



# Application Security Solutions for Financial Services

WhiteHat Sentinel provides a “security safety net” and lowers risk in the financial sector

If you're in the banking or financial services industry, your business is built on trust. Investors need to trust that your profits are based on sound business practices. Government entities need to trust that you are adhering to regulatory requirements and playing by the rules. And your customers need to trust that you are giving them sound financial advice, helping them grow net worth, and keeping their money safe. With advances in technology, the advent of smartphones and tablets, and the explosion of online apps, your stakeholders also need to know that you can protect their personal data and secure your online applications. Failure in any of these areas is not just embarrassing; it can be very costly in terms of customer confidence, brand reputation, and in some cases hefty fines and penalties from regulatory agencies.

“*Regulated industries, such as financial services, have the most costly data breaches because of fines and the higher than average rate of lost business and customers.*”

2016 Cost of Data Breach Study - <http://www-03.ibm.com/security/data-breach>, Ponemon Institute

With a growing number of new applications integrated into the fabric of banking and financial services businesses, security throughout the system becomes a critical success factor. At the same time, new technologies are disrupting existing infrastructures and there is often not enough expertise in key areas. This can cause process performance failures and inefficiencies as financial firms struggle to keep up with new regulations, new cyber threats, and changes in the technology landscape.

## There's a lot at stake

As financial services firms expand their reach into the online world, they become vulnerable to increasingly sophisticated and pervasive cyberattacks. Customers can be exposed to identity theft and fraud. Assets can be misappropriated and result in client reimbursements. Regulators can impose penalties and fines when there are failures to comply with regulations such as GLBA, Basel II, SOX, and others. Breaches disrupt the operation and in the worst cases lower stock prices, erode customer confidence, and damage the brand.

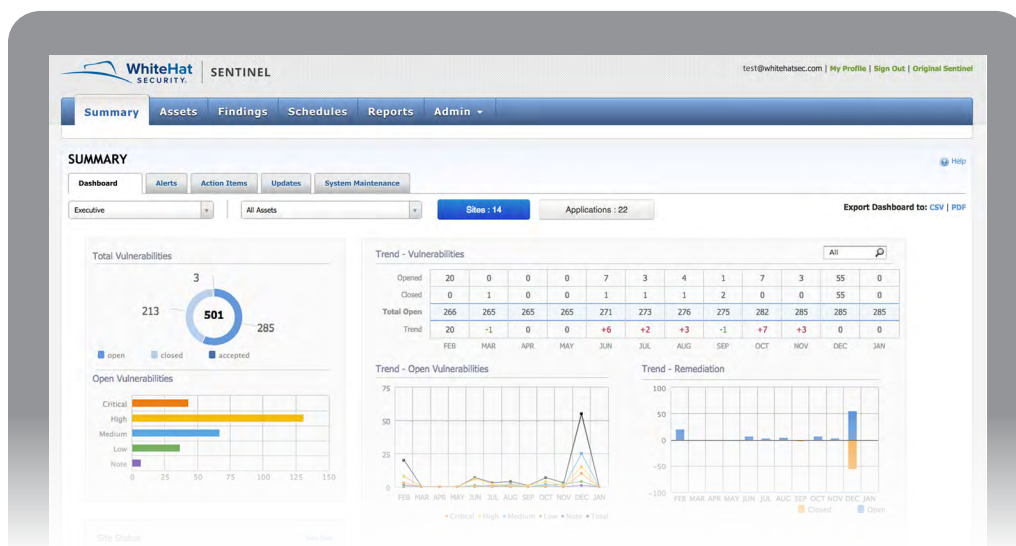
“ Established as part of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the CFPB is responsible for consumer protection in the financial sector. Failure to comply with **CFPB rules** can result in penalties above the \$10 million mark. ”

## Why Application Security?

Web application attacks represent the greatest risk to an organization, and the financial services and banking sector is no exception. Most security budgets are spent on securing and monitoring the perimeter and endpoints, and as a result, the bad guys have found it easier to sneak in through web application vulnerabilities. According to the 2016 Verizon Data Breach Investigations Report, 82% of the breaches in financial services sector were due to web application attacks.

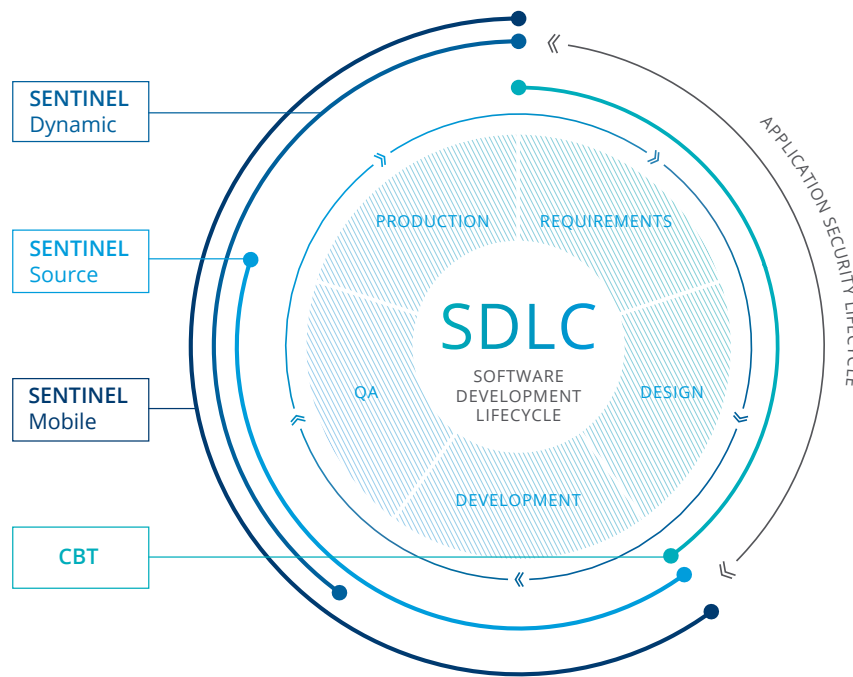
## WhiteHat Sentinel product family offers solutions

The financial industry has always had to deal with security risks. But with today's challenging cyber threat landscape, maintaining a strong application security posture is critical to success. In this high stakes environment, WhiteHat is a trusted application security provider, offering protection across current and emerging risk vectors. With customers that include 4 of the top 5 credit card companies, our patented methodology exceeds the strictest industry standards.



## Comprehensive coverage across the Software Development Life Cycle

By combining technology with the intelligence of human experts, WhiteHat provides a unique approach to protecting applications. Our product family offers dynamic, static, and mobile application security testing. Automated testing results are delivered, reviewed, and analyzed by the security experts in WhiteHat’s Threat Research Center (TRC), where vulnerabilities can be confirmed, risk ratings assigned, and sound remediation advice provided.



Sentinel Dynamic, WhiteHat’s dynamic analysis products consists of the following, with each of the products adding more capabilities and services, starting with the aptly named Sentinel Baseline Edition / Baseline Edition Enterprise:

**WhiteHat Sentinel Baseline Edition (BE) / BE Enterprise:** Provides basic, essential functionality and assesses low risk websites. Core features include a scalable platform, continuous assessment, results that are verified and prioritized to eliminate false positives, PCI compliance, and access to WhiteHat security engineers.

**WhiteHat Sentinel Standard Edition (SE):** Includes all functionality of Sentinel BE / BE Enterprise, plus scanner configuration and continuous tuning which enables WhiteHat to customize assessments to the environment, and multi-level authentication testing for permanent websites, with medium risk.

**WhiteHat Sentinel Premium Edition (PE):** Includes all Standard SE capabilities plus business logic testing to identify vulnerabilities in the workflow and account privileges across roles and between users. The focus is on the testing of mission critical websites with multiple step forms and stringent security requirements.

In addition:

**WhiteHat Sentinel Source:** Sentinel Source, WhiteHat's Static Applications Security Testing (SAST) offering, scans your entire source code, identifies vulnerabilities, and provides detailed vulnerability descriptions and remediation advice, as well as precise ready-to-implement source code solutions for certain vulnerabilities. Sentinel Source enables you to:

- Assess code at any point in the development cycle – even partial code.
- Run scheduled assessment on demand or as often as you need to meet Continuous Integration / Continuous Delivery DevOps workflows.
- Preserve your intellectual property – source code can be scanned within your premises
- Stay up-to-date on the latest attacks with frequent scanner Rule Packs releases that identify and verify vulnerability defects.
- Use plug-ins and integrations to key IDEs, bug trackers, build servers, SCM tools, and ALM tools that support your current development processes



**THE WHITEHAT  
APPLICATION "SECURITY  
SAFETY NET" FOR BANKS  
AND FINANCIAL SERVICES**

- Secure applications
- Continuous assessment
- End-to-end visibility
- Regulatory compliance
- Support from skilled TRC engineers
- Highly effective detection and mitigation processes

**WhiteHat Sentinel Mobile:** Assesses mobile applications and mobile optimized websites. Provides Sentinel Mobile customers access to mobile security engineers.

**Threat Research Center:** Staffed by 150 security researchers, TRC is an integral component of the WhiteHat Sentinel product family. Customers have direct access to TRC engineers about identified vulnerabilities, and they can also learn how to be more "security aware" to prevent future vulnerabilities.

## WhiteHat Application Security Offers a Multitude of Benefits to Financial Firms



### Improve security.

WhiteHat is a trusted application security provider, with customers that include 4 of the top 5 credit card companies.



### Achieve regulatory compliance.

Exceeding the strictest industry standards as established by the PCI Security Standard Council, WhiteHat provides ongoing, verified vulnerability assessments for both internal and public websites.



### Continually assess and make course corrections.

WhiteHat provides an easy to deploy, cloud-based platform and can concurrently scan an unlimited number of sites without slowing you down.



### Understand your risk.

WhiteHat's risk-based approach to application security provides visibility into the risk and security of your applications.



### Reduce TCO for application testing.

It is very difficult to attract and retain application security professionals. For this reason, solutions that combine continuous application testing alongside threat teams that verify security vulnerabilities and address false positives are a big plus. WhiteHat Security's TRC serves as an extension of your security team by verifying all vulnerabilities to provide you with actionable, credible results.

## Summary

As highly regulated industries, much is at stake as banks and financial services firms run very complex businesses, meet regulatory requirements, and protect sensitive data from increasingly sophisticated cyber threats.

WhiteHat Security's application security solutions and Threat Research Center offer financial organizations the tools they need to understand risk, secure applications, meet regulatory requirements, and control costs. With WhiteHat Security's Sentinel products, these organizations can operate in an extremely challenging environment and still maintain a strong security posture. They can harness the power of technology to connect with customers and still keep critical applications and information safe. This is the power of WhiteHat Sentinel and the benefits of a WhiteHat Security-financial services partnership.

