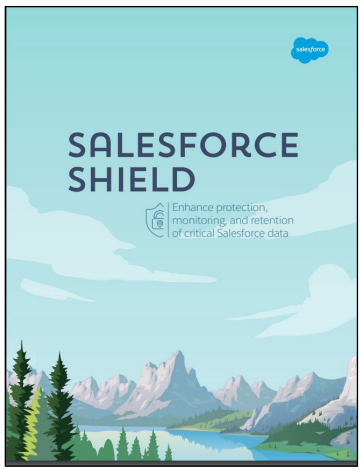


Salesforce Shield

Enhance protection, monitoring, and retention of critical Salesforce data

Thank you for downloading this Salesforce whitepaper. Carahsoft is the master value added reseller and aggregator for Salesforce MultiCloud solutions available via GSA 2GIT, NASA SEWP V, CMAS, NJSBA and other contract vehicles.

To learn how to take the next step toward acquiring Salesforce's solutions, please check out the following resources and information:

For additional resources:
carah.io/SalesforceResources

For upcoming events:
carah.io/SalesforceEvents

For additional Salesforce solutions:
carah.io/SalesforceSolutions

For additional MultiCloud solutions:
carah.io/MultiCloud

To set up a meeting:
Salesforce@carahsoft.com
877-SFDC-007

To purchase, check out the contract vehicles available for procurement:
carah.io/SalesforceContracts

For more information, contact Carahsoft or our reseller partners:
Salesforce@carahsoft.com | 877-SFDC-007

SALESFORCE SHIELD

Enhance protection, monitoring, and retention of critical Salesforce data

Overview

Companies of all sizes and industries are using Salesforce across departments to run their businesses faster. As adoption of Salesforce for critical business capabilities grows, monitoring user behavior, tracking changes to data, and preventing data loss is more important than ever. With more sensitive data in the cloud, security and compliance requirements also become increasingly complex. Salesforce Shield helps address these requirements while allowing you to proactively monitor user activity and enforce security policies.

Salesforce Shield provides enhanced protection, monitoring, and retention of your critical data stored in Salesforce.

- **Native Encryption**: Natively encrypt your most sensitive data while retaining critical app functionality including search, workflow, and validation rules.
- **Detailed Data & Monitoring**: Gain access to detailed performance, security, and usage data for your Salesforce apps in order to monitor critical business data, understand user adoption across your apps, and troubleshoot and optimize custom application performance.
- **Security Policies**: Build flexible, customizable security policies that give IT the power to identify and prevent malicious activity in real time. Retain data history for forensic level compliance as well as greater operational insights into your business.

THE STATE OF CLOUD SECURITY

SECURITY AND PRIVACY CONCERNS ARE THE TOP INHIBITORS IT organizations face when trying to integrate data for a shared single view of customers.*

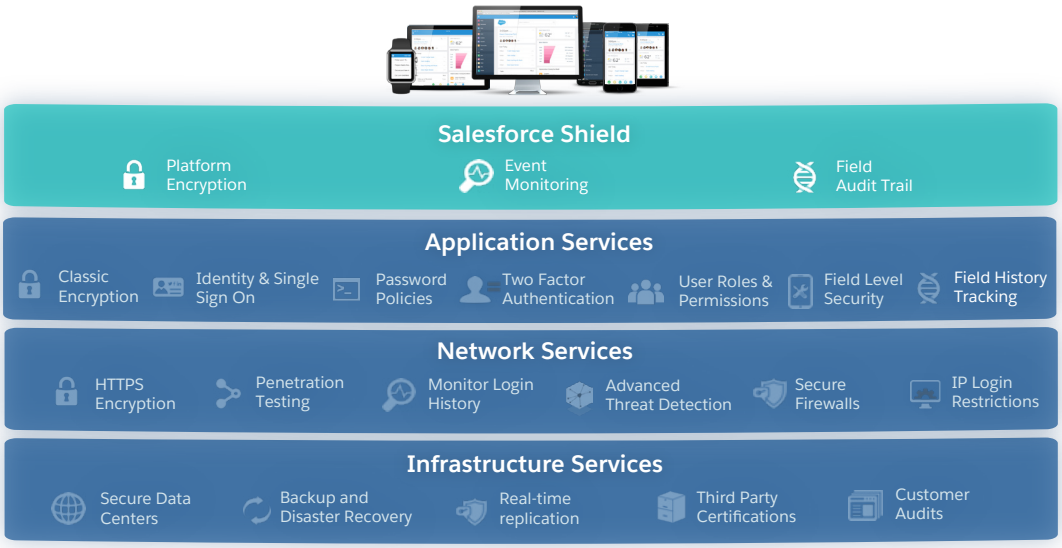
IMPROVING SECURITY POLICIES AND PRACTICES is the top priority for IT teams over the next 12 to 18 months.*

65%
of IT leaders plan on increasing data stored in the cloud over the next 12 - 18 months.*

* Salesforce State of IT Report, 2017

THE WORLD'S MOST TRUSTED ENTERPRISE CLOUD

Trust is Salesforce's #1 value. Customers across industries and geographic regions trust Salesforce with their critical customer, employee, and competitive data. From secure infrastructure and identity services to granular permissions and role-based access controls, the trust services of the Salesforce Platform are available to every customer out of the box. With Salesforce Shield, customers who need additional controls and protection can leverage an additional suite of built-in services to help with priorities such as compliance, driven by industry regulations and internal policies, as well as insight and control.



SALESFORCE SHIELD INCLUDES THREE KEY PREMIUM SERVICES:

1. Platform Encryption

Encrypt your most sensitive data at rest while retaining critical app functionality. Platform encryption is natively integrated with key Salesforce features, so core functionality like search, lookups, validation rules, and Chatter are preserved. Provide your users a full 360 degree view of your customers by bringing and managing regulated, private, or proprietary data with confidence using Platform Encryption.

2. Event Monitoring

Event Monitoring delivers access to detailed performance, security, and usage data for your Salesforce apps in order to help you monitor compliance with your security policies, understand user adoption across your apps, and troubleshoot and optimize application performance. Transaction Security, a key component of Event Monitoring, lets you build flexible, customizable security policies that give IT the power to identify and prevent malicious activity in real time.

3. Field Audit Trail

With Field Audit Trail, you can track changes to your data for up to 10 years and report on its value and state over time for forensic level compliance and greater operational insights into your business.

PLATFORM ENCRYPTION

Strengthen data privacy and confidentiality.

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

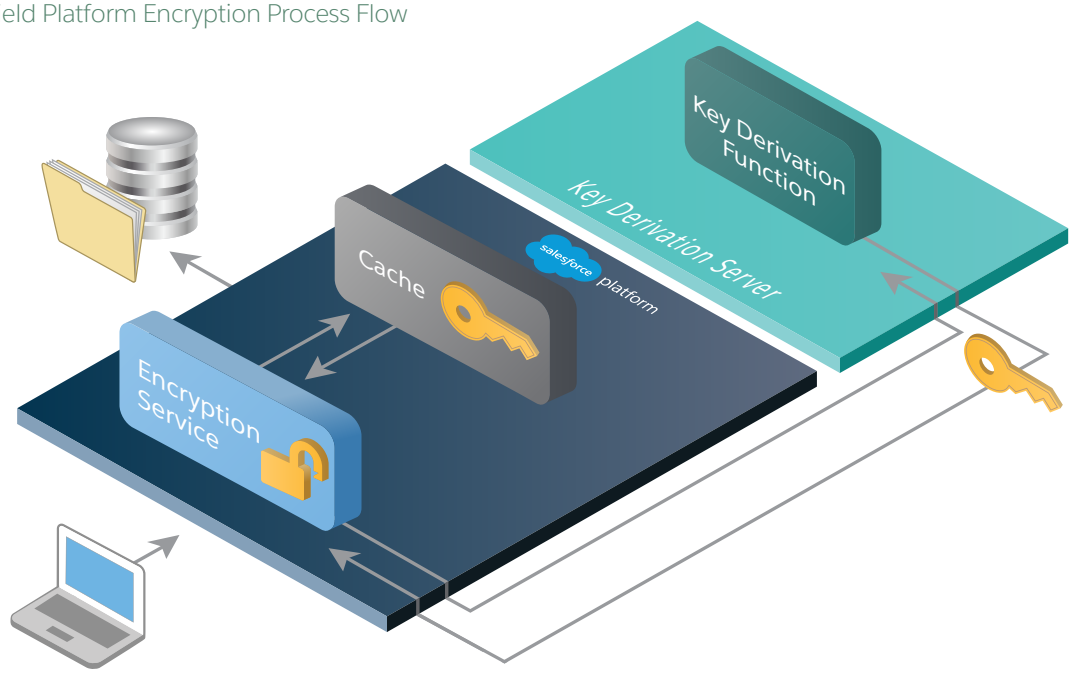
WHO IS IT FOR?

Financial services companies
Encrypt customers' 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 across industries
Encrypt sensitive client information, intellectual property, trade secrets, product roadmap details, and more. Get a complete view of your customer and retain critical business functionality, while layering on additional protection to your business critical data at rest.

Shield Platform Encryption Process Flow



HOW IT WORKS

- Using declarative methods, customers can generate their tenant secret and encrypt fields, files, and attachments with no additional hardware or software.
- Data is encrypted at the application layer, allowing major functionality such as global search and validation rules to work seamlessly.
- Behind the scenes, the architecture leverages full probabilistic encryption and 256-bit AES symmetric keys to ensure strong protection
- Customers have full control of the lifecycle of their Hardware Security Module, or HSM, derived tenant secret, and can rotate, export, and destroy secrets as needed to satisfy compliance requirements.
- Bring Your Own Key (BYOK) allows customers to provide their own tenant secret, generated from their own HSMs, increasing control over their encryption processes.

THE STATE OF CLOUD SECURITY

50%
of companies rely on SaaS for their most critical business applications.*

77%
of companies already use SaaS for IT and data processing, while 92% say it will be more critical within the next 2 years.*

42%
of organizations plan to accelerate their migration to the cloud to meet GDPR compliance requirements.*

* Ponemon Institute Cloud Security Survey

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*

- Grant permission to authorized users
- Apply encryption on selected elements
- 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

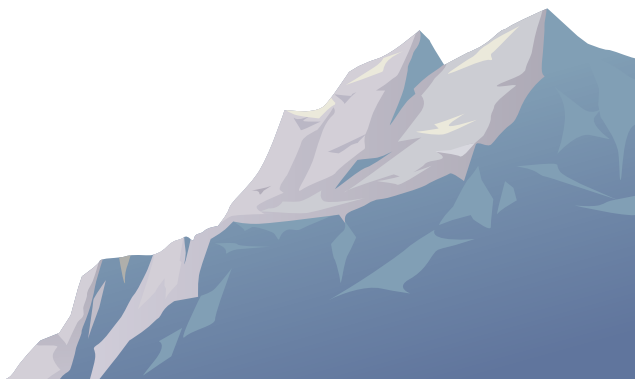
*Test Platform Encryption in your Sandbox before deploying to Production. Once Platform Encryption has been enabled, simply refresh your sandbox to begin assigning permissions, generating keys, and encrypting fields.

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

LEARN MORE



EVENT MONITORING

Get complete visibility into your Salesforce apps like never before.

With the increased use of Salesforce for critical business functionality, monitoring user behavior and preventing data loss is more important than ever. Event Monitoring, a part of Salesforce Shield, gives you access to detailed performance, security, and usage data on all your Salesforce apps in order to monitor critical business data, understand user adoption across your apps, and troubleshoot and optimize custom application performance. Build flexible, customizable security policies that give IT the power to identify and prevent malicious activity in real time. Analyze user behavior to drive training and adoption of Salesforce and drive the strongest return on investment in your Salesforce deployment. Monitor custom application performance to target your IT investment and improve user experience.

Event Monitoring helps both chief security officers and line of business managers answer important questions about the state of their org:

Adoption

- How can I find out what my users are doing on Salesforce?
- How do they use mobile devices to access Salesforce apps?
- What pages and sites are used most?

Performance

- How can I ensure that we are getting the best use out of the platform?
- What actions are automated?
- How long do my custom applications take to load?

Security

- How do I know our users are compliant with our security policies?
- What devices and platforms are being used?
- When do our users log in and where do our users log in from?
- Who is viewing sensitive data?

Event Monitoring answers these questions by providing visibility into user actions and behavior to help you better support your applications, audit your users, and optimize your business processes.

HOW DOES IT WORK?

Event Monitoring includes over 40 different event types, describing each of your users' activities in Salesforce, plus Einstein Event Monitoring Analytics, which offers 16 pre-built dashboards to quickly begin working with event log files and identify anomalous user behavior.

API-based access to event log files allows you to analyze and visualize events in the tool of your choice, and powerful AppExchange apps can help you extend functionality and unlock new insights. Event Monitoring data can be easily imported into data visualization and application monitoring tools like Einstein Analytics, Splunk, FairWarning, or New Relic. Transaction Security, a key part of Event Monitoring, allows you to create security policies that are enforced in real-time with a flexible and customizable policy engine, using clicks or code.

- Monitor report exports by profile, role, or user
- Track report 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 usage behavior
- Block user actions based on customizable policies
- Identify performance concerns for custom Visualforce pages, Apex classes, reports, and more

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

BRYAN YOUNG
Manager, Sales and Marketing, SolarCity

HOW TO GET STARTED

1. Capture read-only event log files:
- 40+ event types captured - View Current List
- 30 days of events retained
- Log files exposed via API

2. Visualize the data to identify critical insights:
- Use included license for Einstein Event Monitoring Analytics, with 16 included dashboards
- Build your own Data Loss Prevention or Adoption & Performance dashboards with Einstein Analytics
- Import into any Business Intelligence tool
- Use pre-built AppExchange apps for added functionality
- Export to CSV file

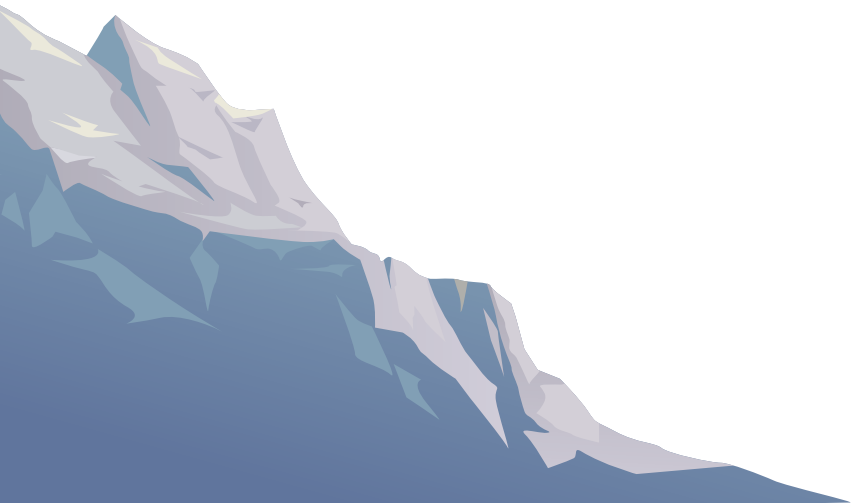
3. Take action:
- Identify gaps in security policies and use access controls and Transaction Security for stronger enforcement
- Modify governance policies
- Drive initiatives to increase adoption
- Automate outcomes with workflow
- Improve app performance

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

LEARN MORE



WHY IS EVENT MONITORING IMPORTANT?

73%
of IT decision-makers are concerned about public cloud security.*

36%
of breaches are from inadvertent misuse of data by insiders.*

$182
is the average cost per lost customer record from data breach.*

42%
of CRM implementation failures are attributed to poor user adoption.**

*20,003 IT and IT security practitioners surveyed, "2014: A Year of Mega Breaches," Ponemon Institute© research report, 2015.

**500 people surveyed, "How To Succeed With CRM: The Critical Success Factors," William Band's Blog, 2015.

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 an audit trail can be complex and resource-intensive. Field Audit Trail, a part of Salesforce Shield, automates much of this process by giving you a forensic data-level audit trail with retention of up to 10 years. With Field Audit Trail, 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 IS IT FOR?

Companies in highly regulated industries

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

Companies with internal security policies

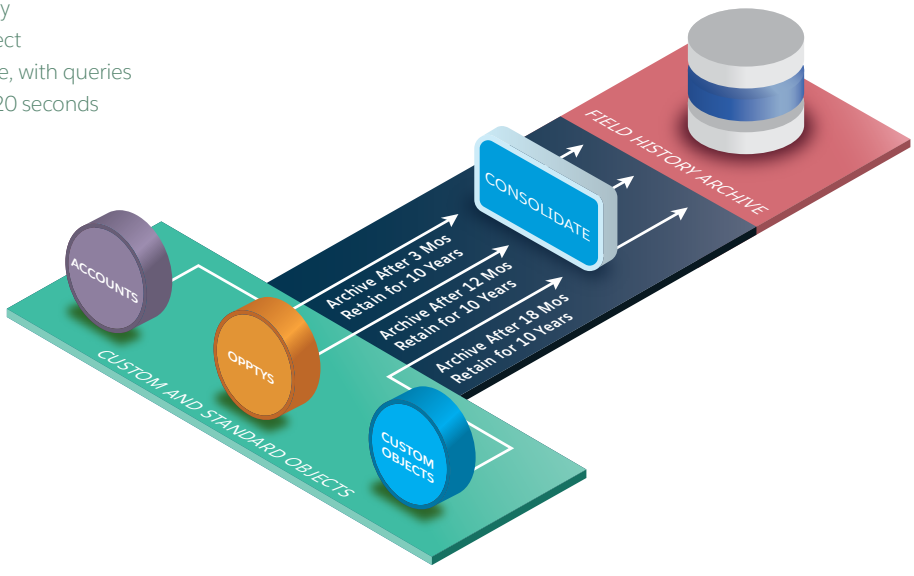
Record the data state of critical records and retaining an audit trail for up to 10 years.

Beyond security – data integrity

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

Field Audit Trail

- Up to 10 years of history
- Up to 60 fields per object
- Consistent performance, with queries completing in under 120 seconds



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 up to 60 fields per object and 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 – less than 120-second query performance – to quickly determine the state and value of your data for any date
- 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 for 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 LEARN MORE