacy Systems Prevents Scaling and Integration

In large enterprise banks, replacing decades-old systems with more modern technology requires time and expense that is not feasible in a fast-moving environment. For example, where a million transactions are getting processed every minute around the world, there's little room left for banks to alter the existing setup.

Many institutions suffer because of the inadequacy of legacy systems that cannot keep up with the drastic rate of change. However, banks must leverage new digital technologies such as the cloud, big data, mobile, and the internet for business expansion to create better customer experiences. API-led connectivity using the lightweight REST protocol can help banks modernize legacy systems. APIs are discoverable and reusable across multiple projects within a large network.

New Architectural Requirements

Pervasive Data Security

Because of cloud adoption, most banks have data stored and processed in multicloud and hybrid environments that keep changing as per business needs. This setup creates data blind spots that are easy for criminals to hack. As a result, the prime focus should not be on securing fluctuating environments but on the data itself.

The security teams can protect data only if they have complete visibility control of data across multi-cloud and hybrid environments. Businesses must use an agile encryption approach that standardizes and centralizes cryptographic operations so that encryption becomes pervasive throughout all applications and works with any IT Infrastructure

Privacy By Design

Data security compliances applicable to the banking industry underline the implementation of Privacy (and Data Protection) by Design and Default.

Privacy by Design demands organizations to incorporate privacy and data protection principles right from the earliest stages and throughout the lifecycle of any development viz product, software, infrastructure, service, etc. This law is applicable, especially when processing personal data.

Under this approach, banks can implement tokenization, encryption, and pseudonymization (replacing personally identifiable information (PII) with anonymous identifiers)
The security teams can anticipate and prevent privacy-invasive events before they happen. They can create auditable logs of when their records are accessed and enforce a disposable data policy for outdated records to avoid data leakage.

New Architectural Requirements

Scalable Security Architecture

Because of global expansion, cloud migration, and mergers, there are several integrated systems into security infrastructure. Banks often must manage each one of them as they lack interconnectivity. However, if you count the possibilities of human error, managing different systems with separate configurations and keys for each of them could result in vulnerabilities.

For instance, creating and managing separate keys for each cloud is time-consuming and complex. They are often controlled by cloud vendors and incompatible with on-prem systems. There are unnecessarily too many tools doing the same job for each cloud. This creates a lack of agility, automation, and control and requires an additional workforce dedicated to each system which is not feasible in the longer run.

Banks need fully API-driven security architecture to easily connect to other systems, cloud-native technologies, and modern DevOps tools. They need a consolidated security platform with a minimum configuration to get complete data visibility across their hybrid cloud environment compared to other multiple products deployed within the infrastructure. It will also reduce the total cost of service (TCO).

Fortanix Data Security Manager (DSM) as a Solution

Unified Data Security

Fortanix DSM is an integrated platform that offers secure key management and cryptography services, including cloud key management, secrets management, and tokenization, to protect sensitive data in public, private, hybrid, or multi-cloud environments.

There's no need for enterprise banks to get tied by the on-prem and other architectural limitations. Fortanix DSM SaaS is infinitely scalable and offers elasticity that matches the agility of new modern cloud-bound IT infrastructure.

Data Controls and Audit Trail

Banks can fulfill compliance regulations with comprehensive data controls and tamper-proof global audit logs. When all access to personal data is automatically logged in a centrally viewable tamper-proof global audit trail, there is never any dispute about who accessed which data and when.

For example, if the decryption keys are deleted, the deletion is logged into the central audit log and is irreversible. Data cannot be reused with key deletions, providing banks greater security.
They can retain control and management of encryption keys with centralized management, consistent access control policy, and centralized audit logs. With BYOKMS and BYOE, banks can also store cloud keys externally to help meet the most stringent privacy laws.

Broad Integration Ecosystem

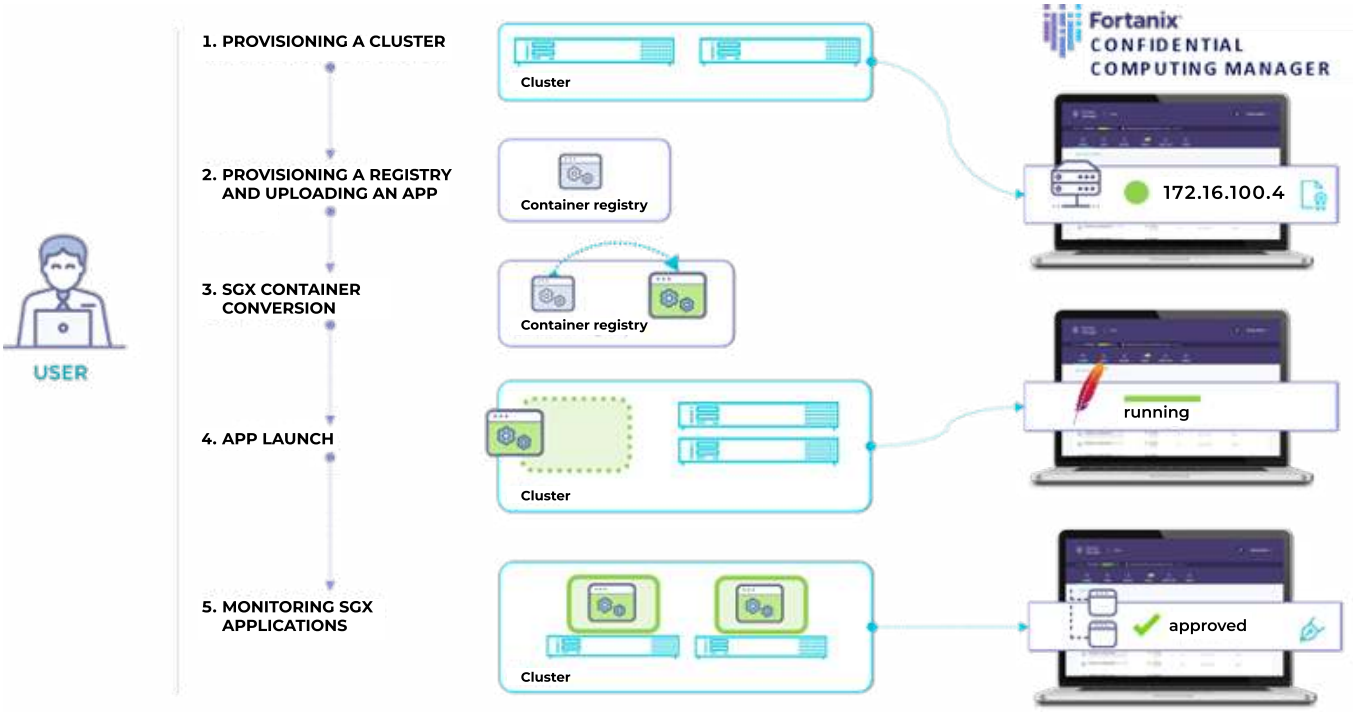
Banks can seamlessly integrate with 100+ Fortanix partners via RESTful APIs in a developer-friendly environment. Powerful RESTful APIs make it easy for developers and DevOps teams to use and integrate data security into their applications. Elastic scalability, high availability, and disaster recovery are built-in with a broad set of Rest APIs.

An unrivalled partner ecosystem of seamless integrations helps banks expand core functionalities to the larger IT ecosystem and eliminates security gaps.

Why Choose Fortanix Data Security Manager

Confidential Computing Powered Technology

Fortanix is a founding member of the Confidential Computing Consortium alongside companies like Google, Intel, and Microsoft.



Confidential computing protects data and applications by running them in secure enclaves that isolate the data and code to prevent unauthorized access, even when the computing infrastructure is compromised. Intel® SGX technology represents one of the leading implementations of Confidential Computing. It allows organizations to isolate the software and data from the underlying infrastructure (hardware or OS) using hardware-level encryption.

Why Choose Fortanix Data Security Manager

Modern Developer-Friendly Architecture

Developers must work with applications that need access to private data. They do not have the expertise to ensure data privacy and security before accessing the information. This is why DevOps and Security teams must collaborate to ensure data privacy. Using REST APIs, they can implement efficient secrets management, integrate crypto into applications in the coding phase, and substitute a token for sensitive data.

Fortanix Data Security as a Service (DSaaS) platform offers restful APIs that developers already use to enable modern cloud and mobile apps. It supports traditional crypto interfaces such as KMIP, PKCS#11, JCE, CAPI, and more, allowing easy application integration. For C/C++ programmers, the solution provides a PKCS#11 interface through the library. Java programmers can access the platform through the JCE interface and Java SDK.

Cloud Friendly Architecture

Fortanix DSM is an integrated HSM/KMS solution that can support multiple deployment options to meet organizations' security, latency, and operational simplicity needs. The solution is deployed on-Prem and SaaS, having the same functionality and integration capabilities.

The SaaS service is 100% remotely controlled, instantly available with zero upfront costs, and can be accessed via the internet with a button click. It is built using FIPS 140-2 Level 3 certified hardware and provides an entirely secure environment that can interact seamlessly with the other clouds (AWS, Google Cloud, etc.). There is no hardware/software maintenance or management required.

External Key Management

Compliance mandates require organizations to separate keys from the data it protects and, in a few cases, to store them within regional or national boundaries. The External Key Management system or Bring-Your-Own-Key-Management-System (BYOKMS) approach is essential.

Fortanix integrates with GCP EKM and AWS XKS service to enable organizations to move the data to the cloud and get the same level of security for keys they're used to in their on-prem environments. Encryption keys are always under organizations' control and stored inside a FIPS 140-2 level 3 certified HSM, away from the cloud. Organizations can enable and disable access to data from specific instances and locations at a click of a button in real-time.

Use Cases

1. Secure cloud migration and cross-border data for a multinational investment bank headquartered in Europe

Challenge

Protect Data and Meet Compliances When Moving Workload to the Google Cloud

· The bank was planning to move its workload to the Google cloud. Transferring data was only possible if they met compliance requirements such as (GDPR and Schrems II).
· They needed an External Key Manager (EKM) to manage cryptographic operations outside the Google cloud.

Solution

We offered Google EKM with Fortanix DSM SaaS in the EU Region.

Problems we solved

· The bank could initiate transferring the data to Google Cloud only because of the External Key Manager.
· The bank did not want to deploy hardware as it would require additional maintenance and operational costs. Fortanix delivered everything as a Service that did not require any physical infrastructure.
· Fortanix DSM is a "cloud service provider agnostic" SaaS solution with integrated Business Continuity and Disaster Recovery. The service is based on FIPS 140-2 Level 3 certified hardware appliances.
· DSM SaaS solution is the most modern, mature, easy-to-handle single-pane-of-glass solution, with the highest level of security the bank needs.
· Fortanix Terraform integration meets the bank's requirements for automation.
· The bank is impressed by the benefits of the confidential computing technology that Fortanix DSM offers.
· Our security architecture gives them the confidence that their keys never will be exposed to unauthorized users and will remain in the assigned region (EU). This arrangement has convinced them to trust Fortanix.

2. Secure analytics and data collaboration for a global investment bank

Challenge

Protect Data and Meet Compliances When Moving Data Lake Backups from On-Premises to AWS S3

· A global investment bank wanted to move its data lake backups (built on the Hadoop platform) from on-premises to AWS S3 (Amazon Simple Storage Service).
· The bank selected AWS S3 to make copies of all uploaded S3 objects across multiple systems and store them.
· They wanted to access centralized data whenever needed from any location and protect it against failures, errors, and threats.
· However, the compliance team insisted on adding a layer of encryption under the bank's control.
· The team wanted to ensure root encryption keys were segregated from the data on AWS. They did not allow the backups to be moved from on-prem to AWS S3 without it.

Solution

We positioned Fortanix Data Security Manager (DSM) leveraging CSE (client-side encryption). CSE, defined broadly, is encryption applied to data before it is transmitted from a user device to a server. With Fortanix DSM, it was easy to configure CSE-C for the AWS SDK (software development kit) and Hadoop.

Problems we solved

· Inside Fortanix DSM, the KEK wrapped the data encryption keys using Authenticated Encryption mode, i.e., AES (Advanced Encryption Standard) 256-bit encryption under Galois/Counter Mode (AES-GCM).
· Fortanix DSM returns the raw and wrapped data encryption keys to the respective Hadoop nodes that initiated the calls through AWS SDK.
· At this point, the content encryption was performed locally, i.e., on the Client-Side.
· Neither Hadoop nor the AWS SDK retained or persisted any information besides the wrapped data encryption keys, which were stored on Amazon S3 against the object Metadata or in Instruction Files if so configured.
· The data was successfully encrypted en route cloud.

3. Ensuring operational/service continuity and meeting compliance for one of the largest Asian bank

Challenge

Lack of Agility, Automation, and Control with Data Security Infrastructure When Moving to the Cloud

· The bank was using too many disparaged data security products. There was a need to centralize it for better visibility and audit capabilities.
· Multiple systems required an additional workforce dedicated to each system and, therefore, was not feasible in the long run.
· As they moved their operations to the cloud, the existing security platform, which was a fragmented setup, became complex and hard to manage.
· Because of the lack of agility, automation, and control, the customer was not confident about its existing data security infrastructure.
· They required a hybrid-cloud data security platform to consolidate all their HSM/KMS infrastructures to move assets to the cloud.

Solution

We offered DevOps-friendly, multi-cloud-friendly application-level encryption with a consolidated platform.

Problems we solved

· Fortanix DSM fulfilled the bank's need to integrate via an API-driven environment and consolidate its data security control under a single platform.
· Our solution provided visibility across their hybrid cloud environment compared to other multiple products the customer had deployed.
· The bank achieved complete control of the data security management that helped in business sustainability and expansion policies.
· With Fortanix DSM, the bank also meets the compliance requirements, as underlined in the Personal Information Protection Act 2011, that regulate the collection, usage, disclosure, and other processing of personal information by government, private entities, and individuals.

4. Improving compliance with privacy and industry standards for an Asia-Pacific bank

Challenge

Compliance gap for their Cloud WAF (Web Application Firewall)

· The bank has its own HSM for on-premises WAF but not for its Imperva Cloud WAF.
· The bank needed to keep its private keys on FIPS 140-2 Level 3 HSM.
· The challenge was that Imperva has dozens of PoPs worldwide, but deploying HSMs would have cost a ton and been inflexible.
· Imperva opted to integrate with FTX to become the cloud HSM. To date, we are the only integration partner for this use case.

Solution

We offered FIPS 140-2 Level 3 certified HSMs delivered as a service.

Problems we solved

· Fortanix DSM secured private keys behind the Imperva Cloud WAF. The bank could meet compliance requirements.
· They get to consume HSMs as a service which is a big win for them because getting anything on-prem requires additional approvals.
· Fortanix also aligned well with Imperva to give the bank the best technical solution.

Conclusion

Banks can now run sensitive applications and data on untrusted infrastructure, public clouds, and all other hosted environments, which gives them more control over the security and privacy of applications and data.

With Fortanix Data Security Manager, enterprise banks can successfully secure data across an extensive branch network, ATMs, and international monetary exchanges. For the ones focused on acquiring smaller banks and fintech firms, they can migrate data securely and fulfill all the necessary compliance requirements such as GDPR, PCI DSS, etc.