autorabit

The State of AI Security in Salesforce DevOps_

Navigating the emerging advancements and vulnerabilities of Salesforce artificial intelligence.

{/} codescan {for einstein GPT}

INTRODUCTION

Artificial intelligence (AI) is everywhere you look these days. Large Language Models (LLMs) and generative AI were initially a novelty to many, but almost immediately, they began to revolutionize the way companies operate.

Salesforce is no different. As a leader in the tech world, Salesforce made it a priority to not only enter the AI arms race but to revolutionize their platform with these exciting tools. This has led to the release of Einstein GPT and Data Cloud, both of which have garnered a lot of attention.

The rush to adopt AI in the workplace is as promising as it is misunderstood. It's tempting to focus on the possibilities of tomorrow without truly examining the implications of how these tools impact your Salesforce environment today.

Data security threats continue to expand. Organizations of all sizes in every industry are facing more complex and sophisticated attacks. Global instability has led to frequent attacks from nation-state cybersecurity threats. The introduction of new technology might seem like a great way to keep your platform safe, but the unknowns that come along with new software create gaps in coverage that could lead to data exposure and compliance failures.

This is a great time for a gut check on new AI software to better understand what it is and how it works, along with how it impacts your data security strategy.

We'll explore these critical considerations to get a comprehensive view on how AI impacts Salesforce data security:

01

Generative AI Is Already Here,

Whether We're Ready or Not

GENERATIVE AI IS ALREADY HERE, WHETHER WE'RE READY OR NOT

The swift rise of generative AI is reshaping the landscape of software development and Salesforce DevOps. With tools like ChatGPT, Microsoft Copilot, and a whole slew of tooling integrating into development environments, developers are already leveraging AI to write code, automate tasks, and enhance productivity.

Generative AI is transforming how developers approach coding. A substantial number of developers have begun to rely on AI tools to generate code, optimize existing codebase, and streamline development processes.

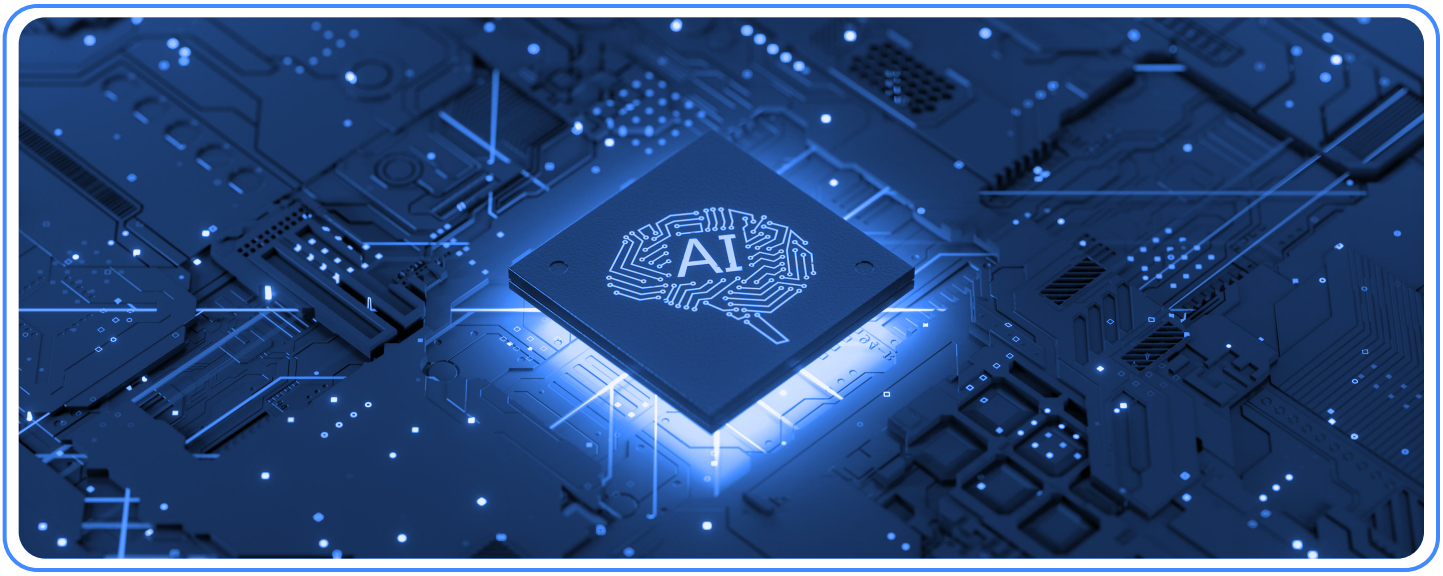
This integration promises to reduce development time and improve efficiency. According to recent surveys, nearly 52% of generative AI users have reported an increase in their usage of AI tools, showcasing the growing dependence on this technology.

Statistics and Real-World Usage

Widespread Adoption: Nearly half of developers have integrated AI tools into their workflow, with a significant portion using these tools daily. This trend underscores the necessity for robust oversight and governance in AI tool usage.

Unauthorized Usage: Surveys indicate approximately 40% of developers have used generative AI tools without formal approval from their organizations. This unregulated usage highlights the need for clear policies and training on the secure and compliant use of AI in development.

GENERATIVE AI IS ALREADY HERE, WHETHER WE'RE READY OR NOT



Future Implications for Salesforce DevOps

As the use of generative AI continues to expand, its impact on the Salesforce DevOps ecosystem will be profound. Here's what we can expect:

Increased Need for Code Review: The prevalence of AI-generated code necessitates rigorous static code analysis. Development teams must employ comprehensive scanning tools, like CodeScan, to identify and mitigate vulnerabilities introduced by AI. This step is crucial for maintaining code quality and security.

Enhanced Security Protocols: Organizations will need to develop stricter security protocols to manage AI-generated code. This includes sandboxing AI tools, restricting access, and ensuring all AI output undergoes a thorough review before deployment.

Evolving Compliance Frameworks: Regulatory bodies may introduce new compliance frameworks specifically addressing AI-generated content. Companies must stay ahead by implementing robust compliance checks and ensuring all AI-generated code aligns with industry standards.

Developer Training and Awareness: Continuous training for developers on the secure use of AI tools is essential. Educating developers about potential risks and best practices will mitigate unapproved AI usage and enhance your overall security posture.

02

What Is Einstein GPT?

WHAT IS EINSTEIN GPT?

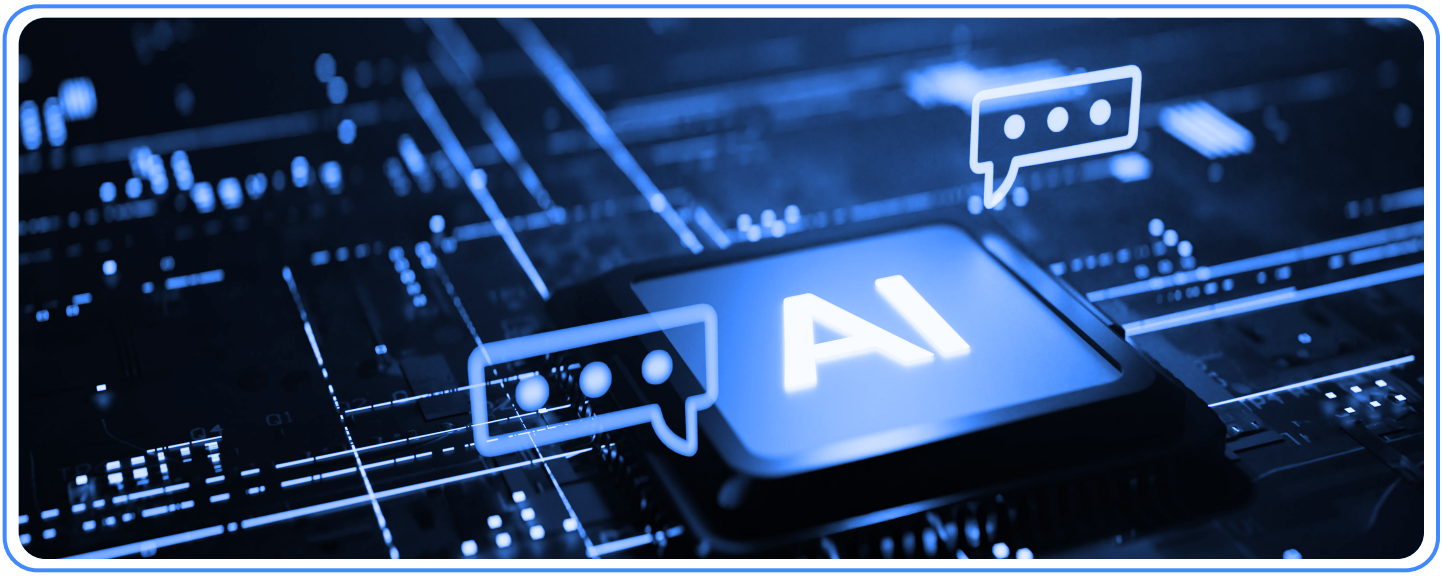
Einstein GPT refers to a suite of AI tools within Salesforce. It's built with OpenAI's ChatGPT and Salesforce's own AI models. It can also be combined with a user's own external AI models. This creates a highly adaptable interface that is continuously being updated with new data.

Users can enter prompts to engage with the software to create AI-generated content within their Salesforce environment. This can take the form of email copy, code, lead qualification, sales cycle summaries, and much more.

Einstein for Developers

Who says not knowing how to write code should stop you from being a developer? Einstein for Developers is a generative AI tool that produces code through prompts. It connects to your environment as a Visual Studio (VS) Code extension and relies on the information stored in the source models. Along with giving non-developers the ability to write code, it enables development teams to quickly generate lines of code.

Einstein for Developers is built right into your Salesforce environment. This gives it access to your metadata so it can use your existing code to make recommendations—which is great if you're particular about how your classes and triggers are written.



03

Expanding AI Into the CRM with Data Cloud and Einstein 1

EXPANDING AI INTO THE CRM WITH DATA CLOUD AND EINSTEIN 1

Salesforce's AI offerings cover the breadth of their platform. And since it was originally designed as a CRM, it's no surprise that a major aspect of their AI arsenal deals directly with managing system data.

CRMS are generally used for tracking marketing initiatives, sales data, and customer support information. However, businesses have a lot more kinds of data than that such as how users behave when working in the product, website metrics, payment information, and more. This information is usually disconnected from the types of data traditionally stored within a CRM.

Modern data collection, storage, and management are too complex for a standard CRM. This is where Salesforce Data Cloud comes in. It's a Customer Data Platform (CDP) that stores customer data throughout the entirety of the customer life cycle. This means that it holds data taken from a variety of sources, making the CDP the source of truth for an organization.

Salesforce Data Cloud unifies your system data while also making it more accessible and actionable. Data can be connected to your Salesforce through Amazon, Snowflake, Google, MuleSoft, and more. And when a representative needs to make an update or action item associated with an account, they can simply ask Einstein to perform the task.

Einstein 1

Mapping data across disparate systems is a complex process. Einstein 1 is the underlying platform that manages this, as well as numerous other functions. Every application is embedded with AI to assist team members with tasks like writing emails, developing code, and updating customer profiles.

Think of Einstein as a chatbot, but instead of simply responding to a question, it generates the type of material you need. It operates in the background of your Salesforce platform and is continually fed data from all connected applications.

04

Common Security Risks of Generative AI

COMMON SECURITY RISKS OF GENERATIVE AI

Generative AI tools like Einstein increase the speed at which you can produce code, but they're subject to errors.

Unreliable Results

The code produced by Einstein is based on what it has learned through its models, but there's no guarantee those models are correct. Internal coding and architectural standards guide your developers as they build new applications and updates. AI tools aren't going to follow these standards, making AI-generated code stand out from the rest of your coding updates.

There's simply no way around the fact that Einstein's coding models aren't 100% reliable.

Generative AI tools are built on public information, so if a pattern is recognized as the solution to a particular query, it's going to be used whenever prompted. But if that pattern contains data security vulnerabilities, anyone who uses a similar prompt will be open to the same attack.

Security and Compliance Concerns

This can lead to performance issues and security concerns. But for those working in regulated industries like finance or healthcare, it can also mean compliance failures.

Introducing generative AI to the world of software development is new and exciting. However, this also means there are a lot of unanswered questions. For instance, what happens to the prompts that are used to generate the code? Are they stored in a master repository? The same goes for the code that is produced—is it stored somewhere?

Proper storage and management of customer data is a critical consideration for both security and compliance. Any unknowns relating to this become liabilities.

05

The Importance of Static Code Analysis

THE IMPORTANCE OF STATIC CODE ANALYSIS

Coding errors are nothing new. Every development project has issues that need to be resolved. The good news is that there are powerful tools currently in the marketplace that have been perfected over the years to find and flag these errors as soon as they are entered into the system.

Development teams need to introduce a security-first workflow, verifying generated code. Static code analysis is a non-negotiable aspect of using generative AI tools like Einstein. Every line of code will need to be checked because of the unreliability of the results.

But Doesn't Salesforce Offer Security Tools?

Yes, it does. But those tools don't cover the breadth of security vulnerabilities that you need to remain secure in today's cybersecurity landscape.

Salesforce's answer to all of the questions in the previous section are contained in the Einstein GPT Trust Layer. Here's what it offers, according to Salesforce itself:

- SECURE DATA RETRIEVAL
- DYNAMIC GROUNDING
- DATA MASKING
- TOXICITY DETECTION
- AUDITING
- ZERO RETENTION

You might notice a gaping hole in this coverage: static code analysis. Salesforce offers a native solution called Code Analyzer, but it doesn't have enough coverage to ensure secure, compliant code. Moving forward with Salesforce's offerings requires an additional layer of security to ensure you aren't introducing vulnerabilities into your system.

06

Common Vulnerabilities

COMMON VULNERABILITIES

Code-scanning software repeatedly finds errors in AI-generated code.

These vulnerabilities were found after a scan of generated code:

XSS Attacks:
Cross-Site Scripting (XSS) occurs when an attacker injects browser-executable code within a single HTTP response.

Cross-Site Request Forgery:
An attacker tricks a user into making an unintentional request to the web server, which is then treated as an authentic request because the system doesn't have a mechanism to verify intentionality.

SOQL Injection:
User inputs are not properly validated before being used in an SOQL query, which exploits Salesforce vulnerabilities.

Potential Security Leakage:
Usernames, passwords, contact information, PII, and other sensitive data are stored in unsecured locations or are otherwise accessible by unauthorized individuals.

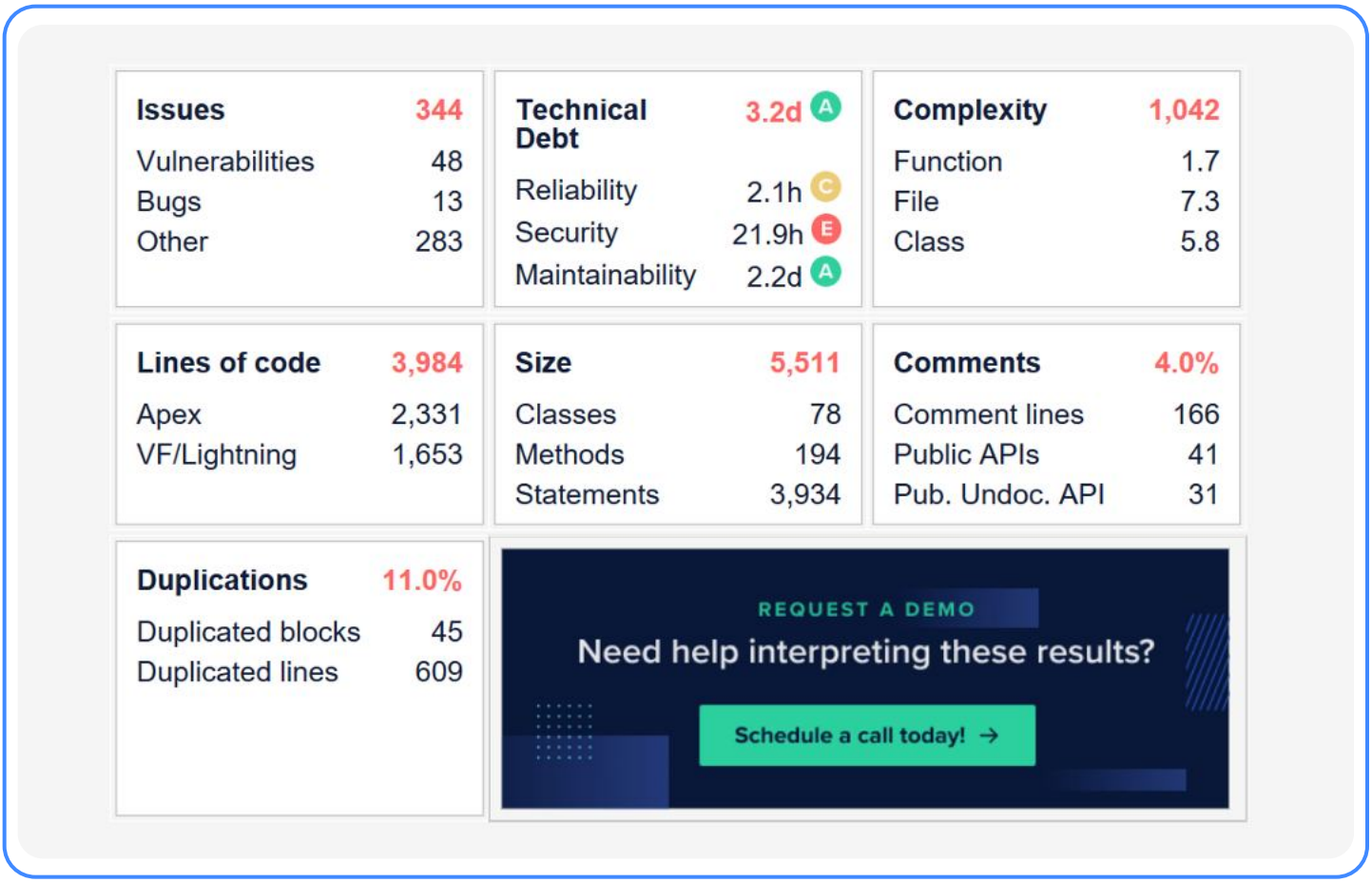
07

Real-World Examples

REAL-WORLD EXAMPLES

CodeScan is a static code analysis solution that has more than 3,100 rules—800 of them specific to Salesforce. And when put side by side with Salesforce's code analysis tool, it's easy to see why you need a third-party scanner to ensure safe, secure code.

Here is the summary of a quick scan run by CodeScan software on code created by Einstein GPT:



These violations are as severe as they are varied. Old APIs and numerous field-level security vulnerabilities could have harmful consequences if the mistakes aren't found and fixed before the update is deployed to a live environment.

REAL-WORLD EXAMPLES

Most violated rules	
API Version is too old	47
API Version is Too Old	36
Avoid Duplicate Literals	34
Field Level Security Vulnerabilities	27
@AuraEnabled should have Proper Error Handling	26

Most violated files	
classes/EinsteinVisionController.cls	30 B
classes/LightningSelfRegisterController.cls	13 B
classes/HandlerFindProperties.cls	13 B
classes/HandlerTravelApproval.cls	10 A
classes/PropertyController.cls	10 C

Most complex files	
pages/MyProfilePage.page	56
classes/EinsteinVisionController.cls	39
classes/LightningSelfRegisterController.cls	32
aura/selfRegister/selfRegister.cmp	27
aura/loginForm/loginForm.cmp	23

Most duplicated files	
pages/HeatMapMock.page	100
pages/HeatMap.page	99
classes/PostPriceChangeToSlack.cls	32
classes/SlackOpportunityPublisher.cls	32
pages/ForgotPasswordConfirm.page	31

08

Additional Security Safeguards

SUPPORTING A CULTURE OF SECURITY

The way development teams utilize AI tools like Einstein GPT has a huge impact on their ability to produce secure updates and applications. Here are seven things your Salesforce DevOps team can do to secure your environment while using AI:

Limit Access:
Control who has access to the AI model and restrict permissions to only those who need it.

Use Sandboxing:
Run the AI model in a sandbox environment to limit its access to system resources and prevent it from executing malicious code.

Update and Monitor Regularly:
Keep the AI model and its dependencies up-to-date with the latest security patches. Monitor usage and performance for any unusual activity that could indicate a security breach.

Review Generated Code:
Leverage a static code analysis tool to review code generated by the AI model before integrating it into your project.

Require User Authentication and Authorization:
Implement strong user authentication and authorization mechanisms to control access to the AI model and the code it generates.

Provide Ample Training:
Mandate security training to developers and users who interact with the AI model to raise awareness of potential security risks and best practices.

Consider Compliance:
Ensure usage of the AI model complies with relevant security standards and regulations.

CONCLUSION

Salesforce's AI offerings are an exciting look forward into what's possible with software and where we are headed in the near future. However, it's important to remember that these tools are new. Their imperfections are not yet fully understood. Treating these AI tools with extreme caution and care will give you the best chance at remaining secure as you implement them.

At the very least, run a static code analysis alongside any generative AI tools used to write code. Don't get suckered in by the promise of drastically increasing your output. Deploying a huge amount of code won't cover up the fact that it's riddled with bugs and errors.

A comprehensive approach to data security will plug any gaps you don't see in coverage. It doesn't take much for a hacker to exploit and gain access to your system. Similarly, a simple mistake by a team member has the potential to create huge vulnerabilities.

Compliance relies on consistent coverage. But even more than that, your customers rely on you to properly protect their sensitive information. Take your time with AI tools in Salesforce. Acquaint yourself with all their capabilities as well as their potential shortfalls.

Generative AI is exciting but dangerous if not fully understood. Take the time to know what you're getting yourself into and be sure to implement the proper tools. Total coverage of your Salesforce environment is critical to properly protecting it.

ABOUT AUTORABIT

CERTIFIED
+ COMPLIANT

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.

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

AutoRABIT ARM accelerates the delivery of business innovation with automated release management tools, including CI/CD automation, Data Loader Pro, and version control integration.

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.

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

SOC 2 TYPE II CERTIFIED

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

ISO 27001 INFORMATION SECURITY CERTIFIED

HIPAA COMPLIANT