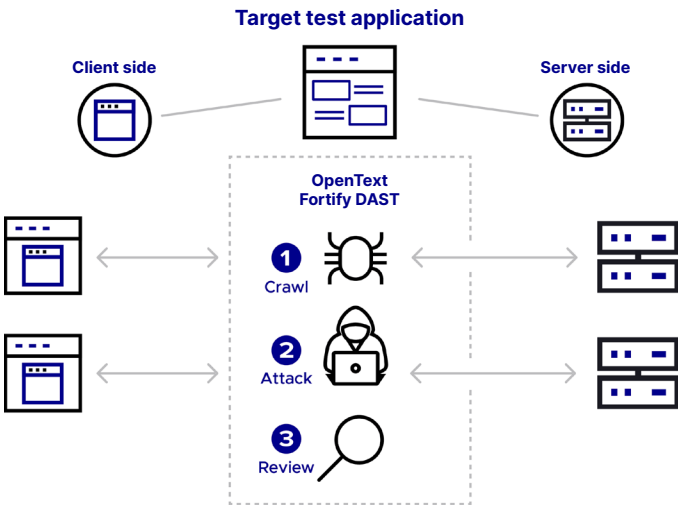
OpenText Fortify DAST

Dynamic application security testing (DAST) tool identifies application vulnerabilities in deployed web applications and services

OpenText™ Fortify™ DAST is an automated DAST 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. OpenText Fortify DAST has numerous REST APIs to benefit integration and has the flexibility to be managed through an intuitive UI or run completely via automation. OpenText Fortify DAST also has a single, cohesive method of defining authentication, whether it be static, dynamic, or pulling tokens from macros.

OpenText Fortify DAST



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.
- **HAR files for workflow macros**
  OpenText Fortify DAST can use HAR files for workflow scanning, ensuring important content is covered during scans.
- **Manage enterprise application security risk**
  Monitor trends within an application and take action on the most critical vulnerabilities first to meet DevOps needs.
- **Flexible deployment**
  Start quickly and scale as needed with the flexibility of on-premise, SaaS, or AppSec-as-a-service.
- **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 OpenText Fortify DAST 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**
  OpenText Fortify DAST allows users to configure API scanning to cover any authentication scenario with GraphQL, gRPC, SOAP, Postman, and Swagger. It also allows users to automatically pull bearer tokens from an identity provider.
- **Client-side software composition**
  Client-side Software Composition Analysis (SCA) provides CVEs of client-side libraries, health data of open source projects, and an exportable CycloneDX SBOM.

Product highlights

Automation with integration

OpenText Fortify DAST 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 OpenText Application Lifecycle Management (ALM), OpenText Application Quality Management, and other security testing and management systems.
- Powerful integrations allow teams to re-use existing scripts and tools. OpenText Fortify DAST can easily integrate with any Selenium script.
- Scan RESTful web services: supports Swagger and OData formats via WISwag command line tool, enabling OpenText Fortify DAST 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.

Key benefits

Find vulnerabilities faster and earlier

OpenText Fortify DAST can be tuned and optimized for your application to find vulnerabilities faster and earlier in the SDLC scans with agent technology that expands the coverage of the attack surface and detects additional types of vulnerabilities.

- OpenText Fortify DAST 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 the number of attacks sent, by avoiding scanning the same class/function in a different part of the app.
- 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.
- OpenText Fortify DAST continues to scan, even in two-factor authentication (2FA) environments.

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

OpenText Fortify DAST crawls modern frameworks and web technologies with a comprehensive audit of all vulnerability classes.

- Support for the latest web technologies including HTML5, JSON, AJAX, JavaScript, HTTP/2, and more.
- Test for a new class of vulnerabilities called “Out of Band” or OAST Vulnerabilities. Using the public OAST server, OpenText Fortify DAST can detect OAST vulns such as Log4Shell.
- 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.
- OpenText Fortify DAST provides features like automatic macro generation, macro validation, and fix validation, to enable small teams to detect and remediate vulnerabilities at scale.
- Run Linux versions of OpenText Fortify DAST and ScanCentral DAST through the API.

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.

- **ScanCentral DAST Visualization:** View and triage DAST vulnerabilities in ScanCentral DAST.
- **User and domain restrictions:** Centralized management of DAST users is complex. User and domain restrictions allow an admin to put rules in place to ensure quality scans when using ScanCentral DAST in a self-service model.

- **PostgreSQL:** MS SQL is an expensive option for a database, so PostgreSQL provides another option when installing ScanCentral DAST without sacrificing speed and quality.
- ScanCentral DAST integrates with Kubernetes for scaling sensors, giving both cost savings and ensuring each scan has a new environment to run on.
- **ScanCentral Credential Management:** Save time and update all passwords in one place.
- **ScanCentral DAST repo integration:** Pull scan configuration artifacts from a repository at runtime, no need to update settings configurations.

About OpenText Fortify on Demand

OpenText™ Fortify on Demand offers a comprehensive suite of products that bring holistic security and visibility to developers and AppSec professionals. They include automated integrations for any tool, anywhere in the SDLC, and a robust set of capabilities available on-premises, cloud-hosted, or as a service.

About OpenText

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

Learn more about application security ›

opentext™