SALESFORCE SHIELD

A new level of compliance and security
for your Salesforce data

salesforce platform

salesforce platform

INTRODUCTION

Companies across industries bring more data into Salesforce than ever before. With more sensitive data in the cloud, the security and compliance requirements that CIOs and CISOs must address become more complex. Salesforce Shield is a premium set of security services that provide additional levels of visibility and protection for sensitive data. Customers can see who is doing what, know the state and value of their data going back up to 10 years, and encrypt sensitive data at rest – all using powerful point-and-click tools.

> "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

Event Monitoring: Get complete visibility into your Salesforce apps like never before.

Companies of every size and industry are using Salesforce across all departments to run their business faster. With the increased use of Salesforce's capabilities, the visibility into secure usage, performance, and adoption becomes ever more important. Event Monitoring unlocks this valuable usage data – delivered as event log files via the Force.com SOAP API and REST API. The API-based access allows you to analyze and visualize events in the tool of your choice.

Who's it for?

Companies in regulated industries

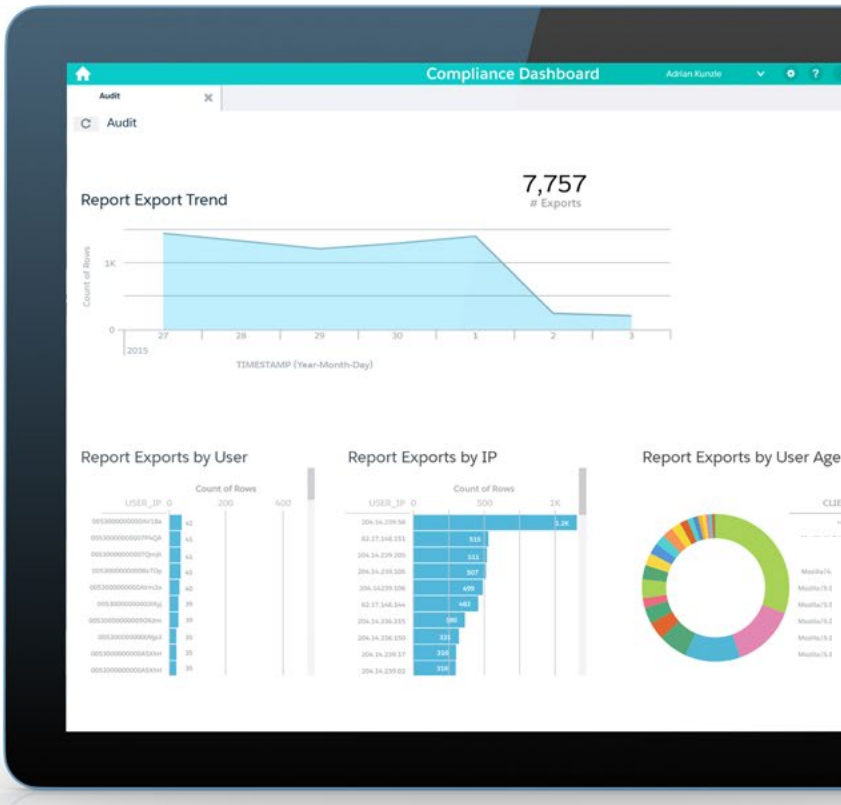
Monitor access to customer or patient data (PII and PHI) in industries such as financial services, healthcare, and tech.

Companies with internal security policies

Prevent leakage of valuable account or trade data by monitoring usage at a granular level.

Beyond security – performance and adoption

Monitor performance of reports, Visualforce pages, Apex classes, and track adoption of key features such as the Salesforce1 Mobile.



WHY IS EVENT MONITORING IMPORTANT?

42%
of CRM implementation failures are attributed to poor user adoption.[1]

36%
of breaches are from inadvertent misuse of data by insiders.[2]

73%
of IT decision-makers are concerned about public cloud security.[2]

$182
is the average cost per lost customer record from data breach.[2]

[1] 500 people surveyed, "How To Succeed With CRM: The Critical Success Factors," William Band's Blog, 2015.
[2] 20,003 IT and IT security practitioners surveyed, "2014: A Year of Mega Breaches," Ponemon Institute© research report, 2015.

salesforce platform

How It Works

- Monitor report exports by profile, role, or user
- Track reports run, including the ones that weren't saved
- Track files previewed, downloaded, and shared with other users
- Monitor bulk, SOAP, REST, and metadata API access
- Detect login compromise
- Get alerts on any usage behavior
- Block user actions based on customizable policies
- Identify performance concerns for custom Visualforce pages, Apex classes, reports, and more

How to Get Started

1 Turn on Event Monitoring for your organization.

- Captured daily
- 29 event types captured
- 30 days of events retained
- Log files exposed via the API

2 DEFINE BUSINESS-CRITICAL INSIGHTS.

- Identify key dashboard elements
- Analyze usage data
- Define threshold and anomalies
- Decide policies, and actions

3 Configure visual dashboards and actions.

- Use Einstein Analytics, or:
- Import data into any BI tool, or:
- Use prebuilt AppExchange apps
- Define and customize policies for actions

"Event Monitoring gave us critical usage insights in an afternoon."

Bryan Young, Manager,
Sales and Marketing, SolarCity

Upgrade to Event Monitoring

To see how Event Monitoring can help your company, contact your account executive or call 1-844-463-0828 today.

CONTACT US

salesforce platform

Platform Encryption at Rest: Strengthen data privacy and confidentiality.

As companies store more sensitive information in the cloud, such as PII, they need to ensure the privacy and confidentiality of that data to meet both external and internal compliance requirements. Platform Encryption allows you to natively encrypt proprietary and sensitive data at rest with a button click while preserving key business functionality.

Who's it for?

Financial services companies

Encrypt customers' personally identifiable information (PII), credit card details, health history, wealth information, and more.

Healthcare companies

Encrypt protected health information (PHI) such as health history, treatment records, and personal information such as ID numbers, social security numbers, and more.

Companies in other industries

Encrypt sensitive VIP client information, intellectual property, trade secrets, product and service roadmap details, and more.

THE STATE OF CLOUD SECURITY

95%
of cloud security failures through 2020 will be the customer's fault.[1]

60%
of global asset servicing companies say cybersecurity has been a leading issue in 2015.[4]

[1] Gartner, "Clouds are Secure: Are You Using Them Securely?," Jay Heiser, Sept. 22, 2015
[2] Ponemon Institute, "The Second Annual Study on Data Breach Preparedness," Sept. 2014

salesforce platform

How It Works

- Set up in minutes to encrypt fields, files, and attachments with no additional hardware or software
- Because data is encrypted at a metadata layer, major functionality such as global search and validation rules work seamlessly
- Behind the scenes, the architecture leverages full probabilistic encryption and 256 AES symmetric keys to ensure strong protection
- Customers have full access to keys and can manage (rotate and destroy) HSM-derived (Hardware Security Module) encryption keys using declarative UI

How to Get Started

1 Identify encryption needs.

- Define threat vectors
- Classify your data
- List "must-encrypt" data elements
- Evaluate business functionality

2 Apply field-level encryption.

- Apply encryption on selected elements
- Grant permission to authorized users
- Test how business processes work with encrypted data

3 Define key management strategy.

- Identify users who can manage keys
- Define approach for backing up, rotating, and archiving keys

4 Maintain your organization's encryption policy.

- Manage the lifecycle of your keys
- Back up your organization data periodically
- Review encryption policies as your data grows
- Ensure encryption is applied only to data that must be encrypted

Upgrade to Platform Encryption

To see how Platform Encryption can help your company, contact your account executive or call 1-844-463-0828 today.

CONTACT US

salesforce platform

Field Audit Trail: Retain data history for compliance and greater operational insights.

Tracking the massive quantity of data companies generate is an essential part of IT governance strategy. But maintaining a data audit trail can be complex and resource intensive. Field Audit Trail from Salesforce automates much of this process by giving you a forensic data-level audit trail with up to 10 years of history. Now you can ensure the integrity of your data, deriving insights into how your data and your company has evolved. With nearline storage for high-volume data, your business can easily meet compliance and security guidelines.

Who's it for?

Companies in highly regulated industries

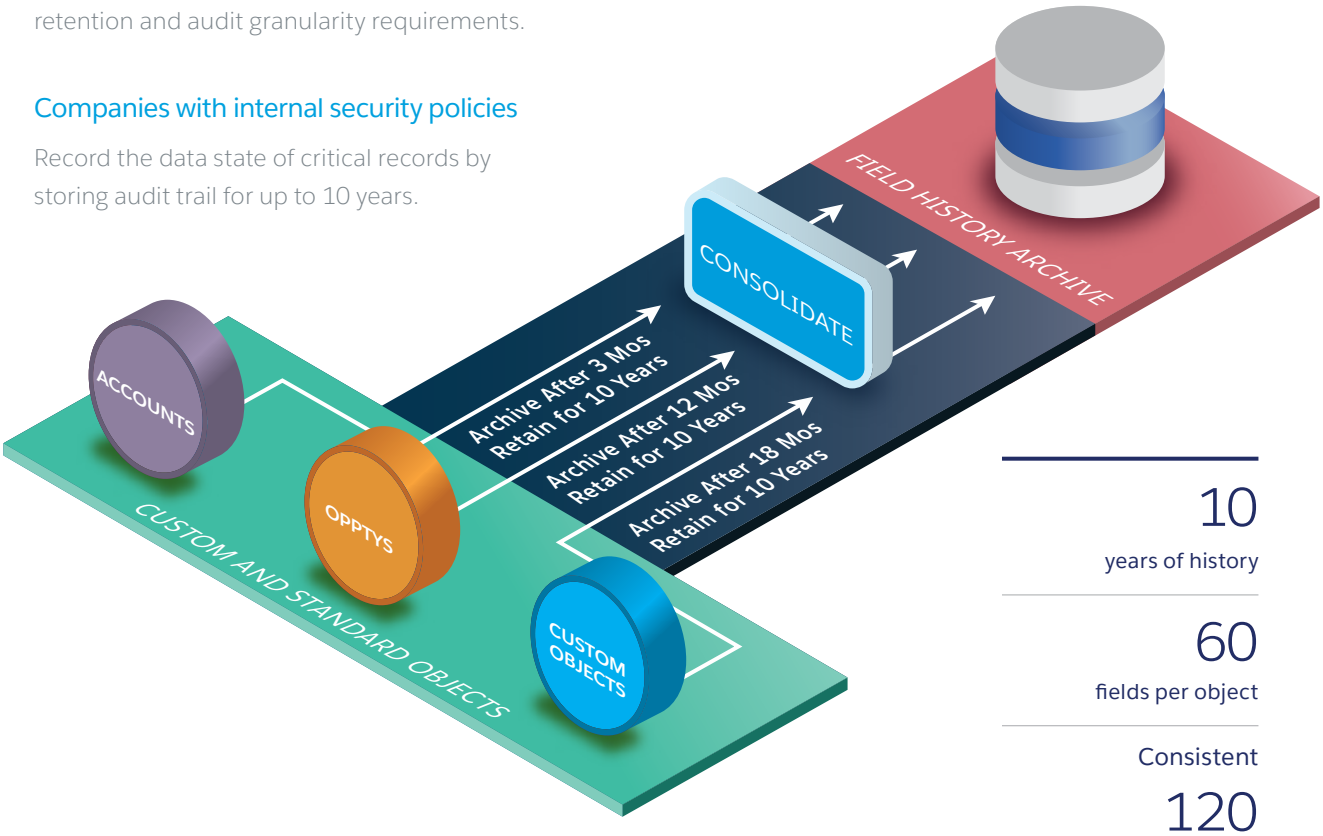
Retain patient or customer data (PII or PHI) in industries such as financial services or healthcare to ensure compliance to data retention and audit granularity requirements.

Companies with internal security policies

Record the data state of critical records by storing audit trail for up to 10 years.

Beyond security – data integrity

Query and view important data over time, identify trends, and draw valuable insights.



10
years of history

60
fields per object

Consistent
120
second query performance

salesforce platform

How It Works

- Automate field retention – define standards and rules for what field data is retained, for how long, and when it should be archived
- Retain field history data for 60 fields per object for up to 10 years
- Configure custom retention policies for key objects including custom objects, accounts, cases, contacts, leads, and opportunities
- Gain quick access at massive scale – 120-second query performance – to quickly determine the state and value of your data for any date, at any time
- Capture the full lifecycle of your data – field history data is retained, archived, and deleted when no longer needed

How to Get Started

1

Consult with the business to understand your retention and audit period and depth of audit.

- Retention period per object basis
- Regulatory guidelines

2

Set retention policies.

- What fields and objects
- When and how long to archive

3

Identify practices for retrieving and auditing data.

- Set up an audit dashboard
- Define standard queries
- Provide access to auditors
- Draw insights

Upgrade to Field Audit Trail

To see how Field Audit Trail can help your company, contact your account executive or call 1-844-463-0828 today.

CONTACT US

salesforce platform

THE WORLD'S MOST TRUSTED ENTERPRISE CLOUD

Trust is our #1 value. Customers across all industries and geographic regions trust the Salesforce cloud with their customer, employee, and competitive data. From secure data centers to single sign-on and granular permissions, the trust services of Salesforce platform are available to all customers out of the box. Salesforce Shield is an additional suite of built-in services to help with an increased compliance driven by industry regulations and internal policies.

Is Salesforce Shield right for your business?

LEARN MORE


salesforce
platform