cirrius solutions

Salesforce Security Best Practices in 2026

Protecting Data, Managing Access, and Preparing for AI



cirrius solutions

Why Security is Critical



Salesforce holds sensitive customer data



Security impacts trust and compliance



Most risks come from misconfiguration



Security must be continuous



cirrius solutions

Salesforce Security is Layered

Salesforce Security Model

1. Org-Level Security
2. Object-Level Security
3. Field-Level Security
4. Record-Level Security

Security works best when implemented in layers.



cirrius solutions

The Biggest Security Mistake

Overusing Profiles

Old model:

- Many profiles controlling permissions

Modern best practice:

- Profiles = baseline access
- Permission Sets = specific permissions
- Permission Set Groups = job roles



Modern best practice:

Permission Set Groups = job roles

Permission Sets = specific permissions

Profiles = baseline access



cirrus solutions

Principle of Least Privilege



Goal: Reduce risk surface area

cirrius solutions

MFA and Identity Security

Multi-Factor Authentication (MFA)



cirrius solutions

Automating Access with User Access Policies

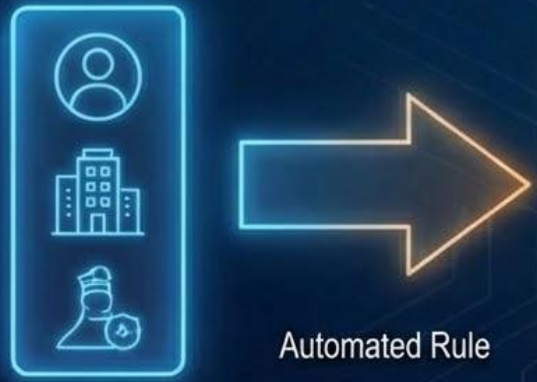
User Access Policies

Automate permission assignment based on user attributes.

Example:

If
Department = Sales

Then
Assign Sales Permission Set Group



Automated Rule



cirrus solutions

Integration Security

Integration Security Best Practices



curius solutions

Data Security & Compliance

Tools available in Salesforce:



Field Level Security



Data Classification



Shield Platform Encryption

(Available with SF Shield Purchase)



Event Monitoring

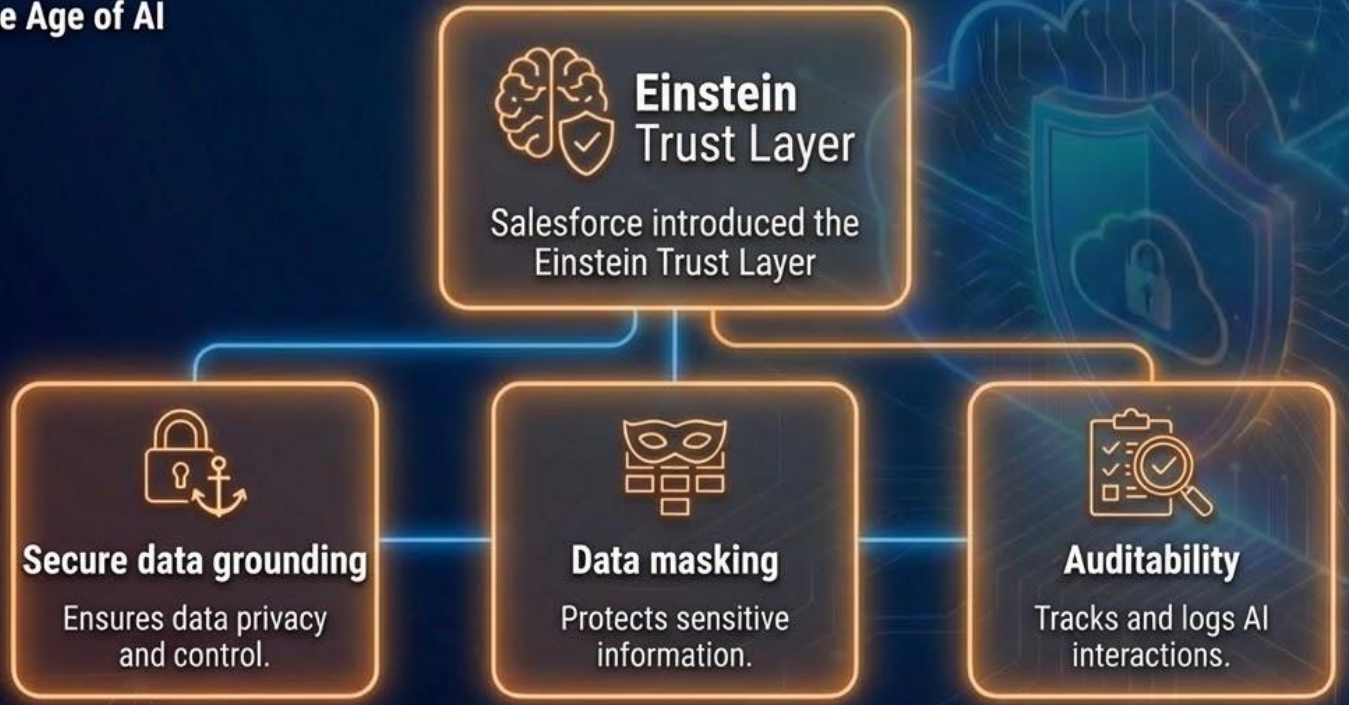
(Available with SF Shield Purchase)



cirrius solutions

AI and the Future of Security

Security in the Age of AI



curius solutions

Security Best Practices Checklist

Top Security Actions for Every Org



cirrius solutions

Key Takeaways

Salesforce Security Key Takeaways

