WhiteHat Sentinel Product Family

Combining technology with human intelligence to deliver the world's most powerful and accurate application security

WhiteHat Sentinel™ is a software-as-a-service platform that enables your business to quickly deploy a scalable application security program across the entire software development lifecycle (SDLC). By combining our scalable application scanning platform with the world's largest threat research team, we identify where you are vulnerable with near zero false positives. WhiteHat Sentinel is incredibly easy to use – it requires no additional staff or software. No matter how much code, how many websites or how often they change, Sentinel can scale to meet any demand without slowing you down.

THREAT RESEARCH CENTER

WhiteHat Security Engineers serve as an extension of your own website security team, providing:

- Verification of vulnerabilities to remove false positives
- Direct access to a security engineer for remediation guidance
- Active management of your risk posture
- Proof of concepts for vulnerability exploits

Highlights

Continuous and Concurrent Assessment

Always-on risk assessment delivers:

» Alerts for newly discovered vulnerabilities

» Metrics to identify improvement in security measures over time

» Automatic detection and assessment of code changes to web applications

Near Zero False Positives

Verified, prioritized results eliminate false positives and streamlines the remediation process, including:

» Vulnerabilities are custom prioritized by risk – to target high priority issues

» Clear actions and notifications for fixing issues

» Eliminate triage of false positives and save valuable developer time and resources

Trending Analysis

Tracks real time and historical data to measure your risk exposure over time. Trending analysis offers:

» At-a-glance view of exposure ratings and progress at closing vulnerabilities

» Comparison of your company's security profile against other organizations in your industry

» Effortless visibility into your most and least secure web applications at-a-glance

Scalability

Scalable to fit any environment and match your pace of development, as demonstrated by:

» Customers ranging from start-ups to the Fortune 500

» Tens of thousands of simultaneous assessments

» Millions of vulnerabilities processed per week

Static Analysis

SENTINEL **SOURCE**

» Assess code at any point in the development cycle – even partial code.
» Supports a variety of coding languages
» Run scheduled assessment as often as needed or on demand
» Preserve your intellectual property – source code can be scanned within your premises
» Access to the security engineers via the built-in "Ask a Question" feature

WHITEHAT **SCOUT**

This is a fully automated static application security testing (SAST) product that:

» Scans code in minutes
» Integrates with tools Developers already use
» Identifies common but critical vulnerabilities with greater accuracy than any other Developer SAST product in the market
» Delivers the most accurate results in the industry

	SENTINEL **SOURCE**
Verified, prioritized results eliminate false positives	●
Preserves intellectual property	●
Detailed vulnerabilities reporting	●
Early risk remediation	●
Highly scalable across the enterprise	●
Unlimited assessments	●
Software Composition Analysis	●
Flexible assessments configuration	●
Broad repository support	●
Multi-level authentication testing	●

Sentinel Source Software Composition Analysis

This feature leverages Maven, Nuget and Gradle to display a list of third party libraries being used in the source code. This provides a per app breakdown of every library being used and identifies:

- Licenses for each library being used
- Out of date libraries that may benefit from an upgrade
- Vulnerabilities in libraries and security risks associated with them

With Software Composition Analysis, you can accelerate the time-to-market for your applications, by safely and confidently utilizing open source code, without introducing unnecessary risk

Sentinel Source Directed Remediation

Directed Remediation is a WhiteHat Sentinel Source feature that offers targeted and customized remediation fixes for a growing list of vulnerabilities, significantly reducing the burden on the development team. This enables you to:

- Easily fix the vulnerabilities in the source code by utilizing precise code
- patches that are immediately ready to implement.
- Utilize WhiteHat's secure libraries to protect your applications.
- Establish security best practices for the development teams by emulating WhiteHat's security fixes in other development areas.

Sentinel Source Comprehensive Integration with SDLC

CATEGORY	INTEGRATIONS	BENEFITS
IDE Integrations	Eclipse, Xcode, Visual Studio, IntelliJ	Vulnerability details available right within the development environment
Bug Tracking Systems	Atlassian Jira	Automatically open or close tickets for bugs and defects found or fixed by Sentinel Source
Supported Repositories	Git, SVN, Perforce, CVS, TFS	Scan source code from any repository
Miscellaneous	Jenkins (Build Management Plugin), Nuget, Maven, Gradle	Resolve code dependencies using popular Continuous Integration Servers and Dependency Management Systems
ALM Systems using WhiteHat Integration Server (WIS)	Atlassian JIRA, Borland StarTeam (Dev Services Required), HP ALM, HP Quality Center, IBM Rational Team Concert (Rational Quality Manager), IBM Rational Requirements Composer, Microsoft Team Foundation Server, ThoughtWorks Mingle, Rally, VersionOne, Bugzilla, Serena Business Manager, ServiceNow (Deployment Services may be required)	Integrate to best-of-breed ALM tools with WhiteHat Integration Server (WIS) which provides bi-directional integration between Sentinel artifacts and ALM tools

Dynamic Analysis

WhiteHat Sentinel Dynamic

SENTINEL **PE**
Premium Edition

» For mission critical permanent websites with multistep forms and rigorous compliance requirements

» Includes all SE features and business logic testing

SENTINEL **SE**
Standard Edition

» For permanent websites, not necessarily mission critical.

» Includes all BE features and tests for issues involving multi-step forms and logins

SENTINEL **BE / BE ENTERPRISE**
Baseline Edition / Baseline Edition Enterprise

» BE is the foundational solution for basic, less critical websites

» BE Enterprise is massively scalable "best value" solution for any environment

	SENTINEL **PE**	SENTINEL **SE**	SENTINEL **BE / BE ENTERPRISE**
Verified, prioritized results eliminate false positives	●	●	●
Continuous assessment	●	●	●
PCI Compliance	●	●	●
Highly scalable across the enterprise	●	●	●
Access to WhiteHat Security Engineers	●	●	●
Production safe	●	●	●
WhiteHat Security Index (WSI)	●	●	●
Peer Benchmarking	●	●	●
Full configuration and Form training	●	●	
Multi-level authentication testing	●		
Business logic testing	●		

WHITEHAT SECURITY INDEX

The WhiteHat Security Index (WSI) gives you an instant, visual overview of the robustness of your website security with one score to monitor and manage the overall application security. Calculated from a comprehensive set of indicator data and based on our extensive experience with intelligence metrics and our broad base of customers in a variety of industries, this score truly reflects the state of application security across all your websites. With WSI insights, you can reduce risks, save time, prioritize activities and improve overall security.

Runtime Application Self Protection

WhiteHat Sentinel provides the option of mitigating Sentinel detected vulnerabilities automatically via Runtime Application Self Protection (RASP), which allows the applications to protect themselves at runtime without requiring changes to the application source code. Supported vulnerability classes can be instantly mitigated with this solution, allowing you to focus on remediation. With the Sentinel-RASP solution, you can:

- Gain visibility into the attacks your application environment is experiencing at runtime, including pinpointing the location and target of attacks
- Optimize your use of development resources, reduce risk through lowered exposure to vulnerabilities and lower the cost of remediation

Business Logic Testing

Sentinel Premium Edition subscribers receive special testing to find business logic vulnerabilities. This service entails:

- Creating a customized testing scheme developed and performed by WhiteHat Security Engineers
- Mapping out your Web application, users, roles, and custom business workflow
- Identifying and validating account privileges across roles and between users
- Prioritizing vulnerabilities based on your business goals and intentions

Mobile Analysis

WhiteHat Sentinel Mobile

SENTINEL **MOBILE EXPRESS**

Mobile Express identifies vulnerabilities within mobile applications in production, helping create a secure ecosystem for organizations and users alike. Every vulnerability finding is verfied by our Threat Research Center (TRC) to curate the results against the OWASP Top 10 vulnerability list for nearly zero false positives and negatives.

- Assesses mobile client applications in developer-signed binary form
- Supports Java for Android, Objective C for iOS, and swift
- Provides access to mobile security engineers
- Client-side testing, behavioral testing, network testing

SENTINEL **MOBILE**

WhiteHat's cutting-edge mobile application security testing employs a combination of dynamic and static automated scanning, as well as a manual mobile business logic assessment by the expert security engineers of our Threat Research Center (TRC).

- Assesses mobile application source code and mobile optimized websites
- Supports Java for Android and Objective C for iOS
- Provides access to mobile security engineers
- Client-side testing, behavioral testing, network testing, client-server testing, business logic assessment, source code testing

	SENTINEL **MOBILE EXPRESS**	SENTINEL **MOBILE**
Code Obfuscation / encryption	•	•
Dynamic code loading / decompiling	•	•
Certificates, Improper SSL/TLS, SSL downgrade, enforcement	•	•
Sensitive data leakage	•	•
SQL Injection, XSS, Path Traversal		•
Authentication analysis, Password strength / complexity, insecure credential transmission		•
TouchID implementation check (iOS)		•
Insecure credential & data storage		•

Training Resources

Acceleration Services

WhiteHat Sentinel delivers a proven and scalable enterprise application security platform, accelerating the identification and remediation of security vulnerabilities. WhiteHat Remediation Outsourcing resources can be integrated into existing software processes to reduce risk without impacting project delivery schedules. Directed Redevelopment delivers remediation of specific vulnerabilities and trains developers on efficiently fixing security vulnerabilities.

Computer Based Training

Our computer based training (CBT) provides an interactive experience to quickly bring security and professional teams up to speed. Your team will learn secure coding, mitigation, and defensive remediation at their own pace – in a webbased environment, accessible from anywhere.

- Continuing Professional Education (CPE) credit
- Enable you to meet PCI requirements
- Flexible pricing options
- Vulnerability detection and remediation with highly targeted virtual patching.

WHITEHAT CUSTOMER SUPPORT

WhiteHat Customer Support Engineers provide enterprise class software support through email, phone or the Customer Support Portal. Unlimited user accounts and Standard Support is included in all Sentinel subscriptions. Gold or Platinum Support options are available as upgrades.

WhiteHat Sentinel Benefits

Unlimited Assessments

- Verification of every vulnerability
- Re-test every vulnerability on demand
- Eliminate trade offs between security and cost with single annual fee

Easy to Manage SaaS-Based Platform

- Cloud based with no hardware or scanning software to install
- Eliminate time-intensive configuration and management concerns
- Assess thousands of websites simultaneously
- Integration with Web Application Firewalls (WAFs) to create virtual patches to remediate vulnerabilities

Open API Integration

- Developers environment such as bug tracking systems
- Security Information and Event Management (SIEM)
- Governance Risk and Compliance (GRC)
- Web Application Firewall (WAF) products

Flexible Reports

- Enterprise class reporting with business unit level aggregation of data in flexible formats
- Advanced analytic capabilities to monitor trends and key statistics such as remediation rate, time to fix vulnerabilities and age of vulnerabilities
- Effectively manage application security program using the WhiteHat Security Index

PCI Compliance

- WhiteHat Sentinel PE, SE and BE services exceed requirements of the PCI DSS by providing ongoing, verified vulnerability assessments for both internal and public websites
- WhiteHat Sentinel PE service includes business logic and penetration testing required by PCI DSS.
- WhiteHat Sentinel integration with Web application firewalls (WAFs) supports the creation of virtual patches to fix vulnerabilities while providing the reports needed to pass auditor inspections.

Asset Identification and Risk Profiling for the Enterprise

- Rapidly identify all website assets – even sites you didn't know you had
- Prioritize Web applications based on business risk to your organization
- Gain a comprehensive understanding of potential attacks

Production Safe

- Customized testing for safety first by analyzing web application inputs, state-changing requests and sensitive functionality
- No performance degradations due to scanning payload being equivalent to a single user
- Assured data integrity due to using benign injections in place of live code
- Custom tuning of scans permitting full coverage without performance impact

WhiteHat SECURITY

WHITEHAT SECURITY, INC. 3970 Freedom Circle Santa Clara, CA 95054 • 1.408.343.8300 • www.whitehatsec.com