A web and mobile application provider

Reduces development costs substantially by detecting and fixing application vulnerabilities early

Overview

The need

The company's security team and application developers wanted to detect and fix web and mobile application vulnerabilities earlier in the software development lifecycle, to better protect client data.

The solution

With IBM® Security AppScan® software, the company's application developers can easily scan code for vulnerabilities as soon as it is logged.

The benefit

Testing applications earlier and more often gives security staff, executives and customers more peace of mind and reduces the cost to fix vulnerabilities by up to 95 times.

This web and mobile application provider delivers solutions that help thousands of companies and millions of users control costs and save time.

Protecting mobile and web applications from the threat of attacks and data breaches

When this web and mobile application provider hired its new security and risk manager several years ago, the company sought to leverage his application security expertise.

Like most companies, this web and application security provider actively performed penetration tests before new applications were put into production, to detect and fix application vulnerabilities that hackers could exploit. Additionally, each year, the company underwent a rigorous audit of all its web and mobile applications in production.

One of the surprising results has been the positive impact application security has had on overall application quality. "We expected just to get security findings," says the security and risk manager for this application provider. "But we also obtained code quality findings and made recommendations to our developers that significantly benefited application performance."

Solution components

Software
- IBM® Security AppScan® Source
- IBM Security AppScan Enterprise

However, according to the company's security and risk manager, those tests only provided a "point-in-time" view, and became outdated almost as soon as they were finalized. Company application developers and executives wanted to do more to help protect client data—which could include credit card numbers, personally identifiable information and itinerary data.

"As a cloud services company, we're stewards of our customers' data and it's our duty to provide them with the assurance that we're handling their data correctly and appropriately," says the company's security and risk manager. "As part of this commitment, our application developers were asking: 'How can we do security testing more often and earlier in the development cycle?'"

New processes were also required to help the company better address mobile application security.

"Mobile users can have anything from a fully locked down, secured mobile device to something that's several years old and missing patches," says the company's security and risk manager. "Devices also can easily be lost or stolen. Because of the platform diversity and the varied states of security, we have to make sure that our mobile applications are of the highest quality."

Identifying vulnerabilities early in the software development lifecycle

To strengthen its application security program, the security and risk team sought to combine static application security testing with traditional dynamic application security testing.

As the team evaluated vendors to support this work, IBM immediately rose to the top of the list.

"IBM is helping us to stay ahead of hackers and make sure that our applications are secure and that our customers' data is protected."

—Security and Risk Manager, A Web and Mobile Application Provider

"Not only is IBM top of the field, but I had used its products previously so knew firsthand the quality of its solutions, security research and support," says the company's security and risk manager.

Today, using IBM Security AppScan Enterprise and IBM Security AppScan Source software, the company is able to detect and fix vulnerabilities in its web and mobile applications early in the development lifecycle to minimize risk, increase customer confidence and reduce development costs.

"IBM is helping us to stay ahead of hackers and make sure that our applications are secure and that our customers' data is protected," says the company's security and risk manager. "We've seen, in some cases, as much as a 100-fold decrease in the time spent resolving issues because we caught them early."

Gaining buy-in from developers

Even though application developers were asking for additional testing capabilities, the security team still had to demonstrate that the solution they chose would not impede the development process.

"We met with our development team early on to discuss the benefits," says the company's security and risk manager. "We also discussed the types of findings we expected to get and how we would prioritize them so that it wouldn't slow them down."

The security team also examines the reports for any false positives before sharing results with the development team.

"One false positive in a report when a developer is busy can call the whole report into question, so our team looks at the data and the context upfront before we send it to them," says the company's security and risk manager.

"If a defect is found during development, it costs USD80 on average to fix….if we don't find it until production, it can cost nearly USD7,600 to fix—95 times more."

—Security and Risk Manager, A Web and Mobile Application Provider

Gaining greater peace of mind while lowering development costs

Performing testing more often and earlier in the software development lifecycle has given the company's security staff, executives and customers greater peace of mind.

"We don't want vulnerabilities to happen at all, but if they do happen, we certainly don't want them in production," says the company's security and risk manager. "The fact that these vulnerabilities are discovered so early in the process means that I can sleep better at night."

There's also a tremendous cost savings that comes from conducting security testing earlier in the application development cycle.

"The IBM solution helps us to reduce the cost in resolving vulnerabilities," says the company's security and risk manager. "A study by the National Institute of Standards and Technology shows that the later a defect is found in the application development cycle, the more costly it is to fix. For example, if a defect is found during development, it costs USD80 on average to fix. If that same defect is uncovered in QA and testing, it would cost USD960 to fix. And, if we don't find it until production, it can cost nearly USD7,600 to fix—95 times more."

Additionally, application developers are using the new insight to develop more secure applications from the start.

"We're seeing fewer vulnerabilities because our developers are taking the knowledge and designing their applications with security in mind," says the company's security and risk manager. "As a result, rather than delivering a report that has hundreds or thousands of findings, we're typically dealing with only one or two findings here and there."

Finally, the company's new approach to application security has increased customer confidence, and, in turn, accelerated client acquisition.

"What it comes down to with cloud security is: Can they trust us with their data?" says the company's security and risk manager. "With AppScan, we're able to provide proof that we are doing what we say we're doing, which has helped us to reduce the due diligence process by approximately two weeks. This benefits the customer because they're able to start using our solution sooner and it benefits us because we can realize revenue sooner."

Take the next step

To learn more about IBM Security solutions, please contact your IBM sales representative or IBM Business Partner, or visit the following website: **ibm.com**/security

IBM Security
Route 100
Somers, NY 10589

Produced in the United States of America
May 2015

WGC12360-USEN-00