OpenText Core Application Security: FedRAMP application security as a service

OpenText Core Application Security is uniquely designed to help government agencies adhere to internal risk management policies and government mandates. Developers confidently build security throughout the entire software development life cycle, and security professionals review findings and achieve required compliance reporting.

OpenText™ Core Application Security for the U.S. Federal sector, is the first and leading cloud-accessible managed application security testing platform. It is the only application security-managed vendor that is operating on AWS GovCloud. It is JAB-certified and FedRAMP-authorized. With access to OpenText Core Application Security, government agencies and programs can quickly, easily, cost-effectively, and confidently perform application security testing and obtain the fastest, most accurate results.

Product highlights

Take control of open-source security

OpenText Core Software Composition Analysis Assessment Subscription allows customers to perform automated software composition analysis to identify open-source components and other third-party software in an application. The results of a OpenText Core Software Composition Analysis Assessment include the software bill-of-materials (SBOM) along with security issues and license information associated with the identified components.

Identify and eliminate vulnerabilities earlier

Our comprehensive static scan assessments help developers identify and eliminate source or byte code vulnerabilities. Powered by OpenText Static Application Security Testing, OpenText Core Application Security static assessments detect over 1,166 unique categories of vulnerabilities across 29 programming languages that span over 1 million individual APIs.

- **Static assessment capabilities with**

OpenText Core Application Security are among the most comprehensive and flexible available worldwide. That includes support for ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (with VBScript), COBOL, ColdFusion CFML, GoLang, HTML, Java (including Android), JavaScript/ AJAX/ Node.js, JSP, Kotlin, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML.

- **Quick and easy scan initiation**

Upload application source code from IDE, repository, build, or CI server. Manual upload via the FoD portal and automatic upload via our ecosystem of integration and flexible API.

Access detailed reporting of static scan results and vulnerability management

Our vulnerability management is purpose-built for the FedRAMP environment and spans:

- Mapping to required and relevant vulnerability frameworks, including FISMA (NIST 800.53), DISA Application Security and Development STIG, MITRE CWE, OWASP, PCI, and many others.
- Reporting in detail the application against the DISA Application Development STIG in support of the Risk Management Framework (RMF) controls. This reporting provides a “pass/fail” score of the application vs. the DISA Application STIG and, thereby the RMF controls.
- Submitting vulnerability reports as part of the documentation packages for the Authority to Operation (ATO), Certification and Accreditation (C & A), Command Cyber Readiness Inspection (CCRI), and other Department of Defense (DoD) or federal certification milestone reports. Such documentation packages provide the artifacts required to demonstrate that automated source code analysis has been completed per the mandatory DISA Application Security and Development STIG requirement.

Conduct dynamic application security testing

OpenText Core Application Security Dynamic Application Security assessments mimic real-world attacks using automated techniques to comprehensively analyze complex web applications and services. Featuring OpenText Dynamic Application Security Testing for automated dynamic scanning, OpenText Core Application Security provides a full-service experience as all scans include macro creation for authentication and a full audit of results by our experts to remove false positives and for overall quality.

Assessment includes:

- Ability to recognize over 250 unique vulnerability categories for web applications in QA, staging, or production.

- Expanded coverage, accuracy, and remediation details with IAST runtime agent.
- Assess public-facing and internal websites and web services.
- Generate virtual patches for all leading web application firewalls (WAFs).

Conduct Dynamic API Assessments

OpenText Core Application Security offers Dynamic API Assessments that mimic real-world hacking techniques using automated techniques to analyze your API endpoints comprehensively.

API Assessment includes:

- Verify the API URL and customer provided OpenAPI JSON specification or Postman collection that describes API endpoints to be assessed.
- Perform an automated OpenText Dynamic Application Security Testing assessment of designated API endpoints using customer provided.
- OpenAPI JSON specification or Postman collection
- Review of prioritized results by an OpenText Core Application Security security expert, including false positive removal

Flexible plans to fit your business's mission

- OpenText Core Application Security testing services are available by purchasing and redeeming Assessment Units. Assessment Units are prepaid credits redeemed for single assessments or application subscriptions, offering flexibility to allocate your investment throughout the year.
- Assessment Units are valid for 12 months and may be redeemed individually. An application subscription allows for one application to be assessed an unlimited number of times for basic Static service or monthly for Static+ service during the 12 months commencing on the date of purchase.

Key benefits

- Enables agencies to extend and scale their Software Security Assurance Programs quickly and efficiently.
- Combines the most advanced, comprehensive application testing methodologies with manual expert review.
- Provides access to a centralized portal with intuitive, user-friendly, and comprehensive application dashboards, vulnerabilities, and work streams for a single application or across your entire portfolio.
- Integrates on-premise and cloud-based application security testing and program management solutions for U.S. government agencies.
- Over 29 programming languages covered: ABAP/ BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (with VBScript), COBOL, ColdFusion CFML, GoLang, HTML, Java (including Android), JavaScript/ AJAX/ Node.js, JSP, Kotlin, MXML (Flex), Objective C/ C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic, and XML.
- Automate CI/CD pipeline security with Swagger-supported RESTful APIs, GitHub repository, and plugins for Azure DevOps, VSTS, and Jenkins.
- Integrates with defect management tools and covers security issues caused by open-source components with software component analysis tools integration.

Key features

Leader in Gartner® Magic Quadrant™
OpenText Core Application Security has been named a leader in AppSec testing for the 10th year in a row.

Comprehensive assessments
OpenText Core Application Security static assessments detect over 1,166 unique categories of vulnerabilities across 29 programming languages that span over 1 million individual APIs.

Achieve compliance requirement
JAB Certified, FedRAMP authorized.

Quick and easy scan initiation
Upload application source code from IDE, repository, build, or CI server. Manual upload via the OpenText Core Application Security portal and automatic upload via our ecosystem of integration and flexible API.

Save time with Smart Fix
Access a flow diagram for better usability to isolate, identify, and remediate vulnerabilities across functional relationships within the application.

Flexible scanning options
AppSec testing services are available by purchasing and redeeming Assessment Units for single assessments or application subscriptions.

Security expertise and account support
Access to a dedicated technical account management team 24/7.

Let's get started

We have a team dedicated to the application security needs within the U.S. Federal sector. Let us share how we can help your agency meet its business objectives.

Learn more ›

opentext™