

How a Top Financial Firm Scaled Its Application Security Program and Accelerated Digital Transformation

Company overview

This Fortune 500 financial corporation is one of the 10 largest banks in the U.S. It needed to

- Ensure stronger application security for enterprise and consumer-facing applications
- Improve and meet regulatory compliance
- Reduce time and resources spent triaging false positives

“We love the fact that WhiteHat Dynamic is production safe, [enables us to] do authenticated scanning, and above all that ALL of the findings are verified and we are 99% false positives—free.”

—Application security manager

Overview

Working on a transformational technology project under time and budget constraints, this innovative financial organization was building new applications to address the mobile banking and eBanking needs for its hundreds of thousands of customers. Operating in a sensitive and highly regulated financial industry, the organization’s security team also needed a proactive approach to security to protect sensitive customer and financial data.

The challenges

The banking organization, which operates as a technology company, was searching for a best-in-class end-to-end AppSec solution provider to implement a robust application security program, and needed to quickly scale application security for hundreds of its applications. The company faced several challenges.

- **Scaling AppSec automation.** With 400+ developers and a handful of experts in application security, scaling its red teams and the entire application security portfolio was a big challenge. Modern banking applications powered by APIs exacerbated the problem.
- **Compliance.** The organization was struggling to achieve key regulatory compliance during annual audits. Since application security is a critical element for PCI compliance, it was apparent that its existing application security solution was not effective.
- **Triaging false positives.** Automated scanners were generating a lot of false positives, seriously impacting development processes, application security, and resource management. As a result, security teams were spending more hours verifying and cross-checking the findings than remediating actual vulnerabilities.

The solution

Synopsys demonstrated that it provided the most comprehensive and industry-proven dynamic application security testing (DAST) solution. WhiteHat™ Dynamic can monitor and scan hundreds of applications in production 24/7 in a production-safe manner, and it provides the rich business logic assessment that the organization needed to confidently release its applications to its customers.

Given the size and complexity of the project, Synopsys proposed a comprehensive AppSec portfolio and later added WhiteHat Auto API. The organization's application security team scaled its program with a suite of Synopsys solutions.

- **WhiteHat Dynamic.** WhiteHat provides continuous scanning, a low false-positive rate, access to security experts, and reporting metrics that detail performance over time in discovered and remediated security vulnerabilities by criticality.
- **Business logic assessments.** Business logic assessments (BLAs) are manual assessments performed by Synopsys security engineers who look for application security vulnerabilities that cannot be tested for effectively by an automated solution.
- **WhiteHat Auto API.** WhiteHat Auto API provides highly scalable, accurate, and fully automated vulnerability scanning for web service APIs, and public-, private-, and internal-facing APIs.
- **Security testing services.** Services included designated program managers and support from subject matter experts who work with the organization's in-house team to scale its application security program.

The results

A phased approach to implementing AppSec solutions into the organization's software development life cycle, and monitoring the right set of metrics resulted in a sustainable and scalable approach to implementing application security.

Evolutionary change in application security

Unlimited DAST assessments enabled an accurate window into the true risk surface of the organization's hundreds of applications. Since WhiteHat is designed for production-safe scanning, the security team was able to scale continuous risk assessments to hundreds of applications, saving time and cost without any downtime.

In addition, developer education and a direct feedback loop with Synopsys security experts has met the evolving needs of development teams.

Improved quality of findings

One of the biggest challenges for this organization was dealing with a huge volume of AppSec findings and remediation tasks, which meant triaging a growing number of false positives. WhiteHat proved to be an ideal solution as the organization's risk surface expanded with numerous interconnected applications. By discovering, categorizing, and prioritizing the biggest risks first, teams gained a strategic, targeted plan to address the most vulnerable apps in production.

Synopsys security experts reviewed scan configurations to ensure that the scan would accurately reflect the architecture and data boundaries of the application or platform being scanned. These verified vulnerabilities virtually eliminated false positives, which reduced resource costs. Above all, faster and more accurate security vulnerability identification and remediation improved overall application security and ROI.

Achieving 100% compliance

A huge accomplishment for the organization was reaching and maintaining 100% PCI compliance. The team was able to maintain an inventory of applications, ensure on-time scans and BLAs, and provide regular metrics showing progress toward the goals.

“Within six months of Synopsys onboarding, we were able to increase our PCI compliance from 40% to 100%.”

—Application security manager

Maximized AppSec ROI

By seamlessly scaling and adding program management to the scope of work, the Synopsys Security Testing Services team developed a close working relationship with the organization’s application security and the development teams. Regular collaboration with the teams ensured that vulnerabilities were remediated according to organizational security policies and best practices. The program managers developed measurable success criteria to track progress across the organization, including regular meeting cadences, quarterly program reviews, and annual service review meetings.

Evolving scope

The Synopsys scope of work has evolved to include additional activities such as onboarding new users, integrating systems to automate manual processes within the AppSec team, severity contextualization, consulting on policy changes, and providing application security educational opportunities to development teams.

Synopsys has helped drive and support the successful creation and adoption of an application security program within this organization. Synopsys solutions empower customers with high-performing, measurable, scalable, and repeatable AppSec programs that are best suited to their requirements. Support from Synopsys security experts ensures that customers get highly accurate results and on-time remediation advice.

Synopsys is committed to helping customers keep their digital doors open. As a partner, we help organizations understand and assess their applications’ risk posture. This knowledge adds value and capacity to companies’ existing security teams, which increases confidence and peace of mind to focus on driving the future.

The Synopsys difference

Synopsys Software Integrity Group provides integrated solutions that transform the way development teams build and deliver software, accelerating innovation while addressing business risk. Our industry-leading portfolio of software security products and services is the most comprehensive in the world and interoperates with third-party and open source tools, allowing organizations to leverage existing investments to build the security program that’s best for them. Only Synopsys offers everything you need to build trust in your software.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com

©2022 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. September 2022