SYNOPSYS®

WhiteHat DAST

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. Web applications are an appealing target for hackers, because they can exploit vulnerabilities in these business-critical applications to gain access to back-end corporate databases.

WhiteHat DAST

WhiteHat™ DAST is a software-as-a-service (SaaS) dynamic application security testing (DAST) solution that allows your business to quickly deploy a scalable web security program. No matter how many websites you have or how often they change, WhiteHat DAST can scale to meet any demand. It provides security and development teams with fast, accurate, and continuous vulnerability assessments of applications in QA and production, applying the same techniques hackers use to find weaknesses, so you can remediate them before the bad guys exploit them.

WhiteHat DAST is a cloud-based solution that requires no hardware or scanning software to be installed. It provides

- Unlimited, continuous, and concurrent assessments
- Automatic detection and analysis of code changes in web applications
- Open API integration to security information and event management solutions, bug-tracking systems, and web application firewalls

WhiteHat DAST fits into any environment and is highly scalable, with the ability to assess thousands of websites simultaneously. Furthermore, all vulnerabilities are verified by Synopsys security experts, virtually eliminating all false positives.

Powered by artificial intelligence and machine learning

WhiteHat DAST brings together machine learning (ML), artificial intelligence (AI), and expert vulnerability analysis to deliver the most accurate dynamic application security testing results, so you can verify the security of your web applications without slowing down developers with false positives.

Years of valuable data gathered by our highly trained security experts is used to develop our proprietary AI/ML models. This approach provides fast, automated results augmented by expert validation, enabling earlier detection and faster response to cyberattacks.

How WhiteHat DAST works

WhiteHat DAST combines automated application scanning with the world's largest security expert team to provide you with verified vulnerabilities and actionable reports.

Onboarding

Customer provides URLs, logins, and schedule

Initial scanning

Discovery, fine-tuning, and configuration

Website assessment

Unlimited assessments, vulnerability detection, and verification

Reporting

Results displayed in a portal with customizable reports

Choose the WhiteHat edition best suited to your needs

WhiteHat PE (Premium Edition)	WhiteHat SE (Standard Edition)	WhiteHat BE (Baseline Edition)
• For mission-critical permanent websites with multistep forms and rigorous compliance requirements • Includes all SE features and business logic testing	• For permanent websites that are not necessarily mission-critical • Includes all BE features and tests for issues involving multistep forms and logins	• BE is the foundational solution for basic, less-critical websites • Includes automated scanning and vulnerability verification, ideal for lower-risk websites

FEATURE	DESCRIPTION	PE	SE	BE
Continuous assessment	Websites are scanned continuously to automatically detect code changes to web applications.	●	●	●
Vulnerability verification	All vulnerabilities are manually verified by security experts and augmented by AI, virtually eliminating false positives.	●	●	●
On-demand retests	Websites can be retested on demand after detected vulnerabilities are remediated to confirm that they have been fixed.	●	●	●
Single-page applications	Single page applications scanned in a production-safe and fully automated manner.	●	●	●
Production safe	Only production-safe payloads are used, ensuring no degradation in performance.	●	●	●
Access to WhiteHat security engineers	Unlimited and direct access to security experts via the portal to provide remediation guidance.	●	●	●
WhiteHat Security Index (WSI)	A single score provides an instant, visual overview of the robustness of your website security.	●	●	●
Testing internal QA/staging environments	Internal preproduction/staging environments can be rigorously tested 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 provides an overview of security trends for all your websites, and benchmarks your score against industry averages.	●	●	●
Full configuration and form raining	Scanners can be configured to safely scan websites with forms and logins.	●	●	
Authenticated scanning	Automated and authenticated site scanning, including those that require multifactor authentication.	●	●	
Business logic assessments	Manual penetration testing of the application layer finds complex business logic vulnerabilities that cannot be discovered by scanners alone.	●		

What Makes WhiteHat DAST Unique

Enterprise-class reporting in flexible formats

Understand the performance of your security programs and improve application security posture with powerful built-in reports. Advanced analytics 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 provide you with visibility into your most- and least-secure websites at a glance.

WhiteHat Security Index

The WhiteHat Security Index (WSI) gives you an instant, visual overview of the robustness of your website security, providing one score that indicates 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.

Easy to deploy, concurrent, and scalable

WhiteHat DAST is an easy-to-deploy cloud-based dynamic security testing solution that can onboard and test over 10,000 websites concurrently without slowing you down. It is scalable to fit any environment and matches your pace of development.

Continuous assessment methodology

WhiteHat DAST offers true continuous analysis, constantly scanning your website as it evolves. Automatic detection and analysis 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 offer an "always on" risk assessment.

Production safe

WhiteHat DAST is completely safe for production websites with no performance degradations. Data integrity is assured 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

Every vulnerability is validated by security experts and augmented by AI, virtually eliminating false positives. This enables you to streamline the remediation process, prioritize vulnerabilities based on severity and threat, and focus on remediation and your overall security posture.

Open API integration

WhiteHat DAST can be integrated with popular bug-tracking systems; security information and event management solutions; governance, risk, and compliance products; and web application firewalls (WAFs).

Unlimited access to web security experts

With WhiteHat DAST, you have unlimited access to expert web application security testers and custom remediation guidance. The "Ask a Question" feature enables you to access security experts at any time, right from the portal.

PCI compliance

WhiteHat DAST exceeds the requirements of PCI DSS 3.1 by providing ongoing, verified vulnerability assessments for both internal and public websites. WhiteHat PE includes business logic assessments and penetration testing as required by PCI DSS. Integrations with WAFs support the creation of virtual patches to fix vulnerabilities while providing the reports needed for auditor inspections.

Fully automated single page application scanning

WhiteHat DAST provides fully automated scanning and testing of single-page applications as well as traditional applications. It loads your web application into a browser and interacts with it the same way a user would. Production-safe assessments find vulnerabilities other traditional scanning tools miss.

WhiteHat DAST | Detectable Vulnerabilities

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

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 (Out of Scope)
- A10 - Insufficient Logging & Monitoring (Out of Scope)

Note: A compatible list per product line available upon request

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