GitLab

Driving success in the public sector with DevSecOps

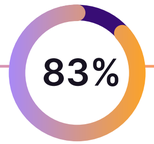
How a DevSecOps platform improves efficiency, boosts collaboration, and increases security and compliance

At a glance

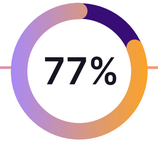
What execs in the public sector need to know about DevSecOps

What is DevSecOps?

1. It is a software development approach that combines 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 production of compliant software



of DevSecOps users rate their organization's security efforts as "good" or "excellent"



of security professionals who are using DevSecOps have incorporated security earlier in the software development process ("shifted left") or plan to in the next 3 years

Stats based on GitLab's 2023 Global DevSecOps Survey

Top benefits DevSecOps users say it has brought to their organization:

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

"It's very typical that we're seeing monthly deliveries turn into weekly. We're seeing quarterly deliveries turn into monthly. I mean, that scale of changes is very common."

- Alan Hohn, Director of Software Strategy, Lockheed Martin

A DevSecOps platform can help your organization by:

- Consistently managing and enforcing security and compliance policies
- Reducing money spent on toolchain licenses and management
- Accelerating speed to mission
- Empowering teams to fix vulnerabilities earlier in the software development lifecycle, while enforcing consistent guardrails
- Aligning to NIST, NSA, and CISA guidance, supporting software supply chain security

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

Try GitLab free for 30 days >

Follow us:

Evolution of DevSecOps ties in security, efficiency, and savings

The evolution of DevOps into DevSecOps isn't about a simple name change. It's actually about a crucial advance in the mindset around DevOps.

Organizations increasingly have been turning to DevOps to make the development and deployment of business-critical software more efficient and reliable. But speeding software development without keeping security top of mind isn't as efficient as it could be, and it doesn't produce the most secure software. DevSecOps takes the next step in DevOps, making the **importance of security** in the software development lifecycle explicit. It's becoming a standard mindset as software development teams realize the value of incorporating security earlier, and throughout, the entire development process.

"There's never a good time for a security breach," says Michael Friedrich, Senior Developer Evangelist at GitLab. "Developers and executives need to understand that a small problem can easily become a bigger one. You need to invest in secure deployments and security observability to help prevent it."

> "It's important to make everyone see value in security and you do that with DevSecOps. It includes everyone on the team, easing pressure on developers so they can focus on creating secure and quality code."
>
> **- Michael Friedrich,**
> **Senior Developer Evangelist, GitLab**

Cloud computing and security – top investments for DevSecOps users

Source: GitLab's 2023 Global DevSecOps Survey

That focus on security **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.

Why DevSecOps is important in the public sector

DevSecOps is important to the public sector — organizations within and working with the military, law enforcement, or federal, state, and local governments — because they have a special focus on security and compliance. DevSecOps is built with those two needs top of mind.

DevSecOps not only eliminates old-school siloed approaches to software development but also works security into every phase of the software development lifecycle. That means everyone shares responsibility for security so vulnerabilities or flaws are caught and fixed more quickly, easily, and with less expense. And by using automated code scanning tools and security dashboards, and setting up compliance enforcement inside the pipelines, it's easier to ensure teams are adhering to all necessary regulations and gathering needed data to prove that compliance.

With that combination of speed, efficiency, and security, the public sector has a way of delivering new software and updated features to customers and partners without sacrificing assurance and compliance.

DevSecOps is all about empowering your teams to work more collaboratively, be more productive, and deliver better, secure, and compliant products to your customers.

What is a DevSecOps platform?

“If I was in a company’s buying seat, I would be looking at DevSecOps,” says Ayoub Fandi, senior field security engineer at GitLab. “Executives want to worry less about compliance issues and security breaches that could have a big impact on their revenue, their ability to grow the company, and customers’ confidence in doing business with them. With DevSecOps, they can worry less about all of that.”

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. **DevSecOps is most effective on a single end-to-end platform.**

> **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.

60%

decrease in time consumed by manual tasks thanks to DevSecOps automation

Source:
GitLab's 2023 Global DevSecOps Survey

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 public sector organization.

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

"We can now look and say, 'Who's doing what? Who's value-added? Who's being a team player, who's slacking off?' all within the GitLab commit history."

– Chris Apsey, Captain, U.S. Army

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. Those abilities are critical to any company working in the public sector.

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," says Abubakar Siddiq Ango, developer evangelism program manager at GitLab. "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**.

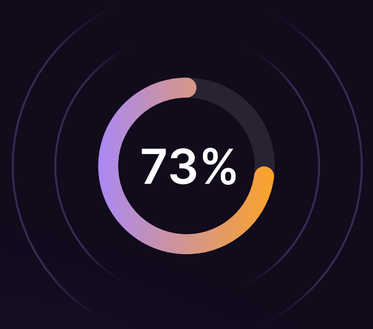
Fostering collaboration across the company

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.

"A DevSecOps platform helps the CIOs, CTOs and CISOs work together with the engineers so they understand what's happening with their software. It increases security, creates visibility and collaboration in a non-confrontational kind of way."

– Ayoub Fandi, Senior Field Security Engineer, GitLab

> “DevSecOps is how security is integrated with the different parts of development and operations. For each stage, you get security baked in.”
>
> - Ayoub Fandi, Senior Field Security Engineer, GitLab



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. “To understand how each piece of software is giving value to the company, managers and executives have to understand the metrics behind each tool,” says Fandi.

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,” says Fandi. “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. “And maybe a company wants to run some apps in Kubernetes, or they are using a lot of Windows Servers so they want to tap into the expertise of Microsoft Azure,” says Ango. “That requires companies to be cloud agnostic because it makes them flexible.”

What DevSecOps benefits look like in the public sector

If you're trying to figure out exactly how important and transformational adopting DevOps can be for your company, check out what a DevOps platform did for Lockheed Martin Corp., an American aerospace, defense, information security, and technology giant.

The company, with about 116,000 employees worldwide and more than 370 facilities, was looking to more efficiently, securely, and quickly develop and deploy software for thousands of its programs, ranging from satellite platforms and aerospace systems to ground control software and maritime surface and subsurface software. Lockheed Martin also had a history of using a wide variety of DevOps tools. Each program or product line at the company had its own toolchain. That led to uneven efficiencies and results. By adopting a DevOps platform, the company was able to greatly reduce its toolchains, cutting complexity, cost, and workload. The move to a platform also enabled them to drive collaboration between programs and across the entire business, implement monitoring and security controls to comply with Lockheed Martin's security policies, and more easily manage compliance regulations.

Since adopting a DevOps platform, Lockheed Martin reported 80 times faster CI pipeline builds, and what were once monthly deliveries have turned into weekly.

90% less time spent on system maintenance

"We want to get to the point, and what we're achieving, is people don't even consider standing up their own toolchain. They just use GitLab because they know that it works.

– Alan Hohn, Director of Software Strategy, Lockheed Martin

80X faster CI pipeline builds

> “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 Defence 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 at 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 the business the most,” says Friedrich. “A security leak. Someone breaking into the infrastructure. GitLab’s DevSecOps Platform provides automated security and infrastructure scanning, and an actionable vulnerability dashboard that will help protect from all of that. **For any executive, and for those as high up as the C-Suite, there’s real value in that.**”

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.