DevSecOps for pharmaceuticals

Cure compliance headaches

Contents

Get the right prescription for secure software delivery

By 2030, 70% of companies will rely on cloud-based platforms for operations, R&D, and regulatory compliance.[1]

Digital transformation in the pharmaceutical industry is accelerating rapidly. By 2030, 70 percent of companies will rely on cloud-based platforms for operations, R&D, and regulatory compliance. While this evolution offers significant benefits, it also exposes organizations to increasing cyberthreats and regulatory scrutiny.

Given the sensitivity of clinical trial data, intellectual property, and patient safety, security is now a top priority. At the same time, global regulations, like FDA 21 CFR Part 11 and GxP, demand rigorous system validation and audit readiness.

A 2023 Deloitte study found that only 21 percent of life sciences and healthcare organizations feel fully prepared to manage rising cybersecurity risks,[2] yet cyber incidents are on the rise. The gap between digital innovation and cyber resilience is widening—creating urgent demand for scalable, automated solutions.

DevSecOps—a methodology that embeds security and compliance into every stage of the development lifecycle—offers a solution. It supports faster innovation while ensuring compliance and protecting critical assets.

This ebook will help pharmaceutical leaders understand the unique demands of DevSecOps in their industry, identify platform must-haves, and adopt best practices for success.

[1] McKinsey & Company, Digital transformation in pharma: Moving past the pilot stage, 2023

[2] Deloitte, Cyber & strategic risk in life sciences and healthcare, 2023

The pharmaceutical industry's unique DevSecOps requirements

The pharmaceutical industry faces a set of digital challenges unlike any other sector. These stem from the sensitive nature of its data, strict regulatory requirements, and the complexity of its digital and physical supply chains.

Data sensitivity

Pharmaceutical companies manage highly confidential data, including proprietary drug formulations, research findings, and clinical trial results. A data breach could result in IP theft, patient harm, or massive financial loss.

Regulatory compliance

Pharma is governed by a dense web of global regulations, such as FDA 21 CFR Part 11, GxP guidelines, and EMA protocols. These rules require rigorous documentation, audit trails, and validation procedures—all of which must be maintained across complex digital systems.

Legacy systems

Many pharmaceutical organizations operate on legacy platforms that are essential but difficult to integrate with modern DevSecOps practices. Bridging the gap between old and new requires platforms that are flexible and interoperable.

Product integrity

Whether it's a cloud-based research tool or a manufacturing execution system (MES), every piece of software impacts product quality. A security lapse could affect drug safety, disrupt the supply chain, or halt production.

By understanding these industry-specific challenges, pharmaceutical leaders can better assess what their organizations need from a DevSecOps platform.

Only 21% of life sciences and healthcare organizations feel fully prepared to manage rising cybersecurity risks.[3]

[3] Deloitte, Cyber & strategic risk in life sciences and healthcare, 2023

The 4 main challenges of implementing DevSecOps in pharmaceuticals

It’s complicated. Implementing DevSecOps in pharmaceuticals is a challenging endeavor, often requiring cultural, technical, and procedural shifts. Below are some of the most common challenges organizations encounter:

1. **Cultural shift**

DevSecOps encourages collaboration between traditionally siloed teams. In pharma, where teams are often highly specialized and compliance-driven, this cultural shift can be difficult, but it’s critical to embrace a shared responsibility model for security.

2. **Resource constraints**

Many organizations lack the internal expertise needed to implement and maintain DevSecOps practices, but hiring specialists or upskilling existing teams can be both time-consuming and expensive. Especially on a tight budget.

3. **Complex infrastructure**

Pharmaceutical companies manage a hybrid ecosystem that includes cloud services, on-premises systems, lab equipment, and external vendors. It can seem overwhelming to integrate security practices across such a diverse environment.

4. **Regulatory hurdles**

The implementation of automated processes and continuous integration (CI) pipelines must be done in a way that preserves traceability, auditability, and validation—all essential to maintaining regulatory compliance.

Yep, it’s complicated. But despite these obstacles, the benefits of DevSecOps far outweigh the costs. A well-implemented platform can significantly reduce risk, accelerate innovation, and enhance regulatory readiness.

Main features of a pharma-focused DevSecOps platform

The right DevSecOps platform must not only support agile development but also meet the rigorous demands of pharmaceutical security and compliance. Make sure you include the following platform features in your "must-have" list:

- **Automated compliance management:** Enables real-time monitoring, audit logging, and automated validation of controls.
- **Robust security frameworks:** Includes threat modeling, intrusion detection, and incident response planning.
- CI/CD **integration:** Supports secure, compliant, continuous integration and delivery pipelines.
- **Interoperability:** Seamlessly connects with systems like MES, LIMS, and ERP platforms.
- **Data encryption:** Offers end-to-end encryption for IP and clinical trial data.
- **Audit and monitoring tools:** Facilitates regular assessments, issue tracking, and performance logging.

Best practices: How to select the right DevSecOps platform

- **Understand organizational needs:** Tailor platform selection based on specific R&D, production, and compliance goals. Identify current infrastructure gaps and define long-term digital transformation priorities.
- **Vendor due diligence:** Choose vendors with proven pharmaceutical experience. Evaluate past performance in GxP-regulated environments, look for references within the life sciences sector, and prioritize vendors that offer long-term support and compliance documentation.
- **Compliance support:** Ensure the platform aligns with FDA, GxP, EMA Annex 11, and international data integrity guidelines. Platforms should offer audit trails, electronic signatures, validation toolkits, and pre-built templates for regulatory reporting.
- **Scalability:** Look for solutions that can adapt to new markets, products, and compliance demands. A scalable DevSecOps platform should support both legacy system integration and cloud-native development, enabling secure deployment across multiple geographies.
- **User-friendly interface:** It's important the UI works for cross-functional teams, including non-technical stakeholders. Look for platforms that support visual dashboards, automated alerts, and easy-to-navigate compliance workflows.
- **Integrated automation and orchestration:** Automation of compliance checks, vulnerability scanning, and access controls improves consistency and reduces human error—both critical in pharmaceutical environments.
- **Strong partner ecosystem:** Select vendors that can integrate with leading electronic lab notebooks (ELNs), quality management systems (QMS), and clinical trial platforms.

The right platform will act as both a security enabler and business accelerator—helping pharma organizations reduce time-to-market, manage risk, and maintain global regulatory alignment.

Real pharmaceutical companies using real DevSecOps solutions

Large Enterprise Pharmaceuticals company used OpenText to successfully deploy public-facing websites with no issues.

Key stats

10/10 Likely to recommend

18 months Time to ROI

“We use OpenText DevOps products for trackability across requirements and protocols. These products help us to confidently know if we have 100% coverage.”

Manager, Pharmaceutical Company

See the source >

Read their story >

Prepare for the future of DevSecOps in pharmaceuticals: 4 emerging trends

DevSecOps is driving forward with advances in automation, data science, and cyber resilience. Pharmaceutical companies stand to benefit enormously from the following emerging trends:

AI and machine learning

These technologies are improving threat detection, automating code reviews, and supporting predictive analytics for system vulnerabilities—speeding up security processes without sacrificing accuracy.

Zero trust architecture

As pharmaceutical companies collaborate more with external partners, zero trust security models ensure only authorized access at every level, dramatically reducing the risk of data leaks.

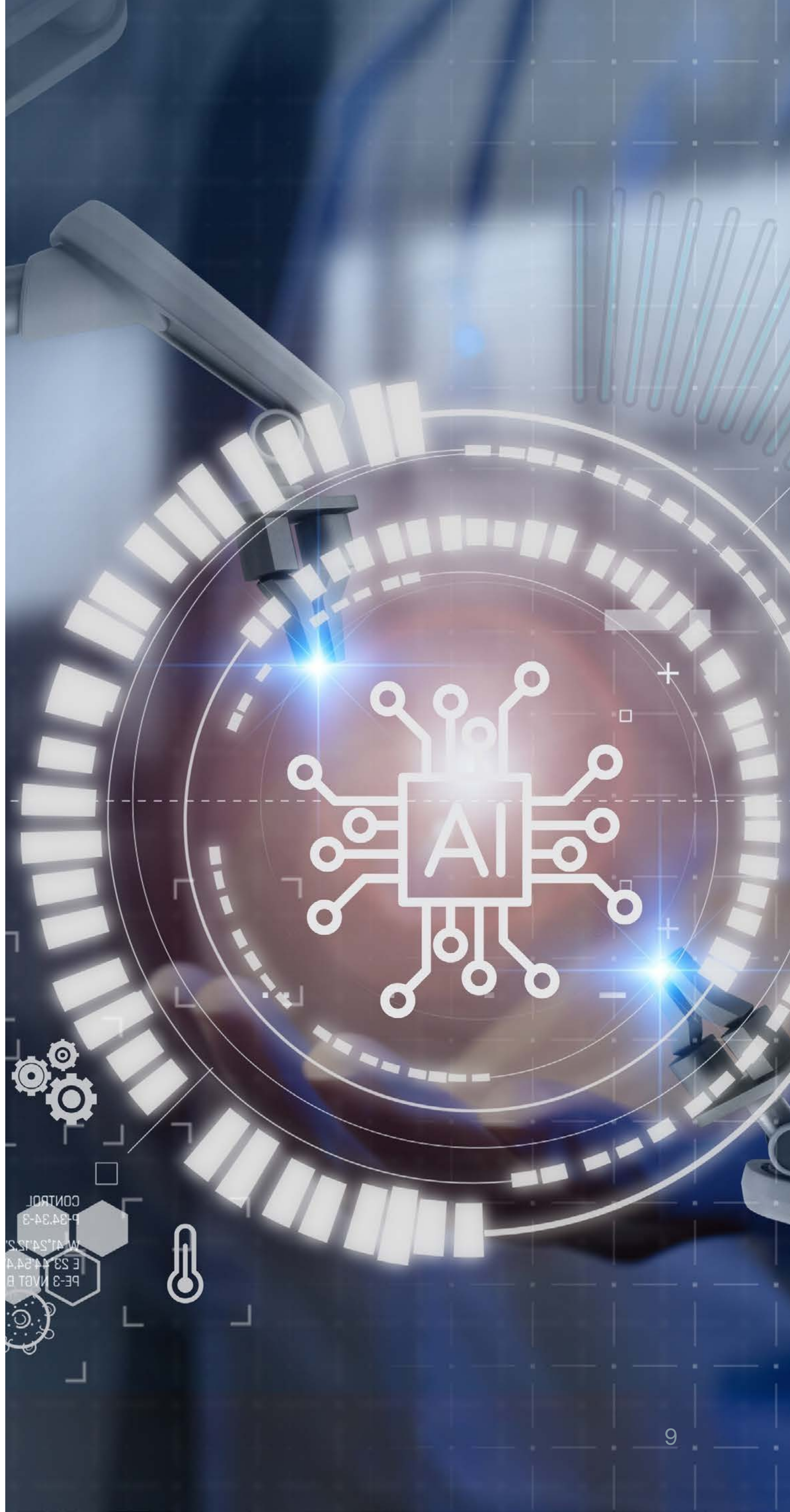
Blockchain integration

Blockchain offers immutable audit trails, improving data integrity and traceability—key components in compliance and clinical research.

Advanced automation

Next-gen DevSecOps platforms support automated software validation, test case generation, and GxP documentation—reducing human error and boosting compliance.

These innovations signal a future where DevSecOps doesn’t just protect pharmaceutical companies—it powers their next breakthroughs.



Additional resources

Learn more about DevSecOps from OpenText

Read the guide, Secure by design: Deliver software faster, safer, and more securely with devsecops

Watch the short video, DevSecOps FAQs: Answers at the speed of delivery

Key takeaways & next steps

The integration of DevSecOps into pharmaceutical IT strategies is not a luxury—it's a necessity. As cyberthreats intensify and regulatory demands grow more complex, adopting the right platform is essential to protecting intellectual property, ensuring compliance, and accelerating innovation.

- DevSecOps brings security into every stage of software development.
- The pharmaceutical industry faces unique challenges that demand tailored solutions.
- Choosing the right platform means balancing compliance, scalability, and usability.

Checklist for implementing DevSecOps in pharma

□ Conduct a current-state assessment of your software development and compliance workflows

□ Identify gaps where DevSecOps practices and tools could make the greatest impact

□ Engage with vendors who have proven pharmaceutical experience and compliance expertise

□ Start small—pilot the DevSecOps platform in a low-risk environment before scaling

By taking these steps, pharmaceutical organizations can strengthen their digital defenses and accelerate time to market, reduce costs, and remain competitive in an increasingly digital world.

Try OpenText™ Core Software Delivery Platform free for 30 days.
Start now: **no credit card required.**

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

Copyright © 2025 Open Text • 06.25 | 243-000105-001

opentext™