GitLab

Driving success in financial services with DevSecOps

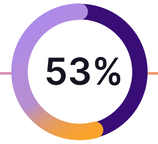
How to cut costs, boost competitiveness, and increase security

At a glance

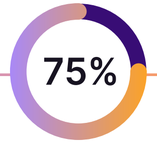
Why DevSecOps matters for financial services

What is DevSecOps?

1. Stands for development, security, and operations
2. A methodology that integrates security procedures and testing from the very beginning of the software development lifecycle
3. Fosters collaboration between all teams to securely and efficiently speed software production



of financial services respondents said their organization uses DevOps or DevSecOps methodologies to build software



of financial services respondents using DevOps/DevSecOps said they are satisfied with their organization's DevOps/DevSecOps practices

Stats based on GitLab's 2023 Global DevSecOps Survey

Top benefits of DevSecOps for respondents in financial services:

- Efficiency
- Productivity
- Security
- Code quality
- Happier developers
- Collaboration

"The biggest challenges in software development today are ensuring that security is a top priority for developers, writing scalable code, and increasing automation. That's where DevSecOps comes in."

Survey respondent, VP of engineering in a financial services company

A DevSecOps platform can help financial institutions:

- Reduce the number of costly security investigations
- Cut costs associated with toolchain licenses and management
- Avoid legal liability connected to security breaches
- Empower teams to fix vulnerabilities earlier in the software development lifecycle
- Identify issues that could hurt the brand and break customer trust

See how GitLab's platform could help your organization with our ROI efficiency calculator >

How financial institutions can build fast — without sacrificing security and compliance

Software development in the financial services industry is complex. Banks and financial institutions are prime targets for cybercriminals due to the valuable and sensitive data they handle, and data breaches can result in significant financial losses and reputational damage. In addition, regulatory compliance can be a challenge for the financial services sector, as industry regulations are often complex and are constantly evolving.

Financial institutions need a way to integrate security and compliance into the software development process: DevSecOps.

With DevSecOps, security measures are embedded at every stage of the software development lifecycle, ensuring that vulnerabilities can be identified and promptly addressed. And by including automated security checks and audits within the DevSecOps lifecycle, organizations can provide comprehensive and accurate data to demonstrate compliance with regulatory mandates. This not only helps avoid penalties but also fosters trust among customers and stakeholders.

That focus on security and compliance **saves companies money and time, while also better securing the business, its customers, and its brand.** It also enables software teams to push software out faster, helping companies meet customer needs before their competitors can. Ultimately, it's about ensuring that shipping software quickly isn't done at the expense of security and compliance.

> "[Our customer] had a lot of requirements, so there was a lot of work we had to do, a lot of new features to build. The DevSecOps platform gave our software development teams the ability to collaborate and to iterate quickly to get it all done."
>
> **– Andy Chow, Technology Chief of Staff, Airwallex**

What is a DevSecOps platform?

Because DevSecOps spans the entire software development lifecycle, many organizations end up piecing various tools together — one tool, for instance, to manage containers, one to automate deployment, another for code review — to create a clumsy, **time-consuming DIY toolchain** that can waste time and money, not just for the initial setup but also over time.

A single, end-to-end **DevSecOps platform brings these disparate tools together** to help eliminate duplicate tasks, reduce costs, and drive critical advantages for both software development teams and the overall business. A full platform gives an organization all the features, security tools, and automation they need in one application so they're not buying, stitching together, and maintaining a complicated jumble of tools.

> **Using a DevSecOps platform, software teams are able to spend a lot less time wondering or worrying if their software is secure. They've been checking it all along.**

This guide will help you understand how DevSecOps and a DevSecOps platform can strengthen not only software development teams, but the entire organization. We'll look at increasing security and collaboration, going cloud agnostic, and giving executives visibility and useful metrics. We'll also take a look at a real-world example of how one company is using a DevSecOps platform to increase collaboration, security, and automation. **Let's dive in.**

Check out this video

to learn about the evolution of DevOps to DevSecOps, and how it can benefit your enterprise.

Quick look at top DevSecOps business benefits

There's no question a DevSecOps platform enables software development teams to accelerate software production, while making them more efficient and their code more secure. And when they're not spending time and effort on chasing down problems and performing hands-on tasks, they have more time to create innovative software. But the benefits of DevSecOps go beyond tech teams, boosting the overall organization.

Here are a few ways DevSecOps, and a full, end-to-end DevSecOps platform, help your business.

60%

decrease in time consumed by manual tasks thanks to DevSecOps automation

Source:
GitLab's 2023 Global DevSecOps Survey

"Speed matters ... Now it takes about eight minutes to run a pipeline. That eight minutes is massive. That alone would have been meaningful enough for us to consider the switch, the promise of this high-speed continuous integration pipeline."

– Mitch Trale, Head of Infrastructure, HackerOne

Ensuring the enterprise is able to produce secure software:

- **Protects the entire business**
- Safeguards customers and their data
- Creates **critical customer trust**
- Prevents damaging headlines about breaches
- Shields company brand
- Attracts high-level partners and suppliers

Rapid and secure delivery with DevSecOps:

- Makes teams more efficient
- Saves time and **reduces costs**
- Speeds up time to market
- **Outdoes competitors**
- Frees up teams to focus on high-value work

A DevSecOps platform:

- Supports a multi-cloud strategy, offering **business resiliency** and stability
- Gives executives visibility and metrics to **gain insights**
- Fosters collaboration across the company
- Makes **compliance** easier
- Includes automation to make teams efficient
- Secures the entire software supply chain
- Makes **developers more productive**

A closer look at what DevSecOps offers up

Advancing software and business security

A DevSecOps platform supplements development and deployment velocity with security. That means **software is rolled out to the company, partners, and customers as fast and as securely as possible.** Old-school thinking had companies simply focused on pushing software out the door, worrying about security later. It was inefficient and insecure. DevSecOps shifts security left, moving security testing, monitoring, and quality and performance evaluation to the beginning of the development process, when it's easier to find and fix any security problems.

Making developers more productive

A DevSecOps platform gives teams everything they need to build, write, test, and deploy software in one platform. They're not wasting time integrating and updating different tools, switching back and forth between tools, having to remember various passwords, and going back to fix bugs that weren't found initially. This eases demand on their time and **lets them focus on building software, driving their productivity.**

Gaining visibility into how it all works

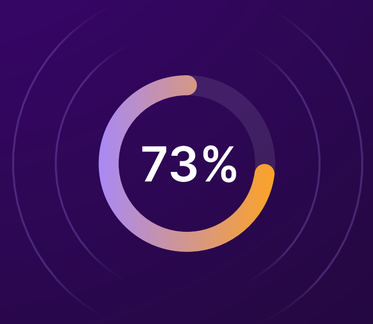
A cornerstone of DevSecOps is empowering teamwork, and one of the ways the platform does that is by creating visibility into the workflow from planning to production. Whether someone is a developer, a backend engineer, a customer relations associate, or a CIO, they all can gain insight into how code is being designed and developed, how it runs on the system, how it integrates with other pieces of code, and **how customers interact with it.**

Fostering collaboration across the company

With that visibility, everyone in software development and across the company can collaborate. By breaking down silos and increasing visibility across the entire software lifecycle, teammates can better share responsibility, communicate in one place, and **work together** to move software projects forward. This creates more, and more diverse, project input, potentially leading to the creation of better, more secure, and more well-rounded products. It enables everyone to contribute. DevSecOps brings everyone into the security tent to share responsibility.

"[Before using a DevSecOps platform] people just chose the tools they were familiar with. That made it difficult for people to work together, isolating teams. It got really messy really quickly in that fractured environment. We needed to bring everyone together."

– Andy Chow, Technology Chief of Staff, Airwallex



of security pros are using a DevSecOps platform or are considering adopting one in the next year

Source: GitLab's 2023 Global DevSecOps Survey

Measuring efficiency and visibility

Executives need visibility into the software running their companies and connecting them with their partners and customers. They need to understand how code is being created and how it's working for the company. A DevSecOps platform's pipeline visibility, along with reports and metric dashboards, give managers the big picture to identify bottlenecks and **tie engineering measurements to business outcomes**. This attention to value streams gives users a way to objectively measure and track the metrics most important to them and their business.

Cutting hands-on work with automation

Part of the appeal of using a DevSecOps platform is the built-in automation that can accelerate software development and deployment, decrease time-consuming, hands-on work, reduce errors due to manual processes, and help push out updates at the speed of business. For instance, new code can be automatically tested, pushed into production, and then monitored once it's launched. And if a problem is detected, automated features can raise alerts and even prompt a rollback to an earlier, clean version. Automation ensures that **increasing production velocity doesn't come at the cost of security** or worker's expensive time.

Securing the software supply chain

Today, software has thousands of dependencies, where components, such as code libraries or packages, are reused in a new piece of software. Components rely on each other to run properly, so development teams need to **make sure each piece is secure**. If one out of thousands of dependencies is insecure, it could lead to holes that attackers could use as entry points. One vulnerable piece of the supply chain hurts the whole company, and that will plague its reputation. Shifting security left with DevSecOps means making sure everything being integrated into the software from that supply chain has been tested and can be trusted.

Business resilience with a multi-cloud strategy

Many companies are **finding resilience in being cloud agnostic**, or using a multi-cloud approach. For instance, if applications or operations are running on one cloud and that provider has trouble or goes down, those operations can be switched to another cloud provider. It's a matter of not putting all your eggs in one basket. With a DevSecOps platform, it's easy and uncomplicated to integrate with different cloud providers.

How DevSecOps is helping a global fintech platform meet customer needs faster

Airwallex is a leading global financial platform for modern businesses, offering trusted solutions to manage everything from payments, to treasury and spend management, and embedded finance. Since adopting a DevSecOps platform, the Singapore-based company has been able to meet customer needs more quickly, cut costs, and win business from competitors.

Airwallex runs a financial platform that has become a global economic infrastructure, supporting organizations of all sizes by offering multi-currency business accounts, local and international transfers, and foreign currency exchanges. Building its customer base is critical for the young company, so when executives had a chance to bring on a leading airline carrier as a high-profile customer in 2022, they were under pressure to prove they could meet the airline's needs in order to gain its business. That meant providing the company with a set of software features better and faster than their competitors could. With the help of the GitLab DevSecOps Platform, that's exactly what they did.

Here are a few of the other benefits Airwallex has seen from its investment in DevSecOps:

- More seamless collaboration between teams, allowing the company to increase delivery speed, while also being more cost efficient
- Reduced costs and maintenance efforts thanks to consolidating more than a dozen DevOps tools into a DevSecOps platform
- Faster onboarding, since engineers and developers don't have to learn multiple tools
- Improved visibility into projects throughout the software development lifecycle for team members across the company

8X faster deployments

"Making sure that we spend our money wisely is very, very important. GitLab allowed us to reduce our costs and centralize our work in one place. It's been money well spent."

– Andy Chow, Technology Chief of Staff, Airwallex

4X faster feature delivery

“It’s simple. All teams operate around this one tool. Instantly, that made communication easier. We wouldn’t be where we are today if we didn’t have GitLab in our stack.”

– Logan Weber, Software Automation Engineer,
Airbus Defense and Space Intelligence

“The cost of running security scans in GitLab is significantly lower than it was previously. And so we’re much more inclined to run more thorough scans, faster.”

– Mitch Trale, Head of Infrastructure,
HackerOne

Take DevSecOps for a spin

In today’s highly competitive landscape, organizations are under more pressure than ever to deliver software more securely, efficiently, and quickly. They need a more mature, all-encompassing platform to **improve their time to market, outmaneuver competitors, and boost their bottom line.** GitLab answers that need with its end-to-end DevSecOps platform.

DevSecOps also is all about awareness: awareness that security has to be part of the entire development and deployment process, and awareness, or visibility, into what is happening throughout the lifecycle so everything from slowdowns to vulnerabilities can be spotted and fixed immediately.

Think about what can hurt your business the most: a security breach, a hack, or a compliance fiasco. The automated security and infrastructure scanning, vulnerability dashboards, and compliance features built into the GitLab DevSecOps Platform help organizations to reduce risk and ensure that security and compliance are incorporated throughout the development process.

Have your team try out this free trial of GitLab’s DevSecOps Platform.

About GitLab

GitLab is the most comprehensive, AI-powered DevSecOps Platform for software innovation. GitLab provides one interface, one data store, one permissions model, one value stream, one set of reports, one spot to secure your code, one location to deploy to any cloud, and one place for everyone to contribute. The platform is the only true cloud-agnostic end-to-end DevSecOps platform that brings together all DevSecOps capabilities in one place.

With GitLab, organizations can create, deliver, and manage code quickly and continuously to translate business vision into reality. GitLab empowers customers and users to innovate faster, scale more easily, and serve and retain customers more effectively. Built on open source, GitLab works alongside its growing community, which is composed of thousands of developers and millions of users, to continuously deliver new innovations.