salesforce platform

Salesforce Shield for Financial Services

How a new level of security can accelerate the financial services industry's move to the cloud

salesforce platform

Contents

salesforce platform

Introduction

The financial services industry is under constant pressures to increase profitability, compete with more nimble financial firms that operate solely in the cloud, and respond to rapidly rising client expectations – all of which are driving the industry to invest heavily in innovation. In this environment, the cloud has grown more attractive as a strategic asset, allowing the industry to become more mobile, social, agile, and respond to changing customer demands more quickly.

Yet some financial services companies remain reluctant to aggressively adopt the cloud because of concerns over data security, privacy, and their ability to comply with a myriad of regulations. Almost all the information collected by financial services firms is regulated, potentially sensitive, or private. Therefore, financial services must be assured they can use cloud computing services in a manner that meets the evolving demands of information security at all levels: infrastructure, network, and application. In addition, new controls for monitoring, auditing, and securing sensitive data (such as Salesforce Shield) will become important tools for streamlining compliance and governance initiatives that will open new doors to innovate at scale in the cloud.

> “We decided to move to the cloud for all the benefits of security, scalability, the fact that we don’t have to manage a data center, currencies and languages, and can easily adopt the enhancements.”
>
> *Paul Risk, Chief of Global Services & Architecture, The Warranty Group*

CHAPTER 1

The million-dollar question: Can the cloud offer greater security than on-premises software?

Since the dawn of the cloud era, the security of cloud vs. on-premises software has been the subject of heated debate, especially in regulated industries such as financial services, healthcare, life sciences, and government. According to Gartner, "No evidence indicates that cloud service providers have performed less securely than end-user organizations. The recent history of public clouds has demonstrated that brand-name, externally provisioned, multitenant services are not only highly resistant to attack, but also are a more secure starting point than most traditional in-house implementations."

Salesforce's multitenant platform most closely resembles how the financial services industry leverages a single, scalable repository for storing, processing, and displaying customer information on demand via their online portals. Salesforce's model of using unique identifiers that extend to each customer transaction should be familiar to any financial institution. However, unlike financial institutions, which often use disparate databases both within a specific business unit and across geographically dispersed regions, Salesforce maintains a single homogeneous platform that stores and process all customer data in a consistent manner – regardless of location or customer.

Trust and security have been cornerstones of Salesforce's success since our inception.

While data de-identification – encryption, tokenization, masking, and obfuscation – play a part in the overall data security model, it is our consistent infrastructure and defense-in-depth security approach that give Salesforce a unique security advantage over disparate enterprise environments.

salesforce platform

CHAPTER 2

Trust never sleeps:
Inside the world's most trusted cloud platform for financial services.

At Salesforce, trust is our number one value. Our world-class security strategies follow the same strict guidelines and approaches that most global enterprises employ to preserve the sanctity and security of their customers' data, at a massive cloud-based scale. Every Salesforce customer receives the same set of comprehensive trust features that are embedded into our platform:

INFRASTRUCTURE LEVEL

Salesforce's secure data centers have strong access control and physical security measures, including, but not limited to, biometric access, environmental controls, near real-time replication for disaster recovery, and backups. Salesforce has dedicated teams to monitor security of the service (CSIRT) 24/7 and a separate team that monitors the availability and performance of the system.

NETWORK LEVEL

Salesforce leverages multiple measures for network security including layers of access control and intrusion detection. Data for customers accessing the system is encrypted in transit using AES-256 encryption standards, ensuring that our users have a secure connection from their browsers to our service.

COMPLIANCE

Salesforce is compliant with key global industry standards including ISO 27001, SSAE 16/ISAE 3402 SOC-1, SOC 2, SOC 3, FedRAMP, PCI-DSS, and TÜV Rheinland Certified Cloud Service.

TRANSPARENCY

Transparency is key to how we operate and is a core tenet of our trust platform. Therefore, we are transparent about our system performance and incidents on our public trust.salesforce.com website. Here, customers can monitor uptimes and response times from instances within our multitenant, geographically dispersed, and multi-failover data center environments.

APPLICATION LEVEL

Every customer, regardless of the size of deployment, gets granular controls to ensure application-level security. From single sign-on and very granular password policies, to role-based and profile-based access to applications, reports, and fields, customers have a high control over how, where, when, and from what device users can access data at the individual field level.

“As a leading payments technology company serving millions of business owners around the globe, First Data adheres to rigorous federal and international compliance standards. Salesforce Shield allows us to incorporate compliance capabilities into our apps to better serve the needs of our global client base.”

Steve Petrevski, Senior Vice President of Technology, First Data

salesforce platform

CHAPTER 3

Salesforce Shield:
A heightened level of security you can bank on.

As companies move more data into the cloud, the need to put proper controls and policies in place to govern access to data becomes ever more important. Salesforce Shield is a set of additional security services built on top of our trust platform for companies that have more complex compliance and governance requirements. It includes three essential services that help manage the entire lifecycle for cloud data governance and compliance:

MONITOR AND PREVENT
Event Monitoring

Use intelligence to detect and prevent data misuse.

- User activity tracking
- Real-time alerts
- Preventative actions

With Event Monitoring, customers can get visibility into detailed usage data across all apps built on Salesforce. It allows customers to not only see who is accessing critical business data when, and from where, but also analyze usage patterns and take steps to implement security policies that alert or block actions in real time.

PREVENT AND PROTECT
Platform Encryption

Implement controls to limit access to data.

- At rest encryption of sensitive data
- Encryption key management

While Salesforce encrypts all data in transit between our cloud and the end user, some regulations or internal policies may require additional levels of protection for sensitive data such as PII while it is at rest. With Platform Encryption, customers can encrypt data and files at rest with a button click while retaining important app functionality such as search, workflow, and validation rules.

RETAIN AND AUDIT
Field Audit Trail

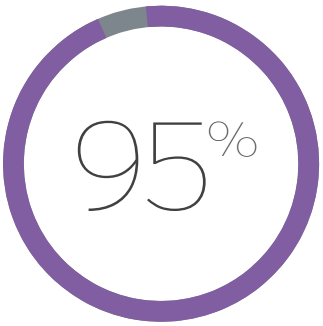
Retain data to ensure integrity and audibility.

- Up to 10 year retention and archival policies
- Query-based retrieval of field history

The financial services industry has a number of regulations requiring proper retention of changes to the customers' financial data for a set period of time. Field Audit Trail helps create a forensic data-level audit trail with up to 10 years of history. Companies can define data retention policies so data is deleted on a timeline they set. This helps automate managing the lifecycle for different categories of regulated data.

"As a financial company, we have a lot of responsibilities. We are holding a lot of sensitive customer PII data. To comply with regulations, we have millions of data points to sift through and manage. Shield helps us simplify our compliance activities and focus on the core of our business."

Franck Fatras, CTO, LendingPoint



of cloud security failures through 2020 will be the customer's fault, according to Gartner.

"Clouds Are Secure: Are You Using Them Securely?," Jay Heiser, 22 September 2015.

salesforce platform

CHAPTER 4

Event Monitoring: Gain visibility into user actions.

Financial firms need visibility into how sensitive data is being accessed by their users. If you have taken part in the postmortem of a data leakage incident, you know that all the logs necessary to uncover the leakage were there all the time. But someone needed to go through thousands of rows of log data and spot the threat.

To respond more quickly, companies need usage logs to be easily available so they can spot any suspicious usage patterns.

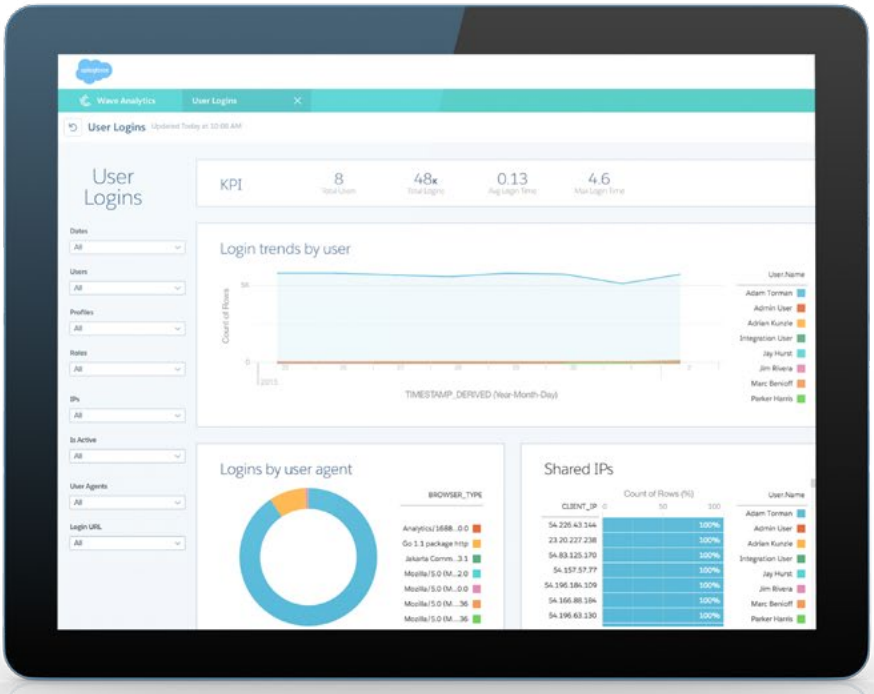
Event Monitoring takes a series of logs around usage and turns them into insights.

It gives customers unprecedented visibility into what data users are accessing, from where, and what actions are being taken in regards to that data.

In the financial services industry, some of the most common uses for Event Monitoring in sales and service scenarios include tracking when someone prints a page or list view, edits a record or creates one, changes ownership, refreshes a list, or even when a user exports the high-net-worth client data.

Flexibility to tailor insights based on your needs, using your tools

Every company is unique in what they need the data presentation layer to be. Event Monitoring provides simple, API-based access to compliance critical data allowing organizations to analyze and visualize events in the tool of their choice, such as Splunk, New Relic, FairWarning, and Einstein Analytics.



salesforce platform

CHAPTER 4

The need for monitoring in financial services.

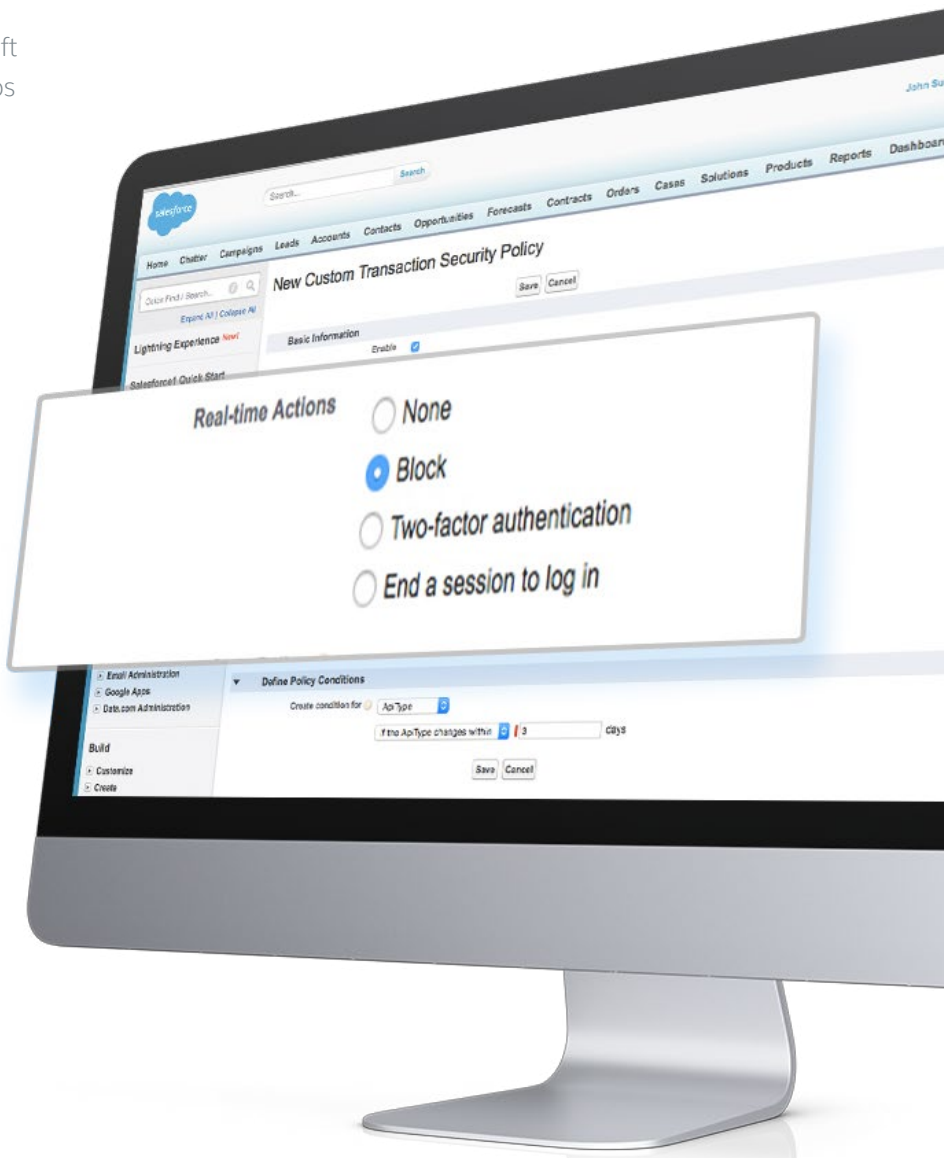
INDUSTRY REGULATIONS

Event Monitoring makes it easy for organizations to monitor user activity in ways recommended by COSO framework. It also helps organizations to comply with regulations like SOX, FFIEC, PCI, and more.

Under the Sarbanes-Oxley Act, companies are required to perform a fraud risk assessment and assess related controls. This typically involves identifying scenarios in which theft or loss could occur. Event Monitoring helps uncover these insights by configuring dashboards that could make abnormal behavior more easily detectable.

FFIEC security controls require banks to log and monitor user access to sensitive resources and alerting on security events. Event Monitoring puts logs such as the time, place (IP address), action, and subsequent actions taken into actionable views.

Not only does Event Monitoring provide more actionable insights, it also allows automating alerts and actions based on those insights.



salesforce platform

INTERNAL RISK AND GOVERNANCE

Financial services firms need a more automated way to monitor operations via logs to address security risks.

Banks can safeguard client data by monitoring who views and downloads it.

With Event Monitoring, they can better investigate the cases of account login compromise if a hacker steals a user's account info and performs an operation. Banks can analyze behavioral anomalies that either signify a data loss or are potentially the precursors to one. Additionally, banks can monitor how users interact with complex workflows such as loan processing, and by monitoring usage patterns they can create a better process.

Wealth management firms can track agent activity to protect competitive client data contained in reports, lists, and files, and mitigate risks around leakage of customer data to competitors.

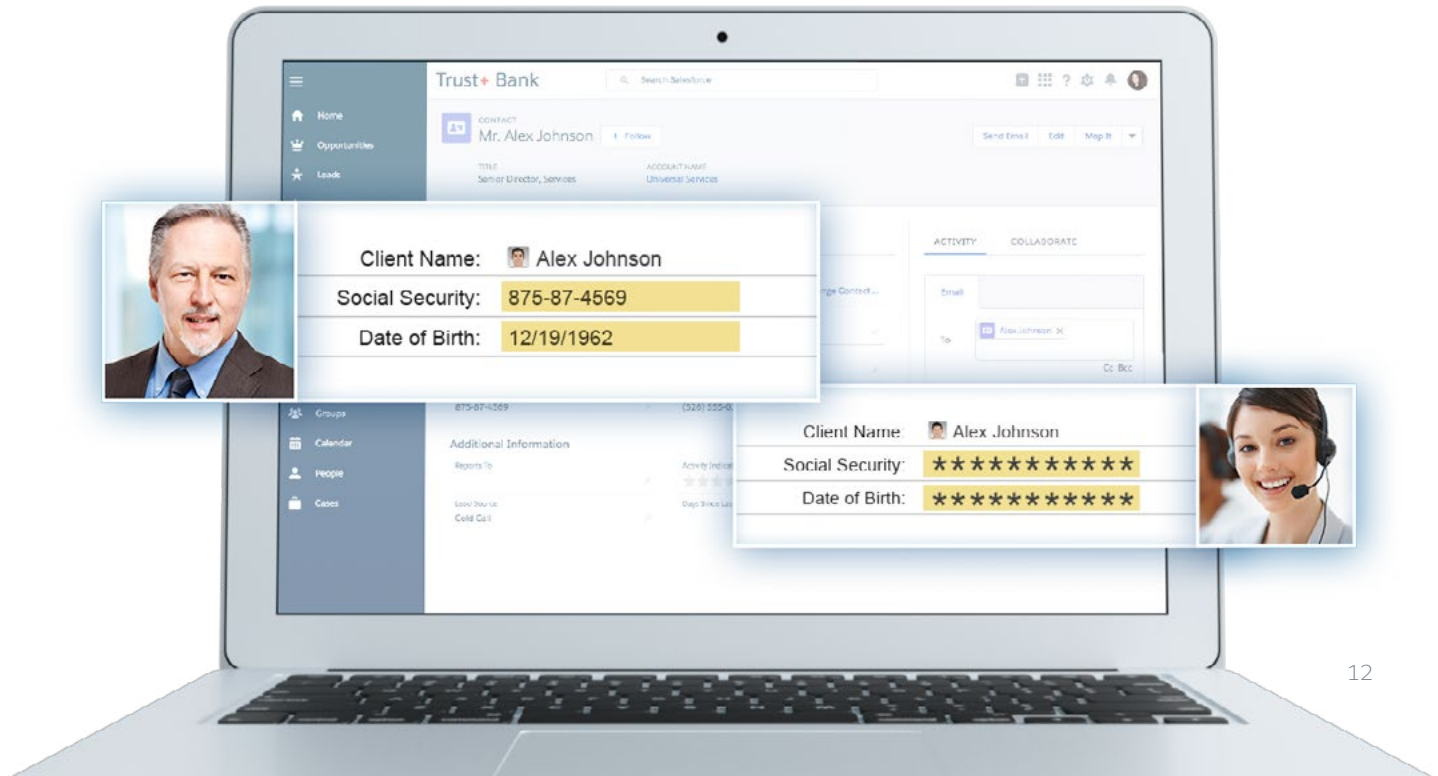
CHAPTER 4

Platform Encryption:
Encrypt PII data without breaking functionality.

Salesforce provides strong protection of customer data, including encryption of data in transit. However, as financial services customers bring more of their workloads into Salesforce, they put more sensitive data into the cloud subject to additional data-at-rest protection requirements such as PCI DSS for credit card-related information, SOX/J-SOX, NCUA, GLBA, and data privacy and data residency laws. These regulations require firms to protect sensitive data wherever it resides. While most do not specifically call for encryption as a requirement, customers choose to adopt this additional protection vehicle to ensure higher levels of compliance.

Platform Encryption lets customers encrypt sensitive application data – contained within fields, files, and attachments – at rest.

Because data is encrypted at the metadata layer in the database, key Salesforce application functionality such as global search and validation rules can be made "encryption aware" and work despite the data being encrypted. Platform Encryption is built natively into the platform and can be set up in just a few minutes with a button click.



salesforce platform

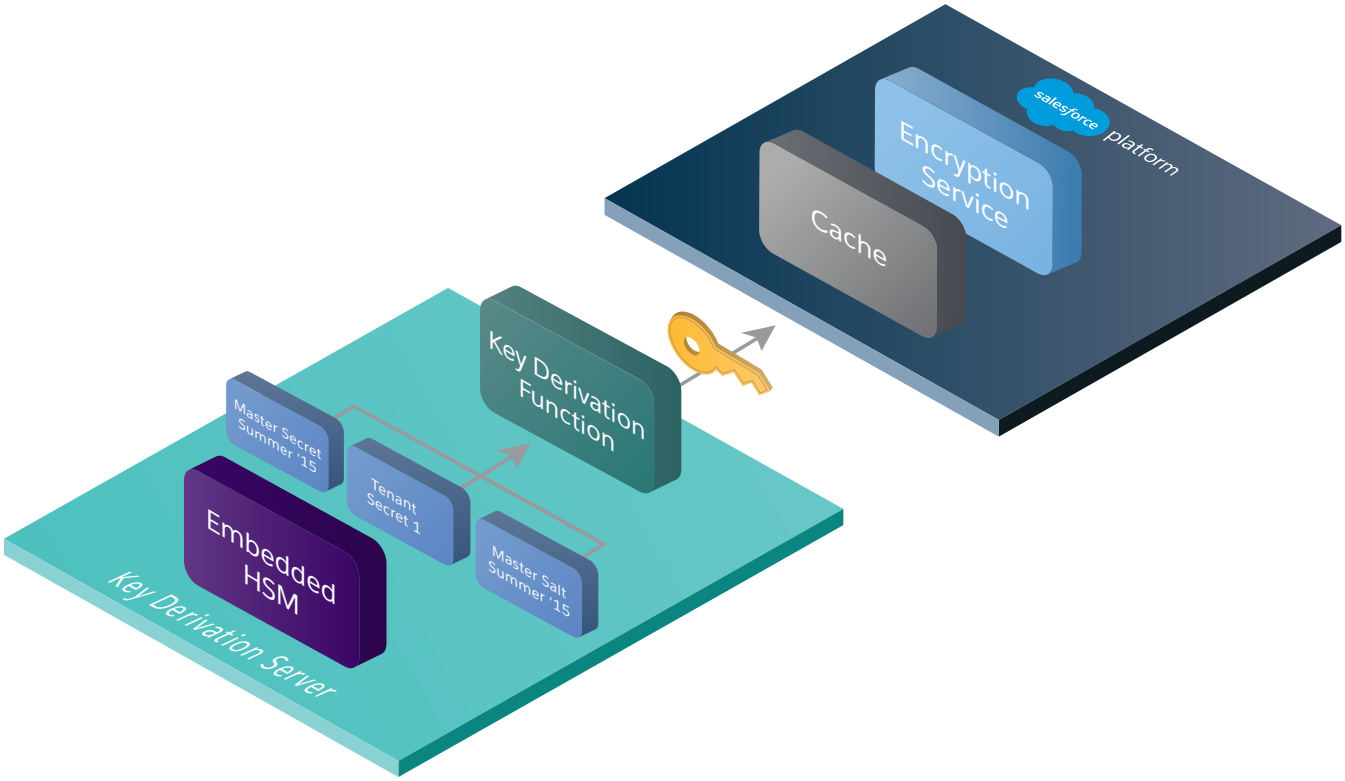
CHAPTER 4

A sophisticated engine behind a simple, declarative user interface.

Platform Encryption leverages industry standard, and FIPS certified 4096-bit RSA asymmetric keys and 256 AES symmetric keys in Cipher Block Chaining (CBC) mode. The unique combination of these keys as well as the rotating per-release Salesforce master secret produces unique customer-specific 256-bit length derived data encryption keys to encrypt and decrypt data. The individual secrets used to generate these keys are further fragmented, wrapped, and unwrapped in a unique sequence to create strong separation of duties, and provide a robust key management model.

See the blueprint for Salesforce Platform Encryption.

DOWNLOAD WHITE PAPER



salesforce platform

CHAPTER 4

The need for encryption-at-rest in financial services.

Financial services customers across various geographic regions are considering encryption at rest as an additional level of protection to comply with regulations and strengthen their security posture. Banks are especially concerned about storing NPPI/PII data (social security number, credit card number, account number, name, etc.). Below are three key drivers for encryption at rest:

1 INDUSTRY REGULATIONS

PCI regulations require that card data must be encrypted at rest. If card data is stored in documents (images, PDFs, etc.), those documents must be encrypted as well. According to FFIEC (Federal Financial Institutions Examination Council), it is important that financial institutions maintain a comprehensive data inventory and a suitable data classification process, and that access to customer data (including PII data) is restricted appropriately through effective identity and access management. A multitenant cloud deployment, in which multiple clients share network resources, increases the need for data protection through encryption.

2 INTERNAL POLICIES

Financial services companies can protect sensitive customer data from misuse use by internal users. For example, if a wealth management company has clients with high net worth or nationally recognizable profiles, its information may be encrypted to protect their identity. Only select users of the system may be able to have access to their data in clear text.

3 REGIONAL REQUIREMENTS

Expanding internationally may be another key driver for extra level of protection for cloud data. Banks opening branches in some Asian or European markets, for example, may choose to encrypt data due to strict local regulations, even though the regulation might not specifically call out encryption at rest as a required measure.

CHAPTER 4

Best practices for deploying Salesforce Encryption.

Salesforce encourages each customer to first leverage the various native access controls that are available to all customers as inherent data security tools. Platform Encryption can then be layered on top of these controls to provide a defense-in-depth approach to securing data at rest.

Before enabling encryption, customers should undertake a comprehensive data lifecycle management exercise to define, catalogue, and classify each data element according to their internal information security guidelines and principles.

Ensuring a consistent security approach of data regardless of where data is retained or processed, will help pinpoint which data elements require additional security through encryption.

Before rushing to adopt encryption as a global default setting, customers must thoughtfully focus on how they apply their use of Platform Encryption service. Only data elements that require at-rest encryption by regulation, or statute, should be targeted for encryption. The remaining fields/objects should be maintained in their original clear text format to preserve enhanced functionality.

salesforce platform

CHAPTER 4

Field Audit Trail: Strengthen data integrity with forensic audit trail.

From PII to agent activity and other electronic communications many types of financial services data are subject to regulations that require retaining a forensic data-level audit trail. It is important that the person performing the audit is able to easily understand the state of data correlated with a specific event.

The sheer volume of all customer-generated data makes it increasingly challenging to manage retention of audit data. How many years should field-level audit data be stored? How easy is it to access the historical data when audit needs to be performed? Companies need tools to simplify retention of field-level audit trail data.

Field Audit Trail gives customers a time machine so they can go back and see the state and value of their data on any date, at any time.

It gives a complete trail of how values in a particular field changed over time. Salesforce customers can set custom data retention policies at a field level for up to 10 years and 60 fields per object. Field Audit Trail is built on a big data back end enabling massive scalability and letting customers access audit data in just under two minutes.

Customers can also leverage analytics solutions like Einstein Analytics and Splunk to visualize and analyze audit history and produce insights.

salesforce platform

CHAPTER 4

The need for audit trails in financial services.

Integrity of customer's data through an easily auditable track of changes is a key requirement in Financial Services. Below are some examples of such compliance and governance requirements Field Audit Trail can help meet.

INDUSTRY REGULATIONS

A number of regulations require banks to keep audit changes to key business elements (KBEs) like, name, address, email, phone, and communication preferences. PCI requires banks to track the table/object changed, name of the changed field, type of change (insert, update, delete), value before the change and after the change, and so on. With Field Audit Trail, customers can automate retention and archiving of this data. Additionally, Banks can streamline audit procedures by making field auditing data available through real-time or batch APIs. That way, banks can easily produce regulatory reports, make the data available for forensic analysis and incident response teams.

INTERNAL GOVERNANCE POLICIES

Data integrity and internal incidence response is a key use case for Field Audit Trail. Wealth management firms, for example, can audit changes to key financial data elements like AUM (Assets Under Management), account balances, fees, and commissions in order to detect invalid changes or fraudulent activity.

Another key risk and governance use for Field Audit Trail is to recover data that's been corrupted by unauthorized activities or human errors.

Finally, in order to detect and prevent social engineering, firms can audit changes to system administration and security-related fields, such as user profiles, roles, permissions, groups, and so on. This gives security personnel additional insights to suspicious activity of privileged users of the system such as administrators.

salesforce platform

CHAPTER 4

Salesforce Shield: Use cases in banking.

- Restrict access to cardholder data using permissions (available to all Salesforce customers out of the box) or encryption at rest for an additional level of security
- Encrypt card data stored in documents (images, PDFs, etc.) to further restrict access to sensitive data
- Audit changes to key business elements (KBEs) like name, address, email, phone, and communication preferences using Field Audit Trail
- Encrypt mortgage documents and manage access to files to safeguard the customer PII data

78%

of customers put a priority on a bank's reputation for cybersecurity.[1]

57%

of bank managers say the sophistication of cybersecurity threats are on the rise.[1]

56%

of companies say lack of visibility into end-user access of sensitive data is a barrier for responding to security incidents.[2]

[1] CDW Research: "In Cybersecurity We Trust?," August 2014
[2] Ponemon Institute: The Second Annual Study on Data Breach Preparedness, September 2014

salesforce platform

CHAPTER 4

Salesforce Shield: Use cases in wealth management.

- Encrypt the information of high-net-worth clients or nationally recognizable profiles to protect their identity
- Monitor access to client data such as who accessed it, what action they took, when, and from where
- Maintain a trail of changes made to wealth management clients' portfolio and asset ownership
- Retain audit trail on fields that capture edits to advice given by agents to their clients
- Audit changes to key financial data elements like AUM (assets under management), account balances, fees, and commissions
- Monitor and detect valid data changes from invalid changes or fraudulent activity

55%

of wealth management firms are satisfied with the quality of their cloud data [risk] management.[1]

31%

of companies have security event management technologies.[2]

60%

of of global asset servicing companies say cybersecurity has been a leading issue in 2015.[3]

[1] EY: Risk management for wealth and asset management, 2014
[2] Ponemon Institute: "The Second Annual Study on Data Breach Preparedness," September 2014
[3] Cerulli Associates Europe, February 2015 report

salesforce platform

CHAPTER 4

Salesforce Shield: Use cases in insurance.

- Monitor and control access (alerts and actions) to sensitive insured information
- Encrypt sensitive insured information, such as PII and PHI, as an additional measure of security
- Define policies for storing changes to the records of the insured for audit purposes
- Monitor and alert on the suspicious usage patterns by agents of the customer account data and associated reports
- Set policies to retain changes made to the incident data by the claims agent
- Encrypt sensitive data associated with an incident case

86%
of insurers expect their security budgets to increase in the next three years.[1]

81%
of insurers say cybersecurity threats are becoming more sophisticated.[1]

72%
only have policies and procedures to mitigate security risks in the cloud.[1]

[1]New York State Department of Financial Services (NYDFS) study: "Report on Cyber Security in the Insurance Sector," February 2015

salesforce platform

CONCLUSION

The cloud is ready for financial services.

Customers today expect the same kind of on demand, context-aware experience from their bank as they do from Uber. The cloud is the key that opens the way for companies to move fast and deliver that experience. More than ever, the financial services CIOs face the decision to continue to hold their data in silos or seize opportunities in the cloud for a better service, stronger loyalty programs and real-time contextual experiences – across mobile, social, and millions of connected devices.

Our financial services customers have been expanding their use of Salesforce from sales to marketing, service, and operations. As a result, more sensitive data such as PII gets stored in our cloud than ever before. With 16 years of innovation in our trust platform, our security capabilities surpass what most organizations are able to provide on their own premises. So the question is not whether the Salesforce cloud is secure, but, how do you better govern and manage access to that data?

Salesforce Shield provides the essential security services financial firms need to move more of their business processes and data into the cloud. From analyzing usage, devising better policies, fortifying protection for sensitive data, Shield allows companies in regulated industries to focus on innovating and responding to their customers more quickly than ever before.

Is Salesforce Shield right for your business?

LEARN MORE

Contact us for hands-on experience 1-844-463-0828.

CONTACT US