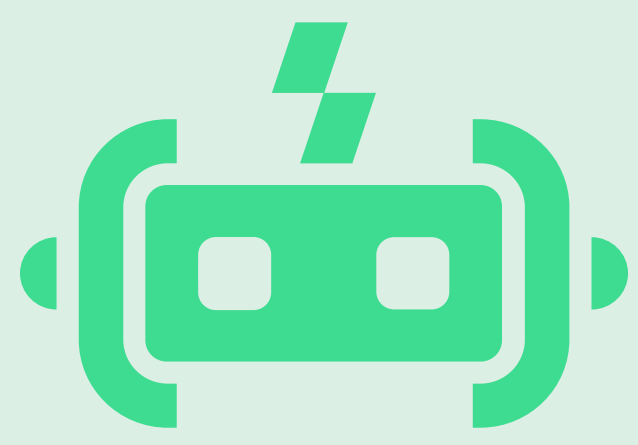


Continuous Quality Journey:

3 Test Strategies to Mitigate Risk and Enhance Compliance



You only live once (YOLO!). Seize the day. Throw caution to the wind.

While this is great advice for living your best life, it can be a terrible approach to creating your best apps. Innovation or growth shouldn't come at the cost of your customers. Take a moment to think about what an outage might mean to lives (or just ask customers of Sonos or CrowdStrike), or the damage a security breach could mean to their data.

While a move-fast innovation mindset is the goal, it can't come with a break-things ethos. The cost of ignoring risk can be dire: with downtime costing an average of \$5,600 per minute¹ and 76% of companies saying they suffered downtime in 2022,² businesses are already just one inadvertent bug away from major financial issues. That's why testing plays a crucial role in helping developers identify and remediate vulnerabilities to ensure the security of sensitive data, reduce the risk of cyberattacks, and maintain customer trust.

By leveraging a continuous quality testing strategy, you can improve your risk and compliance management by catching minor bugs before they become major security issues. This ability to reduce risk and enhance compliance is a key reason why Gartner® believes that 70% of engineering teams will shift to a continuous quality approach by 2026, up 20% from just last year.³

Per Gartner, "A continuous quality strategy fosters a companywide cultural change to drive quality ownership and engage everyone in achieving the set quality goals. It shifts focus from testing (an activity) to quality and digital immunity (outcomes) and encompasses the practices that help mitigate risks before progressing to subsequent stages of the software development life cycle."

In this guide, you'll learn how enterprise companies leverage testing strategies rooted in continuous quality to enhance their risk and compliance management. By understanding how leading organizations leverage continuous quality, you'll learn how to use testing to protect your organization, your users, and your bottom line.

¹ [Atlassian](#), Calculating the cost of downtime.

² [Acronis](#), Cyber Protection Week Global Report.

³ Gartner, Innovation Insight: Continuous Quality, By Joachim Herschmann, Thomas Murphy, Jim Scheibmeir, 17 October 2023.



Inaction Has Consequences

Why is quality code necessary? Consider this: 70% of users agree that a poor digital experience impacts their decision to purchase,⁴ while over 50% will consider switching to a competitor after just 3-4 negative interactions with a website, software, or mobile app.⁵

Not only do you have to worry about customer churn due to buggy products, but poor quality code is bait to hackers and cybercriminals; with the average cost of a data breach in the US reaching nearly \$9.5 million,⁶ your approach to risk and compliance has a real and significant cost.

For many organizations, their developers' approach to risk and compliance is likely more laissez-faire than anyone realizes:

68%

of developers have merged their own pull requests without a review.

67%

of developers admit to pushing code to production without testing.

61%

of developers admit to using untested code generated by ChatGPT.⁷

It's not that developers are lazy or malicious; it's that time is money. If they want to get code out the door, then a time-consuming task like testing represents an obstacle, not an opportunity for improvement. But in a world where it paradoxically costs nearly three times as much to be out of compliance than to maintain compliance,⁸ why does reducing risk still take a backseat?

^{4, 5} Sauce Labs, Every Experience Counts. 2024.

⁶ IBM, Cost of Data Breach 2024.

⁷ Sauce Labs, Developers Behaving Badly. 2023.

⁸ Globalscape, The True Cost of Compliance with Data Protection Regulations, 2017.



The answer is that the old-school approach to testing isn't built for the needs of today's organizations:

Testing is expensive

Developers who spend their time testing aren't spending their time coding. In fact, inefficient testing processes can cost up to 15 hours per week per developer.⁹ As a result, organizations must either pull developers away from the money-making work of generating new code to find and fix potential security flaws or cut testing back to the bare minimum and roll the dice. Guess which one many choose?

Testing doesn't scale

While almost half of organizations have doubled their application production in the past three years,¹⁰ two-thirds haven't been able to scale their current testing strategy alongside production.¹¹ When testing is a bottleneck, it becomes easy to skip it to get a product on track and out the door.

Testing is hard

Developers have to ensure their code works perfectly not only once but across an average of 82 unique device/OS/browser combinations.¹² The time and cost it takes to maintain all these options is a key reason why organizations say that maintaining their testing infrastructure is the toughest challenge facing their mobile application development efforts.¹³

Testing is difficult to secure

While testing is meant to improve your security, the way you test can actually introduce security issues. That's because few testing platforms are fully certified with major security certifications such as SOC 2 Type II, ISO 27001, and ISO 27701, or use the highest level of secure proxy tunnels to connect their test platform to their IT infrastructure.

⁹ ESG, Economic Validation: Analyzing the Economic Benefits of Sauce Labs for Mobile Testing and TestOps, April 2023.

^{10, 11, 12, 13} ESG, Economic Validation: Analyzing the Economic Benefits of Sauce Labs for Mobile Testing and TestOps, April 2023.



3 Ways to Continuously Manage Risk and Compliance

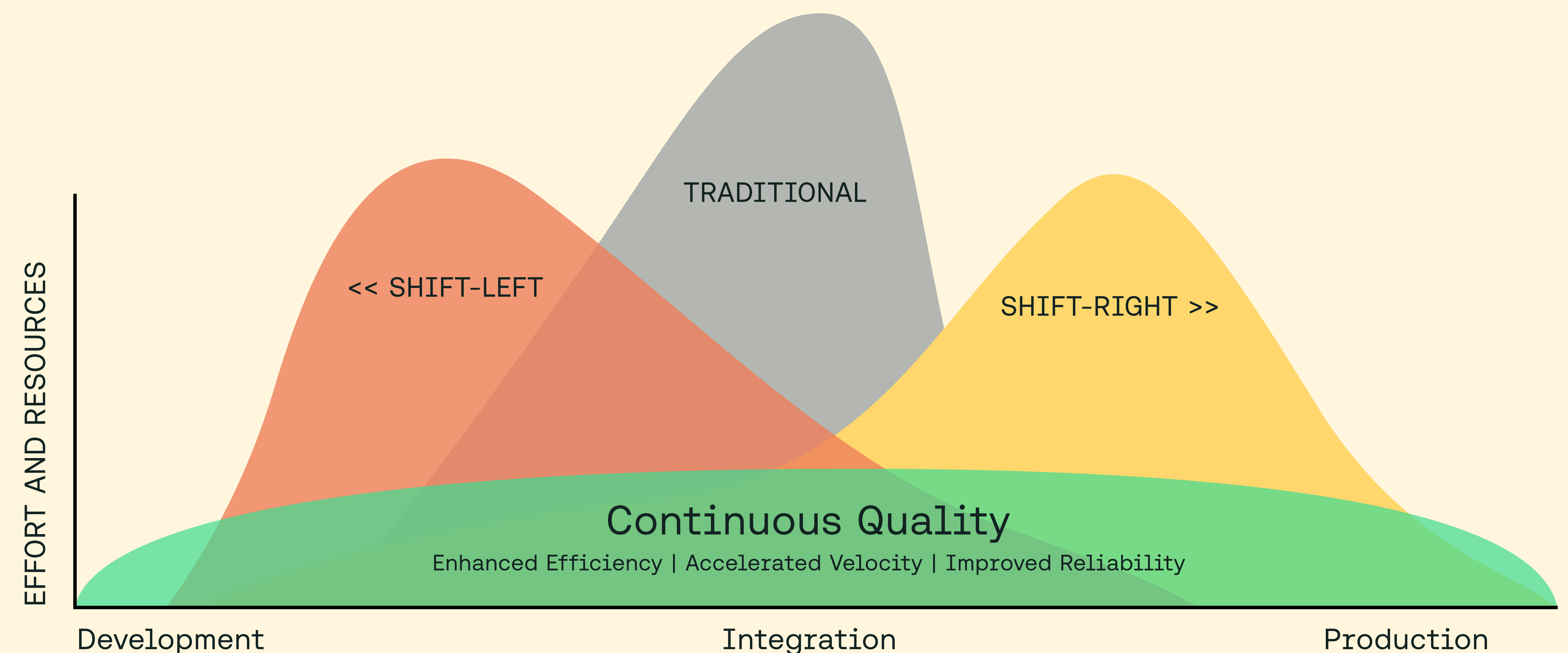
The best way to reduce risk and improve compliance is to embrace it as a core purpose, not a checkbox.

With a testing strategy driven by continuous quality, testing is no longer relegated to a specific stage or line item. It is instead something that is continuously and regularly done across every stage of development. By shifting testing both left and right across the software development lifecycle (SDLC), a continuous quality approach empowers developers to produce better code the first time, get rapid feedback on their code when it's still easy to implement improvements, and catch unexpected bugs before they escape into the wild.

Leveraging an automated, end-to-end testing platform purpose-built for enterprises allows your organization to use powerful AI-augmented tools to detect bugs and errors faster, at less cost, and at enterprise scale.

The proper testing platform provides everything you need to manage your testing infrastructure from top to bottom, allowing you to effortlessly scale your testing program while maximizing engineering productivity.

This efficient system allows developers to overcome the testing complexity that often holds quality control back and introduces unnecessary risk or compliance issues.



Here are the three key components to look for in an automated testing platform to improve your risk and compliance management program.



Reduce risk with automated testing throughout the SDLC

How can you ensure that your developers are catching all your critical bugs when you're using a manual testing process? Answer: You can't. But with an automated test platform, you don't have to worry if software-crashing bugs are slipping through the cracks.

The right automated test platform should:

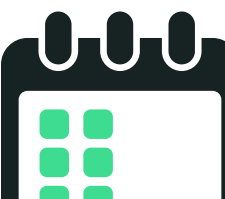
- Allow you to execute thousands of parallel tests at every development stage for unparalleled extensibility, flexibility, and scalability across the SDLC
- Let you use a private device cloud to test thousands of device, browser, and OS combinations using your framework of choice to ensure your standards for risk and compliance are met
- Make it easy to use different testing tools at various stages of the SDLC so you can run tests earlier with virtual machines, use real devices for real-world scenarios, and use private devices for a higher degree of control and security
- Be SOC 2 Type II, ISO 27001, and ISO 27701 certified so you have confidence that your testing platform meets your compliance requirements

The quality and business benefits of an automated testing solution

 **95 %**
More issues caught during QA and testing¹⁴

 **217 %**
ROI¹⁷

 **0**
App issues impacting the business per year (down from 4)¹⁵

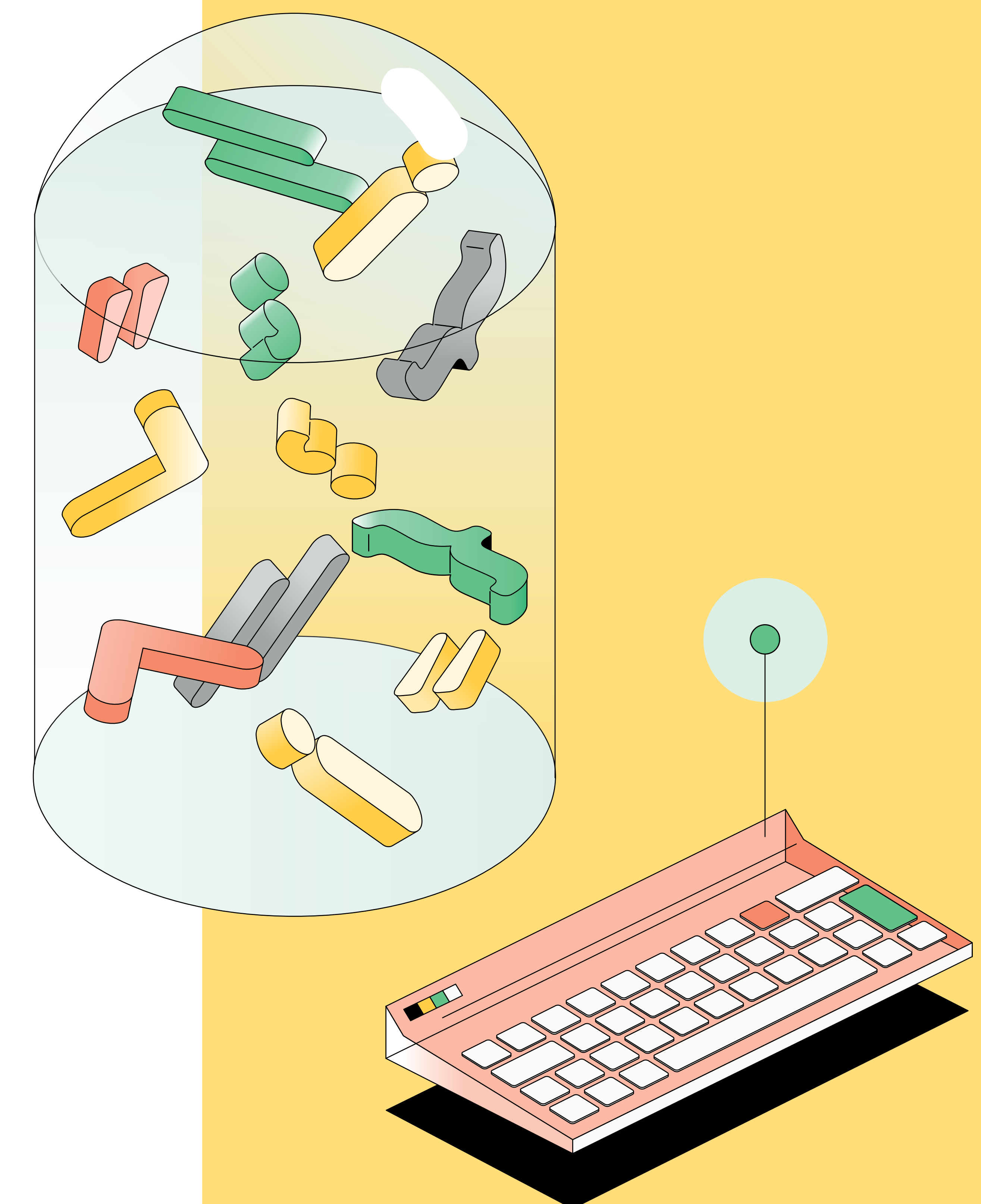
 **<6 months**
Payback¹⁸

 **5x**
Test speed improvement¹⁶

 **+90 %**
Developer and QA Time Savings¹⁹

^{14, 15, 17, 18, 19} Forrester, The Total Economic Impact of Sauce Labs, June 2023.

¹⁶ Sauce Labs, Unlock a Seamless and Secure Network Connection with Sauce Connect 5.0, November 2023.



Prioritize work with debugging and test analytics

An automated testing platform that executes thousands of tests in parallel will inevitably reveal numerous bugs. The question then becomes: where should you start?

The right automated test platform helps you leverage debugging analytics to prioritize the issues that expose you to the most risk. By automatically identifying and ranking issues as part of your continuous quality strategy, your team can take a strategic approach and fix the bugs that leave you most exposed to risk and compliance problems, not the ones that they happen to find first.

In addition, leveraging test analytics helps you optimize your testing strategy for continuous quality by automatically executing the right tests at the right time and in the right sequence. This helps you deliver more secure applications and minimize the unproductive tests and failure patterns that can often undermine your testing strategy or inadvertently introduce risk.

The benefits of leveraging debugging and test analytics



41 %

Faster triage²⁰



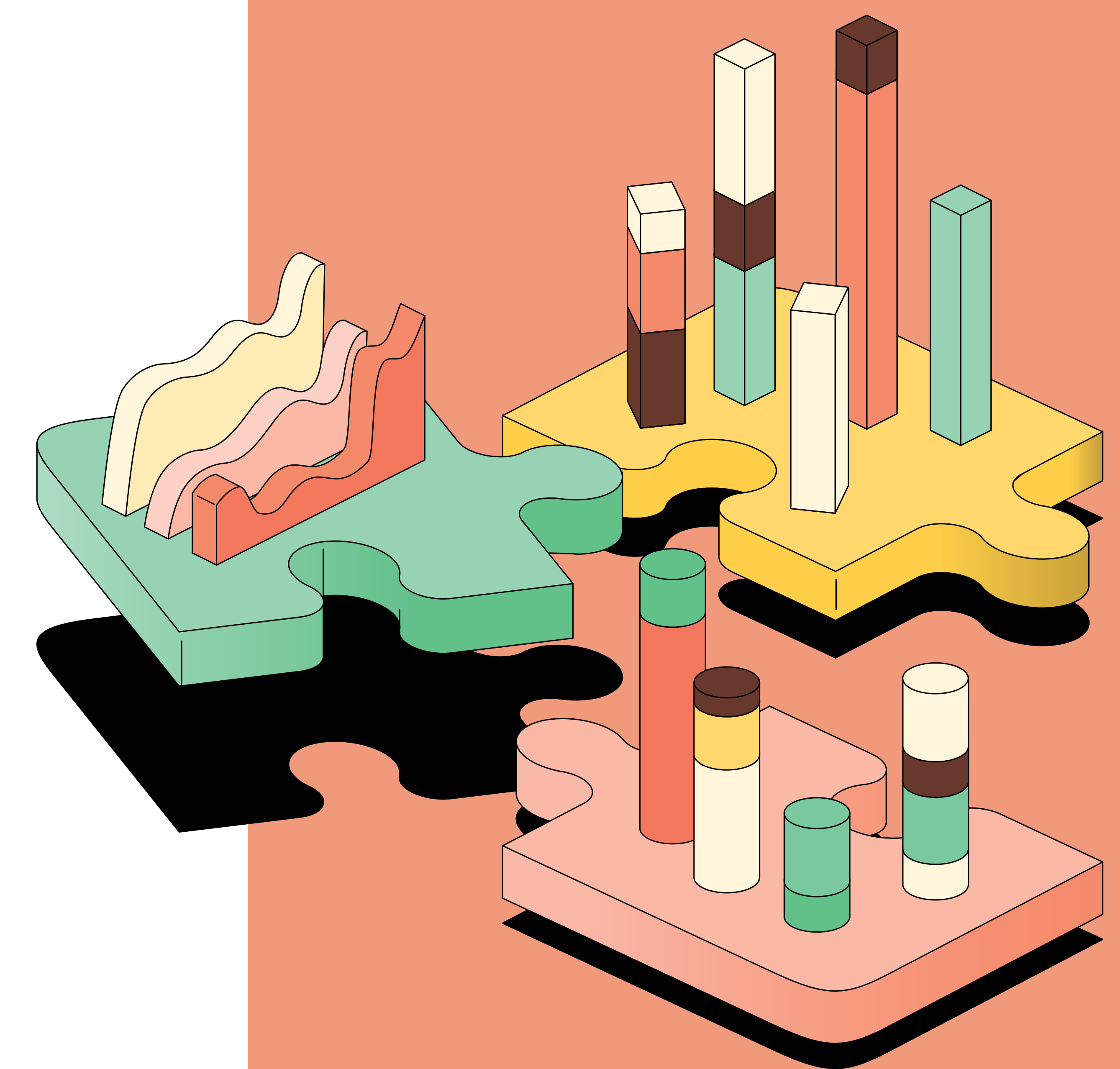
150 %

Reduction of false-negative reporting²¹



50 %

Reduction in resolution time²²



^{20, 21, 22} Enterprise Strategy Group, ESG Economic Validation Report: Analyzing the Economic Benefits of Sauce Labs for Mobile Testing and TestOps, April 2023.



Discover and resolve root causes with error monitoring

When it comes to testing, the best result isn't finding a critical bug. It's finding and fixing the root cause of that bug so it never occurs again. This makes error monitoring a pivotal element to continuous quality.

Identifying the root causes of test failures and errors in code gives your developers the critical insight they need to triage, prioritize, and eliminate the problem at its source. Their role is necessary to improving the long-term security of your products. A best-in-class test automation platform makes it simple to identify the root cause of bugs, especially in the critical production stage. By collecting, filtering, and grouping error data in production, developers can resolve the issue before it can introduce security or compliance issues while future-proofing your application against additional risk.

Fix bugs at the source

Quickly identify root cause issues to pinpoint and resolve bugs permanently.

Be proactive, not reactive

Detect errors in production sooner before it can be exploited by hackers.

Keep customers safe

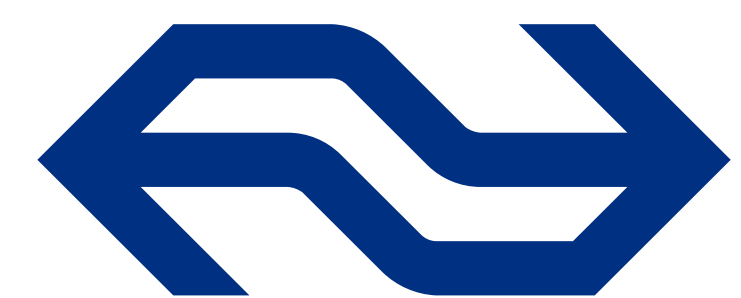
Ensure that the high-priority, high-severity errors that most impact security and compliance are taken care of first.



The Case For Continuous Quality: Real-World Examples

By automating testing, leveraging debugging and test analytics, and incorporating error monitoring, leading organizations have used a continuous quality approach to reduce their organizational risk, harden their security, protect their users, and maintain compliance with internal and external requirements.

Examples of leading enterprises leveraging Sauce Labs to achieve continuous quality include:



The national railway system in the Netherlands gave its distributed team a single source for testing, enhancing security while improving performance by 50%.

[READ THE STORY -->](#)



With one of the most widely used email services on the internet, the Yahoo Mail team leveraged debugging and test analytics to reduce its debugging time by 500% and build time by 86%.

[READ THE STORY →](#)



This financial data and analytics platform leverages automated crash monitoring and alerting to improve its time to diagnose and fix issues.

[READ THE STORY →](#)



The data solutions provider used error monitoring to discover customer crash data they weren't aware of, allowing their team to improve the security and usability of their product.

[READ THE STORY →](#)

These top enterprises and thousands of others like them rely on Sauce Labs to provide the single-platform approach required to streamline test automation, run thousands of parallel tests, and catch bugs long before they ever reach production. By using Sauce Labs to power their continuous quality testing strategy, their developers leverage the only end-to-end solution on the market to spend more time writing code so they can create better products, happier users, and a healthier bottom line.

Ready to learn more?

[REQUEST A DEMO WITH OUR TESTING EXPERTS →](#)



LEARN MORE AT [WWW.SAUCELABS.COM](https://www.saucelabs.com)



About Sauce Labs

Sauce Labs is the leading cloud-hosted platform for automated testing of web and mobile applications, enabling fast delivery of high-quality software across the development lifecycle. Founded by the creators of Selenium, Sauce Labs has been the testing leader for over 15 years and now runs over 1 billion tests annually. Trusted by Fortune 500 companies like Toyota, Walmart, Verizon, Gannett, and Fidelity Investments, its scalable, secure platform supports testing across thousands of operating systems, browsers, and devices while meeting the highest compliance standards.

hi@saucelabs.com

www.saucelabs.com