opentext™

DevSecOps for financial services

Count on secure application delivery

Contents

Strengthen financial security with DevSecOps 3

How DevSecOps transforms financial software development 5

Challenges of implementing DevSecOps in financial services 6

Key features of a financial services-focused DevSecOps platform 8

Best practices for selecting the right DevSecOps platform 9

Case study: Bci 10

Prepare for the future of DevSecOps in financial services 12

Key takeaways 14

Strengthen financial security with DevSecOps

Financial institutions are rapidly adopting cloud-native applications, open banking APIs, and AI-driven services—all so they can serve customers better. However, these advancements also introduce new cybersecurity risks, making security a top priority.

DevSecOps integrates security into every phase of software development, ensuring that financial applications remain secure, compliant, and resilient against cyberthreats.

Who can forget some of the most infamous data breaches?

1 Equifax (2017)

The 2017 Equifax breach exposed 148 million individuals' personal data due to an unpatched Apache Struts vulnerability.

Affecting more than 40% of the US, the breach led to legal action, regulatory scrutiny, and reputational damage.

2 Capital One (2019)

A former AWS engineer exploited a vulnerability in Capital One's cloud infrastructure, exposing 106 million customers' data.

It included 100 million credit card applications. The breach underscored cloud security risks and insider threats.

3 JPMorgan Chase (2014)

Hackers infiltrated JPMorgan Chase's network, gaining administrative access to 90+ servers. Data was compromised from 76 million households.

Data from 7 million small businesses was also compromised. Using malware and phishing, they exposed banking vulnerabilities.

Why security must be embedded at every stage

Traditional security models often involve testing applications late in the development lifecycle, leading to delays, vulnerabilities, and increased costs. DevSecOps shifts security left—embedding security at every stage, from design to deployment, to reduce risk and enable faster, more secure software releases.

The rising cyberthreats in financial services

The financial sector is one of the most targeted industries for cybercrime. According to recent studies:

- **77% of financial institutions** experienced a cybersecurity incident in 2023 (source).
- Cybercrime costs are expected to reach **$10.5 trillion** in 2025 (source).
- JPMorgan Chase invests **$15 billion** to protect itself from cyberattacks (source).
- Cybercriminals most often use stolen cards, ransomware, and phishing to steal funds and sensitive data (source).

As digital banking and fintech solutions grow, it is essential to implement a robust DevSecOps strategy to mitigate these risks.

How DevSecOps transforms financial software development

Unique security challenges in the banking and financial services industry (FSI)

Financial applications differ from other industries due to their high-stakes nature. DevSecOps helps address these challenges by:

- **Protecting high-value assets:** Financial data and transactions are prime targets for hackers.
- **Ensuring regulatory compliance:** Organizations must adhere to *PCI DSS*, *GDPR*, *SOC 2*, *FFIEC*, *ISO 27001*, and other regional financial regulations.
- **Securing customer data:** Protecting personally identifiable information (PII) and payment details against breaches.
- **Modernizing legacy infrastructure:** Balancing security for traditional core banking systems and cloud-native services.

Benefits of DevSecOps in FSI

DevSecOps enables financial organizations to:

☑ **Reduce security vulnerabilities early** through automated security testing.

☑ **Achieve faster and more secure software releases** with streamlined CI/CD pipelines.

☑ **Enhance fraud prevention** with real-time security monitoring.

☑ **Increase resilience against cyberthreats** through proactive threat intelligence.

Challenges of implementing DevSecOps in financial services

1. **Cultural resistance to change**

Many financial organizations have traditionally operated in siloed teams, where security is handled separately from development. DevSecOps requires a cultural shift towards collaboration between developers, security teams, and operations.

2. **Complex compliance and regulatory landscape**

Financial services operate under strict regulations, including:

- **PCI DSS** (for payment security).
- **GDPR** (for data privacy in the EU).
- **FFIEC** (for US financial institutions).

Ensuring continuous compliance while adopting agile DevSecOps practices is a significant challenge.

3. **Legacy IT and hybrid environments**

Many financial institutions still rely on **mainframe-based core banking systems** that are difficult to integrate with modern DevSecOps tools.

4. **Sophisticated cyberthreats**

Financial institutions face:

- **Account takeover (ATO)** via credential stuffing attacks.
- **Insider threats** from employees with privileged access.
- **API vulnerabilities** in open banking integrations.

Key features of a financial services-focused DevSecOps platform

Essential capabilities for secure financial software development

A **DevSecOps platform** tailored for financial services should include these features:

Automated security testing:
Static and dynamic application security testing (SAST/DAST) in CI/CD pipelines.

Real-time fraud detection:
AI-driven monitoring to identify suspicious activities.

API security:
Preventing unauthorized access and data leaks in financial APIs.

Zero-trust architecture:
Strong identity and access management (IAM) for all transactions.

End-to-end encryption:
Protecting sensitive customer data at rest and in transit.

Threat intelligence integration:
Continuous monitoring for evolving financial cyberthreats.

Best practices for selecting the right DevSecOps platform

Evaluate DevSecOps solutions for FSI

To choose the best DevSecOps platform, financial organizations should look for:

☑ **Regulatory alignment** with industry standards (PCI DSS, GDPR, etc.).

☑ **Cloud security** and seamless integration with cloud-native services.

☑ **Threat intelligence**, including real-time insights on emerging threats.

☑ **Secure CI/CD pipelines**, with security embedded in development workflows.

☑ **Scalability** to support high transaction volumes and rapid fintech innovation.

Case study: Bci

Bci is a principal player in the private banking system of Chile, with over 300 offices and 10,500 staff serving millions of customers in Chile, the United States and other international locations. Management of the bank remains with the same family that has led the bank since its inception.

Challenge

Bci wanted to maintain their first-mover status in a disruptive industry with many new trends and competition that sometimes emerge from unexpected angles.

Bci

Solution

Bci adopted the OpenText™ DevSecOps platform, which provided:

- **Integrations with open source tools to introduce more test automation**, which in turn enhances the role of the traditional tester and empowers QA engineers.
- **Built-in testing, compliance tracking, security, and quality assurance** to catch defects early in the development process.
- **Scalability** to support high transaction volumes and rapid fintech innovation.

Outcomes

- 90% defect reduction
- 95% of manual regression tests replaced with automated tests
- 75% reduction in time to market
- 21% cost reduction

> **“By measuring test coverage and testing early in the development cycle we deliver higher quality applications faster, resulting in a better customer experience. Deploying more advanced Software Delivery Management capabilities will enable us to move even faster and integrate QA more deeply into our development cycle.”**

Luis Dujovne
Head of DevOps and Quality Assurance (QA), Bci

Read their story >

Prepare for the future of DevSecOps in financial services

5 emerging trends in financial cybersecurity

1 AI-powered security

AI-driven security solutions are revolutionizing fraud detection, threat intelligence, and anomaly detection. Machine learning models analyze vast amounts of transactional data in real time, identifying patterns indicative of fraudulent activity. AI can also automate responses, blocking suspicious transactions and reducing false positives, which improves both security and customer experience.

2 Zero-trust security adoption

Zero trust assumes that no entity—internal or external—should be trusted by default. Every access request undergoes continuous authentication, reducing the risk of insider threats and unauthorized access. Implementing zero trust in financial services means securing all endpoints, enforcing multi-factor authentication (MFA), and leveraging behavior analytics to detect anomalies.

3 Blockchain security

The rise of decentralized finance (DeFi) and blockchain-based transactions necessitates enhanced security measures. Smart contract audits, cryptographic key management, and secure consensus mechanisms are critical to preventing vulnerabilities that could be exploited in DeFi applications. Additionally, financial institutions are exploring blockchain for fraud prevention, secure identity verification, and transparent transaction tracking.

4 Automation in threat response

Financial institutions are turning to security orchestration, automation, and response (SOAR) platforms to mitigate cyberthreats quickly. AI-driven playbooks can handle incidents such as data breaches, ransomware attacks, and DDoS attempts with minimal human oversight, improving response times and limiting damage.

5 Regulatory technology (RegTech) integration

RegTech solutions leverage automated workflows to streamline compliance processes, reducing the manual effort required for regulatory adherence. By integrating real-time compliance monitoring, financial institutions can quickly detect and address potential violations, remain compliant, and minimize operational disruptions and costs.

Key takeaways

- Financial institutions **must integrate security into software development** through DevSecOps.
- A **proactive security approach** reduces breaches, fraud, and compliance violations.
- Choose a **DevSecOps platform** with **real-time monitoring, automated compliance, and API security** for long-term success.

Checklist for implementing DevSecOps in FSI

☑ Conduct a **security assessment** of existing DevOps processes.

☑ Automate **security testing** in CI/CD pipelines.

☑ Implement **zero-trust** principles for financial transactions.

☑ Choose a **DevSecOps platform** with compliance automation.

☑ Train teams on **secure coding** and cybersecurity best practices.

Start your DevSecOps journey today! Get a free trial or request a consultation to explore the best DevSecOps platform for your financial organization.

Additional resources

Secure the future of banking with DevSecOps >

Learn more about OpenText DevOps Cloud >

Read more OpenText DevSecOps platform customer stories

Credit Agricole Payment Services >

Santander Brazil >

Santander Chile >

Aktif Bank >

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit opentext.com.

opentext.com | X (formerly Twitter) | LinkedIn | CEO Blog