

How We Delivered a Secure DevOps Foundation for the Growth of a UK-based Bespoke Claims Platform

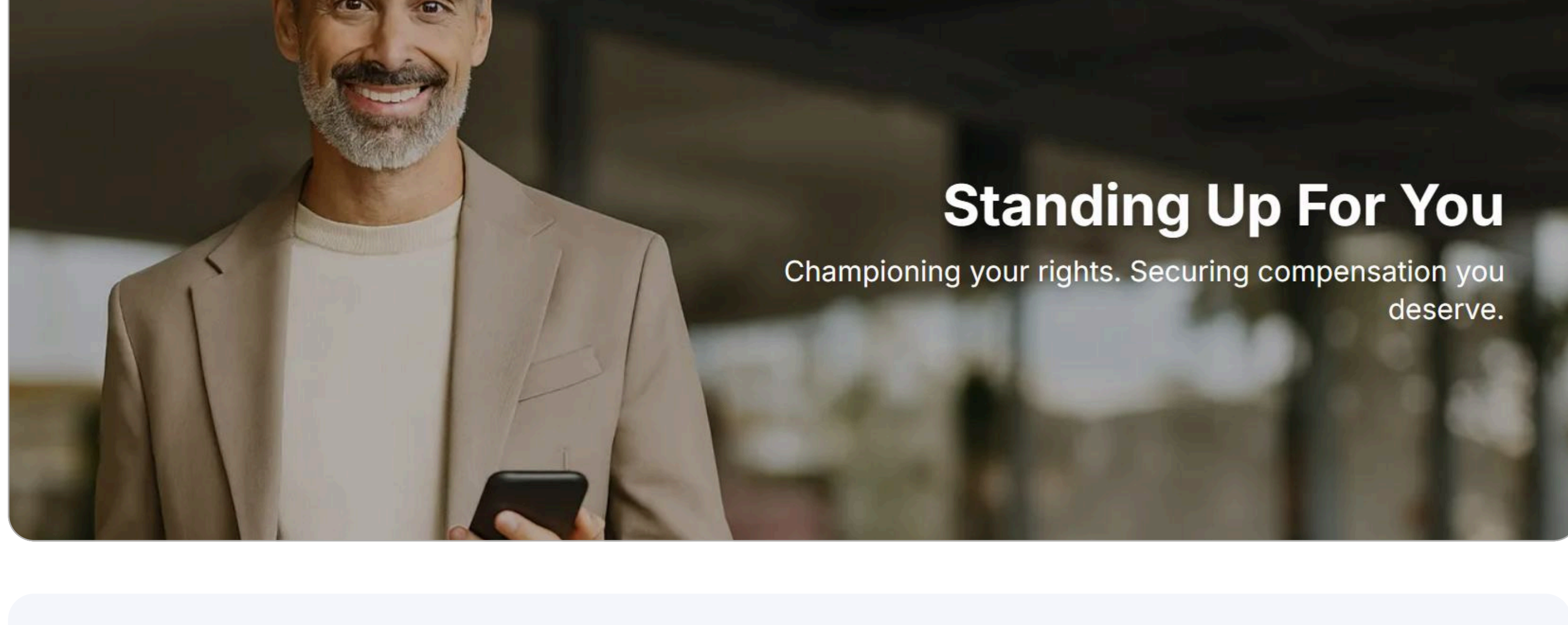
Ashworth & Ingram Compensation Partners is an FCA-regulated claims management firm located in the UK, with a focus on housing disrepair.

The firm's expertise in housing disrepair is reflected in its specialist brand, Council Repair Claims, which provides guidance and support to social housing tenants dealing with disrepair issues. Practical information on housing disrepair claims, tenant rights and landlord responsibilities can be found on their website at www.councilrepairclaims.co.uk.

To manage the process more effectively, Ashworth & Ingram created the ClaimHub Pro platform from the bottom up.

All parties involved in a claim can conveniently use the same system: tenants submit cases, administrators handle them, and law firms take care of the legal work.

Tenants start by reporting the condition of their property and providing other relevant details. ClaimHub Pro then arranges this data, while a claim handler conducts an initial evaluation to determine if there could be a legitimate legal claim. If claims move past this step, they are sent to a partner law firm, which takes over the legal process.



Jump straight to a key chapter

- [Project Description](#)
- [Provided Services](#)
- [Work agenda](#)
- [Project Challenges](#)
- [Solutions](#)
- [Results](#)
- [DevOps tech stack](#)

Project Description

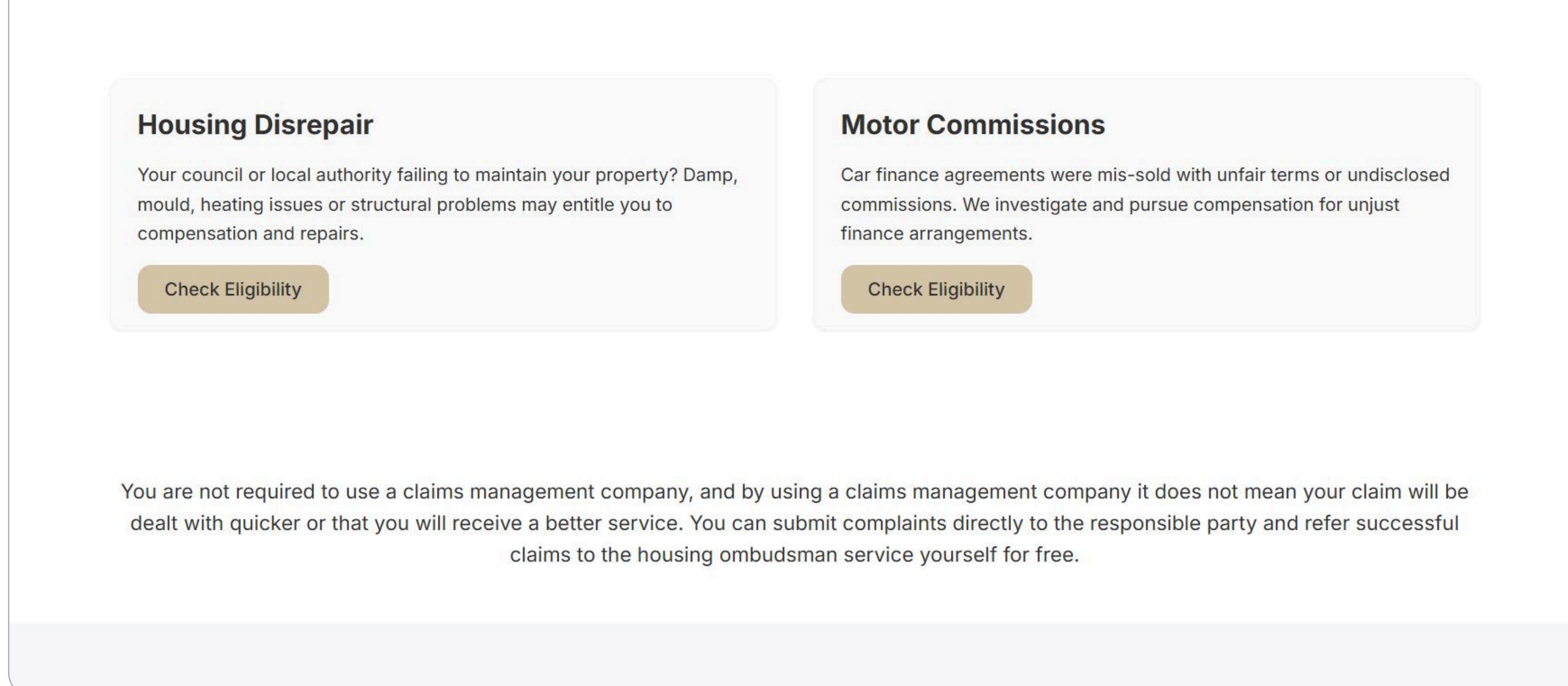
When we joined the project, a production version of ClaimHub Pro was already developed, and several infrastructure decisions had already been made.

For instance, the client was using Vercel to host the product, which allows for reducing the amount of infrastructure teams have to manage themselves. It is a cost-effective option startups often choose in their early stages.

Yet, ClaimHub Pro still lacked some essential DevOps processes, and the client was looking for a partner to run the operational side. We needed to prepare the production infrastructure and deployment processes for the onboarding of the platform's first clients, receive Cyber Essentials certification (to adhere to the UK Government-backed standard for protecting against cyber threats), and help ensure ClaimHub Pro was technically ready for the road ahead. Additionally, we needed to check whether the infrastructure met GDPR and relevant FCA requirements, with the goal of maintaining and improving compliance as the platform grows.

Our team began the project with a technical discovery and DevOps assessment focused on the infrastructure, access management, CI/CD processes, monitoring, backup strategy and production readiness. We also performed a high-level security review and worked alongside our security and compliance partner, whose findings were included in a separate security risk assessment and GDPR/FCA readiness report.

Additionally, during our assessment, our team evaluated whether the existing technology stack would continue to support the platform's growth or whether architectural changes should be considered in the future.



Provided Services

- CI/CD automation
- Disaster recovery as a service
- Security assessment
- Access control and identity management
- Operational cost optimisation

Work agenda

Client Ashworth & Ingram Compensation Partners Limited, developer of ClaimHub Pro, a claims management platform for UK housing disrepair cases	Project goals Establish a reliable operational foundation for ClaimHub Pro so the client could onboard new customers with confidence
Location UK	 Implement an access model across all platform components to ensure adherence to best practices for separating production and non-production environments and regulatory compliance
Technical team 2 DevOps engineers PM	 Create a safer and more predictable way to test, approve, and release changes
Project timeframe February 2026 - ongoing	 Make platform issues easier to detect and resolve
	 Set up reliable backups and disaster recovery so the service and its data could be restored in case of data loss or an outage
	 Prepare the client for Cyber Essentials certification
	 Build a DevOps setup that supports the company's goals at a price the client could justify

Project Challenges

01 Compliance risks from overseas production access	While the client operates in the UK, their development team is based overseas. Technical components such as hosting, databases, file storage and source control were all managed within a shared environment model. To align with regulatory expectations and best practice, the existing access model required further formalisation, including clearer separation between production and non-production environments and stronger governance, oversight, and access management across platform components.
02 Missing CI/CD and release controls	The platform had no CI/CD pipeline to automatically test, build, and deploy changes. It also lacked release controls such as required reviews and branch protection.
03 Unclear error reporting and noisy alerting	The platform's monitoring setup had to be reviewed and adjusted. For instance, Sentry, an error-tracking tool, was already connected, but it was configured in a way that it did not offer clear enough information to help the team resolve issues. For example, the tool generated too many alerts, many of which were not useful, and the error reports did not point back to the original source code but to minified code. This made it harder to understand what had gone wrong and actually fix issues.
04 No backup and disaster recovery plan	ClaimHub Pro was designed to store sensitive information, including claim details, personal data, and supporting documents. However, the platform had no system for backing up its data and files. A tested process for restoring data and bringing ClaimHub Pro back online after an incident was required to be in place, too.
05 Access controls not fully aligned with Cyber Essentials requirements	To meet the requirements for Cyber Essentials certification, access to the main systems needed to be assigned according to each user's role and responsibilities. Multi-factor authentication also needed to be enabled across the necessary areas.
06 A tight, cost-sensitive budget	Last but not least, as the business is still at an early stage, the DevOps setup has to be both effective and affordable. We therefore focused on solutions that could meet the company's objectives while keeping costs at a level the client could justify.

Solutions

	1. Production access restrictions and development environment separation Our team adjusted access across the platform to deliver a clean separation of environments and well-documented access minimisation. We also set up a separate database organisation for non-production environments. The migration of the client team's access and CI/CD credentials to the new non-production setup is currently in progress.
	2. Automated CI/CD checks and controlled production releases We introduced a release process so changes could no longer go straight into the live platform. Each update now goes through automated linting, formatting, type checks, tests and schema validation. Additionally, our engineers added protection to the dev and main branches. A change can reach the main branch only after it has passed all checks and been reviewed and approved by the client's release group. This gives the client a final say before each production release, as they specifically requested.
	3. Improved error monitoring and direct Slack alerting The error-tracking setup was reorganized to make error reports point to readable source code instead of minified code and reduce unnecessary alerts. We also configured monitoring of the main processes such as login, webhooks, scheduled jobs and server-side errors. Alerts reach the team directly in Slack.
	4. Backup setup and recovery planning For the backup solution, we set up Amazon S3 as a dedicated backup location, separate from the client's existing storage setup. Production files are copied there every week, while development backups can be started when necessary. Our team also documented the backup process for the client. The next step is to run a full recovery test.
	5. Role-based access, MFA, and security scanning Now, access is set up for all the client's systems. We reduced the default permissions and introduced a team-based access model. There is a documented access matrix that shows who can use each system and what permissions they have. Designated code owners are responsible for reviewing changes to specific parts of the codebase. Multi-factor authentication is also being enabled wherever it can be supported. Furthermore, security scans now happen automatically as part of the CI/CD pipeline. They check dependencies for known vulnerabilities and scan the code for possible security issues.
	6. Cost-conscious approach to infrastructure On each project, we look for solutions that are both effective and cost-effective. Our team at IT Outposts took the same approach with ClaimHub Pro. For instance, when it came to monitoring, the client had an option to rely on a paid observability platform. However, this solution, although a bit faster to configure, would have led to higher operating expenses. Our engineers created a similar setup using low-cost client resources like Oracle Cloud along with Grafana, Prometheus and Loki. Additionally, we configured budget alerts and checks for unusual spending, which allow the Ashworth & Ingram team to notice any increase in costs promptly.

Results

	Automation and improved infrastructure enabled Vidy to release new features and updates much quicker.		Security checks were added across the delivery pipeline
	Automated testing and controlled production releases were introduced		Better cost visibility thanks to configured budget alerts
	Potential issues are now flagged directly in Slack, helping engineers investigate them before customers report them via support tickets		Cyber Essentials certification was achieved
	Regular data backups were put in place		The platform gained a stronger operational foundation for secure, compliant, and cost-effective growth

We replaced a mix of customer-managed setups with a unified, centrally managed platform. This simplifies daily operations, reduces costs, and provides better performance. Our hybrid architecture design offers a great balance of price and performance for Europe and covers data residency requirements.

The platform is already configured to support country-specific deployments and can easily handle different subscription options.

DevOps tech stack

