GETTING DEVSECOPS RIGHT
IN FINANCIAL SERVICES

INTRODUCTION

Financial services institutions, including banks, investment firms and insurance companies, face intense pressure to continually strengthen their cyber security and boost the speed of their software releases. At first glance, these two goals seem at odds with each other. However, a way exists for financial services companies to harmonize and accomplish these seemingly conflicting objectives: DevSecOps.

DevSecOps is the end-to-end collaboration of development, security and operations teams throughout the SDLC (software development lifecycle) and the automation of their tasks, resulting in the frequent and secure release of the software that powers digital business -- mobile apps, web services, APIs, IoT networks and more.

In this ebook, we'll explain:

- The main challenges financial services providers face when trying to improve the security and agility of their SDLC
- How DevSecOps protects these companies' digital business and gives them a competitive edge
- Why binary management is key for a DevSecOps strategy, and the **software bill of materials (SBOM)'s** critical role in understanding the composition of your binaries

FINANCIAL SECTOR CHALLENGES

While businesses across all vertical industries strive to boost their software pipelines' speed and security, financial services companies face challenges that are unique or more pronounced.

A favorite industry for cyber crooks

The treasure trove of personal and financial data handled by banks and other financial services companies makes them a primary target for cyber criminals. Breaching a bank can get hackers access to invaluable confidential data about individual and commercial customers, bank processes, financial records, and more. Consequently, these institutions are under intense and constant attack on all fronts and with all methods, including the latest and most sophisticated.

At any particular moment, a bank could be the target of DDoS (distributed denial of service) attacks, ransomware strikes, phishing campaigns, zero-day vulnerability exploits, advanced persistent threats (APTs), malware infections, man-in-the middle hacks, cross-site scripting, IoT compromises and **supply chain breaches**.

Heavy regulatory burden

Financial services is one of the most regulated industries, subject to a vast and complicated array of industry mandates and government rules throughout the world. Clearly, it's a burden on DevOps teams having to ensure that all software they release to employees, customers and partners complies with a huge and growing number of complex and often confusing regulations in all the countries and regions their companies do business in. Failure to comply can result in heavy fines, legal liability, reputation harm and lost business.

Here's just a sampling:

- **Strong Customer Authentication (SCA)**, a European regulation that requires finance apps to have at least two forms of user authentication
- **Payment Card Industry Data Security Standard (PCI DSS)**, a global industry standard for protecting the collection, storage, processing and transmission of cardholder data

- Markets in Financial Instruments Directive (MiFID), a European regulation intended to protect investors
- Revised Payment Services Directive (PSD2), a European regulation that aims to improve the security and transparency of electronic payments
- Sarbanes-Oxley Act, a U.S. federal law designed to deter and punish corporate and accounting fraud and corruption, and protect workers and shareholders
- Dodd-Frank Act, a U.S. federal law that tightened regulations across the financial services industry to promote stability and oversight of the U.S. financial system
- General Data Protection Regulation (GDPR), a European regulation not specific to the financial industry whose goal is to protect the privacy and personal data of EU residents
- White House Executive Order on Improving the Nation's Cybersecurity, which isn't specific to financial firms, seeks to boost prevention and remediation of cyber incidents impacting the U.S. government and the U.S. private sector

Highly restrictive digital environment

More than in other industries, IT infrastructures in the financial services sector are characterized by severe restrictions that hamper agility, including: air-gapped systems; heightened access control; minimal cross-team collaboration; slow change management and approvals; rigorous auditing and governance; and limited flexibility for developers.

Compounding matters is the fact that IT infrastructures in this sector tend to be complex, large and heterogeneous, ranging from conventional, on-premises data centers to modern hybrid cloud deployments featuring microservices architectures and containers. They must also support broad and varied endpoints, such as smartphones, ATMs and POS terminals.

Pressure from technology disruptions

Financial sector companies feel constant pressure to keep pace with the dizzying technological innovation in their industry, and remain competitive against both disruptive startups and established players. Recent "fintech" advances include robo-advising, digital-only banks, cryptocurrency, blockchain, AI-based service

customization, and P2P transactions.

This means that financial services companies must release new and updated software frequently in order to continually enhance their digital services. This is a pace of change that these companies historically avoided -- as recently as a decade ago -- precisely because it increases the risk of deploying software that contains vulnerabilities, misconfigurations or other security and compliance gaps.

Intensifying customer demands

Customer expectations continue to climb with regards to the digital experience from their financial services providers. Customers want the convenience of banking, stock trading, making payments, managing retirement accounts and more via digital channels using their mobile phones, PCs, and tablets. They expect these service offerings to be increasingly personalized, feature-rich, fast and always available -- and, obviously, they expect all digital transactions to be secure.

Thanks to the digitization of financial services, it's easier than ever for customers to change banks and other providers, which adds to the urgency of these companies to continually improve their customer digital experience.

DEVSECOPS PROTECTS AND ACCELERATES YOUR SDLC

How do you address these challenges? How do you retain your software release velocity and innovation without sacrificing security? Whether your IT environment is on premises, in the cloud, or both, the focus should be on making sure your SDLC processes are not only nimble but also safe, and DevSecOps makes that possible.

With the people, process and technology changes that DevSecOps adoption brings, **financial services institutions** can:

- Establish a culture of open communication, collaboration and shared accountability among all teams and stakeholders involved in the SDLC -- primarily development, operations and security, but also QA/testing, business leaders, GRC and upper management

- Increase the speed and agility of their SDLC by automating tasks, including as many security and compliance checks as possible, and natively build them into every step, starting with the design phase, so that issues are detected and fixed early and often

- Granularly manage and trace their software binaries across the SDLC, so if they're found to contain a severe vulnerability or compliance issue, you can see where they're used, understand their "blast radius" scope of impact, and quickly remediate the problem

- Validate the authenticity of every artifact generated through their SDLC, so developers and operators can ensure builds created by a pipeline don't contain compromised artifacts

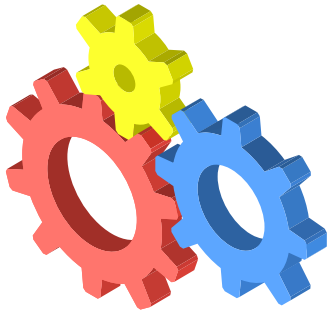
BINARY MANAGEMENT AT THE HEART OF DEVSECOPS

As soon as source code is compiled into binaries during the build phase, binaries become the primary assets in the DevOps pipeline, because they are the **single source of truth** for what developers build, test, promote and release into production. For this reason, managing the flow of binaries is key for ensuring the integrity and reproducibility of a software build, and consequently the quality and safety of an application.

The core piece needed for achieving fast and secure software releases is an end-to-end, extensible **DevOps platform** anchored by a repository manager that handles all types of software packages. This platform should be easy to integrate with all your third-party DevOps tools via REST APIs, and should include components for security scanning, distribution and monitoring of software in production.

The platform's repository should store and uniquely identify all binaries, whether they came from outside the organization or were built in-house. This provides a single source of truth that a financial services company can use to match potential threats, and write rules and policies accordingly to trigger specific actions against those binaries, including:

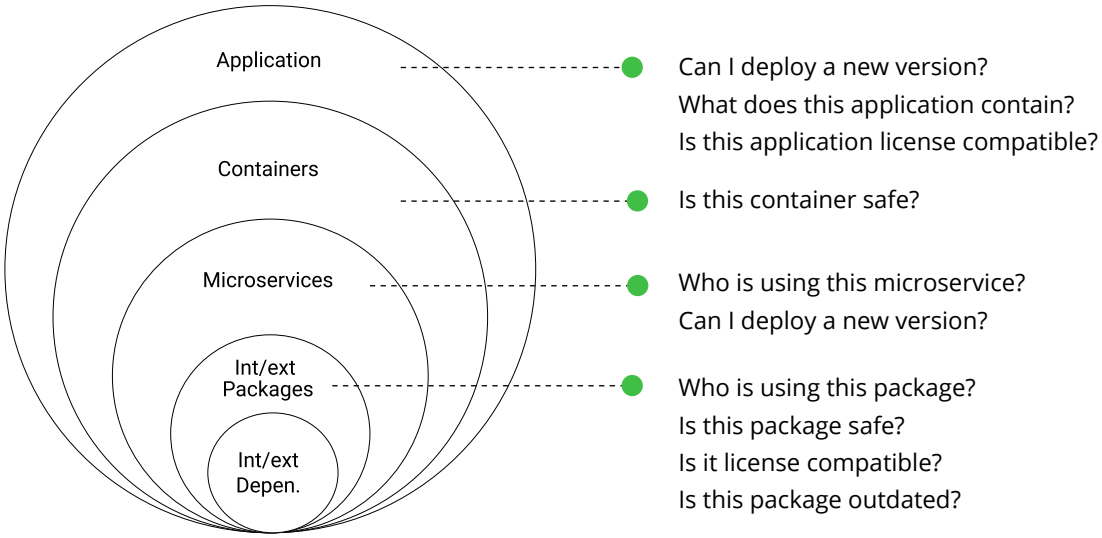
- Blocking their consumption
- Flagging them
- Adding new metadata to them
- Initiating a secondary process
- Notifying appropriate team members



An important feature for DevOps teams in the financial sector is **support for air-gapped environments** -- meaning those that don't have a connection to the internet. Normally, development organizations access remote public resources such as Docker Hub to download dependencies for builds. However, financial institutions often have stricter security requirements in which they can't expose their operations to the internet, so having a DevOps platform that supports this air-gap scenario is essential.

Financial services companies also need deep, detailed visibility into their binaries, including their third-party transitive dependencies, and in particular open source components, which often make up 90%-plus of an application's code base -- APIs, libraries, base OSes and more.

To understand the composition of your binaries, your DevOps platform should generate a **software bill of materials (SBOM)** for all the software you release, distribute and deploy. An SBOM contains a list of all the "ingredients" that make up a piece of software, including libraries and modules -- whether they are open source or proprietary -- as well as information about the development tools and CI environment used during the build process.

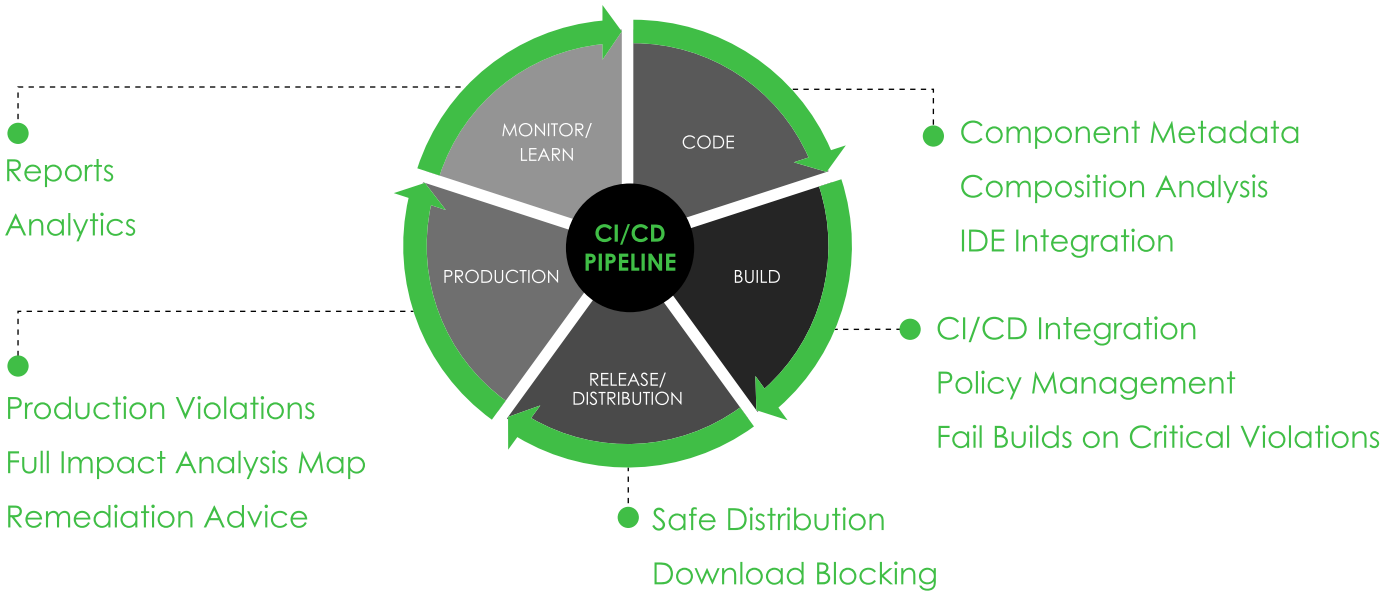


The SBOM can also outline when the software was built, what SDLC stages it went through -- dev, QA, staging, production -- and what **security and compliance** issues have been detected and fixed.

This information boosts DevSecOps efforts and helps maintain security and compliance in a variety of use cases. For example, an SBOM details all the upstream components being used in an application, and in its various versions. That way, when a vulnerability that affects the application is disclosed, it's easy to detect which versions are impacted and how.

The platform should also continuously scan all software components to detect and remediate vulnerabilities, license compliance issues and other problems, across the SDLC phases:

- Code, including capturing component metadata, performing composition analysis, and integrating with the organization's IDE (integrated development environment)
- Build, including integrating with the CI/CD system, conducting policy management, and failing builds with critical violations
- Release / Distribution, including ensuring safe software distribution and blocking of downloads
- Production, including detecting production violations, creating of a full impact-analysis map, and offering remediation advice
- Monitor, including creating reports and generating analytics



In summary, an **end-to-end DevOps platform** with native security and compliance capabilities allows financial services institutions to have full accountability, traceability and auditability of their binaries. So if something goes wrong with a binary, they can perform precise and quick root cause analysis and take the appropriate actions.

CONCLUSION:

In this ebook, we've explained why adopting DevSecOps is a must for financial services institutions. DevSecOps helps them properly secure their SDLC without slowing down their pace of software releases.

Key DevSecOps benefits for banks and other financial services providers include:

- Protection of the SDLC from end to end
- Acceleration of software releases
- Improvement of productivity for dev, ops and security teams
- Increase in cross-team communication and collaboration
- Boost in quality, performance, reliability and innovation of digital services
- Business growth and expansion, including:
  - increased revenue
  - better customer retention
  - lower costs
  - enhanced customer experience

Want to learn more about how to successfully adopt DevSecOps in financial services? **Join us for a demo!** The JFrog DevOps Platform has all the features and functionalities to help you deploy an end-to-end DevOps pipeline that releases secure and compliant software quickly and frequently.

THE JFROG PLATFORM