Deloitte. Digital | salesforce

Protecting Salesforce Environments in an Age of Advanced Cyber Threats

February 2026

The Salesforce security imperative in an Artificial Intelligence (AI)-driven threat landscape

Security risks for Salesforce environments in the era of AI are becoming more sophisticated and complex:

- **Social engineering and malicious third-party application tactics have evolved** to be able to bypass strong technical controls
- **Bad actors are exploiting organizations** that have a Salesforce environment by **compromising third-party applications that integrate with Salesforce**
- **Attackers are using creative methods in the age of AI**, utilizing new avenues like **AI chat bots and voice phishing** to steal valuable data out of Salesforce environments
- **Highly sensitive business data is centralized in Salesforce**, creating a valuable target for attackers
- **Risks are heightened** when organizations grant external applications or managed packages **broad permissions**
- Breaches can **severely disrupt business operations, undermine data security, and damage customer trust,** underscoring the need for vigilant access management and continuous monitoring

Shared responsibility model: Collaborative security measures for the Salesforce Platform

MAINTAINING THE SECURITY OF YOUR SALESFORCE ENVIRONMENT IS A SHARED RESPONSIBILITY. BY UNDERSTANDING YOUR ROLE, YOU CAN HELP CLOSE SECURITY GAPS AND SAFEGUARD YOUR ORGANIZATION'S MOST SENSITIVE INFORMATION.

Salesforce responsibility areas

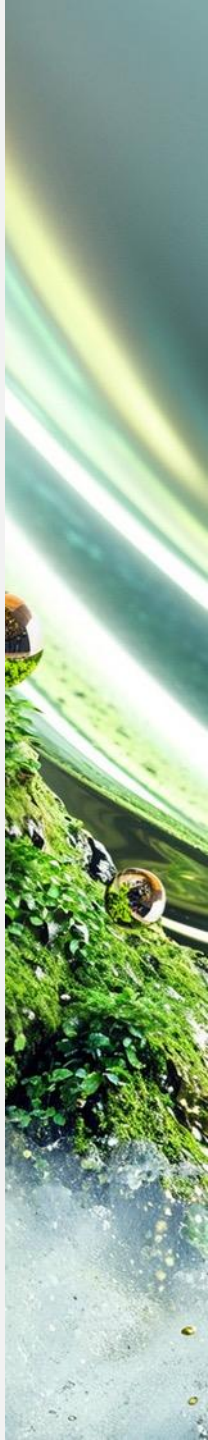
- Metadata-driven architecture
- Contractual assurance & transparency
- Secure software development
- Host, storage, and network security
- Third-party auditing & testing
- Least privilege access & segmentation
- Hyperforce
- Site reliability & disaster recovery

Salesforce is responsible for securing the underlying platform, infrastructure, and core services, creating a solid foundation for customer applications.

Customer & shared responsibility areas

- Multi-factor authentication
- IP Allowlisting
- Principal of least privilege
- Application Security
- Auditing
- Health checks
- Logging, monitoring, and platform controls
- Network controls

Clients are responsible for configuring security controls within their Salesforce environments, such as managing authentication, permissions, auditing, and application-level protections, to safeguard their own data and usage.



Potential security vulnerabilities within client-controlled Salesforce configurations

SALESFORCE PLATFORM MISCONFIGURATIONS UNDER CLIENT RESPONSIBILITY THAT COULD COMPROMISE SECURITY INCLUDE:

- Bypassing object and field-level access settings
- Using software that has known vulnerabilities (vulnerable third-party platforms)
- Bypassing sharing rules in Apex
- Storing sensitive data insecurely
- Using insecure TLS (Transport Layer Security)/SSL (Secure Sockets Layer) configurations
- Cross-site request forgery
- Insufficient escaping in Lightning components
- Loading JavaScript files from third-party endpoints
- SOQL (Salesforce Object Query Language) injection due to insecure database query construction

Deloitte delivers multi-layer Salesforce environment security, from risk insights to rapid recovery

Accelerated, end-to-end deployment

Deploy Shield, Security Center, Privacy Center, and OwnBackup swiftly and seamlessly across your Salesforce environments, leveraging Deloitte's demonstrated accelerators, leading practices, and deep platform experience.

Tailored strategy & integration

Align platform security, privacy, and backup solutions to your organization's specific regulatory, operational, and risk landscape providing—enabling coverage without disrupting business processes.

Continuous risk & compliance management

Proactively monitor, classify, and protect sensitive data; automate policy enforcement and drive ongoing compliance through advanced analytics, risk intelligence, and managed services.

Broad visibility & ongoing optimization

Connect insights across all layers (security, privacy, backup) to provide a single, actionable view of risks, enabling your teams to adapt as threats and regulations evolve.

Rapid recovery & business continuity

Establish resilient backup, proactive alerting, and rapid disaster recovery processes so you're prepared for data loss, cyber threats, or regulatory incidents—helping to limit downtime and business impact.

Trusted Deloitte & Salesforce relationship

Benefit from Deloitte's leading global alliance with Salesforce, cyber risk credentials, and a track record of enabling secure digital transformation for many of the world's most complex organizations.

Integrated Salesforce Cyber defense—powered by Deloitte

Harness Salesforce Shield, Security Center, Privacy Center, and OwnBackup—implemented by Deloitte—to monitor, secure, and govern your data ecosystem, aiding in reducing the risk of breaches from third-party applications.

SALESFORCE TRUSTED SERVICES:

Shield

- Robust data encryption at rest
- Event monitoring & field audit trail
- Real-time threat detection & policy enforcement
- Automated sensitive data discovery & classification

Security Center

- AI-powered threat & anomaly detection
- Proactive alerts & policy enforcement
- Eliminates blind spots across all applications
- Monitors for social engineering & AI-driven risks

Privacy Center

- Data de-identification and minimization
- AI-driven policy monitoring
- Consent & retention management
- Data Subject Access Request (DSAR)/Right to be Forgotten (RTBF) automation

OwnBackup

- Encrypted daily backups
- Powerful search & recovery
- Visual change tracking
- Sandbox/data loss prevention
- End-to-end governance & privacy controls to align with global policies

Integrated Salesforce Cyber defense—powered by Deloitte (cont.)

DELOITTE CYBER ACTIVITIES AND OFFERINGS BY SECURITY SOLUTION:

- Enable and optimize platform encryption without impacting business processes or user productivity.
- Set up event monitoring and full field audit trail to capture, retain, and analyze detailed user, admin, and third-party app activities for compliance.
- Customize permission tracking and configuration monitoring, helping to facilitate continuous compliance and proactive identification of emerging platform risks.

- Configure AI-driven monitoring and proactive alerts to rapidly detect and address changes that indicate risk—such as privilege escalation, sensitive data exports, or unusual user activity.
- Deploy and automate security policies across all Salesforce organizations to help remove blind spots and enable consistent policy enforcement.
- Leverage advanced data classification and risk intelligence to surface vulnerabilities and prioritize remediation across your Salesforce landscape.

- Establish and automate policies for data classification, retention, deletion, and anonymization to help organizations manage sensitive data and meet privacy obligations.
- Configure and monitor end-to-end workflows for DSARs, RTBF, and consent management, accelerating regulatory response times and reducing manual intervention.
- Support secure de-identification and pseudonymization of personal data, leveraging Privacy Center features to enforce least-privilege access and help reduce regulatory risk.

- Develop and analyze encrypted, compliant backup strategies to safeguard Salesforce organizational data, metadata, and attachments from unauthorized access and accidental loss.
- Deploy automated tools to track, alert, and visualize changes to backed-up data, enabling rapid detection of data corruption, deletion, or unusual activity and supporting investigative readiness.
- Orchestrate rapid, secure recovery workflows enabling business continuity and fast response to ransomware or accidental deletion scenarios.

Contact our Deloitte Cyber Salesforce Alliance team:

Niloo Bedrood
Managing Director
Deloitte & Touche LLP
nbedrood@deloitte.com

Chirag Patel
Principal
Deloitte & Touche LLP
chirpatel@deloitte.com

Huy Vo
Senior Manager
Deloitte & Touche LLP
huvo@deloitte.com

Kelli Wolfe
Alliance Manager
Deloitte & Touche LLP
kelwolfe@deloitte.com

Andrew Haggen
Sales Executive
Deloitte & Touche LLP
ahaggen@deloitte.com

Michael Moore
Sales Executive, Vice President
Deloitte Consulting LLP
mimoore@deloitte.com

Dave Pearson
Managing Director
Deloitte Consulting LLP
dpearson@deloitte.com

Karl Rupilius
Principal
Deloitte Consulting LLP
krupilius@deloitte.com

Deloitte. Digital | salesforce

Thank you.