CARFAX improves security, cuts pipeline management and costs with GitLab

CARFAX, Inc., a U.S. company, 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, offering users vehicle information, like odometer readings, number of owners, and damage history. CARFAX receives this information from more than 139,000 data sources, including every U.S. and Canadian provincial motor vehicle agency.

> With DevSecOps, security is always front and center. It's part of every step of the process and not easily missed.
>
> *Mark Portofe, Director of Platform Engineering, CARFAX*

Alleviating toolchain troubles

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, along with new features for its most popular software products. Over the years, CARFAX development teams had amassed a toolchain of DevOps tools that were not meeting all of the company's needs and, even worse, were creating additional challenges.

"We were spending too much time and budget procuring and supporting our toolchain, which had grown to 12 tools," says Mark Portofe, Director of Platform Engineering at CARFAX. "We needed to minimize toolchain maintenance and support as much as possible so our teams could focus on actually creating new feature delivery and not just taking care of all these different tools."

In addition to their efficiency and productivity concerns, CARFAX development teams needed a way to find vulnerabilities earlier in the software development lifecycle. Problems that surfaced during periodic, manual scans, instead of during the development process, were costing the organization time and money. CARFAX wanted to turn that around.

Leveraging GitLab's DevSecOps Platform

To make these needed changes, CARFAX decided in mid-2020 to use GitLab's DevSecOps Platform, specifically GitLab Ultimate. "With GitLab, we knew we'd get a lot of features we could leverage without doing all the stitching together," Portofe says.

To get started, CARFAX first focused on mirroring the codebase into GitLab and leveraging the GitLab security scans across all of their code. This was completed within the first six months. Next, the company began using GitLab for its code repository and CI/CD pipeline capabilities. While there hasn't been a hard migration mandate or time table, software development teams have created plans to use the GitLab platform within their individual product roadmaps. And to help the development teams that were starting to use GitLab, CARFAX established a central team to work directly with them.

GitLab use at the company largely started with customer-facing apps. At the same time, teams began migrating corresponding pipelines for those same applications. Non-customer-facing software, along with large, legacy apps, will have a longer migration path.

"We allowed dev teams to plan it themselves," says Portofe. "We gave a lot of flexibility to our development teams because a lot of their roadmaps had already been baked. Doing it this way created excitement because they saw the benefits of things like security scans and better code insights."

Reducing the toolchain and fragility

In the early stages of using GitLab, CARFAX replaced various DevOps tools in their toolchain. Ultimately, Portofe says they plan to cut their toolchain by about half.

“The full toolchain was costing us money both in license costs and inefficiencies,” says Portofe. “By using GitLab, we saw a huge increase in security scanning because CARFAX was then able to scan the whole codebase without manual steps. And it gave us a much better picture of our security vulnerabilities. We saved money and increased security.”

He also points out that reducing the toolchain streamlines engineers’ workloads, increases productivity and efficiency, and makes the entire development and deployment effort more stable.

“There was some general fragility with other tools we have used in the past and we’re not seeing that with GitLab,” says Portofe. “Indirectly, it’s a benefit for the whole business. That’s what it’s all about, really — how to be as efficient as possible to get features out to customers.”

Increasing security with automation and a shift left

Another aspect of GitLab’s DevSecOps Platform that added efficiency was its built-in automation, which brought a whole new level of security.

CARFAX has been able to use GitLab’s automated security features to do dependency and container scanning, as well as secret detection. “Prior to using GitLab, performing security scans on our codebase was a manual, cumbersome task. It’s much easier today,” says Portofe. “While security is always an ongoing battle, GitLab’s security features are making it easier for developers to spot issues early.”

The platform’s automated scanning has enabled CARFAX to find nearly one-third of its vulnerabilities much earlier in the development lifecycle over the past year.

And Portofe points out that using a platform has the entire development team thinking about security at the earliest point in the software lifecycle. By shifting their focus on security as far left as possible, they’re considering security needs and implications as they are coding and not later downstream — when it’s more difficult, more expensive, and less efficient to fix any problems.

“We are always thinking about security while we design and build software,” he says. “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.”

20%

boost in deployments YoY

30%

of vulnerabilities found earlier in SDLC

12 tools to 1

Growing deployments with a smaller team

CARFAX has made some serious productivity gains with DevSecOps. By automating processes, shifting security left, and reducing toolchain complexity, teams have been able to simplify processes, boost productivity, and increase deployment velocity. In 2022 alone, the company saw a 14% increase in production deployments.

“It seems that everything is just cleaner now when moving code to production,” says Portofe. “We’re putting out more new product features because teams are spending more time creating code than making sure their pipelines are running.”

And what’s even more impressive about this increase in deployments is that CARFAX is making that happen with a smaller team.

The company’s tooling team, which is focused on building common pipelines and utilities that CARFAX’s approximately 250 software engineers can use to build code, normally has five members. However, they’ve been down to just two for a while and they’re still making productivity and deployment gains. “The platform has allowed us to operate as a two-person team and still keep things going,” says Portofe. “Actually, our production deployments, overall, went up roughly 25% for the first five months of 2023, compared to the previous five-month period. It’s pretty amazing.”

Easing a cloud migration

CARFAX, which leverages Amazon Web Services (AWS) capabilities, has had different teams with different assets on the cloud over time. They’ve also had some on-premises infrastructure. It’s been a mixed environment. Now, though, they are migrating most of their infrastructure, servers, and codebase to the cloud, with the help of GitLab.

“Going down this path, it’s helpful that GitLab has tools to make the move to the cloud easier,” says Portofe, adding that they also are consolidating their cloud compute platform.

And he adds that GitLab’s platform allows CARFAX to be cloud agnostic. “When we go to commonize our CI/CD pipelines, we can move them with a common on-ramp that makes it easier,” says Portofe.

All information and persons involved in case study are accurate at the time of publication.

