Hewlett Packard Enterprise

Case Study

天津銀行 BANK OF TIANJIN

Bank of Tianjin strengthens test security processes

HPE Fortify creates standard testing environment to enable faster time to market

Objective
Improve the efficacy and efficiency of security testing process, allowing new banking products to reach the market faster

Approach
Met with HPE, aware that HPE Fortify was in use with leading international banks and had a solid reputation with Chinese users

IT Matters
- Saves time and manpower during source code vulnerability, scanning through automated processes
- Easily identifies security issues in the code and fixes vulnerabilities promptly

Business Matters
- Code audits are standardized and accurate, improving efficiency and allowing new products to reach the market faster
- Meets the high-level requirements of Chinese industry regulator
- Ensures software quality, reducing business risks

By deploying HPE Fortify products, Bank of Tianjin has strengthened its security testing. The solution improves the system test process, eliminates potential code risks and improves code quality, readability and maintainability, to protect banking applications.

Challenge

Creating a secure online environment
Today, the tentacles of financial IT have spread everywhere, from capital transactions between multinational corporations to consumers' everyday banking. Consequently, the quality of financial software needs to keep pace with the new demands.

The experience of the Bank of Tianjin, a Chinese bank serving the corporate and consumer markets, reflects this. As the bank launches a series of new products to market it has been compelled to strengthen its IT security infrastructure. To ensure the security of software systems, the bank has adopted a series of actions such as to create firewalls and encryption mechanisms.

"Code audits have become more standardized and accurate. The previous manual method was unable to monitor computer memory vulnerabilities, let alone pinpoint the actual line of code where the memory vulnerability appeared. HPE Fortify has fixed this problem and effectively reduced the risk of new products developing faults when they go online, accelerating the deployment of high quality applications."

– Xu Ping, deputy general manager, Information Technology Department, Bank of Tianjin

Functional and business stress testing is performed whenever new products go online or systems are upgraded. Quality management tools are used to reduce risk and prevent code from being altered.

The most important aspect of the bank's quality control is the testing of its application systems and the comprehensive risk analysis of all new software. Targeted corrective actions have also become an essential step in stabilizing products before they go online.

This work must be completed by test personnel through code audits. Code audits focus on security holes or architecture design flaws that may threaten software. These vulnerabilities are often exploited by hackers.

Bank of Tianjin had previously performed code security testing manually. However, this method took time and manpower. Audit efficiency was poor, it was impossible to conduct in-depth testing on all systems. In addition, testing task loads, complexity detection failures and error detection problems increased due to differences in several of the products outsourced by the bank. This made things worse for the bank's streamlined software testing department.

Bank of Tianjin urgently needed to adopt automated testing tools to find and manage security threats during the software development and testing processes.

"There were real problems with the code audits, such as standards not being unified, irregular source code scanning and being unable to find small errors," says deputy general manager Xu Ping, responsible for software development at Bank of Tianjin. "Even though the software may have passed its audit and gone online, there was still a great deal of risk during actual operation."

Xu Ping wanted to be able to use sophisticated code detection tools to improve the system test process, to eliminate potential code risks and improve code quality, readability and maintainability. Ultimately, this would protect banking applications.

Solution

Powerful source code analysis
Bank of Tianjin selected HPE Fortify security testing tools to meet its objectives. Xu Ping says the choice was made because of the HPE Fortify reputation amongst its users within the industry, and the fact that nine out of the world's ten largest banks use HPE Fortify.

HPE Fortify supports the most diverse range of popular programming languages in the market and its security vulnerability checks are also the most thorough. Plus, says Xu Ping, Hewlett Packard Enterprise was able to demonstrate a rich implementation experience with Chinese clients, along with the quality of its professional services team.

With HPE Fortify, the bank's developers can carry out powerful source code analysis. Security testers can make testing more quantifiable and fix vulnerabilities more easily. Reviewers use HPE Fortify to identify security issues anywhere in the code, set primary and secondary sequences and solve problems.

The full path generated by the HPE Fortify fully automated testing processes, multi-dimensional analysis of source code security issues and accurate pinpointing of vulnerabilities, along with its 10,000 line per minute scan speed, reveals detailed vulnerability information. Developers will be able to communicate bug locations to the application development outsourcing team immediately and fix vulnerabilities promptly.

HPE Fortify uses its five main built-in analysis engines to conduct statistical analysis on data flow. During this analysis, it carries out comprehensive matching with its unique software security vulnerability rule set, identifying vulnerability within the source code. HPE Fortify has more than 50,000 secure code rules covering several languages, including ASP.NET, C/C++, C#, Java, XML and VB.NET.

This is precisely the kind of multilingual environment that Bank of Tianjin's current system architecture uses. It can perform cross-layer and cross-language analysis on the causes of code vulnerabilities. HPE Fortify has the industry's most authoritative world-synchronized security rule base, which ensures the bank prevents the latest security vulnerabilities.

Benefit

A significant reduction in business risk
After deploying the HPE Fortify solution, Bank of Tianjin performed source code security testing on all the online applications within its intranet and extranet. This greatly enhanced software performance and was able to meet regulatory requirements. The protective system will not allow malicious code attacks, which significantly reduces business risks.

"Code audits have become more standardized and accurate," says Xu Ping. "The previous manual method was unable to monitor computer memory vulnerabilities, let alone pinpoint the actual line of code where the memory vulnerability appeared. This problem has now been solved and the risk of new products developing faults when they go online has been effectively reduced, accelerating the deployment of high quality applications.

"Moreover, reducing the frequency of vulnerabilities being exploited has helped reduce disaster recovery costs."

Case study
Bank of Tianjin Co., Ltd.

Industry
Finance

Customer at a glance

Software
- HPE Fortify

"In the past, we mainly relied on the professional knowledge of individual test personnel. It was not possible to evaluate test results objectively. After using HPE Fortify, code audits have become more standardized and comprehensive."

– Xu Ping, deputy general manager, Information Technology Department, Bank of Tianjin

The solution specifically involves:

- Improving code audit efficiency: HPE Fortify products are simple to operate and easy to use. Their features, which include thorough vulnerability checks, rapid scanning speeds and the visual presentation of vulnerability locations and their corresponding solutions, significantly improve the efficiency and accuracy of software code audits.
- Code audits that cover all applications: Code detection system types are integrated into core software security testing at an early stage and all internal and external applications are included in the test range. This achieves genuine full system scanning that is accurate to one level of code.
- The standardization and systemization of security testing: The security testing of new products and applications before they go online has now become the standard system at Bank of Tianjin. A three-part security scan is required for new online systems on key dates every month. Scans can be performed at any time during the review and development process when systems are designed and code audits are performed before systems go online.
- More standardized and comprehensive test results: Security testing will often lead to unexpected results. In the past, Bank of Tianjin mainly relied on the professional knowledge and experience of individual test personnel. It was not possible to evaluate test results objectively. After using standardized test tools, code audits have become more standardized and comprehensive.

In the future, Xu Ping hopes to build a platform to promote collaboration between the test team and those in project development, enabling communications between both teams throughout the whole product life cycle. This will ensure that any vulnerabilities detected by the product development team are communicated to the test team. This will result in improved communications between the two teams and improved development quality in order to ensure new products are online faster.

To prevent risks, Bank of Tianjin has also researched and formulated an information technology risk management system and completed the construction of a disaster recovery system based on three centers in two locations. These series of initiatives will further enhance the bank's IT support capabilities.

Learn more at
hpe.com/security

Sign up for updates

Hewlett Packard Enterprise

© Copyright 2015-2016 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Java is registered trademark of Oracle and/or its affiliates.

4AA5-5684ENW, July 2016, Rev. 1