VERACODE

Veracode Case Study | *Secure Development*

KEY HIGHLIGHTS

- ✓ **Reduced application flaw risk by 20 percent in one year**
- ✓ **Increased security scans from 75 per month to 300+ per month**
- ✓ **Internally developed and outsourced code is scanned prior to pipeline integration**
- ✓ **Developers fix coding flaws early in the SDLC, where it's most cost effective**

Global Insurer Reduces Risk of a Breach Without Slowing Down Development

Veracode Developer Sandbox empowers outsourced and internal development teams to secure code early in the development lifecycle

Summary

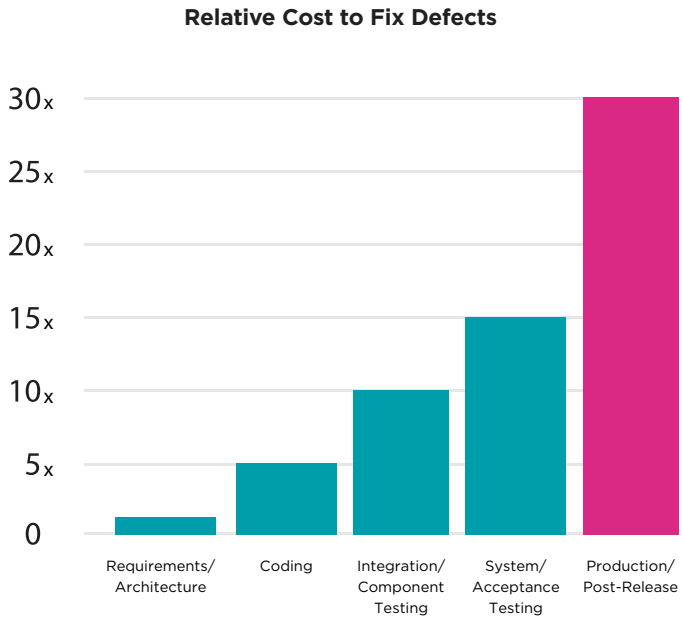
A global life insurance company required an application security solution to safeguard more than 800 applications and stay compliant with industry regulations and customer requirements. In addition, after outsourcing a portion of its development, the company needed systems to ensure all outsourced code met the same high standards as their internally developed code. Veracode's unique technology enabled development teams to independently test code in sandboxes before scanning against policy, giving them time to fix flaws at the most cost-efficient part of the development lifecycle.

VERACODE

The Challenge: Securing Applications During Development

One of the world's largest insurers had a host of application security challenges. With more than 700 developers and 800 applications serving customers in more than 50 countries, securing those applications was a major technical challenge. The company also faced intense scrutiny from regulators and customers, at the same time as market pressures demanded continuous delivery of new applications and features. These demands as well as other factors prompted the insurer to expand its resources by outsourcing a portion of its development to contractors.

The security team was tasked with reducing the number of application flaws found by static testing. However, the company did not want scanning just before deployment to production to slow release times, inflate costs and potentially hold back innovation.



Source: National Institute of Standards and Technology

With an eye towards reducing risk in today's environment of financially-motivated attacks on business applications, the Chief Information Security Officer and security team wanted to enable development teams to secure code early in the software development lifecycle (SDLC). At the same time, the security solution needed to enable easy assessment of code developed by contractors.

The insurance company's security team was already using static analysis during development, but this presented additional challenges. Developers were scanning for policy compliance even for small releases. And although developers were supposed to distinguish from assessments in pre-production by labelling production tests as "final," this left little margin for human error. Security was being inundated by unreliable reports showing high failure rates against policy.

AppSec Requirements

- Scalable solution to support hundreds of applications in various platforms and technologies
- Provide visibility to security teams on security posture of applications in pre-production and production
- Empower internal and outsourced development team to detect issues early in the development lifecycle

VERACODE

The Fix: Scanning Code Early in Developer Sandboxes

The company's security and development leaders found an innovative solution in developer sandboxes that allowed developers to scan new features or modules on a development branch before running policy scans on the release branch. The security protocols established by the company call for three separate sandboxes for each application – one for internally developed code, one for code developed by contractors, and one for the release candidate with integrated internal and outsourced code.

Before the development teams are ready to combine modules and scan the application as a whole, they scan them in a developer sandbox, where they can fix flaws without affecting other teams or alerting security. Then the complete application can be scanned in the release candidate sandbox. These release candidate sandbox scans allow development teams to run static analysis to see how a build would stack up against policy, but do not affect current policy evaluation and executive reports.

When the application meets the desired security posture and is ready to move to production, a security or development lead can promote the release sandbox scan to policy scan. The application passing policy signals to the business that the app is ready to be deployed in production. The policy scan results flow downstream to custom dashboards, GRC and other tracking systems that provide executives with visibility into the security of the entire application profile.

Security and compliance teams at the insurance company have seen major improvements:

- Number of monthly security scans increased by 3 times due to scans in developer sandboxes
- Flaw density (potential vulnerabilities per MB of executable code) of applications declined 20 percent
- Flaw density is now 1/4th the rate typically seen in the financial services industry

Securing Your Applications Early in the SDLC With Veracode Developer Sandbox

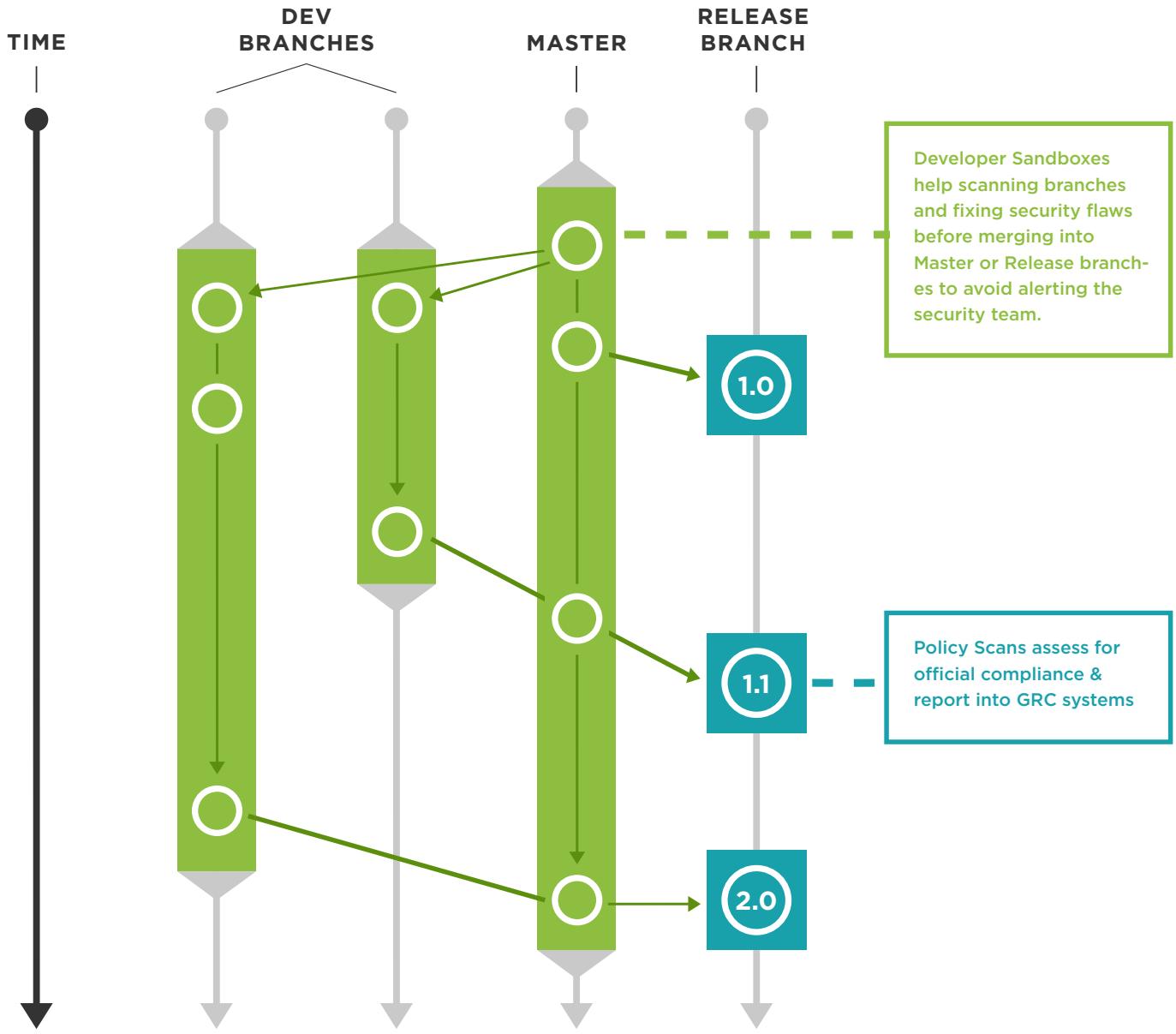
Veracode Developer Sandbox is a way for individual developers or development teams to assess new code against security policy – without affecting compliance reporting for the version of the application currently in production. Because only the policy scan is reported to senior management, developers have the freedom to test their code as much as they want before policy, without being concerned about incomplete or inaccurate scan reports. And developers can launch a Developer Sandbox scan simply, within their integrated development environments (IDEs) using Veracode IDE plugins.

By allowing developers to scan early in the lifecycle, Developer Sandbox gives organizations the ability to fix coding flaws where it's the most cost effective. Developer Sandbox can be an effective tool for shifting security left without slowing down development, which is instrumental to development organizations moving from Agile towards a DevOps model.

Teams may adopt Veracode Developer Sandbox to meet various needs:

- Developers measure the security posture of a new feature on a Developer Sandbox even before committing code to the master branch
- Development teams automate scanning of a complete application using a Developer Sandbox as part of a CI/CD workflow
- Organizations transitioning to DevOps test components in individual Developer Sandboxes for faster feedback during the coding stage

VERACODE



Developer Sandbox puts developers in the driver's seat when it comes to creating secure software. And teams using Developer Sandbox can scan applications more frequently and sooner in the lifecycle than teams that only perform a policy scan. The result is development teams embracing application security and fixing more issues, reducing risk to the organization.

CONTACT US: TALK TO ONE OF OUR KNOWLEDGEABLE REPRESENTATIVES ABOUT YOUR NEEDS.

Veracode's powerful cloud-based platform, deep security expertise and systematic, policy-based approach provide enterprises with a simpler and more scalable way to reduce application-layer risk across their global software infrastructures. Veracode serves hundreds of customers across a wide range of industries, including nearly one-third of the Fortune 100, three of the top four U.S. commercial banks and more than 20 of Forbes' 100 Most Valuable Brands. Learn more at www.veracode.com, on the Veracode blog and on Twitter.