GitLab

A real-world guide to building secure software faster with DevSecOps

Check out success stories from companies like CARFAX, Lockheed Martin, and Southwest Airlines

Table of Contents

With DevSecOps becoming a critical component in software development, leaders often are in search of proven strategies to begin or enhance their existing practices. Today, security has become everyone's responsibility—making it imperative to weave it seamlessly across the development lifecycle.

DevSecOps represents that comprehensive approach, blending development, security, and operations into an integrated process. It can seem like a daunting transition: What are the advantages of shifting security left? What about automating security scans? What's the best way to secure the software supply chain? How can teams take advantage of artificial intelligence (AI)? What can they do to more easily ensure compliance with various regulations? But with practical insights from industry peers who have successfully implemented these measures, the path becomes clearer and more approachable.

Various forward-thinking enterprises, from global travel agencies to the public sector, have embraced DevSecOps and its methodologies—with success driven by GitLab's AI-powered platform. In this guide, you'll get actionable insights on increasing security with automated tools, creating a single source of truth for compliance needs, ensuring tools are updated, and building best-in-class security practices into the entire software development lifecycle. Hear how Lockheed Martin, CARFAX, and other leading organizations redefined their company's security tactics and better meet customer needs.

Let's dive in.

> "And the platform's security features are efficient in that they cover everything I'm looking for. Now I have a single source of truth for governance, compliance, and security audits."
>
> Nadav Robas,
> DevOps & DevSecOps Manager,
> Agoda

78%

of respondents who said they were using a DevSecOps platform were more likely to rate their organization's security efforts as "good" or "excellent" compared to 66% of non-users.

(According to the 2023 Global DevSecOps Report)

27%

of respondents who said they were using a DevSecOps platform were more likely to say they have shifted security left compared to 13% of non-users.

(According to the 2023 Global DevSecOps Report)

CARFAX increases security with automation and a shift left

U.S.-based CARFAX, Inc. helps millions of people shop for vehicles every day. With more than 31 billion records, it has the most comprehensive vehicle history database available in North America. Many of CARFAX's customers interact with the company online, so it relies on software to maintain and grow customer relationships and stay ahead of competitors. To do that, the company needs to efficiently and securely create new, innovative, and secure software.

For CARFAX, adopting a centralized DevSecOps platform made all the difference. Mark Portofe, Director of Platform Engineering at CARFAX, says they gained efficiency and a whole new level of security by taking advantage of automated testing tools built into the end-to-end application—like dependency and container scanning, as well as secret detection.

"We are always thinking about security while we design and build software," says Portofe. "It's not just about trying to get features out the door but also ensuring that those features are secure. It's part of every step of the software development lifecycle. That saves time and increases our security."

Read more about how CARFAX is finding nearly one-third of its vulnerabilities much earlier in development.

30%

of vulnerabilities found earlier in SDLC

"While security is always an ongoing battle, GitLab's security features are making it easier for developers to spot issues early."

Mark Portofe,
Director of Platform Engineering
CARFAX

Lockheed Martin boosts security posture, eases compliance work

80x

faster CI pipeline builds

> “Teams now are aware of the security posture of the code they’re writing in a way that they weren’t before. That enables conversations about the security of our software that were not taking place the old way.”
>
> **Alan Hohn,**
> **Director of Software Strategy,**
> **Lockheed Martin**

Lockheed Martin Corp., an American aerospace, defense, information security, and technology giant, is the world’s largest defense contractor. Its DevSecOps teams are tasked with efficiently, securely, and quickly developing and deploying software for thousands of programs, ranging from satellite platforms and aerospace systems to ground control software and maritime surface and subsurface software.

Since Lockheed Martin works with the Department of Defense and federal agencies, the company builds systems that are critical to national security. That means creating secure software and remaining compliant with government regulations are integral to both Lockheed Martin and its customers. To help them do just that, as well as trim what had been a complex toolchain and increase collaboration, the company embraced a comprehensive approach that integrates development, security, and operations into a unified framework.

A challenge for any company using toolchains is that it’s easy to miss an update because of the sheer size and complexity of that chain. Now with a platform, Lockheed Martin doesn’t have to worry about using tools that haven’t been updated because with a single, end-to-end application, an update only has to be done once and every instance is covered. They also are getting a standardized set of automated security capabilities seamlessly built in.

In addition, the company uses the GitLab’s compliance framework to enforce software quality and automation to make releases and dependency management more efficient and faster.

Find further info on how a DevSecOps platform helps Lockheed Martin ease compliance work.

Deutsche Telekom takes on inefficiencies with-out sacrificing security

Deutsche Telekom AG, Europe's leading telecommunications company, serves more than 240 million mobile customers, 26 million fixed-network lines, and 22 million broadband lines in more than 50 countries. Looking to streamline software development and increase collaboration, the company turned to DevSecOps. They achieved all of that and they also made security efforts more efficient.

By integrating security features into one application, Deutsche Telekom was able to shift security left, allowing their teams to find and remediate problems before they moved further down the development pipeline—when they would be more difficult and costly to fix.

Thorsten Bastian, business owner of the CI/CD Hub of Telekom IT, notes that having security features integrated in one application, enables them to immediately jump to the right place and fix any problem. "This is increasing the efficiency of handling security findings," he says. Norman Stamnitz, Product Manager of Telekom IT's CI/CD toolsuite — which is built on top of GitLab, and in Deutsche Telekom's case, GitLab Ultimate — also notes that with one single dashboard, they have been able to improve their security and compliance efforts. "If you can reduce manual security processes, do all this security scanning before a go-live — that brings us the ability to increase speed of development or to reduce the time to market even more," he says. "And of course, we wanted to shift left. We wanted our developers to have security scanners as part of their daily tasks."

For more information about how Deutsche Telekom achieved 6x faster time to market and enhanced security.

6x

faster time to market

"We decided to extend to GitLab Ultimate because we wanted to have the security and compliance features and all in one security dashboard."

Norman Stamnitz,
Product Manager
Telekom IT

Online travel giant Agoda cuts security tool sprawl, looks to AI

3,000

hours developer time saved per quarter

> “And the platform’s security features are efficient in that they cover everything I’m looking for. Now I have a single source of truth for governance, compliance, and security audits.”
>
> **Nadav Robas,**
> **DevOps & DevSecOps Manager**
> **Agoda**

Agoda, based in Singapore, offers customers value deals on a global network of 3.6 million hotels and holiday properties, along with reservations for things like flights, airport transfers, and activities. The company, which employs more than 6,600 staff in 31 markets, is focused on enabling its software development teams to move quickly, collaborate efficiently, and ensure the apps they’re building are secure for customers worldwide.

Nadav Robas, DevOps & DevSecOps Manager at Agoda, says before adopting a DevSecOps platform in 2021, they were spending a lot of time chasing upgrades and security patches. Now that they’re using a single application, Agoda has been able to boost security—while improving the developer experience, keeping developers happier than ever, whether they’re building a mobile app or rolling out support for a new language. “We’re more productive, more secure, and our developers are having a better experience,” he says.

Moving ahead, Agoda is gearing up to use AI features built into the application to further propel their software development and their security. “We’re excited about the AI-assisted features from GitLab, not only for coding, but through the whole software development lifecycle, as aligned with GitLab’s vision,” says Nadav.

Learn how Agoda uses DevSecOps to set up and enforce security policies and shift security left.

CACI better prepared to handle security compliance requirements

CACI International Inc. is a $6.7 billion company whose technology and expertise play a vital role in U.S. national security and government modernization. The company has made a name for itself by delivering critical software and software-enabled hardware to U.S. government agencies, the U.S. intelligence community, and the Department of Defense. One of the reasons they moved to a DevSecOps platform was to increase security, while also boosting efficiency and productivity across the software development lifecycle.

Wesley Monroe, technical project manager at CACI, says they were looking for all the DevSecOps features, like automation, in one application. “With all of the road mapping, issue tracking, and security scanning in one place, it’s hard to even compare it with what we were using before,” he adds.

Meeting government laws, regulations, and standards is critical for a government contractor, so one of the greatest benefits of using GitLab’s platform is that it enables CACI to be prepared to handle emerging security compliance requirements. That means not only being compliant but being able to prove it. With regulatory data tracked and stored all together, the company can attest to meeting security standards, with the data to back that up. “We have positioned ourselves to be able to meet future contract security requirements,” says Kyle Craft, CSDE Service Lead at CACI.

Get even more info about how CACI is using automated testing tools and meeting government regulations.

3x

faster security scanning

“We turned to GitLab to allow us to rethink, and disrupt, the way we develop and build software swiftly, without compromising security.”

Glenn Kurowski,
Senior Vice President and CTO, CACI

Southwest finds scanning consistency, talks the promise of AI

2019

started working with GitLab

> “We want developers to be able to quickly look up a problem, look up a solution, and reduce context switching.”
>
> **Jim Dayton,**
> **Vice President and CISO**
> **Southwest Airlines**

Southwest Airlines Co. is the world’s largest low-cost carrier, with 800 aircrafts, 4,000 flights per day, and approximately 60,000 employees. The U.S.-based company started moving toward a DevSecOps approach to application development in an effort to make their software developers’ jobs easier. The move enabled them to provide developers with more self-service capabilities and knowledge management processes.

Jim Dayton, Southwest’s Vice President and Chief Information Officer, sees promise in AI capabilities built into their DevSecOps process into the platform.

Generative AI, whether in the form of security vulnerability explainers, code suggestions, or code completion, has the ability to dramatically affect workflows across the entire software development lifecycle. Leveraging AI tools built in can increase security and decrease time spent on code reviews and application development. “I think a great example will be when it can provide a solution to a vulnerability that was just identified or when it can tell us what a piece of code is doing,” he says. “What is it integrating with? What data is it accessing and why? Tell me in plain language, for example, that this particular set of coding has been responsible for 20% of the incidents in this application over the past year. That’s where I think AI can help.”

You also can check out this blog post about what Southwest’s chief information security officer sees as the promise of AI.

Want to put these DevSecOps best practices to work?

Get started with a free trial of GitLab's DevSecOps Platform. Or, get in touch with a DevSecOps expert.

Learn more

Talk to an expert >

GitLab

Software.
Faster.