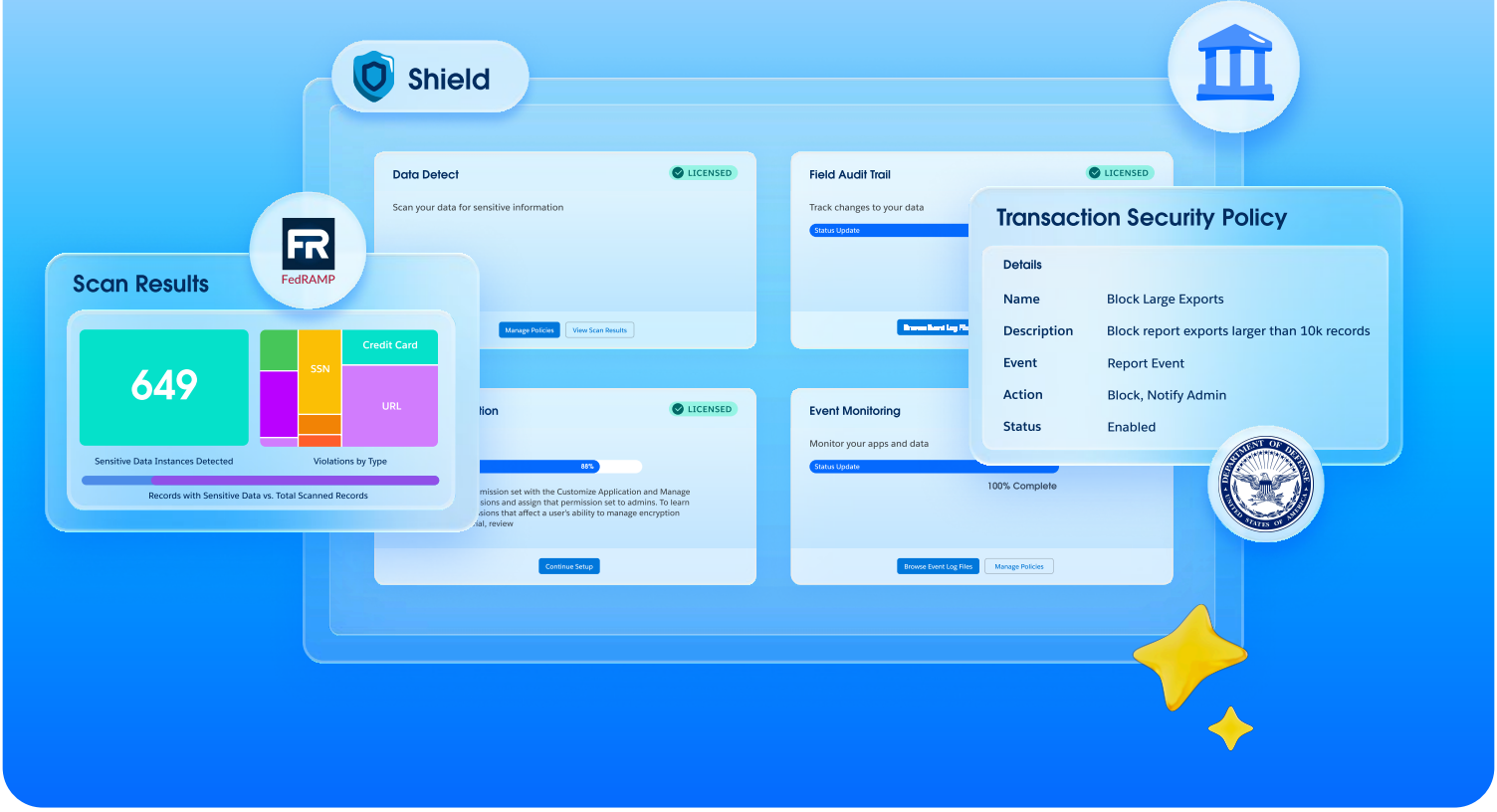
Guide

How Public Sector Organizations Can Secure Their Data with Salesforce Shield

Take a proactive approach to reducing risks and navigating compliance.



Contents

Take a proactive approach to reducing risks and navigating compliance.

Today's leaders across government face more challenges than ever, including mitigating new threats, adjusting to shrinking budgets, and managing multiple outdated systems. Since 2025, IT project requests have increased by 18%, and 29% of projects miss deadlines because limited resources can't keep pace with demand.

18% of IT project requests have increased since 2025.

29% of IT projects miss deadlines due to high demand and limited resources.

To address these gaps, many organizations across the world are using automation and artificial intelligence, with 30% of new applications now including AI. Despite the increase in AI usage, security and privacy remain foundational requirements for all organizations, everywhere. IT security professionals say that the biggest threats in this new environment include data breaches (80%), AI-powered "smart" threats (79%), data poisoning (77%), and model supply chain attacks (75%).

Salesforce Government Cloud Plus helps U.S. public sector organizations scale and secure their AI agents, data, and applications on a trusted platform. For agencies that need advanced security or stricter compliance, Salesforce Shield offers extra protection.

Protect, monitor, and retain critical Salesforce data with Shield

Salesforce Shield offers a level of protection, visibility, and control that goes beyond the native platform baseline. It's products – Event Monitoring, Platform Encryption, Data Detect, and Field Audit Trail – provide advanced controls to amplify the platform's defense-in-depth, delivering rigorous security and compliance essential for securing critical data.

Event Monitoring: Audit access, detect threats, and enforce security policies

It can be challenging for government agencies to monitor data usage at scale. Standard Salesforce logs help track some activities, but Shield: Event Monitoring offers much more detailed logs. This gives public sector organizations real-time insight into who is accessing sensitive data, from where, and when.

Event Monitoring also helps meet FedRAMP and NIST CSF requirements for analyzing and retaining audit records. It gives you a single view to watch for suspicious activity and conduct forensic investigations. You can track things like data exports, risky user actions, and other threats, so you can respond to incidents quickly and simplify audits. These logs also give InfoSec teams visibility into Salesforce orgs, as they send real-time security alerts to their security monitoring systems (e.g., SIEM, SSPM).

Event Monitoring also includes Transaction Security Policies (TSP). Each policy checks for certain conditions and triggers real-time actions when those conditions are met. These actions can include blocking an activity, sending an alert, or requiring multi-factor authentication (MFA).

Event Monitoring is also helpful for responding to and investigating incidents. Log details help create timelines, assess the scope, find the root cause, notify those affected, and report to stakeholders or regulators. Forensic analysis of logs can also help remove unauthorized access and guide risk assessments.

Platform Encryption: Prevent sensitive data from becoming an easy target

Hyperforce automatically encrypts data at rest at the volume level. This means all data on a disk is protected with a single encryption key managed by Salesforce.

For government agencies handling particularly sensitive information or following stringent data requirements, Platform Encryption encrypts data at rest using FIPS 140-3 validated, AES-256-bit encryption, making stolen data useless without the encryption key. With Platform Encryption, you can encrypt your data with unique keys you control and manage, and use field-level encryption to protect specific, highly sensitive fields. And soon, Platform Encryption customers will also be able to use database encryption to protect the entire transactional database.

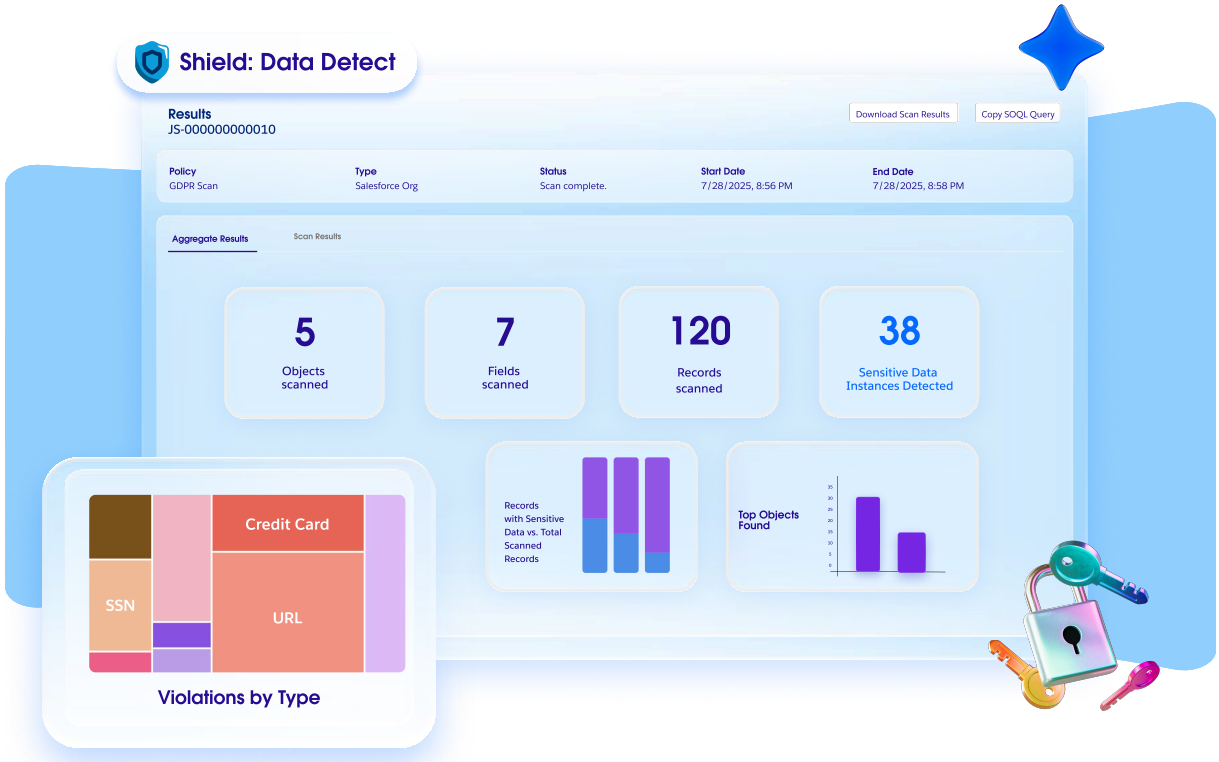
Platform Encryption lets agencies encrypt standard fields, custom fields, files, and attachments, all while keeping critical business operations working.

Data Detect: Find and classify sensitive data quickly

To close readiness gaps, CIOs now spend 20% of their budgets on data infrastructure and management. Data Detect speeds up data governance by replacing slow, manual discovery processes with deep scanning capabilities that automatically identify where sensitive data like PII or PHI is stored, even when it is hidden in unexpected fields.

Through intelligent pattern detection, government agencies can automatically locate hidden PII, such as Social Security numbers and credit card numbers using native scanning with multi-level validation. For more specialized needs, custom pattern and keyword scanning allow agencies to define unique rules to identify proprietary data formats or specific sensitive terms. Once sensitive data has been identified, government agencies can use scan results to make informed decisions to prevent data exposure.

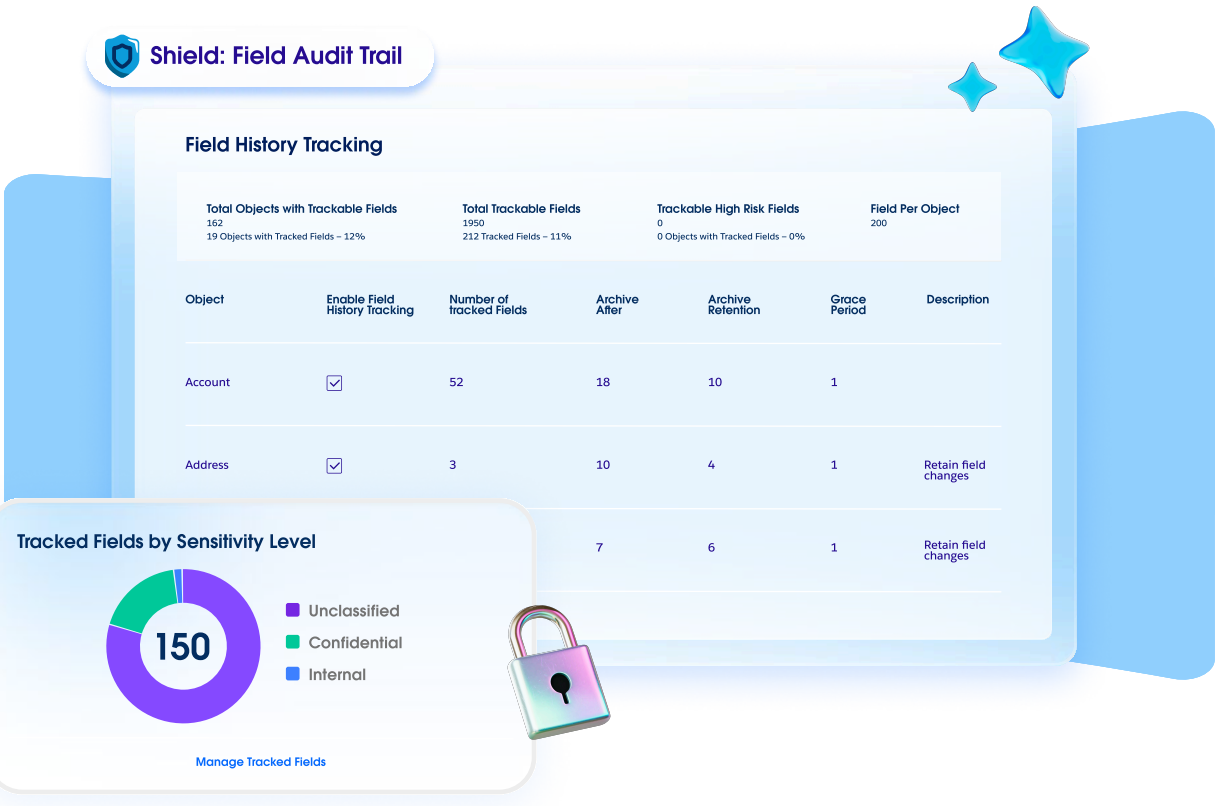
Agencies can update sensitivity and compliance categories directly within Data Detect, and apply additional security controls, like encryption or transaction security policies for enhanced protection. This proactive approach helps organizations spot vulnerabilities, improve data quality, and ensure security controls are in place before using AI agents.



Field Audit Trail: Maintain productivity while preparing for regulatory audits

Getting ready for an audit often means agencies have to pause their main work to gather old records. Field Audit Trail lets public sector teams track when and how sensitive data changes, monitoring up to 200 fields per object. Admins can set custom retention policies and keep field history indefinitely, meeting regulations without interrupting daily work.

This "time-machine" capability provides invaluable forensic visibility, enabling agencies to reconstruct the exact state of a record at any point in history to verify data lineage or resolve internal investigations. By automating the archival process, agencies transform audit readiness from a reactive hurdle into a proactive, immutable record of truth that ensures long-term transparency and accountability.



Address key public sector regulations with Shield

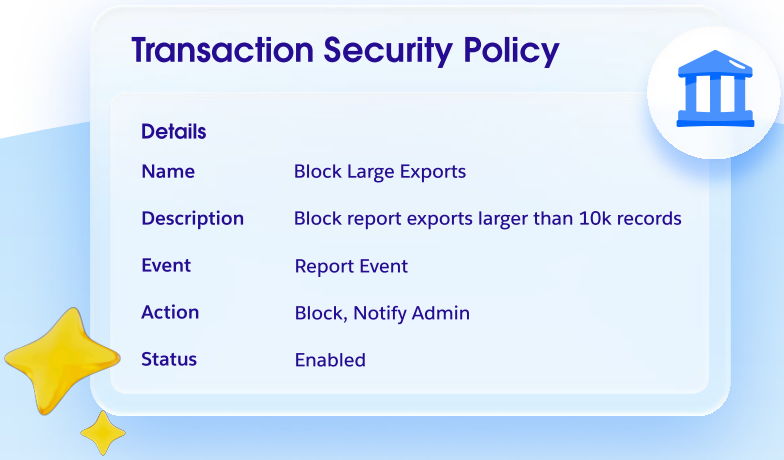
Shield gives government agencies and contractors the tools they need to meet important public-sector regulations.

DoW IL4 and IL5

Department of War (DoW) agencies can leverage Salesforce Shield to satisfy requirements defined in the DoD Cloud Service Provider (CSP) Security Requirements Guide (SRG) and the Cloud Computing Mission Owner SRG. Shield Platform Encryption enables Mission Owners to fulfill the SRG mandate that DOW data be encrypted at rest with exclusive Mission Owner control over encryption keys – from creation through destruction – using Salesforce's Key Management Service (KMS) or Bring Your Own Key (BYOK) capabilities.

Shield Event Monitoring complements encryption requirements by providing Mission Owners and their designated DoW Cyber Security Service Provider (CSSP) with comprehensive user activity logs across 80+ event types – including login/logout events, data access patterns, API activity, bulk data exports, and configuration changes – enabling continuous monitoring, forensic investigation, and SIEM integration aligned to the SRG's audit and accountability requirements. Together, these Shield capabilities address the "last mile" of DoW SRG compliance for Mission Owners operating SaaS platforms within their authorization boundary.

All Shield products have IL5 authorization, except Data Detect (Review In Progress), which is still being reviewed for IL5 by DISA. These certifications lets Government Cloud Plus Defense customers use Shield in a compliant manner, to securely protect their data and systems.



Cybersecurity Maturity Model Certification (CMMC) 2.0

CMMC 2.0 is the Department of War's updated cybersecurity framework for contractors who handle Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). It now has three maturity levels: Level 1 follows FAR 52.204-21, Level 2 matches NIST SP 800-171 controls, and Level 3 pertains to companies handling CUI associated with high-level threats, based on NIST SP 800-172.

To meet CMMC requirements, organizations need to monitor, control, and protect communications at both external and key internal system boundaries. Event Monitoring, Platform Encryption, and Field Audit Trail, part of the Shield suite, offer the tools needed for thorough auditing, secure setups, and strong encryption to protect data everywhere.

GDPR & global privacy laws

The General Data Protection Regulation (GDPR) requires data to be processed lawfully, fairly, and transparently, following key principles like purpose limits, accuracy, and security. According to the law, these principles must be built in by design and supported by risk-based security and accountability. For agencies working internationally or handling global data, Shield helps you navigate GDPR requirements and similar privacy rules by allowing encryption, pseudonymization, strict access audits, and incident monitoring.

IRS Publication 1075 (IRS 1075)

IRS 1075 sets strict rules for public sector agencies and contractors who handle Federal Tax Information (FTI), such as names, addresses, SSNs, and tax returns. Salesforce Government Cloud Plus has been reviewed by a third party to meet these requirements, and Shield products help enforce the needed safeguards and access controls to protect FTI.

Explore more ways to enhance security for the public sector

In addition to Shield, other Salesforce Trusted Services solutions help government organizations meet compliance needs. Here are a few examples:

Security Center

Security Center brings all of your permissions and controls together in one place, making it easier to do regular risk assessments needed for frameworks like CMMC and FedRAMP/NIST. Automated security monitoring helps administrators quickly spot misconfigurations and wrong user permissions. This proactive approach closes security gaps, keeps you compliant, and saves time and money on manual audit prep.

Backup & Recover

It's important to keep backups separate from main systems and regularly test recovery steps for disaster recovery and business continuity (BCDR). Backup & Recover helps agencies meet strict BCDR standards, including showing they can restore critical data within their Recovery Time Objective (RTO) and Recovery Point Objective (RPO).

Unlike traditional methods that require taking a server or database offline during a restore, Salesforce lets you fix affected data while the system stays up and users keep working. Backup & Recover can quickly roll forward, so data repair keep up with the fast pace of AI-driven applications.

Data Mask & Seed

Secure development environments are important because they can be a major vulnerability. Sandboxes often hold sensitive data but may not have the same strict controls or enforcement as production systems.

To reduce this potential, Data Mask & Seed lets agencies keep CUI and FCI out of development environments by anonymizing sensitive fields. This means even developers with high access see less real sensitive data. By using both role-based access controls and data anonymization, organizations can develop quickly without breaking the strict data boundaries needed for CMMC or FedRAMP compliance.

Get in touch

The information provided in this white paper is strictly for the convenience of our customers and is for general informational purposes only. Salesforce, Inc. does not warrant the accuracy or completeness of any information, text, graphics, links, or other items contained herein. Salesforce, Inc. does not guarantee you will achieve any specific results if you follow any guidance in this white paper. It may be advisable for you to consult with a professional such as a lawyer, accountant, technical architect, business advisor, or Salesforce partner to get specific advice that applies to your specific situation. This information is subject to Salesforce's Forward-Looking Statements.