Fortify WebInspect (DAST)

Micro Focus Fortify WebInspect is a dynamic application security testing (DAST) tool that identifies application vulnerabilities in deployed web applications and services.

WebInspect is an automated dynamic testing solution that provides comprehensive vulnerability detection and helps security professionals and QA testers identify security vulnerabilities and configuration issues. It does this by simulating real-world external security attacks on a running application to identify issues and prioritize them for root-cause analysis. WebInspect has numerous REST APIs to benefit integration and has the flexibility to be managed through an intuitive UI or run completely via automation.

Product Highlights

Automation with Integration
WebInspect can be run as a fully-automated solution to meet DevOps and scaling needs, and integrate with the SDLC without adding additional overhead.

- REST APIs help achieve a tighter integration and help automate scans and check whether compliance requirements have been met.
- Leverage prebuilt integrations for Micro Focus Application Lifecycle Management (ALM) and Quality Center, and other security testing and management systems.
- Powerful integrations allow teams to re-use existing scripts and tools. WebInspect can easily integrate with any Selenium script.
- Scan RESTful web services: supports Swagger and OData formats via WISwag command line tool, enabling WebInspect to fit into any DevOps pipeline.
- Base settings: ScanCentral Admin can pre-configure a scan template and provide that to users to scan their apps—no security knowledge needed.

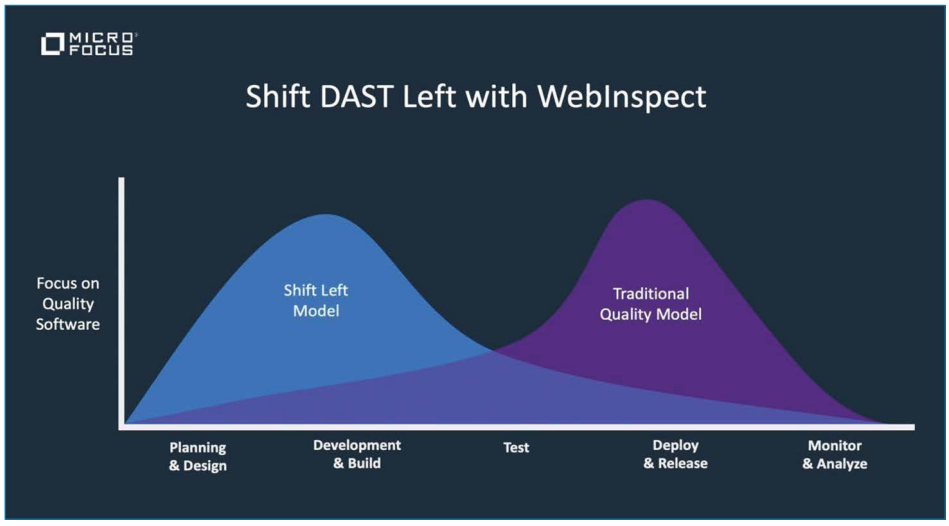

Figure 1. Detect vulnerabilities earlier in the SDLC with WebInspect

Key Features

Functional Application Security Testing (FAST)
Don't be limited by IAST! FAST can take all the functional tests and use those in the same way IAST does, but then it keeps crawling. Even if a functional test misses something, FAST won't miss it.

Hacker-Level Insights
View findings such as client-side frameworks and the version numbers—findings that could become vulnerabilities if not updated.

Manage Enterprise Application Security Risk
Monitor trends within an application and take action on the most critical vulnerabilities first to meet DevOps needs.

Available On-Premise or as a Service
Start quickly and scale as needed with the flexibility of on-premise, SaaS, or hybrid.

Compliance Management
Pre-configured policies and reports for all major compliance regulations related to web application security, including PCI DSS, DISA STIG, NIST 800-53, ISO 27K, OWASP, and HIPAA.

Increase Speed with Horizontal Scaling
Horizontal scaling creates little versions of WebInspect using Kubernetes that just focus on processing JavaScript. This allows the scans to work in parallel, allowing for much faster scans.

Scan Any API for Improved Accuracy
Get a complete story around APIs, whether it's SOAP, Rest, Swagger, OpenAPI, or Postman.

Key Benefits

Find Vulnerabilities Faster and Earlier
WebInspect can be tuned and optimized for your application to find vulnerabilities faster and earlier in the SDLC.

Enhance scan with agent technology that expands the coverage of the attack surface and detects additional types of vulnerabilities.

- WebInspect Agent integrates dynamic testing and runtime analysis to enhance your findings and scope. It identifies vulnerabilities by crawling more of the app, expanding coverage of the attack surface, and exposing exploits better than dynamic testing alone.

Prioritization with advanced technologies:

- Run custom policies that are tuned towards high speed with policy manager.
- Simultaneous crawl and audit.
- Deduplication: Reduce number of attacks sent, by avoiding scanning the same class/function in a different part of the app.
- Check Avoidance: Reduce # of attacks sent by avoiding sending multiple attacks to a specific check type if the agent determines the app can handle the attack. Info is loaded into Fortify Software Security Center (SSC) & used with Fortify Static Code Analyzer (SCA) scan results where issues are correlated.
- Redundant Page Detection allows for reduced scan times.
- Fix vulnerabilities faster as devs are provided with line of code detail and return stack trace info.

Save Time with Automation and Agent Technology

- Save time and resources with features like redundant page detection, automated macro generations, incremental scanning, and containerized delivery.
- Optimize the scanning process, increase speed, and improve accuracy.

Crawl Modern Frameworks and Web Technologies
WebInspect is a comprehensive dynamic application scanner that has the ability to crawl modern frameworks and web technology with a comprehensive audit of all vulnerability classes.

- Support for the latest web technologies including HTML5, JSON, AJAX, JavaScript, HTTP2, and more.
- Single Page Application (SPA) Detection supporting these common frameworks: Angular, AngularJS, React, GWT, Vue, Dojo, and Backbone.
- Test mobile-optimized websites as well as native web service calls.
- WebInspect provides features like automatic macro generation, macro validation, and fix validation, to enable small teams to detect and remediate vulnerabilities at scale.
- A solution to SCHANNEL lockdown issues, OpenSSL Preview provides a simple solution for environments where SSL is being restricted either by registry or group policy.

Manage Enterprise AppSec Risk with ScanCentral DAST
Manage application security risk across the enterprise with reports for remediation and management oversight. Monitor trends and take action on vulnerabilities within an application. Build an enterprise-wide AppSec program that manages and provides visibility to your risk profile via dashboards and reports, so you can confirm remediation, track metrics, trends and progress. ScanCentral DAST can be used as an orchestration platform to run hundreds of thousands of scans, enabling a small team of AppSec professionals to manage an entire organization.

- **Data Retention Policies:** Rather than having to manually delete this data from ScanCentral, an admin can choose how long they want to keep the data before it's automatically deleted
- **Deny Intervals:** Users need to automate when they can and can't scan. If they're in the middle of testing, they need the app to be up, so this pauses the scan automatically.
- **Site Explorer**: Standalone allows developers to get rich remediation information and WebInspect-like views.

Contact us at **CyberRes.com**
Like what you read? Share it.

About Fortify

Fortify offers the most comprehensive static and dynamic application security testing technologies, along with runtime application monitoring and protections, backed by industry-leading security research. Solutions can be deployed in-house or as a service to build a scalable, nimble Software Security Assurance program that meets the evolving needs of today's IT organization.

About Micro Focus

Micro Focus is a leading provider of security and compliance solutions for the modern enterprise that wants to mitigate risk in their hybrid environment and defend against advanced threats. Based on market-leading products from Micro Focus Data Security, ArcSight, and Fortify, the Micro Focus Security Intelligence Platform uniquely delivers the advanced correlation and analytics, application protection, and data security to protect today's hybrid IT infrastructure from sophisticated cyber threats.

Learn more at
www.microfocus.com/en-us/cyberres/application-security/webinspect

CyberRes
A Micro Focus Line of Business