wavemaker

Case Study

BANKING ON SECURITY

Fortune 500 US-based bank adopts WaveMaker low-code platform to create iron-clad applications with stringent security tests.

Industry
Banking

Location
USA

No of Employees
50000+

Rigorous security tests	Strict regulations and compliance	500+ internal users	5+ years of client engagement

REQUIREMENTS

- Secure and safe application development environment to develop in-house apps rapidly

CHALLENGES

- Strict vetting process by the IT team with respect to security
- No internet availability for automatic upgrades

SOLUTIONS

- WaveMaker Enterprise installed on AWS cloud for internal usage
- WaveMaker Enterprise was subject to rigorous internal IT scrutiny
- All apps developed by WaveMaker Enterprise were subject to vulnerability testing

RESULTS

- WaveMaker Enterprise passes all vulnerability tests
- WaveMaker Enterprise apps pass all scrutiny by Nessus
- Continuous renewal of the WaveMaker Enterprise license for the past 5 years.
- IT team is self-sufficient to use the platform in self-service mode

Our customer is a Fortune 500 company based out of USA, with over 755 branches worldwide, and is considered as a pioneer in the field of mass marketing of credit cards. Ranked 13th on the 100 largest bank holding companies list in the United States, this bank is one that invests heavily in technology and security too.

Requirements

The client's main objective was to use a secure and reliable development platform to create customized apps for its in-house business processes. These apps were meant to simplify in-house processes, make them efficient and easy to use for its agents. For instance, the fraud detection workflow, an in-house application that was distributed across multiple segregated systems made it difficult for agents to work with this complex functionality. This resulted in latency when it came to the resolution of issues. Modernization of such kinds of applications was required urgently.

However, security and compliance were considered the topmost priority. Workloads were categorized in different levels of security. Gold tier applications needed the highest level of security and bronze the lowest.

Challenges

One of the most important challenges that the WaveMaker team had to overcome was the stringent security requirements of the bank's internal IT team. As a rule, all applications in the IT department went through rigorous vulnerability and penetration tests under rigid constraints before deployment. Additionally, every application had to be certified for US compliance and regulations. Also, WaveMaker had to conform to the client's internal infrastructure.

Security restrictions prevented internet connectivity for internal systems. This posed a major challenge in releasing updates and dependencies of the WaveMaker platform.

Solution

The bank adopted WaveMaker Enterprise as a platform of choice to create its in-house applications. Initially, a Proof Of Concept (POC) was created by the WaveMaker team in collaboration with our IT partner on WaveMaker Online. WaveMaker professional services provided the IT team with standard training on the WaveMaker Enterprise platform.

The IT department's vetting process was elaborate and strict. Every deployment went through rigorous testing phases. Every library and every bit of code that WaveMaker Enterprise used went through rigorous security testing. This intense testing of the platform was spread across 6 months--one of the most elaborate scrutinizations that the WaveMaker platform has ever gone through. WaveMaker passed all security tests and was certified by the internal IT team as a 'safe and secure' platform for development.

WaveMaker Enterprise was installed on an AWS private cloud environment. Since the platform did not have access to the internet, all runtime dependencies of WaveMaker were provided as a package that was installed internally on the AWS platform. WaveMaker platform needed to be updated and upgraded frequently for security patches and product updates. Related VMs ran in the AWS cloud environment in sync with WaveMaker releases.

While the WaveMaker platform was in the bronze level, applications created using WaveMaker were assigned the gold level, which meant more scrutiny, more testing! All applications at the gold level went through vulnerability tests. All apps created using WaveMaker were scanned using Nessus and underwent rigorous security testing. App penetration testing and vulnerability detection including SQL injection, cross-site request forgery, and cross-site scripting was also performed. Any security issue reported by Nessus was fixed and integrated into the platform.

Results

Every app that came out of the WaveMaker Enterprise stable was subjected to intense security scrutiny and was internally certified by the client. Every single application has been certified to be Personally Identifiable Information(PII) and Payment Card Industry Data Security Standard (PCI DSS) compliant. Additionally, they have also been regulated by the Consumer Financial Protection Bureau (CFPB).

The customized apps built using WaveMaker simplified complex processes and boosted efficiency and productivity. A case in point is the fraud detection system and the credit dispute resolution application. WaveMaker supported the agile process of delivery and also supported Jenkins-based CI/CD deployment.

The bank continues to renew the license and has been working with WaveMaker for the past 5 years in a self-service model without any intervention from the Wavemaker team.

WaveMaker's continuous engagement with the customer is testimony to its capability of not just delivering applications rapidly but also most securely and safely. The intense testing of the platform is evidence of the fact that all applications developed on WaveMaker are iron clad, fortified, and dependable.

Write to us at **info@wavemaker.com**