EBOOK

How Healthcare Companies Can Optimize Salesforce DevSecOps

Maintaining Data Security + Increasing Release Velocity

INTRODUCTION

A quick and reliable Salesforce DevSecOps pipeline helps healthcare companies better serve their patients while remaining compliant with government regulations. The ability to introduce quality applications and system updates positions a company at the forefront of their industry. And when it comes to healthcare, patients gravitate toward those regarded as leaders.

So how does a healthcare company accomplish this?

There are so many aspects of a DevSecOps pipeline that it can be difficult to know where to begin. But with a little intentional attention, healthcare companies can put together the infrastructure needed to get the most from their Salesforce development efforts.

The healthcare industry has a higher need for smooth operations and quality tools. Not only is this dictated by market values and government regulations, it's also an imperative driven by the value of offered services. You owe it to your patients to ensure your systems are operating at the highest level of quality possible.

And an essential aspect of working toward this is to streamline the DevSecOps pipeline.

We'll explore how instituting these considerations will optimize Salesforce DevSecOps for healthcare companies:

1. Reporting + Analysis
2. Data Governance Framework
3. Automation
4. Threat Modeling
5. Reliable Backup & Recovery Solutions
6. Educate Team Members
7. Utilize a Singular Platform

01

Reporting + Analysis

THE PROBLEM

The first steps to begin an overhaul on your Salesforce environment can be confusing—where do you begin? What issues need to be first addressed? Which processes aren't operating smoothly, leading to wasted time and money?

Your Salesforce system contains a lot of information which will need to be analyzed. Compiling this information in a way that can be easily interpreted can seem time-consuming at best, and impossible at worst.

Access to this information can provide valuable insights into potential improvements:

- Success and failure rates for deployments
- System access and login records
- Company-wide permissions settings
- Time stamps for code changes
- Accountability measures

Manually compiling this information is simply not an option. So how can a healthcare company find this information and analyze it to inform the rest of the process?

THE SOLUTION

Automated reports can be put in place to provide the insights you need to improve your DevSecOps efforts. Matrix and summary reports, for example, can be compiled and exported to display various sets of data in a shareable and condensed fashion. These reports will simplify complex data and provide insight into areas that could use improvement.

Performance data is not the only type of information that can inform DevSecOps methods. A major aspect of DevSecOps is to incorporate security considerations throughout every aspect of the development process.

Access reports can be utilized to alert a healthcare company to any unauthorized access of their Salesforce system.

Sensitive data is common in healthcare networks. The ability to recognize security vulnerabilities before they are exploited by bad actors can be a major benefit.

02

Data Governance Framework

> *One of the best release management solutions out there in the market. Highly recommend it."*
>
> STELLA WAGNER

THE PROBLEM

Customer information, system data, vendor information, metadata—there are numerous types of data housed within a healthcare company's Salesforce environment. All of this data needs to be protected, both for regulatory compliance but also because it can provide benefits to a healthcare company.

An unorganized and unreliable set of data amounts to wasted potential and possibly even misguided plans.

How are you going to know what to protect if you don't know what you have? And how can you utilize the insights stored within your data if you can't find what you need?

We've discussed how well-organized reports can provide useful tips on advantageous paths to take. However, these reports aren't going to be reliable if the information that feeds them is disorganized and undependable.

THE SOLUTION

Data governance is a series of practices and principles aimed at maintaining a quality data pool within your Salesforce environment.

Strong data provides a variety of benefits:

- Improves reporting capabilities
- Helps inform automation deployment
- Provides oversight for corporate assets
- Improves efficiency in procurement
- Aids compliance by meeting legal requirements
- Provides insight for marketing efforts

Putting together a data governance plan takes a little time, but the benefits will carry your healthcare company into the future. Appoint a manager and leaders in various departments to direct the efforts. Establish a framework of operations—including clear definitions of each team member's responsibilities and metrics for the data elements.

Each data governance strategy should define the various sets of data, define process components such as managing and protecting data, and monitoring the processes for success.

03

Automation

THE PROBLEM

The process of developing applications and updates to help healthcare workers and assist patients can be time consuming. There needs to be a strict attention to quality and security, which is very detailed work. Failing to meet high standards can have very negative effects on patients and leave the healthcare company open to fines and penalties.

This has a large impact on the ROI of these development projects. A failure to streamline time spent and costs make the development process more expensive.

Human error is another factor that needs to be considered. Even the most detailed workers are bound to make an occasional mistake. This leads to failed deployments and the need for redundant work by your team members.

THE SOLUTION

The healthcare industry has grown more willing to utilize automation in a variety of settings, including the operating room. These types of automation provide precise and repeatable results.

Introducing automation into your DevSecOps pipeline offers many of the same benefits.

There are various tools that can be utilized to improve code quality, increase data security, and facilitate heightened release velocity.

Continuous integration and continuous delivery are two examples of how automation can streamline the DevSecOps pipeline. These solutions automate aspects of the software product development process—including automatically integrating code from multiple developers into a single release, and getting all types of changes into production.

Automation is the best way to streamline your DevSecOps operations as there are a variety of options, and all of them contribute to increasing the speed of production.

04

Threat Modeling

> *Fantastic tool, addresses every major pain point commonly encountered with multiple environments and development streams on Salesforce."*
>
> ERNESTO VALDES

THE PROBLEM

Data security necessitates a complete view of your Salesforce environment. There are a variety of ways cybercriminals can access your system data, and healthcare companies are among the top targets.

There are numerous ways your data can become otherwise compromised or lost. But there are also a lot of measures that can be taken to address these security concerns.

The problem is knowing where to start and what to consider. You can't guard against a threat if you don't know it exists.

Data security measures will vary between each Salesforce instance. Every company has their own unique considerations, structures, and vulnerabilities. What works for one company won't necessarily work for another.

So how do you put together a security plan that will support your DevSecOps pipeline and address your specific concerns?

THE SOLUTION

You want to find vulnerabilities in your applications and Salesforce system before cybercriminals. This gives you a chance to reduce the likelihood of experiencing an attack.

Threat modeling is the practice of recognizing potential threats to your system and prioritizing efforts to address them.

An effective DevSecOps approach inserts security considerations into every aspect of the development pipeline. Every tool and practice that can be used to accomplish this will work toward optimizing the Salesforce development queue.

Examine your system from the point of view of a cybercriminal. Look for weak spots and potential entry points. Speak with the various members of your team to get a well-rounded view of your system. These viewpoints can offer critical insight into areas you might not otherwise understand.

Take what you've found and arrange the potential vulnerabilities by severity. Put together a plan to address these issues and repeat the process periodically to ensure you are on top of emerging security threats.

05

Reliable Backup + Recovery Solutions

THE PROBLEM

Functionality within a Salesforce system can be dictated with metadata. This metadata will continue to grow over time and is relied upon by team members to properly fulfill their roles. Other system data such as metrics, reports, and customer information also build up over time.

All this data is essential to the proper operation of your Salesforce system. Losing access to this information can bring DevSecOps processes to a halt.

Team members will need to redo work that was already performed in the past to get the system back to its original state. This costs time and money. Every minute spent on redundant work is essentially a lost minute in terms of productivity. And healthcare companies simply don't have spare time to waste.

THE SOLUTION

Backing up this information ensures that operations can quickly resume after a data loss event. An optimized DevSecOps pipeline will have systems in place to protect itself against all threats.

Healthcare companies can't afford to go offline. Backup and recovery solutions help regain functionality to keep you in service of your patients and in compliance with regulations.

Backups can be automated so you don't have to worry about an outdated repository of information. However, backups are only one aspect of this solution—a powerful recovery tool must also be in place to repopulate the data fields within your DevSecOps pipeline.

> *" AutoRABIT has helped us add a lot of automation to our software development lifecycle. I highly recommend it! "*
>
> FOREST COOK

06

Educate Team Members

> *I work as a senior developer for my company and I had awesome experience using this tool. In particular, I liked the features related to easy commit, Dataloader pro and CI Jobs."*
>
> JETHA RAM

THE PROBLEM

Our team members can be our greatest asset, but they can also be a liability. Automation will streamline many of the aspects of a DevSecOps pipeline, but team members are still going to play irreplaceable roles in the process.

Improper practices from team members can create security vulnerabilities, threaten data pools, and produce unreliable coding structures that threaten the stability of the release.

The vast majority of issues created from improper practices of team members are accidental. Examples of malicious employees do exist, but other security measures such as reporting and permissions settings will help guard against them.

Simple mistakes through improper use of the system can have sizeable impacts on the success of your DevSecOps pipeline.

THE SOLUTION

Healthcare companies can't afford to suffer the consequences of these mistakes. The overall profitability of a development project can suffer, but even worse, it could impact the experience of a patient.

Open lines of communication, encouraging team members to ask questions when they are confused, and explaining best practices relating to specific roles will reduce the potential for costly mistakes.

DevSecOps involves the cooperation of a variety of teams to work toward a singular goal. This is only possible when everyone's on the same page and knows what to expect. Unifying everyone's approach through adherence to best practices and facilitating communication ensures there aren't any surprises.

07

Utilize a Singular Platform

THE PROBLEM

We've discussed how DevSecOps is the combination of a series of considerations. This will likely involve the usage of a variety of tools—such as Automated Release Management, CI/CD software, backup and recovery solutions, and more.

Piecing together numerous tools from different sources will increase complexity and create confusion amongst your team members.

Healthcare companies need to streamline their operations. This includes the processes involved with DevSecOps. Chasing down tools to integrate within your Salesforce environment will be time consuming and unlikely to create an intuitive interface for the members of your team.

THE SOLUTION

A singular platform that offers everything you need to optimize your DevSecOps efforts will provide the greatest returns. You can be certain the various aspects will work in conjunction with each other. You won't need to research each solution individually. And you won't have to chase down the account information for various vendors.

AutoRABIT's DevSecOps platform provides everything you need to create high quality, secure development projects at a higher velocity.

These solutions include:

- Automated Release Management
- Continuous Integration
- Continuous Deployment/Delivery
- Static Code Analysis
- Data Backup and Recovery

Optimizing a DevSecOps pipeline involves every possible effort to simplify the process without sacrificing speed and quality. The utilization of powerful tools is the best way to accomplish this.

But not all tools are created equal. And the way they work together will have as great an impact on your overall development efforts as the quality of the tools themselves. Securing a complete DevSecOps platform is the only way to be sure all of your efforts will support each other in the most beneficial way possible.

CONCLUSION

DevSecOps efforts exist on a spectrum—there are successful efforts and those that don't quite accomplish their goals. The good news is that no matter where you are on this spectrum, there are available tools and processes that can help you optimize these efforts.

Proper planning, automation, and utilizing a powerful platform like AutoRABIT provides the support you need to increase release velocity, improve code quality, and maintain data security.

Take some time and get a realistic view of how successful your Salesforce development processes really are. Are your team members making productive use of their time? Are there potential security vulnerabilities? Are you working with industry leaders to provide reliable DevSecOps tools?

Healthcare companies have a strong need for optimal performance in their software releases. A streamlined DevSecOps pipeline will provide the capabilities they need to better serve their patients while getting the best return on their efforts.

ABOUT

autorabit

AutoRABIT is a Continuous Delivery suite for SaaS platforms. We automate and accelerate 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. We help enterprises achieve higher release velocity and faster time-to-market.

AutoRABIT provides automated Metadata Deployment, Version Controlling, Advanced Data Loading, Orgs and Sandbox management, Test Automation, Static Code Analysis, 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 Cloud.

VISIT US TODAY TO LEARN MORE

www.autorabit.com

★★★★☆ G2 CROWD