AppOmni

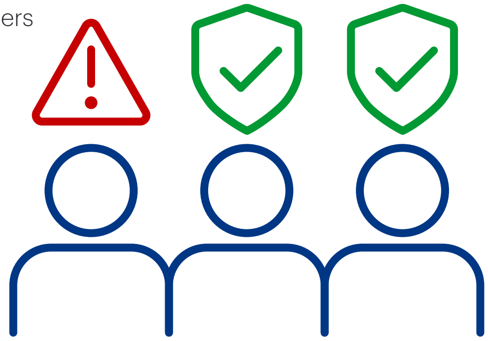
7 Must-Have Salesforce Security Practices You Can't Afford to Ignore

Your Salesforce environment is essential to your business, but securing it against evolving threats is critical. Here are seven essential practices to safeguard your data:

1

Review and Optimize User Permissions

Over-permissioned users can expose sensitive data, either accidentally or intentionally. Continuous monitoring and dynamic adjustment of permissions ensure that users have only what they need, reducing the risk of unauthorized access.

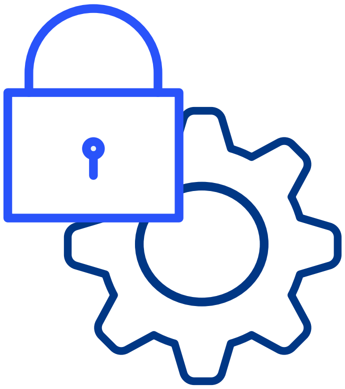


Key Actions:

Monitor and Adjust Permissions Continuously: Automatically flag and correct over-permissioned accounts to reduce security risks.

Enforce Least Privilege: Ensure users only have the permissions necessary for their roles, dynamically adjusting as needed.

2



Secure System Settings

System settings are the backbone of your Salesforce security posture. Misconfigurations can create vulnerabilities that attackers exploit. Regularly align these settings with best practices to prevent exposure.

Key Actions:

Prioritize High-Risk Settings: Focus on securing critical areas like API access and data exports to minimize vulnerabilities.

Enable Drift Alerts: Set up alerts to catch any deviations from approved configurations, ensuring rapid response.

3

Update Your Baseline Policies

System settings are the backbone of your Salesforce security posture. Misconfigurations can create vulnerabilities that attackers exploit. Regularly align these settings with best practices to prevent exposure.

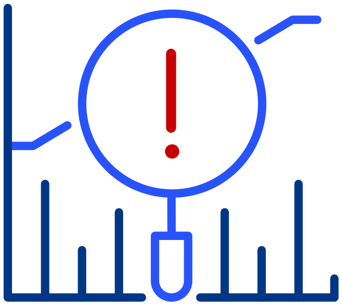
Key Actions:

Automate Policy Enforcement: Keep baseline policies up to date and ensure they are consistently applied across your environment.

Detect and Correct Deviations: Quickly address any departures from established policies to maintain security.

4

Enhance Salesforce Security with Precise Threat Detection



Effective threat detection is essential for identifying and addressing potential risks in your Salesforce environment. Proactive monitoring helps prevent unauthorized access and malicious activities.

Key Actions:

Implement Comprehensive Detection: Use advanced tools to monitor for a wide range of risks, from unusual logins to data extraction attempts.

Customize Alerts: Tailor detection alerts to focus on the most critical activities for quicker, more effective responses.

5

Secure Data Handling for Einstein

Einstein's AI-driven features offer powerful capabilities but can introduce risks if not properly secured. Secure data handling is essential to prevent exposure and unauthorized access.

Key Actions:

Restrict Data Sharing: Limit who can access synchronized data and use filters to protect sensitive information.

Set Secure Defaults: Ensure default settings prioritize security to minimize the risk of data exposure.

6

Govern and Secure Connected SaaS Apps

Connected SaaS apps can introduce security risks if not properly managed. Visibility and control over these connections are crucial to maintaining a secure Salesforce environment.

Key Actions:

Gain Visibility and Control: Regularly review all connected SaaS apps, focusing on those linked through identity providers.

Assess and Monitor Risks: Use tools to map and evaluate app connections, prioritizing actions based on potential security impacts.

7

Enable and Monitor External Client Settings

External Client settings control how third-party applications interact with Salesforce. Proper management of these settings is vital to preventing unauthorized access and ensuring compliance.

Key Actions:

Restrict and Monitor Access: Limit external client access to only trusted apps and continuously monitor data flows for suspicious activity.

Enforce Granular Permissions: Apply detailed role-based access controls to minimize exposure and prevent unauthorized data access.

Secure Your Salesforce Environment with AppOmni

AppOmni simplifies these essential security practices by providing deep visibility and control over your Salesforce environment. With automated management of configurations, permissions, and integrations, AppOmni strengthens your security posture, ensuring resilience against evolving threats.

About AppOmni

AppOmni, the leader in SaaS Security, helps customers achieve secure productivity with their applications. Security teams and owners can quickly detect and mitigate threats using unmatched depth of protection, continuous monitoring, and comprehensive visibility. Trusted by the world's largest enterprises, AppOmni specializes in securing diverse SaaS environments.

Learn more at appomni.com