Data Protection and Monitoring in Salesforce Using Shield

Kiran Konakalla

Kiran.Konakalla7@gmail.com

Abstract

The insurance industry in the European, Middle East, and Africa (EMEA) region faces unique challenges due to stringent data privacy laws such as the General Data Protection Regulation (GDPR). Salesforce Shield offers a robust solution to these challenges by providing encryption, audit trails, and monitoring capabilities. This paper explores how Salesforce Shield can be used to protect sensitive data, particularly Social Security Numbers (SSNs), and monitor user activities in Salesforce. It will also highlight how my experience with Salesforce Shield has been instrumental in managing sensitive financial data, such as custom commission objects and contract values, ensuring compliance with data privacy regulations and monitoring unauthorized data manipulations.

Keywords: Salesforce Shield, Insurance Industry, EMEA, Data Encryption, GDPR, SSN Masking, User Activity Monitoring, Compliance, Audit, API Monitoring

Introduction

In the EMEA region, insurance companies face significant pressure to comply with strict data protection laws like GDPR. Given the sensitivity of customer data, including personally identifiable information (PII) such as personal email or phone, Social Security Numbers (SSNs) in US, companies must take extra precautions to ensure the safety and privacy of their customers. Salesforce Shield is an advanced suite of security tools that provides encryption, monitoring, and auditing features tailored for organizations operating in such regulated environments. This paper examines how Salesforce Shield can help companies operating in different regions by offering advanced encryption and monitoring of sensitive data and activities within Salesforce.

Main Body

Problem Statement

The primary challenge in some industries, especially for companies operating in the EMEA region, is ensuring that customer data, PII, is secure and compliant with regulations like GDPR. The use of Salesforce as a CRM system to manage client interactions, claims, and sensitive financial data necessitates advanced security measures to ensure data privacy and integrity. Furthermore, monitoring user access to such sensitive information and tracking unauthorized changes or deletions is crucial, especially in highly regulated industries.

Solution

Salesforce Shield provides advanced capabilities such as Platform Encryption, Event Monitoring, and Field Audit Trail, which are essential for protecting sensitive information and tracking user behavior. The key features of Salesforce Shield include:

Platform Encryption: Salesforce Shield uses AES (Advanced Encryption Standard) with 256-bit keys and a random initialization vector to encrypt sensitive data at rest. For insurance and financial companies, this is

especially important for encrypting data like SSNs, claims information, and financial data. Fields such as SSN or bank account numbers are commonly stored in the Salesforce case object when customers email this information. Salesforce Shield allows the encryption of these fields to ensure that sensitive data is never exposed to unauthorized users.

Here's an example of how you can set up field-level encryption for sensitive fields like **SSN__c** in the **Case** object:

```
// Example of how to enable encryption using Salesforce Shield
public class CaseEncryptionService {
    public void encryptCaseSSN(Id caseId, String ssn) {
        Case caseRecord = [SELECT Id, SSN__c FROM Case WHERE Id = :caseId];

        // Encrypt the SSN field using Platform Encryption
        caseRecord.SSN__c = ssn.encrypt();  // pseudo-encryption method for illustration

        update caseRecord;
    }
}
```

In this example, the **SSN__c** field in the **Case** object is encrypted when a customer's Social Security Number is entered. Salesforce Platform Encryption ensures that this sensitive information is secure at rest.

1. **Monitoring and Event Tracking**: Salesforce Shield's Event Monitoring enables companies to track who is accessing sensitive information, which records are being viewed, and any changes that are being made. This is particularly useful for tracking data access and modification, especially when opportunities are locked, and no further edits should be allowed.
   In my personal experience, we used Salesforce Shield to monitor custom and standard objects where sensitive information is stored. Once an opportunity was closed, any modifications to these locked records were flagged by Shield, ensuring that no unauthorized changes occurred. Shield allowed us to track every interaction with these records, including API calls made to update Salesforce opportunity values post-deal closure via billing systems.
2. **API Monitoring**: Monitoring API activities is essential in understanding how data flows between systems and ensuring that no unauthorized updates are made to sensitive fields. For example, in insurance or financial companies, billing systems often update Salesforce opportunities once deals are closed. Salesforce Shield enables tracking of these updates through billing APIs and flags any suspicious or unauthorized changes. This is particularly crucial when contract values are being updated post-close, ensuring financial data integrity.
3. **Field Audit Trail**: Field Audit Trail provides a way to track changes to fields over time. For example, if a customer updates their PII information or if modifications are made to contract details, Field Audit Trail can store this information for multiple years. This is crucial for auditing purposes, especially in industries like insurance where changes to customer data need to be well-documented for compliance purposes.

Uses in the Insurance or Financial Industry

Salesforce Shield has proven to be an invaluable tool in the insurance sector, particularly in the EMEA or US regions. Key use cases include:

- **Compliance with GDPR**: Salesforce Shield's encryption capabilities help companies stay compliant with GDPR regulations by ensuring that sensitive information is encrypted both at rest and in transit. This is critical when handling customer PII, passport numbers, and other personal data.

- **Enhanced Data Privacy**: Insurance companies often receive sensitive customer information through various channels (email, phone, chat). Shield ensures that such information is encrypted and securely stored in Salesforce. For example, SSNs submitted via email to case records are encrypted, ensuring that only authorized personnel can access the data.
- **Monitoring User Activity**: Shield's Event Monitoring feature allows companies to track user activity within Salesforce, including what records are being accessed, viewed, or modified. This is particularly useful for monitoring sensitive insurance claims and financial data, ensuring that only authorized users have access to these records.
- **API Call Monitoring**: For insurance companies that integrate Salesforce with third-party billing or claims systems, Salesforce Shield tracks API calls to ensure that no unauthorized updates are made to critical records such as opportunities, claims, or contracts.

Impact

Salesforce Shield's encryption and monitoring capabilities have had a profound impact in multiple industries in different regions.

1. **Improved Data Security**: By providing advanced encryption for sensitive data, Shield helps companies avoid costly data breaches and ensures compliance with regional data protection regulations.
2. **Audit Trail for Compliance**: Shield's ability to track field changes and user activities provides insurance companies with a comprehensive audit trail, which is critical for demonstrating compliance during audits and regulatory checks.
3. **Reduced Risk of Fraud**: The ability to monitor user activity and changes to records helps reduce the risk of fraud and unauthorized data manipulation, particularly when dealing with sensitive financial data.

My Experience with Salesforce Shield

In my past experience, Salesforce Shield has been a game-changer in managing sensitive data, particularly for tracking modifications to custom objects like **Commission** and Standard objects like **Opportunity.** We leveraged Shield to monitor locked records, ensuring that once an opportunity was marked as "Closed," no further changes could be made without triggering an alert. This capability allowed us to maintain data integrity and avoid unauthorized changes to critical financial records. Additionally, we used Shield to track billing API calls, ensuring that updates made to opportunity values post-deal closure were valid and in line with company policies.

Conclusion

Salesforce Shield is an essential tool for insurance companies operating in the EMEA region, offering robust encryption, monitoring, and audit capabilities that ensure compliance with GDPR and other regional data protection regulations. By providing enhanced data security and real-time monitoring, Shield enables companies to protect sensitive customer data, monitor user activity, and maintain compliance with industry standards. My personal experience using Salesforce Shield highlights its value in tracking sensitive financial data and preventing unauthorized modifications to locked records. In the insurance industry, where data privacy and integrity are paramount, Salesforce Shield is an invaluable asset.

References

1. Salesforce. "Salesforce Shield Overview." Salesforce, 2021. Available: https://www.salesforce.com/products/platform/overview/shield.
2. European Commission. "General Data Protection Regulation (GDPR)." 2018. Available: https://ec.europa.eu/info/law/law-topic/data-protection_en.

3. NIST. "Advanced Encryption Standard (AES)." National Institute of Standards and Technology (NIST), 2001.
Available: https://www.nist.gov/publications/advanced-encryption-standard-aes.
4. Thompson, R. "Protecting PII with Salesforce Shield Encryption." Data Privacy Journal, vol. 15, no. 2, pp. 45-58, 2020.
Available: https://dataprivacyjournal.com.
5. Green, T. "Event Monitoring and User Activity Tracking in Salesforce Shield." Cybersecurity Insights, vol. 22, no. 5, pp. 89-101, 2019.
Available: https://cybersecurityinsights.com.
6. Williams, A. "Achieving GDPR Compliance in Salesforce with Shield." Salesforce Security Blog, 2020.
Available: https://security.salesforce.com/blog/achieving-gdpr-compliance-with-shield.
7. Davis, L. "Best Practices for Data Encryption and Monitoring in Salesforce Shield." Cloud Security Review, 2021.
Available: https://cloudsecurityreview.com.