DevSecOps

Flosum

CONTENTS

Introduction

Salesforce is one of the most widely used Customer Relationship Management (CRM) platforms in the world. As organizations continue to rely on Salesforce to manage their customer relationships, the need for secure and reliable applications on the platform has become vital.

The Salesforce platform spends millions of dollars on the iron-clad security of their platform. There is no doubt Salesforce is secure, but it is not their full responsibility to keep your data safe.

Salesforce keeps your data safe ON the cloud, but within the cloud, each organization has a responsibility to secure their processes and functions within their own organizational use of the platform – a concept Salesforce has dubbed “Shared-Responsibility”.

75% of CEOs will be held personally liable for security incidents by 2024.

Source: Gartner

Salesforce Users Require a Security Re-think

Due to the nature of Salesforce development, many security teams and Salesforce dev teams don't work closely together. Because of the siloed nature of Salesforce teams, organizations are faced with many security challenges regarding their DevOps process, including:

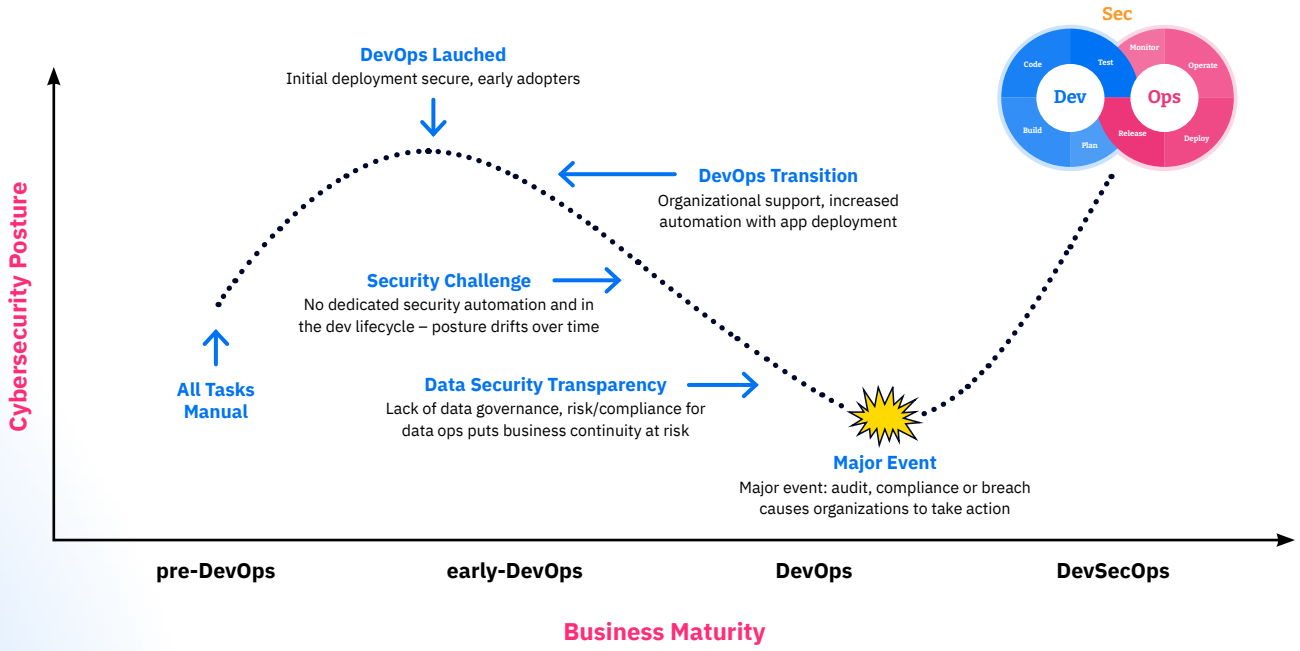
- Unquantified understanding of risk, exposure and coverage of security non-compliance/attack surface.
- Mean-Time-To-Fix security incidents takes weeks/months, with little trackability and auditing. Cost to remediate security incidents is high due to lack of automation.
- Lack of collaboration between Developers, Security and Compliance to resolve security incidents creates risk of cyberbreach and ransomware attack.
- Not meeting audit/compliance requirements around the software development lifecycle.

These unsolved challenges may go on for some time, but often result in exposure to risks that could jeopardize an organization's security posture – their data, applications, time, and ultimately – their bottom line. With any amount of these ongoing risks left unseen, a Salesforce team will eventually have a major security event that prompts them to incorporate security into their devops processes or shift left towards a zero trust security posture.

This major "Zero-Day" event typically leads to the emergence of Salesforce DevSecOps processes within that organization, a framework that integrates security practices into the entire application development lifecycle. But if a major event has already occurred, it's often too late.

In this eBook, we will provide guidance for application security/development managers who use Salesforce to embrace the concepts of DevSecOps and as they become the new norm for DevOps and Security teams, and evaluate the state of Salesforce DevSecOps in 2023 for Salesforce.

DevOps: Cybersecurity Challenge

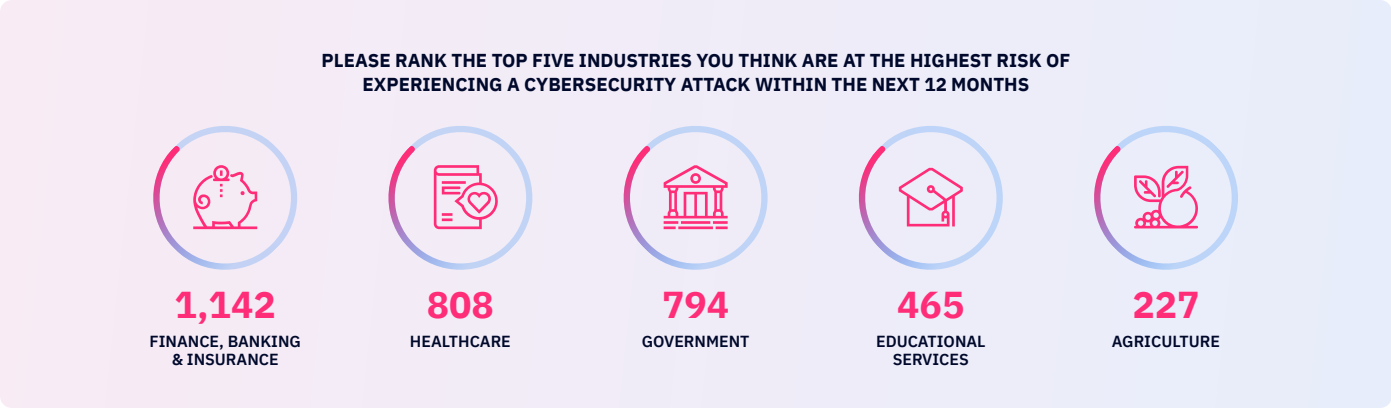


Chapter 1

Understanding Salesforce DevSecOps

Salesforce DevSecOps is a framework that integrates security practices into the application development process – the combination of development (Dev), security (Sec), and operations (Ops) practices that are designed to bake security into every step of the application development lifecycle. Security can no longer be an afterthought, but instead needs to be a core part of the development process and culture of an organization.

The key is to recognize the shortcomings of a traditional Salesforce DevOps process before a major event occurs, and protect against the cyber risk, human risk, application risk, operational risk and environmental risk inherently associated with developing applications. As the risk of cyberattacks grows, this concept is especially important for industries carrying sensitive data or information.



Source: Data Security Trends – Salesforce

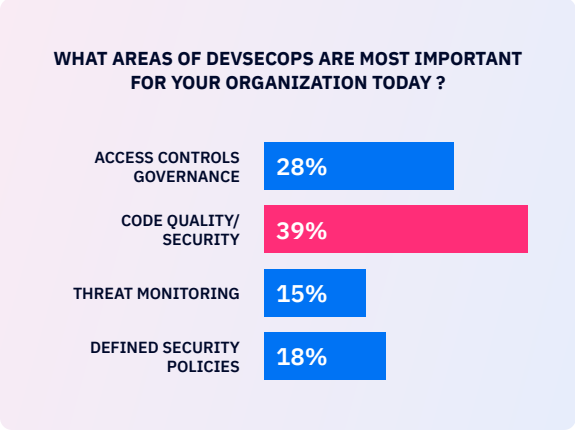
Chapter 2

The Benefits of Salesforce DevSecOps

Salesforce DevSecOps has several benefits for application security/development managers and teams. One of the primary benefits is that it ensures that security is built into the application development process from the ground up, helping to reduce the risk of security vulnerabilities and ensuring that the application is compliant with relevant regulations and standards.

Additionally, Salesforce DevSecOps can help to increase the speed of application development, as security testing and validation is integrated into the development process. So what do organizations care about?

A Flosum survey of both customers and prospects indicated that of these benefits, code quality and security is at the forefront of prioritization and one of the main benefits of a DevSecOps approach.



Source: Flosum Security Survey

Chapter 3

Best Practices for Salesforce DevSecOps

To ensure the success of Salesforce DevSecOps, there are several best practices that application development managers should follow. These include:

Adopting a culture of security and compliance

This means making security a priority throughout the entire organization, from the developers to the executive team, and align DevOps and Security teams to share important context on security issues and remediation. With a zero-trust philosophy gaining traction within many organizations, the key to success in maintaining this posture is each individual recognizing their own role in maintaining zero-trust.

Integrating security into the development process

This involves incorporating security testing and validation into every stage of the application development lifecycle, as well as frequent security scans throughout the process. This can be done with a tool such as the Flosum org security scanner:

> **DevOps teams are running more security scans than ever before: over half run SAST scans, 44% run DAST, and around 50% scan containers and dependencies.** *Source: Top Data Security Trends – Salesforce*

When you get down to the specific strategies incorporated into these best practices, organizations have been trying their hand at incorporating security into their DevOps approach and there are a few key actions that are working. The most effective features in an IT leader's security arsenal are data **encryption, identity and access management, and multifactor authentication**. These technologies provide strong protection against data breaches, unauthorized access, and other security threats that can compromise sensitive information. Budget for, and implement these strategies to ensure your organization's data remains secure and protected, even in the face of evolving security threats and cyberattacks.

Source: Top Data Security Trends – Salesforce

Leveraging the right tools

The right tools can help to streamline the development process and ensure that security practices are consistently applied. DevOps, data management, security and even training tools can make or break your security posture.

For example, data management or backup and recovery tools are key to preventing and recovering from a data loss event. Of those who experienced a data breach in 2021, the majority were unable to recover the lost data properly. With the right tools in place, you can be ready for – and avoid an event like this.

IF YOU EXPERIENCED A SECURITY BREACH IN 2021, WERE YOU ABLE TO RECOVER DATA LOST OR CORRUPTED DURING THE BREACH?

- **57%** **No** we were not able to recover any data.
- **30%** **Yes** we were able to partially recover some data.
- **8%** **Yes** we were able to fully recover data.
- **5%** **Unsure**

Simplifying compliance with regular security audits

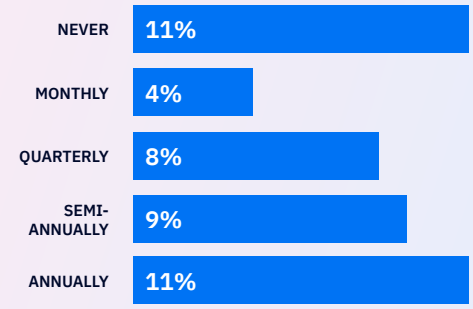
Regular security audits can help to identify vulnerabilities and ensure that the application remains compliant with relevant regulations and standards. A survey of the DevSecOps sector indicated that as of this past year, Salesforce audits are becoming a recurring necessity. While some teams are still lagging, we expect the number of organizations committing to, at minimum, annually recurring audits to increase until there are virtually no teams in the "Never" category.

According to Orca Security Advisor and Author of 1% Leadership, **Andy Ellis**:

> **Right now, CISOs and other leadership may not be fully aware of the size or prominence of teams developing on Salesforce which poses risk, especially in enterprise organizations.**

But awareness will skyrocket after a major security event occurs, and audits will become a requirement for more organizations. Right now, audits remain one of the best practices that allow organizations to stay ahead of a crippling major security event.

HOW OFTEN ARE SALESFORCE AUDITS PERFORMED BY YOUR SECURITY TEAM ON YOUR SALESFORCE INSTANCE?



Source: Flosum Security Survey

Chapter 4

Challenges Implementing Salesforce DevSecOps

While Salesforce DevSecOps has many benefits, there are challenges that organizations face when implementing this framework or complying with a zero trust security posture. One of the primary challenges is ensuring that the entire organization is committed to the culture of security and compliance. This requires buy-in from all stakeholders, including developers, executives, and end-users. Another challenge is integrating security into the development process without slowing down the development cycle. This requires a balance between speed and security.

Adoption challenges

- **40%** find that DevSecOps is expensive to implement. *Source: 30+ DevSecOps Statistics You Should Know in 2023*
- **39%** find they don't have sufficient time to implement DevSecOps.
- **38%** report a lack of education around DevSecOps.
- **36%** feel they haven't acquired adequate DevSecOps skills.
- **35%** agree that organizational inertia can be an issue when it comes to DevSecOps.

The main defenders against adoption challenges are training and process development. When your security tools are built into the process – and the team has a full understanding of how and why – adoption becomes much easier.

Start with a baseline of security training: Ensure that all employees involved in Salesforce software development, including developers, testers, and managers, receive baseline security training. This training should cover basic security concepts, such as the OWASP Top Ten, secure coding practices, and threat modeling.

Provide role-specific training: In addition to baseline training, provide role-specific training to employees. Developers should receive training on secure coding practices, testers should receive training on security testing, and managers should receive training on security risk management.

Lead by example: it's important for leaders to lead by example. Emphasize the importance of security and DevSecOps in all communications and ensure that leaders themselves are trained in security and DevSecOps best practices. To gain commitment from your team, you must show commitment yourself.

Incorporate security into the development process with tools: You can require built-in security process measures by utilizing features in DevSecOps-specific toolsets. These tools will prompt the incorporation of security requirements into the design phase or mandate security testing during the testing phase, guiding users to use security-conscious methods of development instead of leaving them to their own devices.

Challenges balancing release speed and security

- **73%** note that manual security and compliance processes slow down code releases.
- **60%** find DevSecOps technically challenging. *Source: 30+ DevSecOps Statistics You Should Know in 2023*

Use features within DevSecOps tools to automate secure processes such as regular security assessments. AI and automation will speed up your processes and combat any extra steps in the DevSecOps lifecycle so your team can remain efficient.

Focus on incorporating security practices early on in the development lifecycle, rather than later. The faster vulnerabilities can be identified and fixed, the more technical debt and time is saved. One way of implementing this is using security as code. When you implement new security configurations within your release management process, apply the same automation and version control processes to those as you do to your code – ensuring against costly mistakes in the configuration of your DevSecOps process.

Chapter 5

Future Trends in Salesforce DevSecOps

Looking to the future, there are several trends that are likely to impact the state of Salesforce DevSecOps. The increasing adoption of artificial intelligence (AI) and machine learning (ML) in security and compliance may enable more proactive threat detection and automated responses to security incidents.

We also see the growing importance of privacy and data protection, as regulations such as GDPR and CCPA continue to evolve and become more stringent.

Additionally, the ongoing shift towards cloud-native architectures and containerization may require new approaches to security and compliance, such as implementing security controls at the container level.

Finally, as the number of connected devices and applications continues to grow, the need for strong identity and access management (IAM) practices will become increasingly important, with technologies such as biometric authentication and zero-trust architectures gaining in popularity.

The exponential growth in the DevSecOps market hints at a future that will rely on more improved tools and processes that marry DevOps and Security and incorporate the above security trends into Salesforce DevOps processes.

One thing is certain...

If not yet, organizations will hit an unexpected bump in the road that prompts a security transformation of their Salesforce Development process. The question is, who will sit and wait for the inevitable?

And who will be prepared?

Regulatory non-compliance results in a fine of up to **4%** of a company's annual global revenues or **20 million euros** ($22.8 million) – whichever comes first.

IAPP-EY Annual Privacy Governance Report 2021