VERACODE | CASE STUDY

HIGHLIGHTS

- ✔ A state government meets compliance requirements and reduces risk in a scalable application security program
- ✔ Addressed HIPAA, PCI, and state and federal regulations
- ✔ Assessed over 200 applications in the first year of the program
- ✔ Rolled out application security testing in 14 state agencies, using analytics to drive competition and improve performance
- ✔ Fixed over 28,000 flaws in the first year of the program
- ✔ Veracode has helped 77% of the applications achieve compliance with policy over the life of the program

A State Government Protects Citizen Data by Securing Applications

State government rolls out application testing across 14 state agencies, fixing 28,000 flaws in the first year of the program

SHUTTERSTOCK

Summary

A state government, facing concerns from citizens over data breaches and concerned about federal requirements such as HIPAA, implemented a high priority initiative on cybersecurity. Recognizing the importance of application security as part of an overall cybersecurity approach (including security training and data loss prevention technology), the state's CIO brought in Veracode to provide an application security governance program that could be easily rolled out across multiple state agencies.

With Veracode's cloud-based service and policy-based approach, the state has assessed 200 applications across 14 state agencies in the first year of the program, fixing over 28,000 flaws and achieving a 77% pass rate on the state's application security policy. Additionally, the state has begun requiring vendors to meet the application security standards as well.

VERACODE

CASE STUDY

The Challenge: Make Security Easy to Roll Out at Scale

Over the past several years, two trends have increased awareness and importance of application security as a priority for government agencies: the rising tide of data breaches, for which the application layer is the number one attack vector, and the increasing focus of federal and financial regulations and standards like HIPAA, PCI, and others on the importance of securing applications. The risk picture has been brought into sharp focus for many state governments by breaches like those experienced by the State of South Carolina in 2012, in which a server at the state's Department of Revenue exposed 3.6 million Social Security numbers and 387,000 credit and debit card numbers belonging to South Carolina taxpayers; and the State of Oregon, where the website of the state's Employment Department was hacked, revealing job application information, including Social Security numbers, of up to 819,000 individuals.

Application security testing... was far from a "slam-dunk" move; the state had flirted with tools-based approaches to application security testing before, but had been unable to produce business results due to the huge volume of data and lack of useful metrics produced.

Amid rising concerns about data breaches affecting millions of taxpayers, and following a series of measures in the state's legislature, the CTO of a US state government declared cybersecurity the number one priority, ahead of legacy system modernization and data warehousing. And a significant focus of the cybersecurity initiative, alongside security training for both developers and end users and implementation of data loss prevention tools, was application security testing. This was far from a "slam-dunk" move; the state had flirted with tools-based approaches to application security testing before, but had been unable to produce business results due to the huge volume of data and lack of useful metrics produced.

The state first undertook an effort to identify its portfolio of applications and allocate them by state agency. It then evaluated offerings for application security testing, ultimately selecting Veracode's automated cloud-based service and its systematic services approach.

The Solution: Veracode's Cloud Based Platform Provides Easily Scalable Application Security Testing

A Veracode Customer Success Manager helped the state implement a centralized, policy-based program with consistent policies, metrics and reporting. Veracode worked with the state to build its program from the bottom up, including:

- Defining the scope of the program
- Establishing responsible parties in each of the state agencies
- Onboarding each agency
- Demonstrating success on one or more initial applications
- Remediating and/or mitigating vulnerabilities
- Reducing enterprise risk with ongoing monitoring and scaling of the program to cover more of the state's applications

With this program, Veracode enabled the state to:

Reduce risk from application vulnerabilities via testing and remediation guidance. Attackers target the application layer because it is the most exposed and vulnerable part of the state's IT perimeter. Veracode provides an easy way for distributed development teams to identify and fix the vulnerabilities in their applications.

Using Veracode's binary static analysis technology, unique in the industry, developers in state agencies rapidly upload and test their compiled code without exposing their intellectual property in the form of source code. Equally important from the state's perspective, Veracode scans for every possible known vulnerability or flaw type, every time, making Veracode's reports consistent and free of influence or tuning. This kind of independence is important to the state to serve as a trustworthy measure of the security of the software they build and deploy. Thirdly, Veracode had an observed false positive rate of less than 10% in its published results, meaning that the testing results were actionable by the development team and that there was no wasted effort as a result.

Enforce policy easily. Veracode's cloud-based platform is pre-configured to assess applications for OWASP Top 10 and SANS Top 25 vulnerabilities, but provides organizations with the flexibility to tailor custom policies. For the state, the most important factor was not just one-time elimination of risk, though they set a high bar, requiring a weighted average risk score of 90 or better for critical applications. A more important factor was ensuring that applications were tested on an ongoing basis. That meant requiring that applications be periodically rescanned, and flagging any application that had not been rescanned as being out of policy.

VERACODE

CASE STUDY

Rapidly remediate vulnerabilities. Veracode security consultants help the state's developers create actionable plans out of the assessment results — eliminating the need for in-house experts or consultants to interpret the results. Veracode experts sat down with the agency development teams to sift through the assessment results and determine which vulnerabilities were the most critical and needed to be remediated first according to its policies and priorities.

"When I talk to people about Veracode, I talk about the ease of use and the rollout. As compared to on premise options, the startup time is in minutes. And it's easy to use by the developers because it makes it easy to fix the flaws. It's been a huge success."

Build security into the vendor management process. The state now asks existing vendors to undergo testing so that they can meet the same standard as state developed applications. Vendors share testing results with the state securely through the Veracode platform.

Use program data to spur further improvement. Veracode's cloud-based service offers a single centralized location for assessing all program metrics across all stakeholders. Using these key performance indicators, Veracode provided scorecards for each application development organization in the state. The CIO used these reported metrics as a way to call attention to high performers and encourage low performers to improve. This "gamification" was essential for the rapid adoption of application security testing across multiple state agencies.

The program sponsor also mined data about frequently occurring vulnerabilities to identify opportunities to train software developers. This enabled the program team to focus training efforts on areas where there were real vulnerabilities and where the teams could leverage their learning to improve the state's risk posture.

Lastly, the state leveraged data from the Veracode platform as positive input for developer staff evaluation. Developers could use high scores from Veracode evaluation of their software as positive proof that they were performing at a high level.

The Results: Rapid improvement in state agency application risk

In the first year of the program, Veracode helped the state assess over 200 applications. The findings became a baseline from which developers continuously improve the security of their applications. The platform automatically prioritizes findings so that developers can start remediating the most critical vulnerabilities first.

Within the first year of the program, Veracode worked with the state's developers to get 77% of the applications to comply with the state's policy. This required vendors to address any flaws that violated the state's policy.

In the first year of the program, state development teams fixed over 28,000 vulnerabilities. This required developers to make code changes so that the flaw was not found in a rescan of their application. Developers were guided in their remediation efforts by Veracode's Application Security Consulting team, who led the developers through readouts of the scan findings and advised them on remediation strategy.

The state has quickly and easily deployed the program across 14 state agencies. The program sponsor notes, "When I talk to people about Veracode, I talk about the ease of use and the rollout. As compared to on premise options, the startup time is in minutes. And it's easy to use by the developers because it makes it easy to fix the flaws. It's been a huge success."

To learn more, view our demos at: www.veracode.com/resources/demos