Flosum

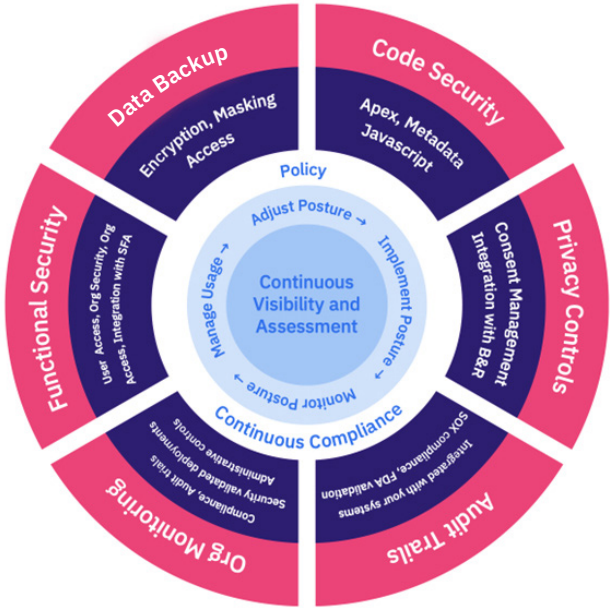
Trust Center

Adaptive Security for Salesforce Environments

Monitor security, audit changes and remediate access violations across multiple Salesforce environments with ease.

Building and maintaining an effective security framework to protect your Salesforce orgs is no easy task. Salesforce instances are constantly threatened by both technical vulnerabilities and improper human activity- both malicious and unintentional. Threats include phishing/social engineering, malware/ransomware, unprotected vulnerabilities, unsecure configurations, data leakage, unauthorized API access, third party interruptions and lack of security awareness.

The task of monitoring and remediating these threats manually is both tedious and cumbersome. When an issue arises, administrators and other stakeholders must often examine individual user profiles, assignments, object access permissions, and other minute details to determine cause. For organizations with a high number of users, this becomes exceedingly time- and resource-intensive. Further, this increases the chances of data not being fully protected. Organizations need an easy-to-use, comprehensive solution that helps protect data, manage compliance needs, regulate access permissions, facilitate change management, respond to violations, and more.



Flosum Trust Center helps organizations monitor security, audit changes and remediate access violations across multiple Salesforce environments with ease. It allows them to deliver best-practice DevSecOps procedures by securing Salesforce environments against cybersecurity threats and data breaches. Flosum Trust Center's single user interface brings full data accessibility and transparency to the entire organization, including sandboxes. With Flosum Trust Center, there is no need to parse through endless Salesforce Setup pages, build reports, or custom logic to monitor and maintain security policies across multiple orgs.

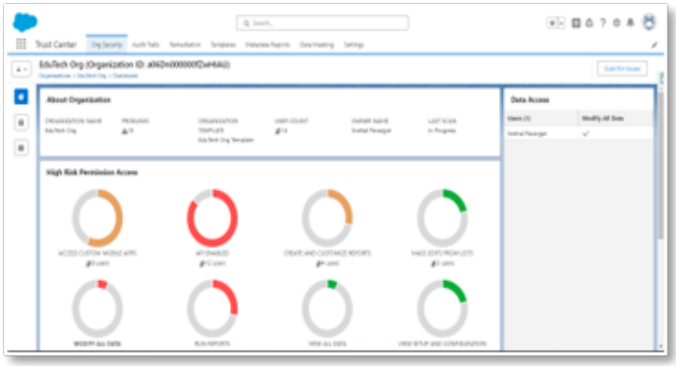
Key Capabilities

- **Security Monitoring.** Build a consolidated view of all org settings so that Salesforce admins, IT and security teams can enforce best practices.
- **Audit Change Management.** Enable detailed tracking of all changes, allowing users to prioritize their risk levels (High Risk, Low Risk, and Ignore)
- **Remediate Violations.** Proactively fix changes or address concerns covered by templates.

Org Security Monitor

Flosum Trust Center Key Features:

- **Org Monitoring.** Define security templates, and scan an org against those templates to automate identification and remediation of violations. View a Consolidated list of all org settings for security enforcement.
- **Data Masking.** Create a masking template that automates the anonymization of sensitive customer data at rest in Salesforce environments, on every refresh. Maintain the integrity of sensitive data while allowing developers and testers to work with realistic datasets without risking sensitive data exposure.
- **Audit Trails.** Track and log all changes within any Flosum-connected Salesforce org, including changes to components (manual or otherwise), processes, setups, and customizations, all centralized in one easy to use UI.
- **Metadata Reporting.** Compare different Salesforce orgs to identify differences, effectively manage audit compliance, and ensure consistency across environments, a crucial step for maintaining uniformity in configuration and customizations across development, testing, and production environments.



Org Dashboard

Why choose Flosum?

☑ Save 30% or more with a comprehensive backup solution.
☑ Our customers achieve 3x faster time to market.

To learn more: Book a Meeting

About Flosum

Flosum is the leading end-to-end secure DevOps, data management, and data protection platform. Flosum DevOps platform is built 100% natively on Salesforce. Our mission is to empower IT teams to innovate and manage the Salesforce cloud with confidence.

Follow us: