autorabit

Salesforce DevOps 2022 Industry Report

Insights + Viewpoints from DevOps Leaders

Looking Forward to 2022 by Looking Back at 2021

Salesforce DevOps is more of a mindset than a playbook. And as such, there are a variety of ways to approach DevOps. Learning from others in your industry—or from outside industries—can be a great way to consider techniques to address your DevOps needs that you might not have previously considered.

2021, much like 2020, saw an increased need for technological flexibility. New needs are constantly emerging from both consumers and team members. An optimized Salesforce DevOps pipeline has become an irreplaceable means of addressing these evolving needs.

But how do you know if you're doing everything you can to get the most from your Salesforce DevOps practices?

We set out to answer this question by analyzing how other experts in the field are approaching their Salesforce DevOps pipelines, what they think could be done better, and what role security plays in all of this.

27
Different Industries

Our Contributors

A wide breadth of viewpoints provides the best insight into the various DevOps approaches. The responses to our survey came from 27 different industries. This includes banking and other financial services, healthcare, consulting, insurance, and more.

Many of these industries are subject to data security regulations, which puts compliance and security measures at the forefront of their concerns.

A proper DevOps strategy is going to combine the efforts of multiple departments and varying levels of seniority. Our respondents cover the same variability of roles within their organizations.

Over half of the responses came from individual contributors, who are most likely to have hands-on experience with DevOps tools. The insight gained from first-hand knowledge is indispensable.

However, a macro view of the DevOps pipeline is also necessary to garner actionable insight. Managers, directors, VPs, and those even higher in their organization’s hierarchy responded to our survey as well.

The variety of industries and positions contained within this report provides a full view of Salesforce DevOps practices used throughout 2021.

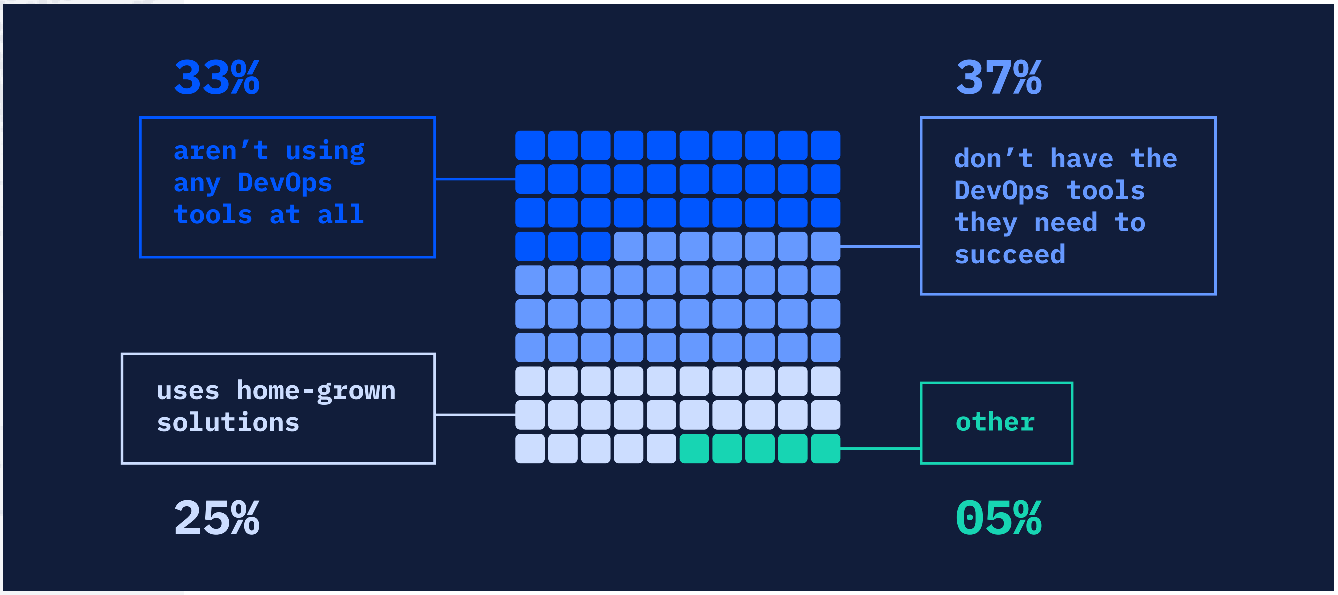
Summary

Salesforce DevOps requires continuous effort to refine and optimize your efforts. This demands constant attention to current successes and potential areas for improvement. We learned that DevOps tools are underutilized, particularly when it comes to automation.

Flexibility was essential throughout 2021, and this trend will continue as markets evolve in 2022. No matter your industry, you are facing unique challenges. A streamlined and reliable DevOps pipeline allows you to address these challenges in real-time and stay ahead of the competition.

However, speed must not be your only focus. Data security concerns grew increasingly dire over the course of 2021, and they don't show any sign of slowing down. It has become essential to introduce security considerations throughout your DevOps pipeline.

Our respondents are excited about the possibilities of an optimized Salesforce DevOps pipeline but cognizant of the challenges facing them. Taking the time to analyze your current methods and seeking improvements either through stronger planning sessions or the integration of automated tools sets team members up to produce secure and reliable applications and updates.



Attitudes on Current DevOps Processes

Analyzing the current state of Salesforce DevOps practices is the best way to find ways to improve your development pipeline. What works? What can be improved?

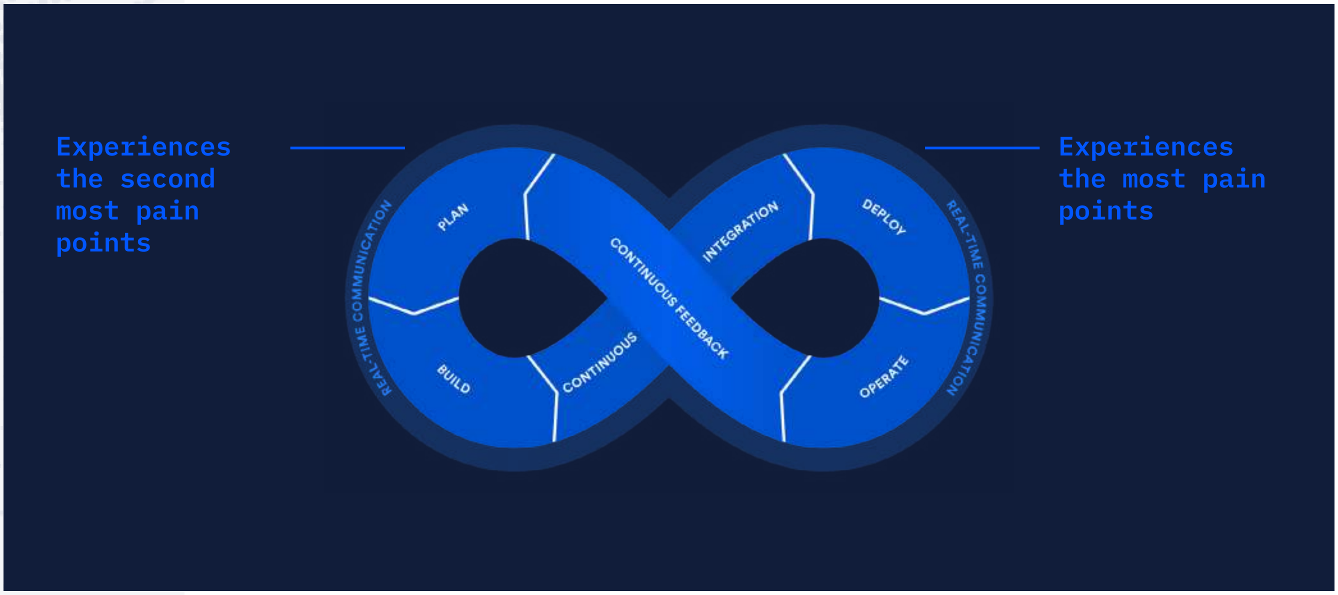
Surprisingly, when asked if DevOps tools are utilized in their development processes, the highest portion of responses came back "No."

Over 33% of respondents aren't using any DevOps tools at all. And 37% say they don't have the DevOps tools they need to succeed.

25% of participants say their company uses home-grown solutions. These metrics show an immediate opportunity for improving a DevOps pipeline simply by utilizing specialized tools that are proven to improve the efficiency and security of development processes.

This idea is solidified by an overwhelming 92% of respondents saying there is room for improvement in their DevOps efforts.

Collaboration between various departments is an integral aspect of a successful DevOps system. However, over 36% of respondents say collaboration between DevOps departments is not where it needs to be.



Experiences the second most pain points

Experiences the most pain points

DevOps Processes in Action

The way our team members view our DevOps processes can hint toward improvements that can be made throughout the next year. Analyzing the actual day-to-day habits of our DevOps pipelines will solidify these insights and direct our attention to concrete solutions.

68% of respondents report either not using DevOps tools to manage their Salesforce releases or being new to the practice.

Even the most skilled developers, testers, and data security teams can expedite and improve their output with the help of DevOps tools. Failing to implement these tools leaves current pain points unaddressed.

According to our findings, the stage of the DevOps cycle that experiences the most pain points is the deployment stage. A surprising finding was that the planning stage experiences the second most pain points.

Deployment and other DevOps processes can be greatly improved through the use of automation. However, 79% of respondents either aren’t using automation at all or have room for improvement in their development pipelines.

The State of DevOps Data Security

Data security threats continued to evolve and expand throughout 2021. A Salesforce DevOps pipeline needs to evolve along with these threats or it's susceptible to new threats and vulnerabilities.

Our study found that over 37% of respondents haven't updated their data security measures at all in 2021.

As a result of this, the average rating of confidence in security practices is 64 out of a possible 100. Multiple layers of protection are going to be needed in 2022 to increase this level of confidence in your team members.

The best way to find vulnerabilities and support your Salesforce environment is to routinely audit your system for risks. Over 22% of participants said their company performs these audits monthly, which is great.

However, 23% of respondents say they don't have a schedule for data security audits at all.

This is an alarming stat, especially considering that 25% of respondents reported experiencing a data loss and/or data breach within the last five years. And of those cases, 33% took more than three days to return to normal operations.

These outages can be extremely costly. Up to $11,600 can be lost every minute of downtime. This is why frequent data backups need to be a part of your 2022 DevOps strategy. However, 60% of respondents are leaving themselves open to data loss by not performing daily data backups.

37% of respondents haven’t updated their data security measures at all in 2021

23% of respondents say they don’t have a schedule for data security audits at all

60%

of respondents recognize regulatory compliance as a driving factor behind their organizations’ Salesforce data security policy

37%

of respondents say their organizations’ Salesforce data security protocols have room for improvement

Improving Data Security in 2022

Now that we understand the need for an increased insistence on data security, let's look deeper into our existing approaches to it.

60% of respondents recognize regulatory compliance as a driving factor behind their organizations' Salesforce data security policy.

But even for those that aren't subject to regulations, data security continues to be a major concern heading into 2022.

84% of respondents say their organizations' Salesforce data security protocols have room for improvement.

Improper usage of company software and overexposure of data were the two main security concerns of our respondents. Accidental deletions, spam/phishing, and team member awareness were also frequently mentioned.

These concerns point to necessary focuses for your data security team in 2022. Integrating these concerns throughout your DevOps pipeline (otherwise known as DevSecOps) greatly diminishes their potential for causing costly corruptions or breaches.

Data security issues seen in 2021 can be more successfully guarded against in 2022. Our respondents reported instances of ransomware/malware, cyberattacks, and phishing attacks on their systems throughout the previous year.

Preparing for the worst is always a best practice. Recognizing the threats facing your DevOps pipeline helps your team find ways to prevent them. Implementing automated tools avoids introducing bugs into your system that can be exploited by cybercriminals. And frequent audits and backups keep you covered even when something slips through your other lines of defense.

WHO WE ARE

autorabit

AutoRABIT is the only unified DevSecOps platform for Salesforce development. We automate and accelerate the entire application development and release process with an eye toward security. This enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides automated metadata deployment, version control, advanced data loading, orgs and sandbox management, test automation, and reporting. Our services complement and extend Salesforce DX. AutoRABIT Vault—our backup and recovery solution—streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery, and endpoint data protection on the cloud. CodeScan provides full visibility into code health from the first line written through final deployment into production.

VISIT US TODAY TO LEARN MORE

www.autorabit.com