

6 Ways a Code Quality Tool Prevents Salesforce Security Risks

Unstable updates and applications can misfire, damaging datasets and even exposing sensitive records. Using a code quality tool to maintain high-quality standards not only makes a better end-user experience, but it also supports your Salesforce data security strategy.

Continuous production of secure updates is a great way to combat data security threats—but only if you guarantee perfect code with a code quality tool. Here are six ways a code quality tool mitigates Salesforce security risks.

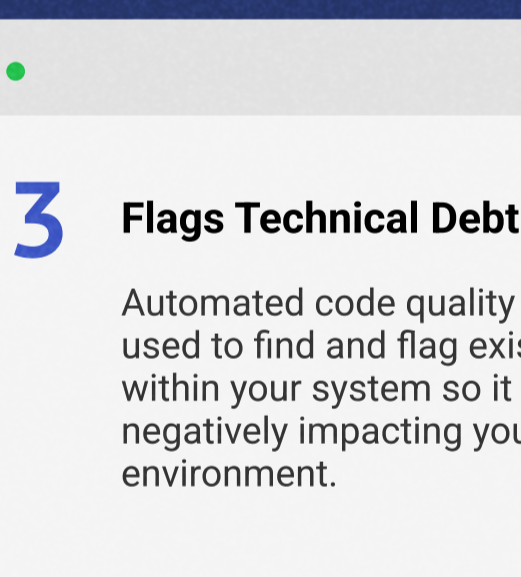
1 Reduces Misfires

A code quality tool enables developers to produce perfect code every time to eliminate the chances of a misfire in the final product.



2 Expedites Integration Processes

Testing your code prior to integration makes the ensuing processes much smoother, faster, and more comprehensive.



3 Flags Technical Debt

Automated code quality scanners can be used to find and flag existing technical debt within your system so it can be fixed before negatively impacting your Salesforce environment.



4 Produces Insights and Reporting

A code quality tool is able to compile the findings of its scans into reports that can be tracked and managed over time.



5 Decreases Manual Processes

Automating scans of your code reduces the strain on your employees while also improving the reliability of the results.



6 Documents Compliance

Automated DevOps tools compile information that can be repackaged for compliance audits, making it much easier to demonstrate adherence to stipulated standards.

