WhiteHat Sentinel Dynamic

Web Application Security for Modern and Traditional Web Frameworks and Applications

Modern organizations deploy a plethora of web applications, ranging from external facing corporate websites, customer portals, shopping carts, and login pages to internal facing HR portals. Accessible from any location, web applications today are an easy target for hackers, who can exploit vulnerabilities in these business critical applications and gain access to backend corporate databases.

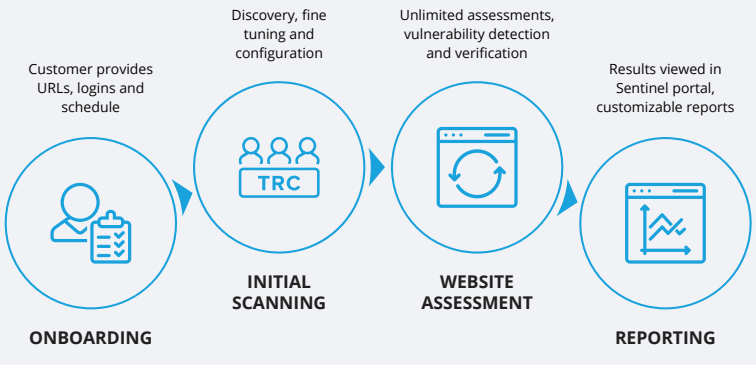
Sentinel Dynamic

WhiteHat Sentinel Dynamic is a software-as-a-service (SaaS) platform that enables your business to quickly deploy a scalable web security program. No matter how many websites you have or how often they change, Sentinel Dynamic can scale to meet any demand. We perform vulnerability assessments pit-crew style, which enables unparalleled efficiency and vulnerability coverage. WhiteHat takes the perspective of the adversary to find weaknesses and help you remediate them before the bad guys exploit them.

- Cloud-based platform with no hardware or scanning software to install.
- Unlimited, continuous and concurrent assessments.
- Automatic detection and assessment of code changes to web applications.
- Open API integration to SIEMs, Bug Tracking systems and WAFs.
- Scalable to fit any environment and assess thousands of websites simultaneously.
- All vulnerabilities verified by the security experts of WhiteHat's Threat Research Center (TRC), virtually eliminating false positives.

Powered by Artificial Intelligence and Machine Learning

WhiteHat Sentinel Dynamic brings together Machine Learning and Human Security Expertise to deliver the most accurate Application Security Testing platform to secure your production applications. Years of valuable data gathered by our highly trained TRC Security experts are used to develop our proprietary AI/ML models. Enables automated and faster delivery of results to customers backed by TRC validation for earlier detection and faster response to possible evolving attacks.



HOW SENTINEL DYNAMIC WORKS

Sentinel Dynamic combines our automated Sentinel Scanner with the world's largest security expert team to provide you with verified vulnerabilities and actionable reports.

SENTINEL PE
Premium Edition

- For mission critical permanent websites with multi-step 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
Baseline Edition

- BE is the foundational solution for basic, less critical websites.
- "Best Value" automated scanning and vulnerability verification solution ideal for low risk, marketing type sites.

FEATURE	DESCRIPTION	SENTINEL PE	SENTINEL SE	SENTINEL BE
Continuous Assessment	Sentinel Dynamic is designed to scan websites continuously and detect code changes to web applications automatically.	✓	✓	✓
Vulnerability Verification	All vulnerabilities are manually verified by the security engineers of our Threat Research Center (TRC), augmented by Artificial Intelligence, virtually eliminating false positives.	✓	✓	✓
On Demand Retests	Ability to retest Sentinel detected vulnerabilities on-demand after remediation to confirm whether the vulnerabilities have been fixed.	✓	✓	✓
Single Page Applications (SPA)	Sentinel Dynamic can scan your single page applications in a production safe and fully automated manner.	✓	✓	✓
Production Safe	Only production-safe payloads are used with no degradation in performance of production websites and applications.	✓	✓	✓
Access to WhiteHat Security Engineers	Unlimited access to the Threat Research Center security engineers, directly from the Sentinel portal to discuss found vulnerabilities found and obtain remediation guidance.	✓	✓	✓
WhiteHat Security Index (WSI)	Access to a single score to monitor and manage instant, visual overview of the robustness of your website security with one score to monitor and manage.	✓	✓	✓
Testing Internal QA/Staging Environments	Internal pre-production/staging environments can be rigorously tested, if needed, to catch vulnerabilities before they reach production.	✓	✓	✓
Flexible Reports, Analytics and Peer Benchmarking	Enterprise class reporting and analytics with business unit level aggregation of data in flexible formats to monitor security trends for all your websites, as well as benchmarking your score against industry averages.	✓	✓	✓
Full Configuration and Form Training	This includes configuring scanners to safely scan websites with forms and logins.	✓	✓	
Authenticated Scanning	Supports automated and authenticated scanning of sites, including those that require multi-factor authentication.	✓	✓	
Business Logic Assessments	Manual penetration testing of the application layer to find complex business logic vulnerabilities that cannot be discovered by scanners alone.	✓		

Supported Vulnerabilities

Sentinel Dynamic tests for a large number of vulnerabilities* including:

** A compatible list per product line available upon request*

Technical Vulnerabilities - WASC Threat Classification 2.0

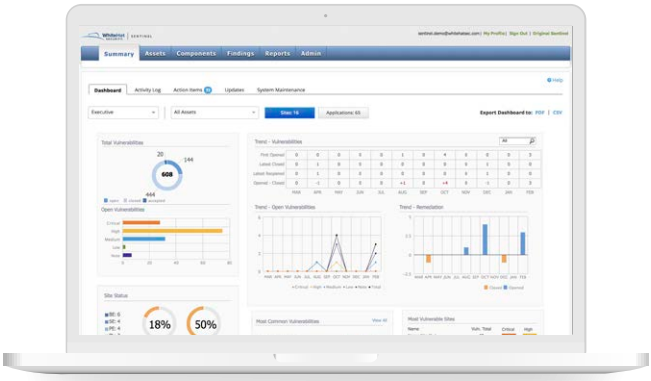
- Application Misconfiguration
- Directory Indexing
- HTTP Response Smuggling
- Improper Input Handling
- Insufficient Transport Layer Protection
- OS Commanding
- Remote File Inclusion
- SQL Injection
- XML External Entities
- XQuery Injection
- Content Spoofing
- Fingerprinting
- HTTP Response Splitting
- Improper Output Handling
- Mail Command Injection
- Path Traversal
- Routing Detour
- SSL Injection
- Injection
- Cross-Site Scripting
- Format String Attack
- Improper File System Permissions
- Information Leakage
- Null Byte Injection
- Predictable Resource Location
- Server Misconfiguration
- URL Redirector Abuse
- XPath Injection

Technical Vulnerabilities - OWASP Top 10:

- A1 - Injection
- A2 - Broken Authentication and Session Management
- A3 - Sensitive Data Exposure
- A4 - XML External Entities (XXE)
- A5 - Broken Access Control
- A6 - Security Misconfiguration
- A7 - Cross-Site Scripting (XSS)
- A8 - Insecure Deserialization
- A9 - Using Components with Known Vulnerabilities
- A10 - Insufficient Logging & Monitoring (Out of Scope)

Enterprise class reporting in flexible formats

The Sentinel user interface provides you with reports enabling organizations to understand the performance of their security programs and improve their security posture. Advanced analytic capabilities monitor trends and key statistics such as remediation rates, time-to-fix and age of the vulnerabilities. Trending analysis tracks real-time and historical data to measure your risk exposure over time and to provide you visibility into your most and least secure websites at a glance.



Site: www.retailsite.com

WhiteHat Security Index	
495	
Global Percentile	Industry Percentile
25%	42%
Industry: Retail	

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.

What Makes Sentinel Dynamic Unique?

Easy to deploy, concurrent and scalable

Sentinel Dynamic is an easy to deploy cloud-based platform and can concurrently scan an unlimited number of sites without slowing you down. It is scalable to fit any environment and matches your pace of development. We can onboard and test 10,000+ websites concurrently.

Continuous assessment methodology

Sentinel Dynamic offers true continuous assessment, constantly scanning your website as it evolves. Automatic detection and assessment of code changes to web applications, alerts for newly discovered vulnerabilities and the ability to retest a vulnerability without having to test from the beginning, therefore, offering an "always-on" risk assessment.

Production safe

Sentinel Dynamic is completely safe for production websites, with no performance degradations. We assure data integrity by using benign injections in place of live code and custom tuning of scans permits full coverage without performance impact.

Verified, actionable results with near zero false positives

WhiteHat's Threat Research Center (TRC) validates every vulnerability, virtually eliminating false positives. We enable you to streamline the remediation process by prioritizing vulnerabilities based on severity and threat, so you can focus on remediation and your overall security posture.

Open API integration

Sentinel Dynamic can be integrated with popular Bug Tracking systems, Security Information and Event Management (SIEM), Governance Risk and Compliance (GRC) and Web Application Firewall (WAF) products.

Unlimited access to web security experts

With Sentinel Dynamic you have unlimited access to our Threat Research Center (TRC), custom remediation guidance, and the "Ask a Question" feature which enables you to access security experts at any time, right from the Sentinel Portal.

PCI Compliance

Sentinel Dynamic services exceed the requirements on PCI DSS 3.1 by providing ongoing, verified, vulnerability assessments for both internal and public websites. Sentinel PE service includes business logic assessments and penetration testing required by PCI DSS. Sentinel integrations with WAFs supports the creation of virtual patches to fix vulnerabilities while providing the reports needed to pass auditor inspections.

Fully Automated Single Page Application (SPA) Scanning

Sentinel Dynamic can scan single page applications, as well as traditional applications. Using proprietary technology, we enable fully automated scanning and testing of SPA sites. Our scanner loads your web application into a browser and interacts with it exactly the same way that a user would. Production safe assessments which find vulnerabilities other traditional scanning tools will miss.

WHITEHAT SECURITY, INC. 1741 Technology Dr. #300, San Jose, CA 95110 • 1.408.343.8300 • www.whitehatsec.com

WhiteHat SECURITY