



Advanced protection for your critical and sensitive data

With the average cost of a data breach reaching \$4.4M¹ and AI-driven cyber threats surging 89% year-over-year², protecting critical and sensitive data has never been more urgent. Salesforce Shield addresses these risks directly, providing the advanced security and compliance controls organizations need to maintain trust, meet global regulations, and expand data visibility and control.

The cost of inaction

\$14.8M

The average cost of a regulatory failure or noncompliance¹

294 days

Avg days to contain a data breach, resulting in downtime and eroded customer trust¹

6 reasons to implement Salesforce Shield

- 1

Mitigate risk and prevent data loss:
Protect sensitive data from internal and external threats
- 2

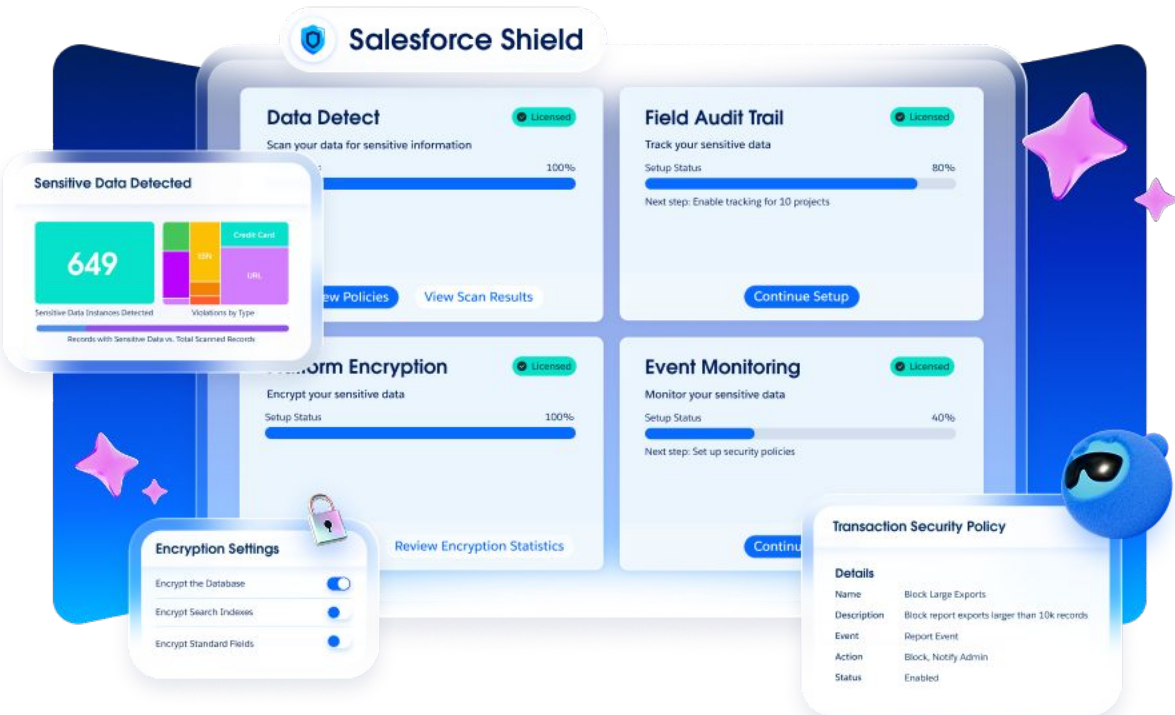
Address evolving compliance needs:
Meet compliance requirements like SOX, PCI DSS, HIPAA, GDPR/CCPA
- 3

Secure your data for agentic AI:
Safeguard your data is secure for agentic initiatives
- 4

Create historical records for audits:
Capture a forensic audit trail of sensitive data changes and their evolution over time
- 5

Satisfy contractual requirements:
Meet contractual agreements for encryption at rest and key management
- 6

Troubleshoot performance and drive adoption:
Assess application adoption and performance with real time event monitoring



1. IBM Cost of a Data Breach Report 2025. 2. Salesforce State of IT Report 2024



Event Monitoring

Real-Time Protection

Block suspicious activity, such as bulk exports or unauthorized logins, instantly with automated security policies. Surface unknown threats and anomalies through threat detection.

Granular Visibility

Track a broad range of events to see what humans or agents are accessing what data, providing increased visibility into user behavior.

Performance Insights

Identify and resolve system bottlenecks using event data and prebuilt dashboards.

Platform Encryption

Seamless Encryption

Secure fields, files, search indexes, attachments, and your entire database without breaking the user experience. Extend encryption to Data 360 to keep critical assets protected.

Key Control

Maintain full control over your encryption keys to safeguard PII and satisfy strict regulatory and data-handling requirements.

Choice and Flexibility

Manage your own encryption lifecycle with Bring Your Own Key (BYOK), External Key Management (EKM), or use Salesforce-generated keys.

Field Audit Trail

Expanded Tracking

Monitor up to 200 fields per object – 10x the standard limit – to ensure no critical data change goes unrecorded.

Extended Retention

Capture an immutable record of field-level data changes indefinitely or for a defined period based on your specific compliance and legal mandates.

Forensic Audit Readiness

Prove the state of your data at any point in time with a tamper-proof audit trail that tracks who changed what, and when.

Data Detect

Intelligent Discovery

Easily locate hidden PII, such as national identification or credit card numbers, using high-speed native scanning. For sensitive terms specific to your business or industry, you can also define custom patterns and keywords.

Scheduled Scans

Set up recurring scans on a weekly, monthly, or yearly basis for continuous monitoring.

Simplified Classification

Based on scan results, easily update data sensitivity and compliance categories to inform security controls such as encryption and monitoring protections.

