Salesforce Shield

compiled by

Svet Voloshin

What is Salesforce Shield?

Salesforce Shield is a suite of security features designed to help organizations protect sensitive data and meet compliance requirements. Here are some key points about Salesforce Shield:

- Salesforce Shield includes several different components, including **Platform Encryption, Event Monitoring, Field Audit Trail, and Transaction Security, as well as Einstein Data Detect**.
- **Platform Encryption** enables organizations to encrypt sensitive data at rest in Salesforce, so that it cannot be accessed by unauthorized parties.
- **Event Monitoring** allows administrators to track and log user activity in Salesforce, providing visibility into who is accessing what data and when.
- **Field Audit Trail** provides a detailed history of changes made to specific fields in Salesforce, enabling organizations to track data modifications and comply with regulatory requirements.
- **Transaction Security** enables organizations to create custom policies to enforce additional security measures, such as requiring two-factor authentication for certain transactions.
- Salesforce Shield is especially useful for organizations that deal with highly sensitive data, such as financial institutions or healthcare providers.
- Salesforce Shield is available as an **add-on** to Salesforce and requires **additional licensing**.

Shield Platform Encryption

Salesforce Shield Platform Encryption is a data encryption solution provided by Salesforce to enhance data security and privacy. It allows users to encrypt sensitive data at rest in Salesforce, such as account records, contact records, and custom objects.

With Shield Platform Encryption, users can choose to encrypt data using **AES-256 encryption**, which is the **strongest encryption method available today**. The encryption keys used to encrypt the data are managed by Salesforce and are stored separately from the encrypted data for added security.

Salesforce Shield Platform Encryption is particularly useful for organizations that handle sensitive data, such as **healthcare, financial services, and government agencies**, as it helps ensure that sensitive information is protected from unauthorized access, even if there is a data breach. It also helps organizations comply with various data protection regulations, such as **HIPAA, PCI-DSS**, and **GDPR**.

It is worth noting that Salesforce Shield Platform Encryption is a paid add-on to the Salesforce platform and requires a separate license. Additionally, enabling encryption can impact performance, as the encryption and decryption process adds an overhead to data processing. Therefore, organizations should carefully evaluate the cost and benefits of implementing Salesforce Shield Platform Encryption before deciding to use it.

Probabilistic Encryption

Probabilistic Encryption is a cryptographic technique that enables data to be encrypted in a way that makes it difficult to identify individual records. Unlike deterministic encryption, which produces the same ciphertext for the same plaintext, **probabilistic encryption produces different ciphertexts for the same plaintext**. This makes it **more difficult** for an attacker to identify individual records based on their encrypted values.

The technique works by adding a random value, called a **nonce***, to the plaintext before encrypting it. The **nonce** is used to ensure that the **same plaintext produces different ciphertexts each time it is encrypted**. When decrypting the ciphertext, the **nonce is also required to recover the original plaintext**.

Probabilistic Encryption is commonly used in applications where **privacy is important**, such as in secure messaging, data sharing, and cloud computing. It is also useful in compliance with various data protection regulations, such as HIPAA, PCI-DSS, and GDPR.

**Nonce in cryptography means “number once,” and this arbitrary number is only used one time in a cryptographic communication. (Source)*

Deterministic Encryption

Deterministic Encryption is a cryptographic technique that produces the same ciphertext for the same plaintext every time it is encrypted. In other words, the encrypted value is **deterministic**, which means that it is **predictable** and **repeatable**.

Deterministic Encryption is useful in situations where the **same plaintext needs to be encrypted multiple times and compared against other encrypted values**. This is because the deterministic nature of the encryption ensures that the **same plaintext** will always produce the **same ciphertext**, making it **easier to perform comparisons and searches**.

However, one **disadvantage** of deterministic encryption is that it can potentially **leak information** about the plaintext. For example, if two plaintexts are very similar, their corresponding ciphertexts will also be very similar, which can make it easier for an attacker to guess the original plaintext.

Deterministic Encryption is commonly used in applications such as **database encryption and file encryption**, where the same data needs to be **encrypted and decrypted repeatedly**.

In Salesforce, deterministic encryption can be used to **encrypt fields on standard or custom objects using a key that is managed by Salesforce**. This can help protect sensitive data and comply with various data protection regulations.

Probabilistic vs. Deterministic Encryption

Feature	Probabilistic Encryption	Deterministic Encryption
Ciphertext	Different ciphertext for the same plaintext	Same ciphertext for the same plaintext
Randomness	Adds a random value (**nonce**) to plaintext	No randomness added to plaintext
Identifiable Records	Difficult to identify individual records	Potentially easier to identify records
Use Cases	Secure messaging, data sharing, cloud computing	Database encryption, file encryption, where repeated encryption/decryption is required
Advantages	More secure due to randomness, more difficult to guess plaintext	More efficient, same plaintext produces same ciphertext
Disadvantages	Can potentially leak information about plaintext	Same plaintext produces same ciphertext, potentially making it easier for attackers to guess plaintext
Salesforce Integration	Available as a data encryption option in Salesforce Shield	Available as a data encryption option in Salesforce Shield

Bring Your Own Key (BYOK)

Bring Your Own Key (BYOK) is a security feature that enables organizations to encrypt and manage their own encryption keys for data stored in the cloud. With BYOK, organizations can use their **own cryptographic keys** to encrypt data **before** it is stored in a **cloud** service provider's **environment**.

BYOK provides several benefits for organizations:

- **Improved security**: BYOK enables organizations to maintain control over their encryption keys, which helps protect against unauthorized access to sensitive data.
- **Compliance**: BYOK can help organizations meet various compliance requirements, such as those outlined in HIPAA, PCI-DSS, and GDPR.
- **Flexibility**: BYOK allows organizations to choose their preferred encryption algorithm and key size, giving them greater flexibility and control over their security measures.
- **Data portability**: With BYOK, organizations can easily move their encrypted data between cloud environments, as long as they have access to their own encryption keys.

In Salesforce, BYOK is available as part of Salesforce Shield Platform Encryption. With BYOK in Platform Encryption, organizations can use their own keys to encrypt their data at rest in Salesforce. This provides an additional layer of security for sensitive data, while still allowing organizations to benefit from the advantages of using a cloud-based CRM platform like Salesforce.

Rotating Keys

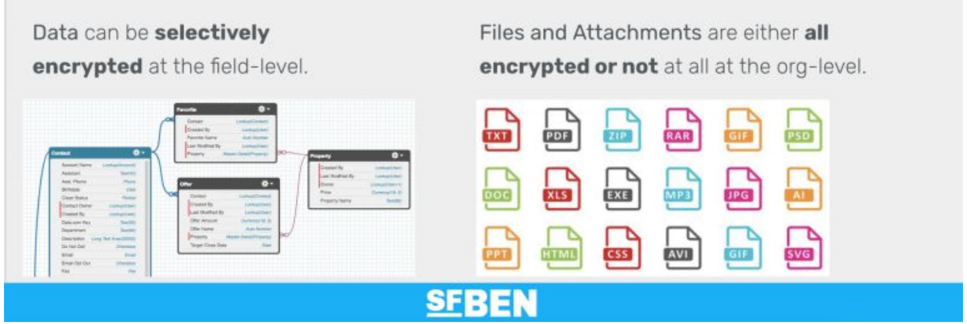
Rotate Your Encryption Tenant Secrets

- You control the lifecycle of your data encryption keys by controlling the lifecycle of your tenant secrets.
- Salesforce recommends that you regularly generate or upload new Shield Platform Encryption key material.
- When you rotate a tenant secret, you replace it with either a Salesforce-generated tenant secret or customer-supplied key material.
- To decide how often to rotate your tenant secrets, consult your security policies. How frequently you can rotate key material depends on the tenant secret type and environment. You can rotate tenant secrets one time per interval.

TENANT SECRET TYPE	PRODUCTION ENVIRONMENTS	SANDBOX ENVIRONMENTS
Data in Salesforce	24 hours	4 hours
Data in Salesforce (Deterministic)	7 days	4 hours
Analytics	24 hours	4 hours
Search Index	7 days	7 days
Event Bus	7 days	7 days

What Shield Encryption is Not

- It’s not **whole disk encryption**. Instead, Shield encryption is at the **field-level**, and for **files and attachments**.



Data can be **selectively encrypted** at the field-level.

Files and Attachments are either **all encrypted or not** at all at the org-level.

- While data can be **selectively encrypted** (i.e. field by field), Shield **cannot selectively encrypt files and attachments**. In other words, encryption for files and attachments is binary – meaning that there’s a setting (an encryption policy) that’s either on or off, and applied to all files and attachments.

- When the encryption policy for files and attachments is enabled, all **new** files and attachments that are uploaded will be encrypted “at rest”. You will need to **contact Salesforce support to have existing files and attachments encrypted**.

- **It does not obfuscate the data**; data is still mostly transparent to your end users from the Salesforce UI.

Tradeoffs and Limitations

1. **Limited searchability**: Encrypted data can only be searched using exact matches, which can make it more difficult to search for data in a large dataset. In addition, searching encrypted data may require additional processing time, which can impact performance.

2. **Limited indexing**: Encrypted data cannot be indexed for full-text search, which can make it difficult to search for keywords or phrases within the data.

3. **Limited functionality**: Some Salesforce features and functions may not be compatible with encrypted data, such as some validation rules, workflows, and formulas.

4. **Key managemen**t: The encryption keys used to encrypt and decrypt data must be carefully managed to ensure that data is not lost or compromised. This can require additional resources and processes to manage the keys effectively.

5. **Impact on performance**: Encrypting and decrypting data can impact system performance, especially when working with large datasets. This may require additional hardware or infrastructure to support.

6. **Limitations on data types**: Not all data types can be encrypted with Shield Platform Encryption, such as some types of multi-select picklists and long text fields.

Selected Tradeoffs Examples

Leads
Lead and Case assignment rules, workflow rules, and validation rules work normally when Lead fields are encrypted. Matching and de-duplication of records during lead import works with deterministic encryption but not probabilistic encryption. Einstein Lead Scoring isn't available.

User Email

- Event functionality that relies on user emails, especially calendar invitations, can be interrupted.
- You can't sort records in list views by fields that contain encrypted data.
- Login Discovery Handler lookups that rely on emails don't work if the email field is encrypted, which can block user logins.

Flows and Processes

- You can store the value from an encrypted field in a variable and operate on that value in your flow's logic. You can also update the value for an encrypted field.
- Paused flow interviews can cause data to be saved in an unencrypted state.

Custom Fields

- You can't use encrypted custom fields in criteria-based sharing rules.

Some custom fields can't be encrypted.

- Fields that have the Unique or External ID attributes or include these attributes on previously encrypted custom fields (applies only to fields that use the probabilistic encryption scheme)
- Fields on external data objects
- Fields that are used in an account contact relation
- You can't use Shield Platform Encryption with Custom Metadata Types.

More Info (Salesforce Documentation)

Unsupported Salesforce Apps

Which Salesforce Apps Don’t Support Shield Platform Encryption?

- Connect Offline
- Commerce Cloud (Salesforce B2B Commerce version 4.10 and later is supported)
- Data.com
- Einstein Recommendation Engine in Marketing Cloud (includes Einstein Recommendations, Einstein Web Recommendations, and Einstein Email Recommendations)
- Salesforce Einstein (includes Einstein Search, Sales Cloud Einstein, Einstein Discovery, Einstein Builders, and Einstein Vision and Language)
- Heroku (but Heroku Connect does support encrypted data) - see *Heroku Shield*
- Marketing Cloud (but Marketing Cloud Connect does support encrypted data)
- Sales productivity features that require data to be stored using a public cloud provider
- Social Customer Service
- Thunder
- Quip
- Salesforce Billing

Legacy portals (customer, self-service, and partner) don’t support data encrypted with Shield Platform Encryption. If legacy portals are active, Shield Platform Encryption can’t be enabled.

Best Practices

1. Define a threat model for your organization.
2. Encrypt only where necessary.
3. Create a strategy early for backing up and archiving keys and data.
4. Read the Shield Platform Encryption considerations and understand their implications on your organization several days lead time. The time to complete the process varies based on the feature and how your org is configured.
5. Analyze and test AppExchange apps before deploying them using Lightning Platform inherit Shield Platform Encryption capabilities and limitations.
6. Use out-of-the-box security tools.
7. Grant the Manage Encryption Keys user permission to authorized users only.
8. Synchronize your existing data with your active key material.
9. Handle currency and number data with care.
10. Communicate to your users about the impact of encryption.

Review full list in Salesforce Documentation

Field Audit Trail

Salesforce offers two different types of Field Audit Trail: **Standard Field Audit Trail and Field Audit Trail (part of Salesforce Shield)**. Here are some key differences between the two:

Standard Field Audit Trail:

- Allows tracking of changes to a limited set of standard fields on standard objects.
- Retains field history for up to **18 months**.
- Does not include access to real-time change event logs or the ability to filter audit trails by user or date.

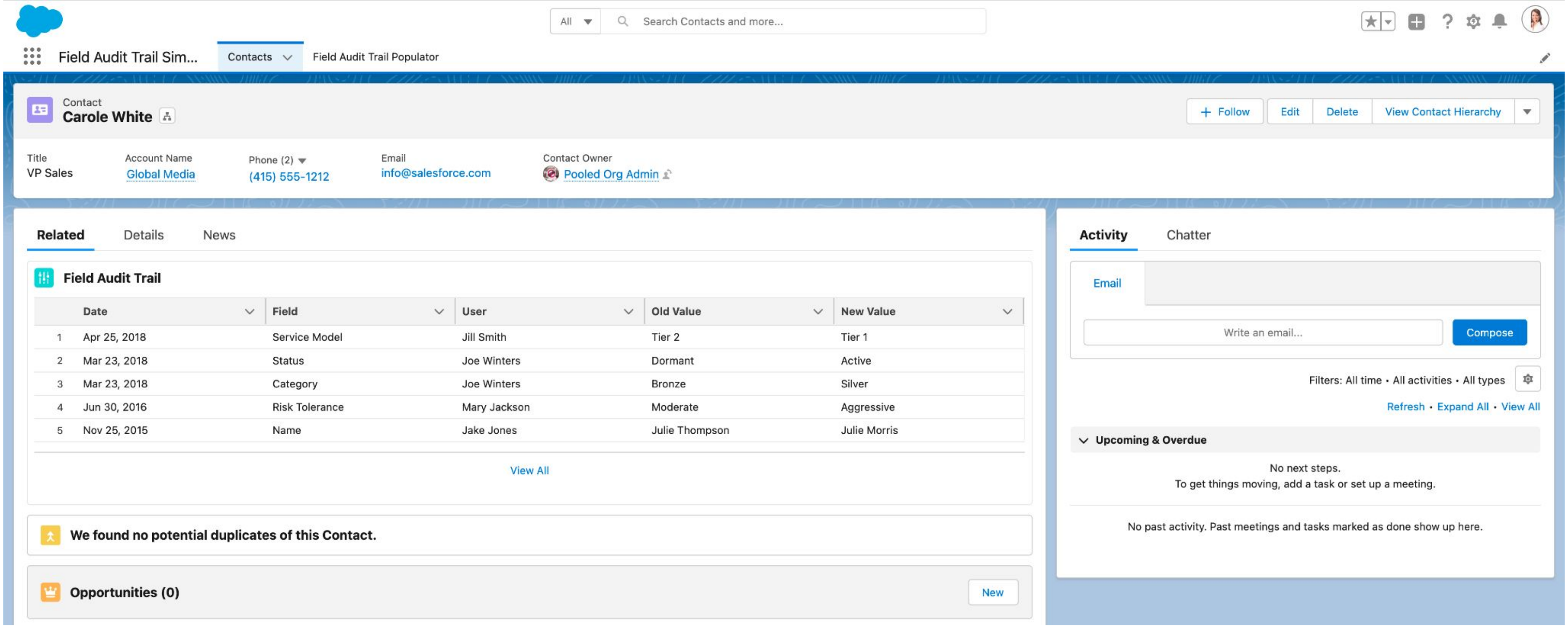
Field Audit Trail (part of Salesforce Shield):

- Allows tracking of changes to a wide range of fields on standard and custom objects.
- Retains field history for up to **10 years**.
- Provides access to **real-time change event logs** and the ability to **filter audit trails by user or date**.
- Includes additional features such as the a**bility to set field audit trail policies for specific users or profiles**, and the ability to store audit logs in an external system.

Overall, Field Audit Trail (part of Salesforce Shield) provides a more robust and customizable audit trail solution than Standard Field Audit Trail. It is especially useful for organizations with strict compliance requirements or those that need to track changes to custom fields or objects. However, it is a paid add-on to the Salesforce platform and requires a separate license.

	Standard Field Audit Trail	**Shield Field Audit Trail**
Number of fields supported:	20 fields per object	60 fields per object
History retention periods:	18 months within your Salesforce org, 24 months via API*	1 month to 10 years
Can retention policies vary by object?	No	Yes
Where is the trail accessible?	[Object] History related list	[Object] History related list. After X number of months, data is sent to the field history archive. This can then be permanently deleted after a period of time. These time periods are defined by your organization

Field Audit Trail UI



Contact
Carole White

Title: VP Sales
Account Name: Global Media
Phone (2): (415) 555-1212
Email: info@salesforce.com
Contact Owner: Pooled Org Admin

Field Audit Trail

	Date	Field	User	Old Value	New Value
1	Apr 25, 2018	Service Model	Jill Smith	Tier 2	Tier 1
2	Mar 23, 2018	Status	Joe Winters	Dormant	Active
3	Mar 23, 2018	Category	Joe Winters	Bronze	Silver
4	Jun 30, 2016	Risk Tolerance	Mary Jackson	Moderate	Aggressive
5	Nov 25, 2015	Name	Jake Jones	Julie Thompson	Julie Morris

We found no potential duplicates of this Contact.

Opportunities (0)

Filters: All time • All activities • All types

Upcoming & Overdue

No next steps.
To get things moving, add a task or set up a meeting.

No past activity. Past meetings and tasks marked as done show up here.

Real-Time Event Monitoring

Event Monitoring vs Real-Time Event Monitoring

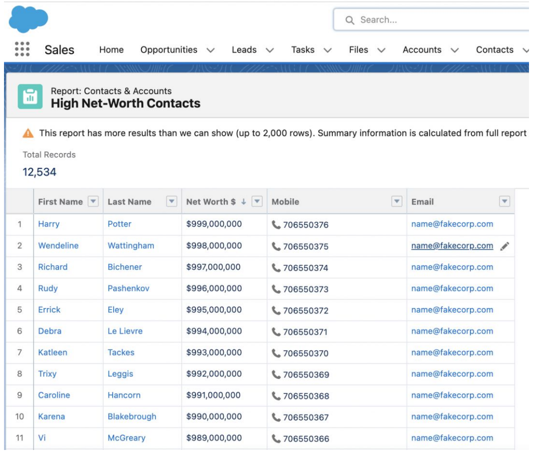
With Real-Time Event Monitoring, you can gain visibility into your Salesforce org in two ways: in near real time by monitoring specific platform events, and through querying events stored in big objects. Before we go any further, let's define some terms.

- **Event**: Anything that happens in Salesforce, including user **clicks, record state changes, and measuring values**. Events are **immutable and timestamped**.
- **Event Monitoring**: One of the many tools that Salesforce provides to help keep your data secure, allowing you to see the granular details of user activity in your organization. We refer to these user activities as events. Unlike Real-Time Events, Event Monitoring doesn't send real-time notifications. Instead, it stores user activity in a log that you can query.
- **Event log file**: In Event Monitoring, all events are stored in **EventLogFile** standard object event types, which are generated when an event occurs in your organization and is available to **view and download after 24 hours**, as well as on an **hourly cadence via Hourly EventLogFiles**. Event Monitoring stores **30 days' worth of event log files**.
- **Real-Time Event Monitoring**: Whereas Event Monitoring allows you to view events after 24 hours, Real-Time Event Monitoring helps you monitor and detect standard events in Salesforce in **near real time**. You can store the event data in **Big Objects** for auditing or reporting purposes.
- **Real-Time Events**: Real-Time Events are platform events that are **streamed in real time based on user actions in Salesforce**. These Real-Time Events are not only streamed immediately as platform events, but they are also stored in Big Objects immediately as well. Once an event is stored in a Big Object, you can query the event with SOQL and Async SOQL.

Event Monitoring Examples

We have a report where we know sensitive information is stored. We want to identify a user's attempt to export 5,000+ rows of data from Salesforce and prevent them from succeeding – perhaps it's the "high net worth contacts" report and a disgruntled salesperson is leaving the organization soon.

When there's an attempt to export the report, it will show the user a message that they don't have permission, therefore blocking the export. This is recorded as an "event", which can be monitored with analytics tools.



Report: Contacts & Accounts

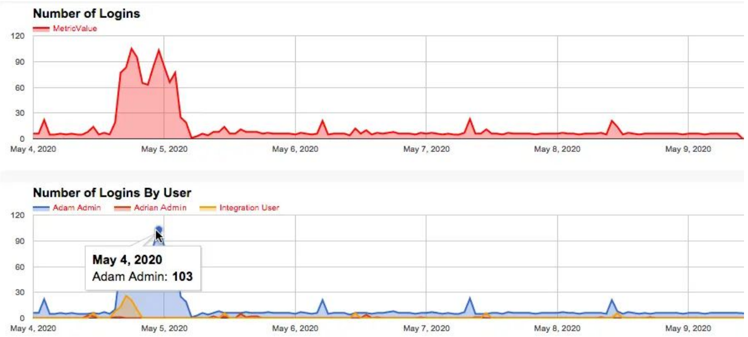
High Net-Worth Contacts

⚠ This report has more results than we can show (up to 2,000 rows). Summary information is calculated from full report

Total Records

12,534

	First Name	Last Name	Net Worth $ ↓	Mobile	Email
1	Harry	Potter	$999,000,000	☎ 706550376	name@fakecorp.com
2	Wendeline	Wattingham	$998,000,000	☎ 706550375	name@fakecorp.com
3	Richard	Bichener	$997,000,000	☎ 706550374	name@fakecorp.com
4	Rudy	Pashenkov	$996,000,000	☎ 706550373	name@fakecorp.com
5	Errick	Eley	$995,000,000	☎ 706550372	name@fakecorp.com
6	Debra	Le Lievre	$994,000,000	☎ 706550371	name@fakecorp.com
7	Katleen	Tackes	$993,000,000	☎ 706550370	name@fakecorp.com
8	Trixy	Leggis	$992,000,000	☎ 706550369	name@fakecorp.com
9	Caroline	Hancorn	$991,000,000	☎ 706550368	name@fakecorp.com
10	Karena	Blakebrough	$990,000,000	☎ 706550367	name@fakecorp.com
11	Vi	McGreary	$989,000,000	☎ 706550366	name@fakecorp.com



You can see that an unusually high number of logins to the organization occurred between May 4 and May 5. But how do you figure out exactly what happened during that time period? Luckily, Event Monitoring provides several ways for you to dig into this data. In this case, you might want to **break down the number of logins by user**.

Other Event Monitoring Uses

- **Monitor data loss.** Imagine that a sales rep leaves your company and joins a major competitor. Later, you find out that your organization is losing deal after deal to this other company. You suspect that your former employee downloaded a report containing leads and shared it with the competition. If you'd been using Event Monitoring, you could have caught this bad behavior before it cost your company sales.
- **Increase adoption**. Event Monitoring isn't just for catching your users' bad behavior. It can also alert you to parts of your organization that aren't performing well. For example, you just rolled out a new Visualforce page in your organization that combines accounts and contacts and allows end users to add custom fields. Without any metrics, it's difficult to tell how users are interacting with this page—if at all. Event Monitoring helps you figure out which parts of your organization need increased adoption efforts and identify areas that need redevelopment.
- **Optimize performance.** Sometimes, it's hard to determine the cause of slow page performance in your organization. Imagine that your company has an office in San Francisco and one in London. The users in London tell you that their reports are running slowly or even timing out. You can use Event Monitoring to determine whether the cause is related to a network issue in London or with the way your app is configured.

Event Monitoring Analytics App - Trailhead

- Salesforce Shield Event Monitoring is a security feature provided by Salesforce.
- It helps organizations monitor and track user activity and access to sensitive data within their Salesforce environment.
- It captures detailed information about user activity, including login activity, API usage, file downloads, and other actions.
- It also captures information about changes made to sensitive data, such as updates to records and changes to permissions and sharing settings.
- It enables organizations to gain visibility into user behavior, monitor security threats, and meet compliance requirements.
- Event Monitoring helps organizations identify potential security threats and investigate incidents.
- It provides a detailed audit trail of user activity and data access, which can be used to demonstrate compliance with regulations such as HIPAA, PCI-DSS, and GDPR.
- It is a paid add-on to the Salesforce platform and requires a separate license.
- It is typically used by organizations that handle sensitive data, such as healthcare, financial services, and government agencies, as well as those with stringent security and compliance requirements.

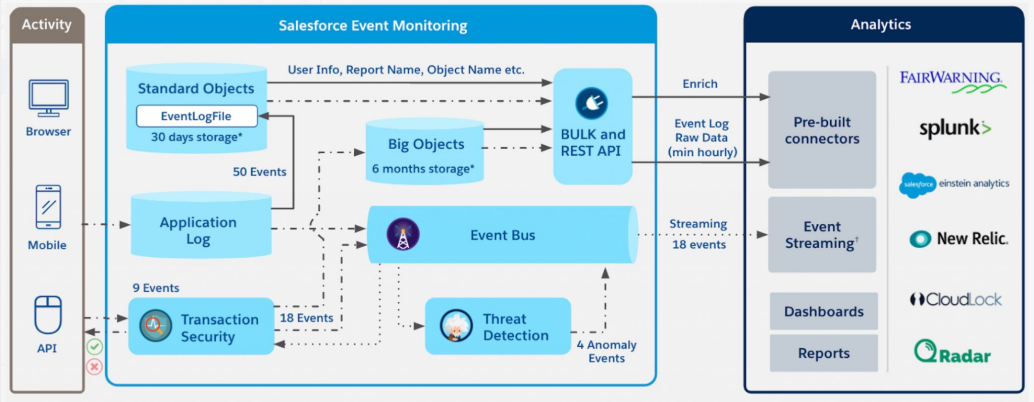
Event Monitoring Analytics

For reporting on Event Monitoring, Salesforce provides a CRM analytics app (pre-built dashboard), which comes with event monitoring (two licenses).

Events, such as our example with the disgruntled salesperson, are logged and shown in a variety of components. You can monitor trends by user, which reports are being downloaded, or how users are accessing certain reports.

Many customers will choose to bring that into Splunk or Qradar to align Salesforce event monitoring with other event monitoring from across their tech stack.

All events are stored in the **Event Log File** standard object, meaning you can run queries to do the analysis and forensics in the face of threats.



*30 days storage for all event types. 6mth storage for all real-time events with 10 yrs for Login and Identity Verification events
†Not supported by Einstein Analytics as part of Event Monitoring. Partner support varies.

- · - · - Sync Request/Reply
——— Async Batch
· · · · · · Async / Streaming

Platform Events and Big Objects

Using Real-Time Event Monitoring, you can interact with events either by subscribing to standard platform events, or by investigating events stored in big objects. Let's take a closer look.

Event Objects

Real-Time Event Monitoring objects have three primary uses: streaming data, storing data, and enforcing policies on data. But these uses don't apply to all objects. For guidance on which objects are available for each use case, see Considerations for Using Real-Time Event Monitoring.

Big Objects

Some Real-Time Events are stored as big objects so that you can look at historical event data for **6 months to 10 years in the past**, depending on the event, which is much longer than what you can do with event log files in Event Monitoring. This unlocks the power for your security team to investigate if an incident occurs because of malicious user behavior.

Big Objects

- Salesforce Big Objects is a feature that allows organizations to store and manage large volumes of data in Salesforce.
- It is designed to handle data sets that **exceed the limits of standard Salesforce objects**, such as Account and Contact objects.
- Big Objects are stored in a **special type of database table** that is optimized for handling **large data volumes**.
- They are accessed using a set of custom Apex APIs that are designed specifically for working with Big Objects.
- Big Objects support data indexing, which enables organizations to search and query large data sets quickly and efficiently.
- They also support **data archiving**, which enables organizations to **retain historical data** while keeping current data easily accessible.
- Big objects **don't support encryption**. If you archive encrypted data from a standard or custom object, it is stored as clear text on the big object.
- They are a paid feature of Salesforce and require a separate license (1 million records are included without incurring additional cost).
- Big Objects are typically used by organizations that require the ability to store and manage large volumes of data.

Enhanced Transaction Security

- Salesforce Shield Enhanced Transaction Security is a security feature provided by Salesforce.
- It enables organizations to create custom security policies that are based on a wide range of attributes and conditions, such as user location, device type, and login time.
- Enhanced Transaction Security policies are enforced in real-time, which means that organizations can immediately detect and block suspicious activity.
- The feature allows organizations to create custom policies for specific user profiles or roles, as well as for specific data objects or fields.
- Enhanced Transaction Security provides a wide range of pre-built policy templates that are designed to help organizations meet various security and compliance requirements.
- It includes integration with external threat intelligence services, which enables organizations to identify and block known threats and malicious IP addresses.
- The feature also includes a real-time event monitoring capability, which enables organizations to gain visibility into user activity and access to sensitive data.
- Enhanced Transaction Security is a paid add-on to the Salesforce platform and requires a separate license.
- It is typically used by organizations that require advanced security capabilities, such as those in healthcare, financial services, and government agencies, as well as those with strict compliance requirements.

Enhanced Transaction Security Examples

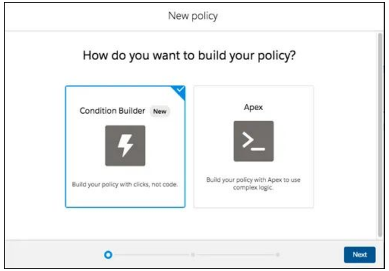
- Trusted IP Ranges: ETS allows you to define a set of trusted IP ranges for your organization. If a user tries to log in from an IP address outside of this range, they will be required to provide additional authentication information.
- Geolocation Restrictions: With ETS, you can restrict logins based on the user's geolocation. For example, if a user attempts to log in from a country outside of your allowed list, they will be required to provide additional authentication information.
- Device Recognition: ETS can also recognize and identify the devices that your users typically use to log in to your Salesforce org. If a user logs in from an unrecognized device, they will be required to provide additional authentication information.
- Time-Based Restrictions: ETS allows you to restrict logins based on the time of day or day of the week. For example, you could require additional authentication for logins outside of normal business hours.
- Multifactor Authentication: ETS can enforce multifactor authentication for specific users or groups. This can help protect sensitive data by requiring users to provide additional authentication information, such as a one-time password, in addition to their username and password.

Create Transaction Security Policies

Condition Builder

- Policies can be built entirely with clicks, though Apex classes are needed for custom use cases.

- Simple example: preventing a large data export. For this use case, we'll use Condition Builder to create the policy with just clicks.



New policy

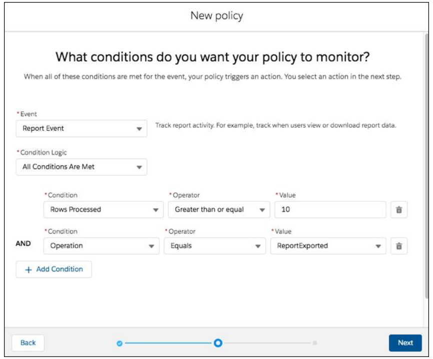
How do you want to build your policy?

Condition Builder New

Build your policy with clicks, not code.

Apex

Build your policy with Apex to use complex logic.



New policy

What conditions do you want your policy to monitor?

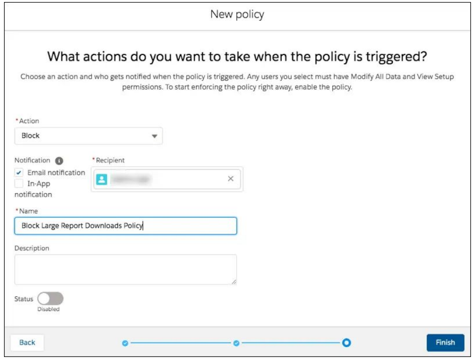
When all of these conditions are met for the event, your policy triggers an action. You select an action in the next step.

*Event: Report Event

Track report activity. For example, track when users view or download report data.

*Condition Logic: All Conditions Are Met

	*Condition	*Operator	*Value
	Rows Processed	Greater than or equal	10
AND	Operation	Equals	ReportExported



New policy

What actions do you want to take when the policy is triggered?

Choose an action and who gets notified when the policy is triggered. Any users you select must have Modify All Data and View Setup permissions. To start enforcing the policy right away, enable the policy.

*Action: Block

Notification
☑ Email notification
□ In-App notification

*Recipient: [redacted]

*Name: Block Large Report Downloads Policy

Description:

Status: Disabled

Einstein Data Detect

Install and Configure the Einstein Data Detect Managed Package

With “Einstein Data Detect” you can now scan your Salesforce Org for sensitive information like social security number or credit card number stored in comments field and take immediate steps protect customer data.

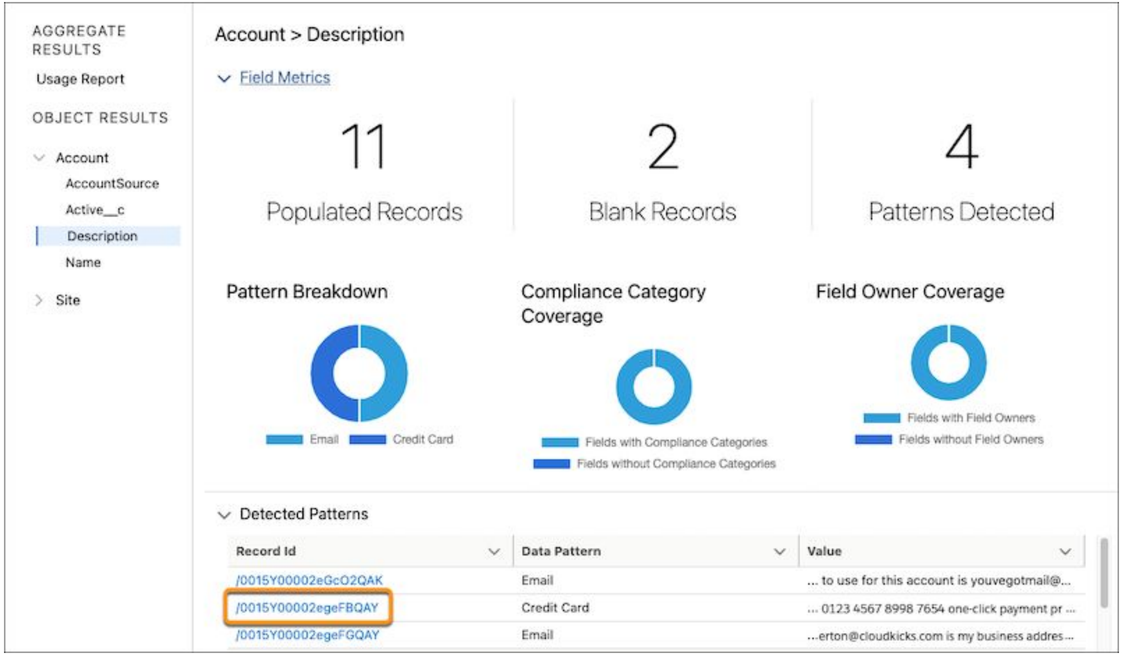
The Einstein Data Detect managed package is available to customers who have purchased the Salesforce Shield add-on subscription.

Einstein Data Detect automatically scans your Salesforce database, and identifies sensitive data based on **five data patterns**:

1. Credit card numbers
2. Emails
3. Social security numbers
4. URLs
5. IP addresses

That’s why Einstein Data Detect works hand-in-hand with platform encryption, informing what needs to be encrypted “at rest”.

While Einstein Data Detect will give you the baseline of where you may have sensitive field data, it doesn’t enable you to classify your data. You can use a third-party tool to support this exercise.



Account > Description

Field Metrics

11 Populated Records

2 Blank Records

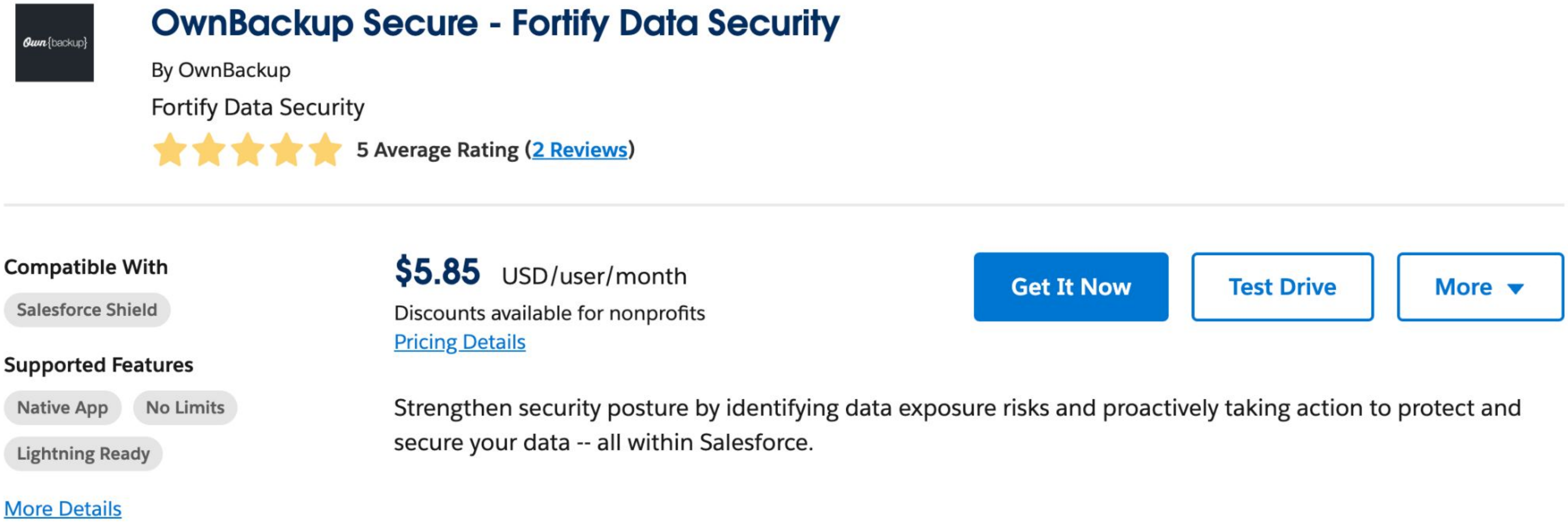
4 Patterns Detected

Detected Patterns

Record Id	Data Pattern	Value
/0015Y00002eGcO2QAK	Email	... to use for this account is youvegotmail@...
/0015Y00002egeFBQAY	Credit Card	... 0123 4567 8998 7654 one-click payment pr ...
/0015Y00002egeFGQAY	Email	...erton@cloudkicks.com is my business addres...

Complementary Product - OwnBackup Secure

OwnBackup Secure



OwnBackup Secure - Fortify Data Security

By OwnBackup

Fortify Data Security

★★★★★ 5 Average Rating (2 Reviews)

Compatible With

Salesforce Shield

Supported Features

Native App

No Limits

Lightning Ready

More Details

$5.85 USD/user/month

Discounts available for nonprofits

Pricing Details

Strengthen security posture by identifying data exposure risks and proactively taking action to protect and secure your data -- all within Salesforce.

Continued Learning

Apex Hours: Shield Platform Encryption

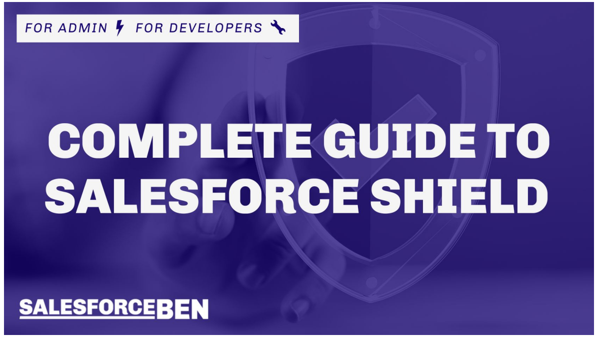
Trail: Secure Your Apps with Salesforce Shield

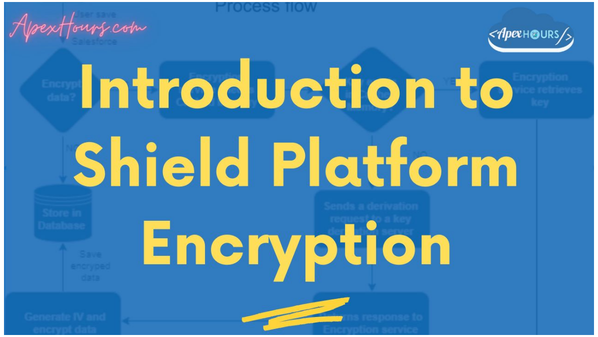
Platform Demos: Platform Encryption

Platform Demos: Field Audit Trail Simulator

YouTube: Discover and Deploy Salesforce Shield in 30 Minutes

Official Salesforce Shield Platform Encryption Implementation Guide





TRAILHEAD