



EBOOK

Under Attack: 7 Healthcare DevOps Threats (*and What to Do About Them*)

Keeping Your Salesforce Platform Secure and Compliant
in 2021 in the Face of New Challenges



INTRODUCTION

2021 has already introduced a series of unique challenges to the healthcare industry. The global pandemic has forced healthcare companies to adjust their daily operations, and institutions are being faced with overwhelming demand.

New technology, systems, and software are being used to address these needs. And this introduction of new services has created many vulnerabilities with the potential to be exploited by cybercriminals. Data security is a constant consideration, but the need for intentional practices is becoming even more crucial.

Regulatory compliance is another constant consideration for the healthcare industry. However, these changes have made it more difficult to keep up with the evolving regulatory requirements.

This ebook will outline 7 main security and compliance issues currently facing the healthcare industry, how to address them, and what you can expect to gain from doing so.

The healthcare industry is an essential aspect of a functioning society. Here's how you can keep your systems, data, and sensitive patient information secure in these trying times.

Increased Reliance on Virtual Services Increases Exposure



PROBLEM

Interactions between patients and healthcare companies changed drastically over the course of 2020. In fact, it's estimated that healthcare professionals are seeing 50-175 times more patients through telehealth than before the pandemic. And that's not just because more people are seeking medical help—46% of these patients are using telehealth to replace in-office visits.

Increased use of your virtual infrastructure creates more opportunities for cybercriminals to breach your system. A higher number of potential entry points requires a consistently high level of attention to security measures.

SOLUTION

Frequent system audits will help spot security vulnerabilities as they emerge. AutoRABIT affords the choice of hosting your Salesforce platform either in the cloud on your own servers. Hosting on-premises drastically reduces your exposure and helps keep sensitive information secure.

Task your development team with producing updates to your system's infrastructure to address any potential weak points in your current data security plan. Communicate a series of best practices to your team members and stress the importance of following them. Reserving access to healthcare systems exclusively for company-issued devices is a great way to remain in control of security measures.

BENEFITS

Hosting your Salesforce development sector apart from the Salesforce platform itself allows you to continue working even during outages. You'll never lose the ability to address any problems or monitor your essential functions and repositories of information.

“AutoRABIT is a rock-solid product for release management of Salesforce Applications. Helped us to reach our goal of continuous deployments from Dev to Prod.”

NAVEEN REDDY

Cyberattacks in the Healthcare Industry Are Expected to Grow



PROBLEM

The healthcare industry handles a lot of sensitive information. And unfortunately, this has made their systems a frequent target for cybercriminals. Cyberattacks on healthcare systems are expected to triple over the course of 2021.

73% of healthcare facilities admit to being unprepared to respond to cyberattacks. This is a potential disaster as the healthcare industry is four times as likely to be targeted by a cybercriminal than any other industry.

SOLUTION

Dedicated, updated, and comprehensive emergency recovery systems are essential to maintaining service when the worst-case scenario occurs. Frequent backups of your data and metadata—along with the ability to quickly and efficiently restore your data—are crucial to avoiding lost service time and redundant work as your team tries to get your system back to operations.

AutoRABIT's Vault Data Backup & Recovery service has everything you need to meet compliance requirements and keep your information secure. It's scalable to your particular needs and is trusted by leaders in a wide variety of industries.

BENEFITS

Cyberattacks threaten the stability of your system by damaging and corrupting important files. This information can be held for ransom, or perhaps simply stolen. Properly backing up your information and putting a system in place to restore it nullifies these threats.

Healthcare companies have more to consider than a bottom line, but finances are never out of the picture. Incomplete backups—or worse, no backups at all—lead to compliance penalties, lost services, and wasted labor hours.

Remote Team Members Create Unknown Security Risks



PROBLEM

The pandemic has led to many healthcare workers performing their duties remotely. Home systems are generally less secure and prone to cyberattacks. Unsecured internet connections, improperly updated hardware, and relaxed user practices create opportunities for cybercriminals.

Data security is important not only to protect patients, but to maintain functionality of healthcare platforms. Ransomware, data breaches, and distributed denial of service attacks can leave healthcare facilities unable to provide essential services.

SOLUTION

Uniform usage of a secure system with multiple levels of access control provides the best scenario to avoid unauthorized visitors to the backend of your system. Secure passwords, two-factor authentication, and awareness of phishing attempts will fortify your security barriers.

Utilizing a release management tool to manage user permissions will provide additional barriers between various sections of your platform even if a team member's account is compromised.

BENEFITS

Remote work is an essential tool to slow the spread of COVID-19. However, this policy inherently creates security issues. Being mindful of these issues and instituting intentional policies and tactics allows your team members the ability to safely work from home without compromising the integrity of your system as a whole.

“AutoRABIT helped us realize our release management goals. We also like their easy-commits feature where without additional tooling, our development team is able to check-in to GITHUB through AutoRABIT itself.”

CHAITANYA KADEM

Slow Deployment of Updates Leaves Your System Vulnerable



PROBLEM

Healthcare systems operate on a constant stream of updates and integrations of new software. These can be used to address newfound security gaps or other potential vulnerabilities.

A development cycle that isn't fully optimized will have trouble keeping up with the increased demand of the current climate, along with more stringent security needs. This can lead to insecure systems, faulty operations, and an overall lag in the company's development schedule.

SOLUTION

Automated Release Management is the best way to increase the speed of your deployments without sacrificing quality. It gives your company the ability to move development projects through quality and security checks without the need for human interaction on each micro level.

Move your data and metadata between different orgs or push it into production—automation helps facilitate productivity no matter where your project is in the DevOps cycle.

BENEFITS

Automation reduces your time to market by as much as 50%. This allows you to address ongoing and current issues by reinforcing your system with intentional updates and rollouts. Equipping your team with the necessary tools to create automated software lifecycles makes this process repeatable and streamlined.



“AutoRABIT has helped us quite a lot in automated rollback package preparation. It is working great and we are able to reduce our manual deployment efforts by more than 60%. ”

VINEET GUPTA

Limited Accountability Through Lack of Transparency



PROBLEM

The necessity of frequent updates means your development team will be expected to increase their output. Collaboration is an essential tool to properly accomplishing these goals. It can be difficult to track the movements of individuals when a variety of people are working on a singular release.

We don't like to think of our team members as threats to data security. The unfortunate fact is that 60% of data breaches come as a result of inside threats. And while many of these threats aren't inherently malicious, it's essential to know which team members have access to sensitive information throughout the development process.

SOLUTION

Set up recurring reports and monitor the employees that are accessing sensitive areas of your system. Permissions should be set so team members can't move into areas that don't directly impact their duties, and access logs will help you verify this.

Version Control offers the ability to allow developers to work on their specific lines of code without affecting the main code repository. Accidents are bound to happen, and automated security checks as these commits are moved into the main repository will keep these coding errors from compromising the functionality of the project.

BENEFITS

A tangible list of the people accessing sensitive information will help you hold bad actors accountable should something go wrong. This knowledge will also alert you to improperly set permission to avoid access issues before they happen.

Repeated mistakes are a learning opportunity for your team members. And if you notice someone frequently trying to commit bad code, you can help them learn from their mistakes to avoid vulnerabilities in the future.

Compliance Standards Continue to Evolve



PROBLEM

Compliance with government regulations is always a concern of the healthcare industry. However, the tendency toward online counseling and processing throughout 2020 and into 2021 has seen an increase in data breaches.

Every breach of patient, employee, and vendor data puts the healthcare company at risk for substantial penalties. Continued monitoring and maintenance of security measures and IT infrastructure is essential to adhering to these important regulations as they evolve throughout 2021.

SOLUTION

Stay apprised of the new HIPAA regulations in 2021. Changes to regulations can occasionally be difficult to keep up with, but it is essential to the continued operation of your institution. Adequate measures need to be taken to protect sensitive data and information.

Securing your Salesforce platform with a trusted provider will help account for compliance regulations when you don't have the time to do it yourself. AutoRABIT is the only SOC2, Type 2 compliant solution and the only HIPAA-certified solution in the market. We can help healthcare institutions secure their data and provide backup & recovery services.

BENEFITS

Keeping up to date with industry regulations means you aren't playing catch up. You can proactively instill new security measures and protocols to protect your data and stay on the right side of the law. Avoid penalties and retain the trust of your patients by properly securing their information.

“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

Privacy Is Difficult to Maintain, but Is as Important as Ever



PROBLEM

Increased internet usage—along with cloud computing—creates more potential entry points for cybercriminals to access your systems. The increased strain on the healthcare industry and the nature of the pandemic have pushed healthcare systems to utilize remote capabilities.

HIPAA stipulations remain in effect for the healthcare industry without regard to special circumstances. This means healthcare facilities need to increase their privacy and protection efforts to remain in compliance with regulatory stipulations.

SOLUTION

Hosting your Salesforce instance in the cloud provides a range of benefits for usability, but it can create security vulnerabilities. However, hosting with on-premises servers drastically heightens your ability to secure your network. AutoRABIT works with your company to host in the cloud if you prefer, or with on-premises servers.

Data masking personally identifiable information (PII) is an effective and low-touch tactic of heightening privacy measures. This adds another layer of protection to your patients' PII and helps keep your company compliant with industry regulations.

BENEFITS

Protecting the privacy of your healthcare clients is an essential aspect of many government regulations. Not only does putting protective measures in place keep you from violating these industry standards, it promotes trust in your brand. *A trustworthy healthcare provider is drastically more attractive to potential patients.*

“Fantastic tool, addresses every major pain point commonly encountered with multiple environments and development streams on Salesforce”

ERNESTO VALDES

CONCLUSION

The healthcare industry will face a variety of unique challenges over the course of 2021. The way in which we interact with each other will evolve as the pandemic reaches new milestones, and healthcare companies will need to adjust accordingly.

Security and compliance are a constant concern. The new technological and social landscape have made healthcare institutions a target for cybercriminals. Continued attention to security measures and adaptable systems—including the ability to quickly introduce new system updates and technology—will help these institutions fight back.

AutoRABIT has ample experience working with industry leaders to maintain compliant standards and practices. Visit us to learn more about how we can help those in the financial industry to backup and secure their Salesforce platforms and meet the year's challenges as they emerge.



**Ready to accelerate your
Salesforce Continuous Delivery
Journey with AutoRABIT?**

[CHECK US OUT](#)





ABOUT

autorabit

AutoRABIT, the Continuous Delivery suite for SaaS platforms, automates & accelerates entire application development and release process. It enables continuous integration and delivery by providing fast, simple, and secure end-to-end automation across all Salesforce implementations. It helps enterprises achieve higher release velocity (days instead of weeks/months), and faster time-to-market.

AutoRABIT provides automated Metadata Deployment, Version Controlling, Advanced Data Loading, Orgs and Sandbox management, Test Automation, and Reporting. It complements & extends Salesforce DX. ARVault, AutoRABIT's backup and recovery solution, streamlines Salesforce data, simplifies data backup challenges, offers disaster recovery and endpoint data protection on Cloud.

CONTACT US AT

info@autorabit.com