CUSTOMER CASE STUDY | TOP 10 US BANK

How a Top Financial Firm Scaled Their Application Security Program & Accelerated Their Digital Transformation

INDUSTRY:

Banking & Financial Services

THE COMPANY:

The Fortune 500 financial corporation is one of nations' top ten largest banks.

BUSINESS NEED:

- Ensure stronger application security for enterprise and consumer facing applications
- To improve and meet regulatory compliance
- Reduce time and resources wasted on triaging false positives

SOLUTION:

- ✓ Sentinel Dynamic for web applications
- ✓ Business Logic Assessments
- ✓ Sentinel Mobile for mobile applications
- ✓ Sentinel Auto API
- ✓ Professional Services

RESULTS:

- ✓ Scaled to thousands of applications
- ✓ Improved key regulatory compliance
- ✓ Extended their security team with WhiteHat SMEs
- ✓ Access to quality support ensures vulnerabilities are remediated according to security policies and best practices

Overview

Working on a transformational technology project under time and budget constraints, this innovative financial organization was building new applications to address mobile banking and ebanking needs for their hundreds and thousands of customers. Accelerating innovation with security in mind, the organization caters to consumer and commercial banking. Currently this well recognized fintech organization is considered to be at the highest level of AppSec maturity.

Operating in a sensitive and highly regulated financial industry, the organization's security team needed a proactive approach to security to protect sensitive customer and financial data. Searching for the best-in-class application security solution, they sought out WhiteHat Security as a competent alternative to the tools and solutions they had already invested in. The application security team chose the WhiteHat solution as it is outcome based, provides fully verified results, and the solution is highly scalable.

This organization uses WhiteHat Sentinel Dynamic for dynamic application security testing (DAST), Sentinel Mobile for mobile application security testing (MAST), Business Logic Assessments and Sentinel Auto API for scanning previously onboarded manually tested APIs. The company also relies on WhiteHat's security experts for added assurance in uncovering security vulnerabilities and program management services to develop and manage a successful application security program.

Identifying security vulnerabilities with unmatched accuracy for their web and mobile applications, over the last few years, WhiteHat has been their strategic partner in helping this organization significantly reduce the risk of data breaches and meet industry-specific compliance.

Challenges

This fintech company faced the following challenges:

Scaling AppSec Automation

With 400+ developers and a handful of experts in application security, scaling their red teams and the entire application security portfolio was a big challenge. Modern banking applications powered by APIs only 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 their existing application security solution was not effective.

Triaging False Positives

Automated scanners by other vendors were generating a lot of false positives seriously impacting their development process, application security, and resource management. As a result, the security teams were spending more hours verifying and cross-checking the findings versus actual vulnerabilities.

Why WhiteHat Security?

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

WhiteHat demonstrated that they were the only company providing the most comprehensive and industry proven dynamic application security solution capable of monitoring and scanning hundreds of applications in production 24/7 in a production safe manner, and also provide the rich business logic assessment that they needed to put their applications confidently out to their customers.

Solution

Given the size and complexity of the project, WhiteHat proposed a comprehensive AppSec portfolio and later added Sentinel Auto API. The organization's application security team is scaling their AppSec program with the following WhiteHat solutions:

SENTINEL Dynamic

WhiteHat Sentinel Dynamic

WhiteHat's DAST solution provides continuous scanning, a low false-positive rate, access to consultative expertise via WhiteHat's security experts, and reporting metrics that detail performance over time in discovered and remediated security vulnerabilities by criticality.

SENTINEL Mobile

WhiteHat Sentinel Mobile

WhiteHat's MAST solution is the unique combination of automated DAST+SAST for full testing on real mobile devices. Sentinel Mobile analyzes developer-signed binaries and mobile-optimized websites for OWASP TOP 10 Mobile vulnerabilities, client-side issues and more.

Business Logic Assessments

Business Logic Assessments (BLAs) are manual assessments performed by WhiteHat security engineers for application security vulnerabilities that cannot be tested effectively by an automated solution.

SENTINEL Auto API

WhiteHat Auto API

Sentinel Auto API provides highly scalable, accurate and fully automated vulnerability scanning for web service APIs, public, private and internal facing APIs.

WhiteHat PROFESSIONAL SERVICES

WhiteHat Professional Services

Resources included designated program managers and support from subject matter experts who could work with their in-house team to scale their application security program.

Results & Business Impact

Evolutionary Change in Application Security

A phased approach to implementing AppSec into their software development life cycle and monitoring the right set of metrics resulted in a sustainable and scalable approach to implementing app security within.

Using unlimited DAST assessments to discover risk enabled this financial institution to get an accurate window into the true risk surface for their hundreds of applications. Since Sentinel Dynamic is designed for production safe scanning, their security team has been able to scale continuous risk assessments to hundreds of their applications, saving time and cost without any downtime.

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

> **"We love the fact that WhiteHat is production safe and we can do authenticated scanning and above all that ALL of the findings are verified and we are 99% false positives free!"**
>
> **- Application Security Manager**

Improved Quality of Findings

One of the biggest challenges for this organization was dealing with an increasingly huge volume of AppSec findings and remediation tasks along with triaging through the growing number of false positives. Though they were developing their own tools using internal intellectual property or using open source tools, WhiteHat Sentinel proved to be a competent alternative and an ideal solution as their risk surface expanded with numerous interconnected applications. By discovering, categorizing, and prioritizing the biggest risks first, through DAST risk discovery, teams now have a strategic, targeted plan to address the most vulnerable apps in production.

WhiteHat's security experts review scan configurations to ensure that the scan is set up to accurately reflect the architecture and data boundaries of the application or platform being scanned. These verified vulnerabilities virtually eliminate false positives, resulting in a reduction of resource costs. Above all, faster and more accurate security vulnerability identification and remediation improves overall application security and businesses' ROI.

Achieving 100% Compliance

A huge accomplishment for this banking institution has been having the confidence to reach and maintain 100% PCI compliance. From maintaining an inventory of applications, ensuring on-time scans and BLAs, to providing regular metrics showing progress towards the goals, the WhiteHat team helped the organizations' security team achieve desired compliance.

Maximized AppSec ROI

By seamlessly scaling up and adding program management to the scope of work, the WhiteHat Professional Services team has developed a close working relationship with their application security and the development teams. Regular collaboration with the development teams ensures vulnerabilities are remediated according to organizational security policies and best practices. The program managers develop measurable success criteria to track progress across the organization, including regular meeting cadences, quarterly program reviews, and annual service review meetings.

> **"Within six months of WhiteHat onboarding we were able to increase our PCI compliance from 40% to 100%!"**

Looking Ahead

Building trust over the years, WhiteHat's scope of work has evolved to include additional activities such as onboarding new users, integrating various systems to automate manual processes within the appsec team, severity contextualization, consulting on policy changes, and providing application security educational opportunities to development teams.

WhiteHat Security is pleased to drive and support the successful creation and adoption of an application security program within this organization. We are empowering our customers with high performing, measurable, scalable, and repeatable AppSec programs that are best suited to their requirements. Support from our security experts ensures that our customers get highly accurate results and on-time remediation advice.

WhiteHat Security is committed to helping our customers in keeping their digital doors open and safe. 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.

ABOUT WHITEHAT

WhiteHat Security is the leading advisor for application security with the most comprehensive platform powered by artificial and human intelligence. Trusted for nearly two decades by Fortune 500 organizations, WhiteHat Security helps organizations accelerate their digital future in our application-driven world. Gartner has positioned WhiteHat Security as a leader in the 2020 Magic Quadrant for Application Security Testing for the fifth time. The company is an independent, wholly-owned subsidiary of NTT Ltd. and is based in San Jose, California, with regional offices across the U.S. and Europe. For more information, visit **www.whitehatsec.com**.