Trustway DataProtect

Financial services and Insurance

Three reasons you need to secure your data in the cloud

Financial institutions have been forced to accelerate digital transformation to improve customer experience and enable the remote workforce. This transformation helps businesses evolve, but distributed access, online working, data in motion and increasingly sophisticated cyberattacks have expanded the threat landscape. Data sharing, business process outsourcing and supply chain attacks also contribute to increase risks.

The move to cloud is an important step in digital transformation — and improving data security is critical to reducing business risk exposure. By leveraging encryption technologies and techniques, financial institutions can benefit from better controls, enhanced digital autonomy and increased visibility. Here are three reasons you must secure data in the cloud, and the Atos approach to making it possible.

To mitigate risks

With traditional IT, the owner is responsible for everything from networking equipment to applications. However, security is different in the cloud and in data centers.

In the **shared responsibility model**, cloud providers are responsible for the security of the cloud, while customers are responsible for data security in the cloud. The model varies by service model (IaaS, PaaS SaaS) and cloud service provider, but regardless of the model or service provider, data and access are ultimately the customer's responsibility.

It is up to cloud customers to verify shared responsibilities and controls over data (at rest and in motion) and encryption keys in the cloud-native and customer key management systems (CKMS)[1]. CSPs must provide the ability for customers to manage their own data encryption keys[2].

To ensure data sovereignty in the multi-cloud

There are many reasons to embrace a multi-cloud strategy: avoiding vendor lock-in, backup and disaster recovery, better fit for needs, regulatory compliance and data sovereignty.

Relying on multiple cloud vendors increases the operational complexity of managing data security and creates a risk of losing control and visibility over encryption keys. In addition, cloud-native key management services have a limited ability to automate the lifecycle of encryption keys.

You need to level up protection controls of sensitive and regulated data (Personal, health and banking information) across multiple environments by taking centralized control of encryption mechanisms and keys, also making sure there is a separation of duties for key management based upon organization and location.

To comply with regulations

Cybersecurity regulations are growing and evolving to keep up with the evolving technological environment, and sensitive data protection regulations are becoming more stringent.

The Payment Card Industry Data Security Standards (PCI DSS) require encrypting credit card account numbers stored in databases and ensure data stays secure when transferred outside. Encryption keys should be protected from unauthorized access. (PCI DSS Requirement 3[3]).

The upcoming EU Digital Operational Resilience Act (DORA[4]) aims to ensure that all participants in the financial system have the necessary safeguards in place to mitigate cyberattacks and other risks. Data encryption and key management can significantly reduce the risks of cyberattacks.

The EU General Data Protection Regulation (GDPR) requires appropriate security of the personal data to ensure integrity and confidentiality, which can be achieved using pseudonymization and data encryption. (GDPR Art 5[5] and 32[6]).

The European Data Protection Board (EDPB) adopted recommendations on the measures following the Schrems II decision on compliance with the EU level of data protection of personal data. Encryption or pseudonymization can help protect data prior to being transferred to the data importer.

[1] Cloud Key Management System with External Origin Key | CSA (cloudsecurityalliance.org)
[2] CCMv4.0 Auditing Guidelines
[3] PCI Data Storage Do's and Don'ts
[4] DORA
[5] GDPR - Article 5 - Principles relating to processing of personal data
[6] GDPR - Article 32 - Security of processing

Atos

Atos Trustway DataProtect: Advanced data security for financial services and insurance

Trustway DataProtect offers a comprehensive encryption solution to protect your sensitive data:

- Removes complexity for securing data everywhere and gives back control (data sovereignty).
- Gives visibility for reporting and compliance.
- Provides an integrated platform (hardware security module and key management system) for enhanced data security.
- Enables the transition from partial customer control (Bring your own key - BYOK) to stronger customer control (Hold your own key - HYOK).
- Based on a 100% French-certified physical hardware security module (HSM) for high assurance and security.

Adopt BYOK for an extra layer of protection

By encrypting the data and controlling encryption keys, financial institutions can mitigate risk, comply with regulations and ensure that third parties cannot gain access to sensitive information stored in the cloud or transferred between affiliates.

Bring your own key (BYOK) is an encryption key management capability supported by many software as-a-service (SaaS) providers, which allows cloud service customers to retain control and manage encryption keys.

Imported keys are generated securely in a tamper-resistant certified hardware security module (HSM) and key export is controlled.

Atos Trustway DataProtect integrates with many SaaS platforms that support BYOK.

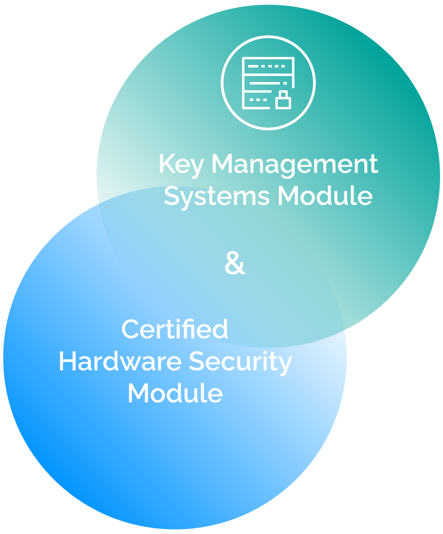
Manage keys from a single pane of glass

A panoramic view and centralized management of all data encryption keys reduces operation complexity while helping ensure data sovereignty and compliance.

Atos Trustway DataProtect provides a unified view of all encryption keys and eases the lifecycle management to remove dependency on third parties by offering:

- Customer management of key creation, rotation, deactivation, and destruction.
- Granular access controls and auditing for compliance.
- High-performance, scalable platform with no limit on the number of appliances that can be added to a cluster.
- Encryption key material storage separated from key usage locations.
- Separation of duties for key management, based upon organization and location.
- Auditing of encryption key management, usage and access.

Trustway DataProtect: Unique flexibility, undeniable benefits and 100% certified European technology expertise


Key Management Systems Module
&
Certified Hardware Security Module

For more information: Trustway DataProtect: ensure data security and bring compliance