CI/CD & AI Trends: Stay Updated in 2024

Future CI/CD & AI: Stay Updated in 2024

As AI/ML transforms our world, 2024 brings exciting IT advancements.

The CIO Report notes 82% of organizations update software every 12 hours or less in UK, thanks to AI boosting automation in CI/CD processes. In United Kingdom, where 30% of time is manual, this collaboration streamlines processes for innovation.

Yet, integrating AI technologies isn't plug-and-play.

Expertise is crucial for secure incorporation, choosing solutions that align with future innovations and current infrastructure parameters.

Plot

Chapter 1
Navigating SaaS for different usage

Chapter 2
CI/CD Trends for SaaS Providers

Chapter 3
Data Poisoning in LLM Training

Chapter 4
Unit Test Automation by AI Integration

Chapter 5
Roadmap for Implementing AI in CI/CD

Chapter 6
Our Expertise

The SaaS Landscape: Personal vs. Company Usage:

According to the Developer Ecosystem Reports, let's kick off with a glance at how different SaaS vendors are utilized, both for personal needs and within corporate environments.

As we see, GitHub Actions remains the most common choice for personal use, while companies tend to prefer Jenkins.

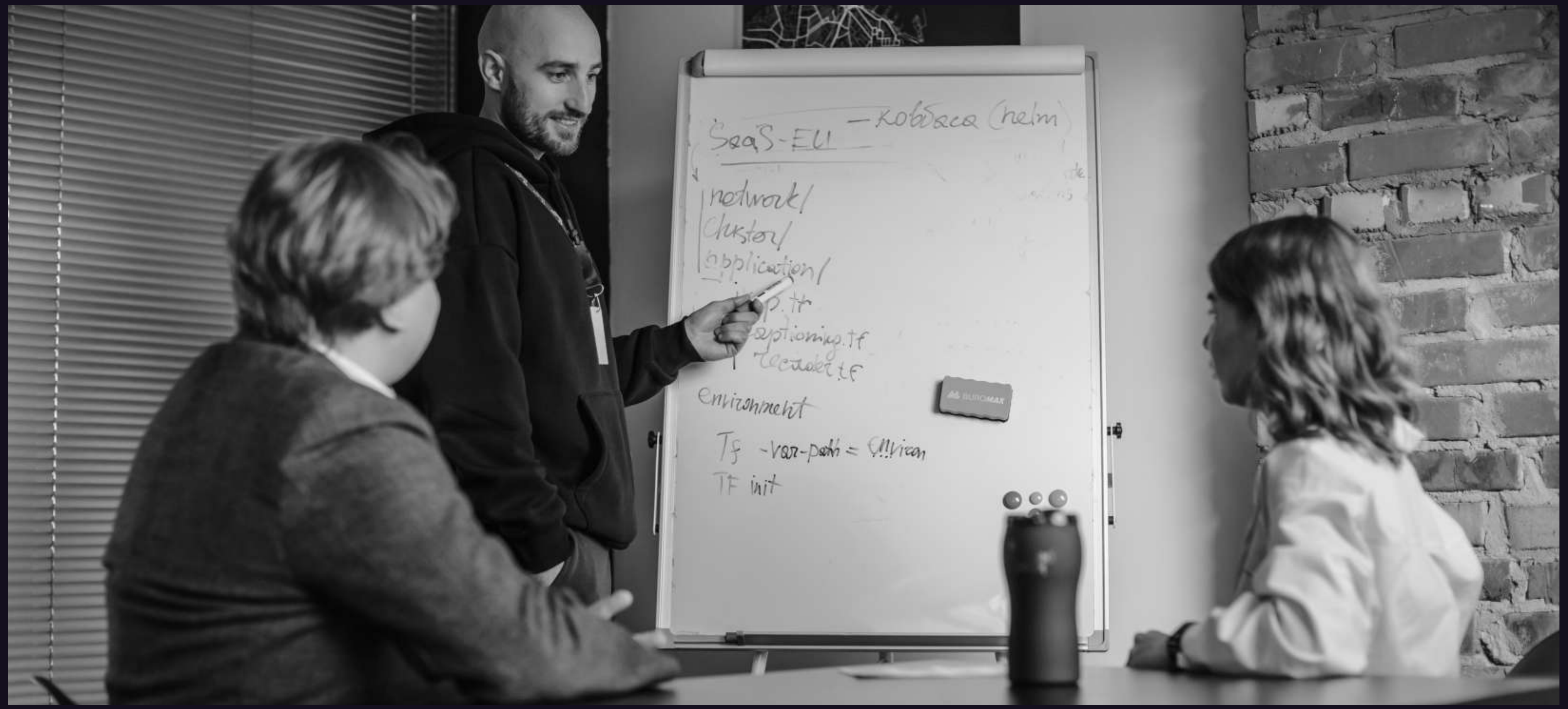
Total	Company	Personal	
53%	27%	42%	GitHub Actions
52%	47%	12%	Jenkins
35%	27%	17%	Gitlab CI

But what about reviewing and analyzing the AI-related roadmaps?

What are the implications of AI in CI/CD pipelines for the TOP 3 CI/CD SaaS vendors?

CI/CD Trends with GitHub, GitLab, and Jenkins

Jenkins is known for its customization options, dominating 47% of corporate environments. However, GitLab and GitHub, actively embrace AI and offer native integrations that contribute to accelerated development cycles and enhanced software quality.

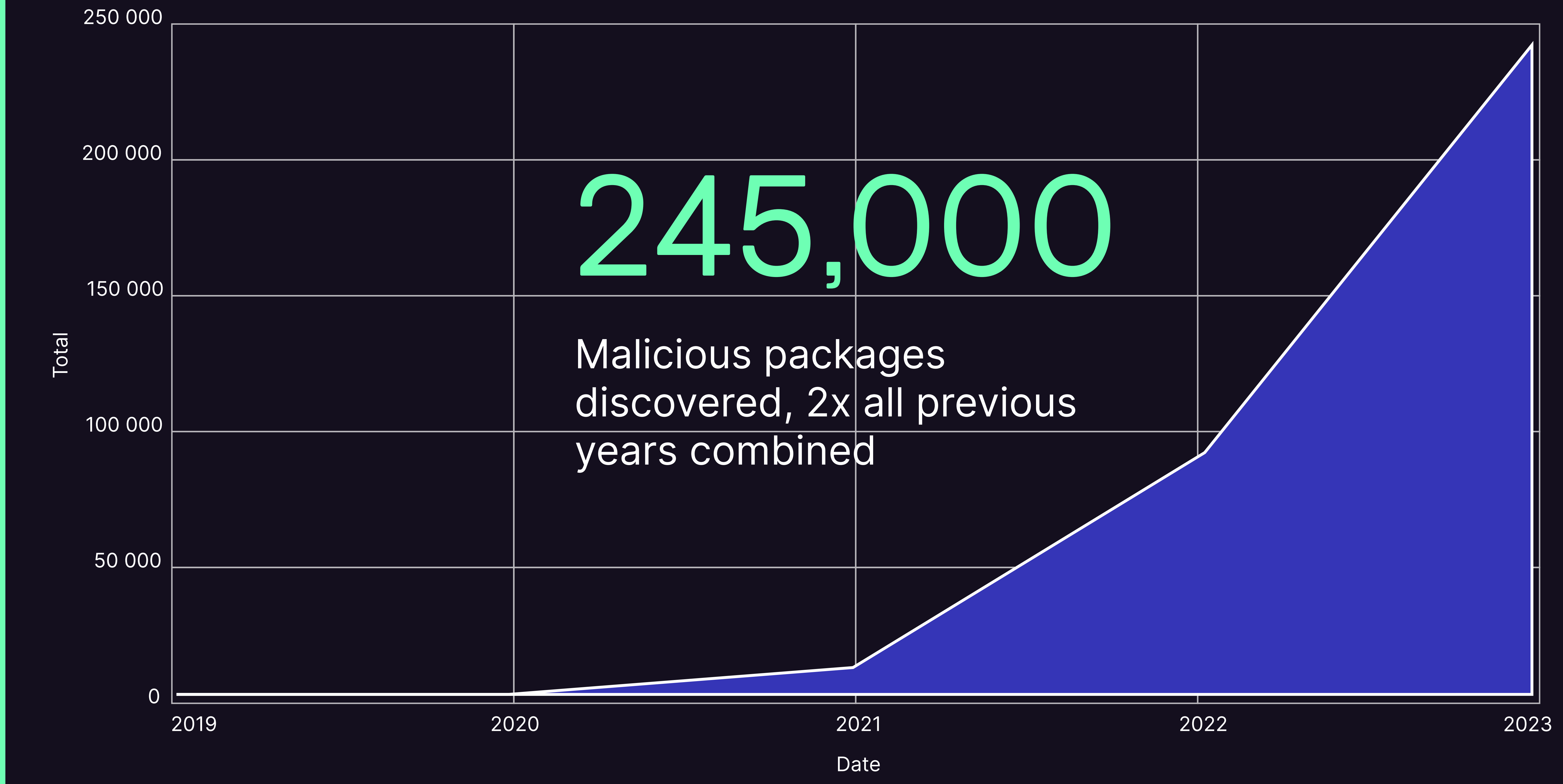


	GitHub	Jenkins	GitLab
AI Implementation	GitHub Advanced Security powered by AI.	No specific plans for AI shortly.	Generative AI Assistant, predictive analysis, security capabilities, and test generation in alpha/beta testing stages.
Security Focus	Almost 40% of the 2024 roadmap is dedicated to GitHub Advanced Security.	Unique focus on core development, including UI, RBAC, and plugin management.	Heavy investment in AI products as part of their DevSecOps offering.
Supply Chain Measures	Preventive measures include secret scanning, advanced vulnerability scanning, and preventing PR merge in case of security threats.	Not applicable due to the unique nature of Jenkins' open-source plugin foundation.	GitLab Duo features include a Generative AI Assistant, that analyzes code, predicts SDLC trends, identifies vulnerabilities, and generates unit tests, and integrates them with CI/CD.
Future Predictions	Predicted to introduce static code scanning, a framework for vulnerability scanning, and built-in DLP mechanisms.	Has no immediate plans to integrate AI due to its reliance on open-source plugins.	The majority of AI-powered features are in alpha or beta-testing stages, with a focus on stabilizing and improving over the next year.

GitHub's Proactive Security Approach

Sonatyte reports a staggering **700% yearly growth in** supply chain attacks. In 2023 alone, **245,000** malicious packages were uncovered, doubling the total from all previous years combined.

FIGURE 1.7. NEXT GENERATION SOFTWARE SUPPLY CHAIN ATTACKS (2019-2023)



245,000

Malicious packages discovered, 2x all previous years combined

Those a truly mind-blowing numbers and alarming news for 2024.

What's the solution? Avoiding AI altogether, or harnessing it effectively?

Let's delve into the impact on the CI/CD landscape with real-world examples, examining both the positives and challenges.

Data Poisoning in LLM Training

Challenge:

The AI ecosystem faces a risk of data poisoning attacks, marked as ML02:2023 by OWASP. This attack involves manipulating training data to make the model behave undesirably. While still a relatively new threat, notable examples include a group attempting to overflow Google's SPAM filters to alter email classifications.

Solutions we recommend:

Although there isn't an out-of-the-box fix, treating this attack as a supply chain issue suggests **these recommendations:**

1. Version the training dataset and track hash sums for each file.

2. Apply the same release process policy to ataset changes as you would to code.

3. Restrict dataset access through Role-Based Access Control (RBAC).

4. Implement audit logging, monitoring, and alerting.

Results:

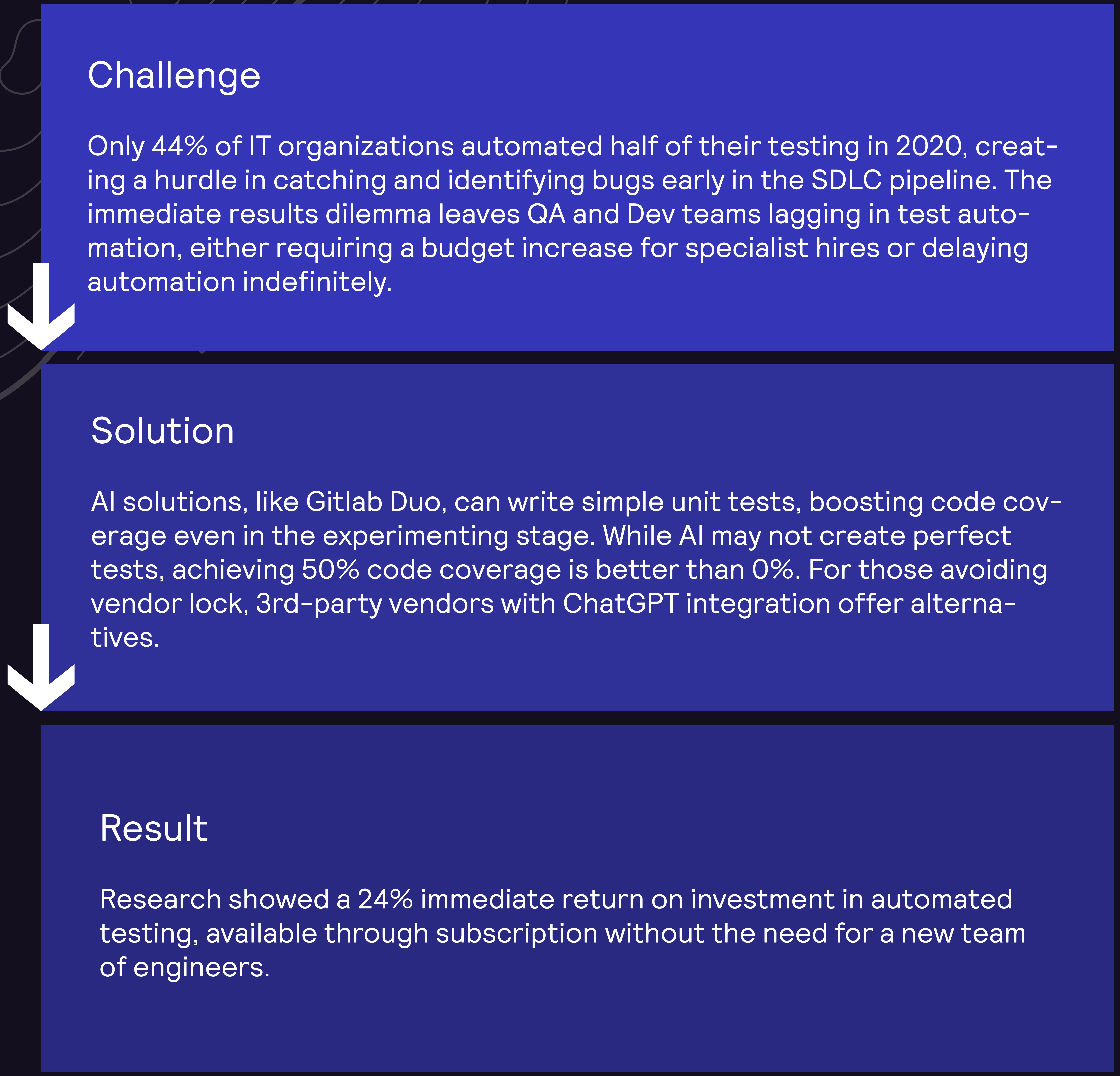
This minimal set of measures ensures awareness of any training dataset modifications and provides both proactive and reactivedefense mechanisms.

Unit Test Automation by AI Integration

AI vendors, in their pursuit of data for training models, often encounter ambiguous EULAs regarding personal data usage. User errors can lead to severe consequences, as seen in cases like ChatGPT and Samsung. Let's explore the details:

What do we recommend?

Choose a self-hosted AI option for flexibility, avoiding vendor lock, and improving testing effectiveness. Take cues from cases like ChatGPT and Samsung, where self-hosted models could have been a valuable alternative.



Challenge

Only 44% of IT organizations automated half of their testing in 2020, creating a hurdle in catching and identifying bugs early in the SDLC pipeline. The immediate results dilemma leaves QA and Dev teams lagging in test automation, either requiring a budget increase for specialist hires or delaying automation indefinitely.

Solution

AI solutions, like Gitlab Duo, can write simple unit tests, boosting code coverage even in the experimenting stage. While AI may not create perfect tests, achieving 50% code coverage is better than 0%. For those avoiding vendor lock, 3rd-party vendors with ChatGPT integration offer alternatives.

Result

Research showed a 24% immediate return on investment in automated testing, available through subscription without the need for a new team of engineers.

Roadmap for Implementing AI in CI/CD

Step 1

CI/CD Base for Successful AI Integration

Step 2

Select AI-Integrated CI/CD Platform

Step 3

Build Predictive Models with testing and validation

Step 4

Continuous Monitoring and Security Integration

Step 5

Get Impact on CI/CD with AI Integration

Step 1

CI/CD Base for Successful AI Integration:

Take action now by exploring the roadmap to avoid common mistakes seen in various cases.

See if your CI/CD base can leverage AI benefits.

Automation:

- Automated builds and tests are stable and reliable.
- Continuous integration is triggered with each code commit.

Testing:

- Automated end-to-end tests provide meaningful coverage.
- Continuous testing is an integral part of the CI/CD pipeline.

Deployment Frequency:

- Deployment frequency is optimized based on project requirements.
- Rollbacks are automated and tested.

Stable Infrastructure:

- IaC is implemented for consistent environments.
- Autoscaling is in place for handling increased workloads.

Security:

- Security scans are automated and integrated into the pipeline.
- Access controls and permissions are well-defined.

Monitoring and Feedback:

- Monitoring dashboards capture relevant metrics.
- A feedback loop for continuous improvement is established.

Resource Management:

- Resources are dynamically allocated and released as needed.
- Resource bottlenecks are identified and addressed.

Compliance and Governance:

- Compliance checks are integrated into the CI/CD pipeline.
- Governance policies are well-defined and followed.

Step 2

Select AI-Integrated CI/CD Platform:

Selecting the right CI/CD platform with AI integration is crucial for streamlined development.

While Jenkins dominates with customization, it lacks a clear AI integration plan. On the other hand, GitLab and GitHub actively embrace AI, promising seamless integrations for faster development cycles and mproved software quality. Choose wisely for optimal efficiency in your workflow.

> Concerned about compatibility? Customize your options! We've got you covered with an alternative solution.

Alternative Approach - Hosting AI Models

There is an alternative way to harness the benefits of AI, – host the models yourself.

Leaked code and data breaches – not a good scenario. Hosting models on your own is a choice that helps avoid such problems.

While self-hosting may take more time and resources than using SaaS vendors, it is a more secure option with a wider selection of models.

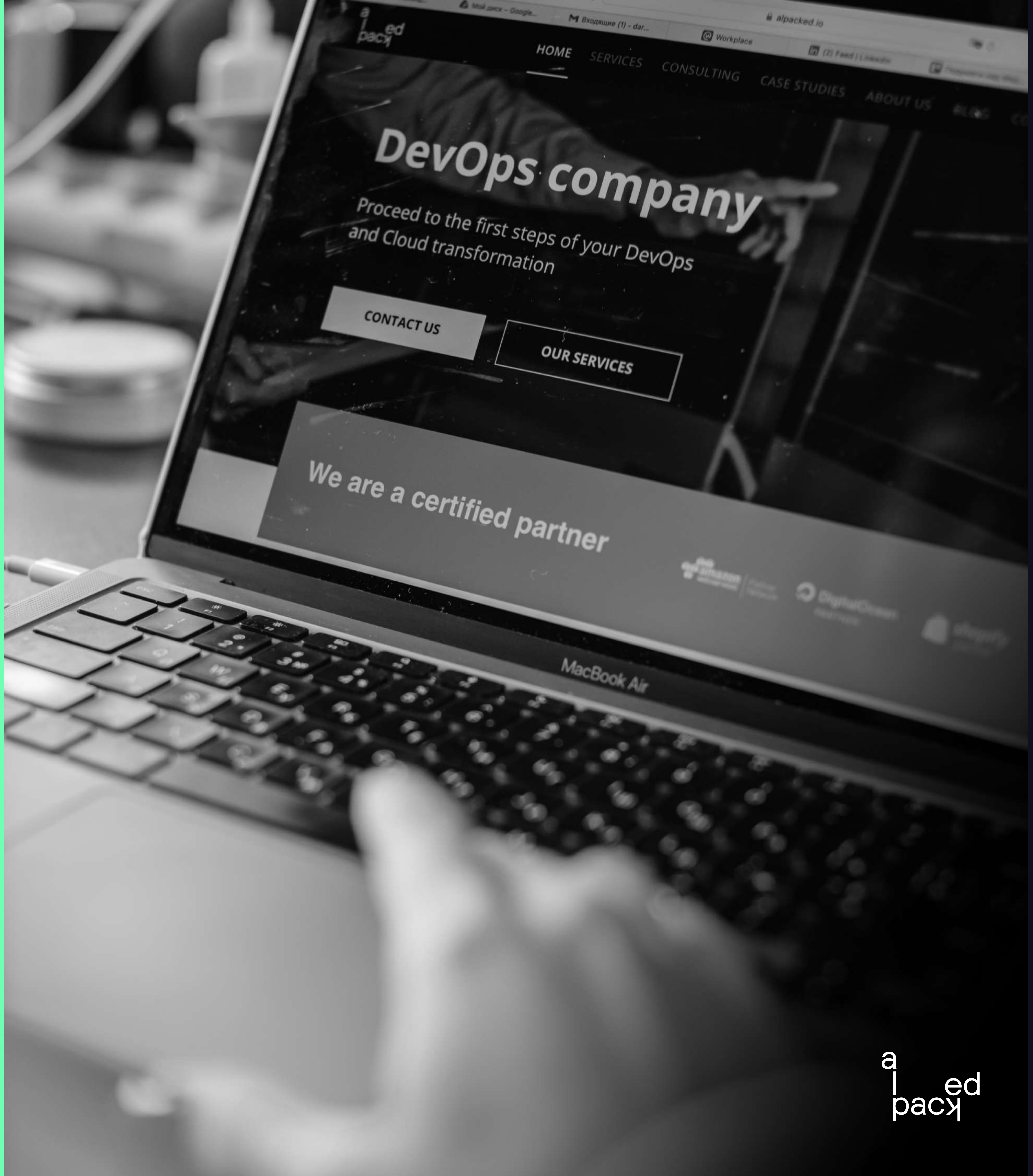
Step 3

Build Predictive Models with testing and validation:

Use historical data to train models for predicting build success/failure, deployment success/failure, and performance issues.

Validate models using separate datasets to ensure accuracy and reliability.

Perform A/B testing to compare the new AI-enhanced process with the traditional one.


HOME
SERVICES
CONSULTING
CASE STUDIES
ABOUT US
DevOps company
Proceed to the first steps of your DevOps and Cloud transformation
CONTACT US
OUR SERVICES
We are a certified partner
MacBook Air

Step 4

Continuous Monitoring and Security Integration:

Implement monitoring of the CI/CD pipeline using AI.

To detect and alert on anomalies or deviations from expected behavior.

Utilize AI-driven Risk Assessments to automate security scanning of code and dependencies. Companies planning to leverage AI with sensitive intellectual property should acquaint themselves with these practices and data or begin implementing such features.

Step 5

Get Impact on CI/CD with AI Integration

AI significantly reduces manual efforts, enabling teams to concentrate on strategic tasks. It also minimizes response time to accurate issues, providing early notifications and suggesting solutions for emerging problems.

For those with reservations, consider establishing a sandbox where AI recommendations undergo evaluation by in-house or hired experts. This process not only validates the AI but also refines it with valuable insights from top-notch DevOps professionals, amplifying the impact and efficiency of your business.

Our Expertise

Discover how Alpacked can elevate your CI/CD strategy.
Our expertise ensures a secure and efficient implementation, bringing measurable success to your business.

Our Approach:

- Explore the roadmap to avoid common mistakes and gain a competitive edge.
- Ship to your users 55% faster, building a more loyal customer base through faster adaptation and fewer errors.
- Foster a culture of innovation, boosting team productivity by 35%.
- Focus on accelerating existing processes, reducing technical debt and turnover by 25%.
- Enable rapid feedback loops for seamless alignment with user requirements.

Learn more here

> In the first few months of the project, incidents decreased by 90%. Their collaborative approach made them feel like part of the client's team. They efficiently commnicated well across time zones via email and adjusted to the client's workflow.
>
> \- Founder and CEO of BairesDev

Contact Us

Alpacked is a DevOps firm that offers a wide range of end-to-end services, from consultancy to managed services. We believe in transforming software development processes to drive innovation and efficiency. With a commitment to excellence, our CI/CD consultation and implementation services redefine the way you approach software delivery.

Scan to book a call

Learn more about Alpacked at our website, or contact us directly today!