EBOOK

Banks In the Crosshairs

6 Tips for Securing Your DevOps Strategy

INTRODUCTION

Every year, the financial services industry is among the most highly targeted by cybercriminals. This is due to the incredibly sensitive nature of the data stored within their IT systems.

According to the International Monetary Fund, “The financial sector has suffered more than 20,000 cyberattacks, causing $12 billion in losses, over the past 20 years.”

This has led to a dramatic increase in security spending, but sourcing the best data security tools doesn’t guarantee the safety of your customers’ personal data. The way your team interacts with this data has a massive impact on the success of your data security strategy. You can have the best tools in the world, but they won’t help secure your data if the people using them aren’t employing safe habits.

Homogenizing your team’s approach around proven, secure habits creates a company culture that is much more conducive to protecting sensitive data. And when it comes to financial institutions and the level of sensitivity associated with their data, every possible way to increase security needs to be addressed.

Here are six best practices banks need to adopt to maintain a secure and reliable Salesforce DevOps strategy:

01

Lock Down Permissions and Access

LOCK DOWN PERMISSIONS AND ACCESS

It’s important to know who can access sensitive data. Personal identifiable information (PII) and financial data are valuable on the black market. Customers whose data is exposed face a variety of negative consequences—and the institution responsible for an exposure is liable to face repercussions as well.

You can’t protect your data if you don’t know who can interact with it. The potential for security failures increases with every additional person who can access sensitive data. Cybercrime is always a threat in this circumstance, but even an innocent mistake can lead to data exposures.

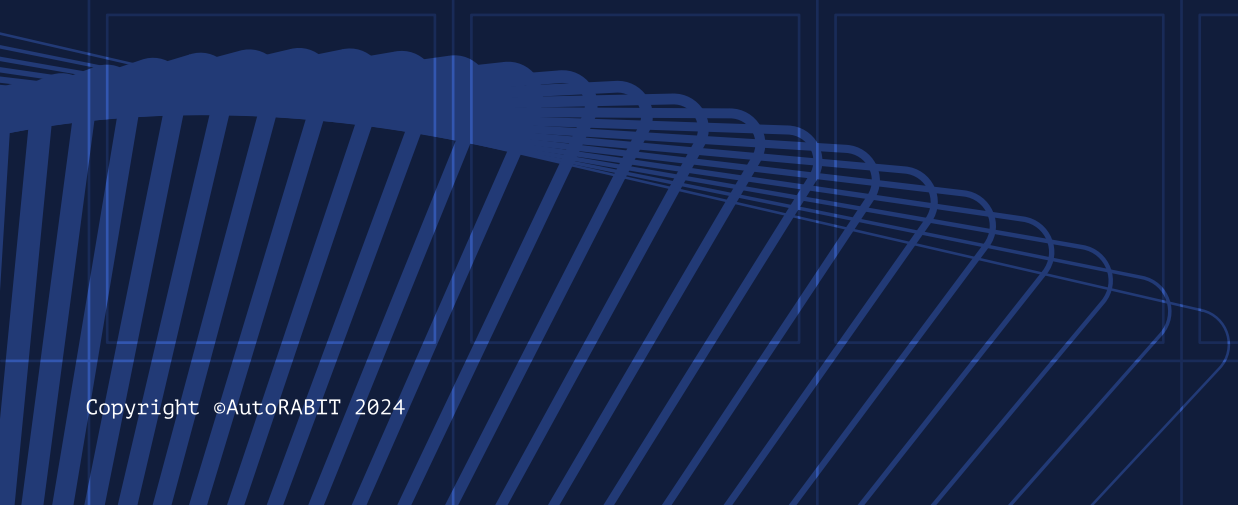
What Can You Do?

First, lock down your platform from external threats. Multifactor authentication should be implemented at every login screen to ensure your platform is only accessible by team members. The second layer of protection occurs inside your system. The principle of least privilege should be leveraged to reduce the number of people with access to sensitive information. Only those who need access to perform their job duties should have permission to interact with sensitive data sets.

An automated scanner can be used to ensure these settings are established and maintained. Every additional layer of protection reinforces your impenetrability and makes it less likely your system will experience an exposure.

02

Analyze Security of Third-Party Applications



ANALYZE SECURITY OF THIRD-PARTY APPLICATIONS

Many financial organizations integrate third-party applications to expand the capabilities of their Salesforce environments. And while this opens up the potential for new services and processes, it also increases their attack surface.

For example, a ransomware attack on a cloud IT service provider in 2023 caused outages across 60 credit unions in the U.S.

More than 57,000 Bank of America customers had their data exposed in November 2023 when an authorized party access their data through Infosys McCamish, a financial software provider.

The emergence of artificial intelligence will only increase banks' reliance on third-party applications. This technology is still new. The data security implications of AI aren't completely understood, so it's important to instill security processes now before it's too late.

What Can You Do?

When considering a new application, banks should screen the vendor and perform a risk assessment. Has this vendor experienced security issues in the past? Do they have proper measures in place to secure their platform? Is the vendor compliant with applicable data security regulations? Considerations like proper access controls and encryption are critical.

Institute continuous monitoring practices specific to your third-party applications. The points of connection between your platform and theirs need to be analyzed for unauthorized access or potential weaknesses.

Incident response protocols need to be established and maintained—both on the vendor side as well as on the bank's side. These protocols need to be aligned to minimize downtime should an outage occur.

03

Automate as Much as Possible

AUTOMATE AS MUCH AS POSSIBLE

Protecting sensitive financial and customer data requires a flawless approach to data handling. Manual processes are notoriously inefficient compared to automated processes, which never tire and don't lose focus on long, repetitive projects. A simple mistake can have drastic ramifications for customers, which can then create problems for the bank itself.

When it comes to manually approaching highly repetitive processes such as data entry and code reviews, human errors are increasingly likely to have negative impacts.

Consistency is key to managing data, and manual processes often lack uniformity. Large teams working on a single project are likely to follow disparate procedures for security considerations, compliance checks, and managing data.

These inefficiencies compile over time to diminish the returns a bank sees on their DevOps products.

What Can You Do?

Automated Salesforce DevSecOps tools increase release velocity, heighten security, and maximize productivity. The trick for banks is to source a suite of tools that are tailored specifically to the heightened needs of the financial industry.

- **Static code analysis** removes the burden of lengthy code reviews so developers can focus on more complex tasks.
- **Data backup snapshots** can be captured multiple times each day to adhere to data protection regulations and expedite seamless recoveries after an outage.
- **CI/CD tools** further automate critical testing and integration processes to eliminate manual errors and reduce time to market.
- **Policy scanning** ensures adherence to internal best practices and external requirements for proper data handling.

These automated tools give DevOps teams the support they need to consistently produce reliable, secure applications and updates without lengthy testing and review processes. The reduction in errors creates a more stable environment that further protects sensitive financial data.

04

Monitor and Audit Your Environments

MONITOR AND AUDIT YOUR ENVIRONMENTS

You can't fix a problem if you don't know it exists. IBM reports it can take about 197 days for companies to even realize they have an active data breach. And on average, these breaches cost $3.86 million.

The cost and degree of impact a breach will have depend entirely on how long it is active. Shoring up vulnerabilities before a breach occurs is obviously preferred, but quickly addressing an active breach also needs to be a priority.

With so many potential entry points for a bad actor, it can seem impossible to keep an eye on every corner of your IT platform. However, banks that fail to do this open themselves up to data exposures that put their customers' data and their own compliance at risk.

What Can You Do?

Regular security reviews and audits are critical for maintaining proper oversight that enables your team to keep sensitive data safe. This can be accomplished with the help of automation such as a security posture management tool.

Real-time alerting can be set up to flag any unusual behavior such as unauthorized access, empowering your team to respond quickly to any potential breaches. Deploy automated audit trails to log and review every change in the system, from code deployments to user access adjustments. This type of reporting is crucial for maintaining proper oversight, but it will also come in handy in the event of a regulatory audit.

Continuous monitoring is the only way to know your data is safe. When it comes to financial information, constant verification of secure practices is essential.

05

Provide Continuous Training to Team Members

PROVIDE CONTINUOUS TRAINING TO TEAM MEMBERS

Automating critical processes will offer the capability to produce more secure and reliable products, but without proper knowledge and habits, your team members can introduce new and unchecked data security vulnerabilities.

Insufficient training significantly undermines data security and leaves banks open to data exposures. Up-to-date knowledge and intelligent experience with DevSecOps tools help teams avoid costly errors that threaten sensitive data.

Cyberthreats are always evolving. A bank's approach to securing financial and personal data needs to be similarly fluid. Frequent, updated training provides the contemporary insights needed to navigate these threats and stay one step ahead of cybercriminals.

What Can You Do?

Ongoing training programs that cover both technical skills and security best practices should be established for all team members. These should be informed by threat assessments and analyses of recent cybersecurity events.

Training materials provided to team members should be updated regularly to reflect new software, regulations, and threats facing the financial sector. Security drills that simulate data security breaches should be held to give your team practice for responding to security events.

Banks are subject to stringent data security regulations. Your team should be trained on these regulations and have documentation on-hand so they are never confused about how to maintain compliance habits.

Continuous training helps banks ensure every team member stays current on the latest best practices and reduces the risk of security breaches, data loss, and falling out of compliance with applicable regulations.

06

Keep Systems Up to Date

KEEP SYSTEMS UP TO DATE

Your IT platform is not something you can set up once and never think about again. Software continually introduces new patches and updates that need to be maintained to withstand evolving threats.

As systems age, cybercriminals learn about vulnerabilities inherent in the software. This opens your network up to unauthorized access, malware injections, or even stolen data.

Encryption tools, for example—while critical for banks to maintain proper levels of security and compliance—are tailored to address contemporary data security measures. These protections can also become out of date and fail to offer the level of security banks need.

What Can You Do?

Automated patch management tools ensure all systems, software, and dependencies are updated as soon as new versions are available.

Regular reviews of third-party dependencies are critical to ensure they are up to date and still supported by other connected vendors. These connection points frequently become data security vulnerabilities when they aren't properly maintained. Similarly, outdated systems and components can introduce security risks, but these vulnerabilities can be flagged and fixed through scheduling repeated security assessments.

Monitoring tools are critical to tracking system performance and detecting security issues that might be caused by outdated software. Analyze dashboards and reports compiled by these tools to find areas that are underperforming and check for updates to any software connected to problem areas.

By keeping systems up to date, banks can significantly reduce the risk of data security issues and the negative consequences that come along with them.

CONCLUSION

Financial organizations face steep data security challenges, which can be met with a comprehensive approach. Sourcing a holistic DevSecOps platform will go a long way toward protecting sensitive data and maintaining compliance with data security regulations, but the way your team interacts with your data will be the deciding factor between costly exposures and a secure IT environment.

A streamlined application delivery lifecycle enables banks to be flexible in their response to emerging data security issues. A fast release cycle enables real-time responses. Multiple layers of testing create reliable updates and applications that won't introduce vulnerabilities of their own through misfires.

Automated tools take critical, yet repetitive, processes out of your team's hands so they can focus on more complex tasks. At the same time, automation increases consistency, minimizing the risk of bugs and errors in live environments.

Banks handle their customers' most sensitive information. It is their responsibility to protect this data as vigorously as possible. This can be accomplished through a combination of adherence to best practices and a suite of powerful, automated DevSecOps tools.

ABOUT AUTORABIT

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.

CERTIFIED
+ COMPLIANT

SOC 2 TYPE II CERTIFIED

CALIFORNIA CONSUMER PRIVACY ACT

GDPR

ISO 27001 INFORMATION SECURITY CERTIFIED

HIPAA COMPLIANT