EBOOK

Preventing Salesforce Security Risks Through Code Quality

Addressing Vulnerabilities with Automation

INTRODUCTION

We are always updating and refining our Salesforce environments. New updates, applications, and integrations go a long way to expand our capacity for serving our customers, but they also introduce data security vulnerabilities if they aren't properly constructed.

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

Why is this so important?

- Failing to produce stable products creates back doors for cybercriminals to access your Salesforce data.
- Code quality tools support proper functionality of both the eventual application as well as the other DevOps tools used in the development pipeline.
- The synergy created through these tools increases ROI while supporting data security and compliance.

So how can you guarantee the consistent production of reliable updates and applications? Automated code review tools provide the coverage you need. Even the best developers make mistakes.

Here are six security risks that can be mitigated by integrating an automated code quality tool in your Salesforce environment:

1. Costly Misfires 004

2. Clunky Integration Processes 007

3. Technical Debt 010

4. No Reporting Insights 010

5. Error-Prone Manual Processes 010

6. Lack of Compliance Documentation 010

01

Costly Misfires

THE PROBLEM

Nobody sets out to produce anything less than perfect code. However, even the best developers are going to make mistakes; it's unavoidable. Human error is simply part of the process. That's why DevOps teams need to install multiple quality checks to ensure these mistakes don't make it into a live environment.

Coding errors lead to potentially dangerous misfires in an application or update, which can open a back door to cybercriminals while also damaging system data.

Code reviews are a standard aspect of a DevOps pipeline, but without proper tooling, the possibility of human error that threatens the code also means these errors can be missed during review. It's important to give your team the tools they need to account for these vulnerabilities.

THE IMPACT OF HIGH-QUALITY CODE

Automation is a DevOps team's best chance at avoiding the negative consequences of bad code. Costly misfires impact your Salesforce environment in a variety of ways, and none of them are good.

Equipping your team with an automated code review tool supports their efforts to attack the code-writing phase of the application life cycle skillfully and creatively.

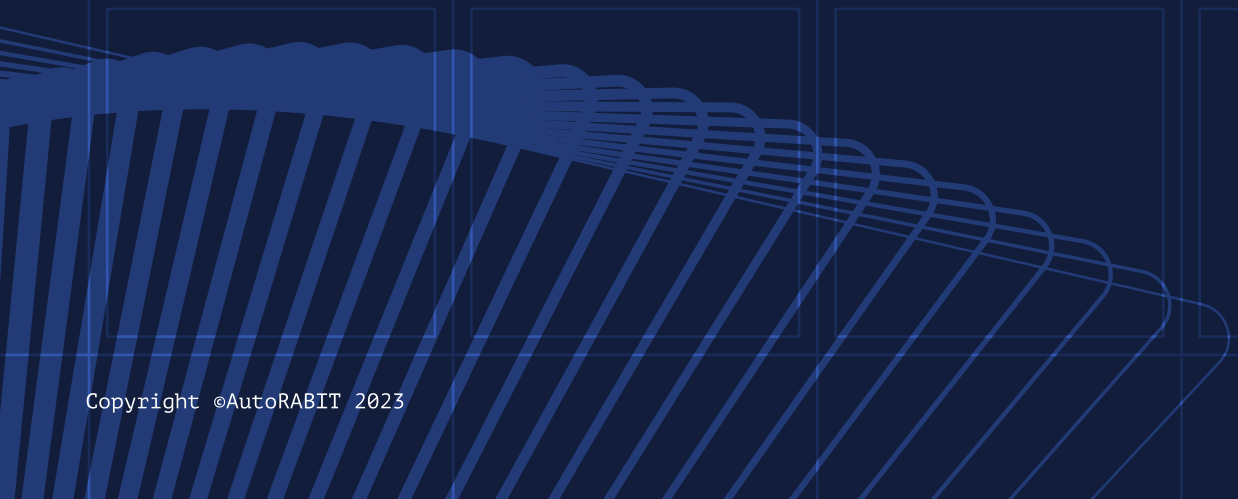
The strengths of our team members truly come into play when they let their creative minds run free and innovate while they work. A developer who is tied down by hours of code review isn't able to spend the time and energy creating new functionalities that make end users pay attention.

Automated code review tools don't get tired. They are just as accurate on the first line of code as they are on the 10,000th line.

> *"The CI/CD pipeline integration of AutoRABIT with Salesforce is a true life-saver and pretty seamless."*
>
> **- SABITHA ALI**

02

Clunky Integration Processes



THE PROBLEM

Any hiccups in the various stages of the DevOps pipeline will negatively impact both the ensuing processes as well as the overall quality of the update or application. Integrating multiple changes and components creates a cohesive package that verifies proper functionality of the update before sending it off to production.

Faulty code can complicate this process and lead to the inclusion of errors in the final product, risking functionality and exposing security issues.

Finding these problems during the integration stage causes developers to undo hours of work to correct the update. It's much better to find these issues prior to the integration phase to support a higher-quality release while reducing wasted time.

THE IMPACT OF HIGH-QUALITY CODE

There are many rounds of testing with a Salesforce DevOps pipeline—or at least there should be. Failing to properly test your lines of code before they hit production leaves you open to costly errors and bugs that can result in data security vulnerabilities in your environment.

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

Maintaining a secure environment requires frequent upkeep. The ability to quickly produce reliable updates greatly expands the security capabilities of an organization.

> *"AutoRABIT's continuous integration and deployment capabilities have been impressive. It has streamlined our Salesforce deployment process, saving us significant time and effort when implementing new features*
>
> **- ELLA NANUTI,** F&I MANAGER, SPARTANBURG TOYOTA

03

Technical Debt

THE PROBLEM

Even though every DevOps team wants to create the most secure application or update possible, speed is still occasionally prioritized as the most important factor. And while we'll argue that quality doesn't need to come at the expense of speed, teams will still chalk up a few bugs as "the cost of doing business" with the goal of getting an update to market as soon as possible.

The idea is that these bugs will be addressed down the road, but there are a lot of problems with this line of thinking. First, these bugs can create data security vulnerabilities through misfires and back doors, which we discussed earlier. The second is that these errors become much more expensive to fix once they are released. And third, these bugs create a poor experience for the end user.

THE IMPACT OF HIGH-QUALITY CODE

Simply put, it's better to get it right the first time. This might sound so simple it's not worth saying, but DevOps teams continue wracking up technical debt with the idea that they'll get to the inevitable bugs later.

Manual code reviews are incredibly time consuming, especially for large updates and applications. But remember when we said you don't need to sacrifice quality for speed? This is where automation comes in.

Automated code review tools address the potential security vulnerabilities of technical debt in two ways. First, they expedite the process of finding and flagging coding errors early in the DevOps pipeline, long before they reach production and have the potential to create security vulnerabilities. And second, they can be used to locate existing technical debt within your Salesforce environment.

Cleaning up your environment can go a long way toward avoiding costly data exposures or outages.

04

No Reporting Insights

THE PROBLEM

When it comes to data security, information is king. There is absolutely no way to know you have a problem unless you have the data that shows it. Data security vulnerabilities aren't like a squeaky wheel—they're more like a wheel that has already fallen off.

Without access to actionable insights and reports, you aren't going to know if you have a data security vulnerability until it's already been exploited. And even then, security breaches can go on for months before they're noticed, compounding the negative consequences.

Many data security strategies include creating a disaster recovery plan, communicating best practices, and integrating security tools. While this is a great start to protecting your Salesforce data, it doesn't provide the comprehensive coverage you need to stay safe. Continuous upkeep and monitoring are also crucial.

THE IMPACT OF HIGH-QUALITY CODE

The same tools that enable your team to produce reliable, consistent code can also be used to track and manage the health of your Salesforce environment. Utilizing a code scanner to assess the health of your environment creates metrics and reports that can be used to assess the success of your DevOps efforts over time.

Failure rates for integrations, code quality assessments, technical debt scans, and other quality assessments are indicators of the stability of your environment.

High-quality code supports a successful data security strategy, and these types of metrics help assess the overall health of your Salesforce DevOps efforts. Use these insights to redirect your efforts to account for any deficiencies. Further streamlining your processes makes you more agile, flexible, and secure.

05

Error-Prone Manual Processes

THE PROBLEM

Unintentional errors are a major source of data security vulnerabilities, which come in many forms. We've mentioned how coding errors can result in misfires and how bugs in a live environment can create back doors for criminals. It's essential to maintain high-quality code to avoid this, but these aren't the only ways human error can negatively impact your data security efforts.

People get tired, especially when they are performing an incredibly repetitive task. Reviewing lines of code, for instance, becomes increasingly difficult and at a heightened risk of mistakes when there are thousands of lines of code in a single update.

But other areas of our Salesforce environments are also prone to data security vulnerabilities resulting from human error, such as team member permissions. Large organizations can find it difficult to maintain updated permission settings, overexposing data and increasing the potential for damaging errors.

THE IMPACT OF HIGH-QUALITY CODE

Automating manual processes reduces strain on your employees. This frees them up to focus on more pressing matters and other tasks that can't be automated. Your team members will enjoy a better work experience while you simultaneously strengthen your data security efforts by drastically reducing your capacity for damaging errors.

Automating these processes will also increase the reliability of the results. Accuracy is important, especially when it comes to quality testing for your code. Any reduction in the possibility of mistakes is a great way to improve your DevOps efforts.

Data security relies on a comprehensive approach. Using a code quality tool in conjunction with a data backup and recovery tool, for instance, provides the infrastructure your organization needs to reduce the chances of experiencing an outage while also covering your bases should the worst-case scenario occur.

06

Lack of Compliance Documentation

THE PROBLEM

Organizations in regulated industries have a higher standard for data security requirements. Not only are they responsible for protecting their clients' and customers' most sensitive information, but they are also subject to strict regulatory requirements. Failing to adhere to these requirements can result in stiff fines and penalties.

The ability to properly navigate a compliance audit streamlines the process while also ensuring that an organization has everything needed to prove adherence to regulations.

These metrics and reports can be difficult to compile if strict procedures are not maintained. And when it comes to gathering compliance information, manual processes leave an organization susceptible to the accidental omission of necessary documentation.

THE IMPACT OF HIGH-QUALITY CODE

The good news is that utilizing automated DevOps tools serves a dual purpose: it makes it easier to maintain proper levels of security to protect sensitive information while also compiling the necessary documentation to prove adherence.

Automated DevOps tools store information that can be repackaged for compliance audits, making it much easier to produce reports demonstrating adherence to stipulated standards.

Regulatory compliance and data security go hand in hand. High-quality code supports a strong environment that protects sensitive data with proper functionality. The available reports double this support with proof that everything is exactly where it needs to be.

> *"AutoRABIT has provided us with the capability to efficiently manage and tackle complex Salesforce development challenges."*
>
> **- DIEGO RIN MARTÍN,** HEAD OF TECHNOLOGY, SCALEFAST

CONCLUSION

Everything an organization does will touch security in one way or another. Every interaction with our Salesforce environment—including every customization, integration, and add-on—has the potential to introduce a data security vulnerability.

A strong DevOps pipeline is critical to maintaining the ability to address emerging issues in real time with security patches, updates, and new applications. However, if you can't guarantee strong code in every one of these releases, you could end up doing more damage than good.

A code quality tool is a non-negotiable aspect of a comprehensive DevSecOps toolset. Not only does it reduce errors, but it also speeds up the process of producing these critical updates.

Data security threats are always evolving. Organizations need to do everything possible to remain safe and compliant in the face of these emerging data security challenges—including the automation of critical processes.

ABOUT AUTORABIT

AutoRABIT is a DevSecOps suite for SaaS platforms that automates and accelerates the entire application development and release process. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. AutoRABIT tools help enterprises achieve higher release velocity and faster time to market.

AutoRABIT features static code analysis, automated metadata deployment, version control, advanced data loading, orgs and sandbox management, test automation, and reporting. Its services complement and extend Salesforce DX.

AutoRABIT Vault is a backup and recovery solution that streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and provides end-point data protection in the cloud.

CodeScan gives Salesforce developers and administrators full visibility into code health from the first line written through final deployment into production, along with automated checks of Salesforce policies.

FlowCenter helps Salesforce delivery teams achieve heightened release velocity and DevSecOps maturity goals with flow automation, DevOps metrics, and visualization tools that can't be found anywhere else.

Visit us at www.autorabit.com to learn more.

CERTIFIED
+ COMPLIANT

SOC 2 TYPE II CERTIFIED

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

ISO 27001 INFORMATION SECURITY CERTIFIED

HIPAA COMPLIANT