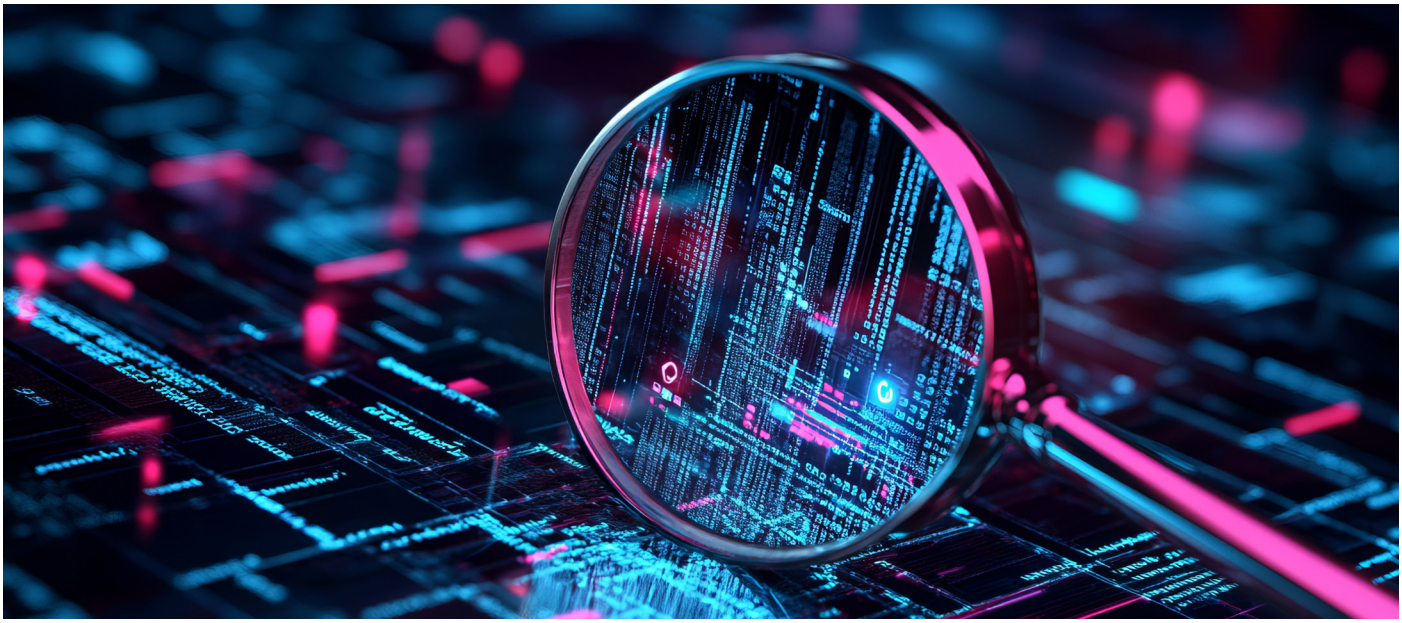
OpenText Core Application Security

As a service application security testing, vulnerability management, expertise, and support



Benefits

- Comprehensive AppSec as a service
- Built for DevSecOps
- Enterprise-grade
- Accelerates AppSec initiatives

Comprehensive AppSec as a service

OpenText™ Core Application Security is a powerful AppSec solution that can jumpstart your application security program. Comprehensive features, scalability, and integration capabilities make it an ideal choice for organizations looking to identify vulnerabilities, prioritize remediation efforts, and establish a culture of continuous security improvement.

- The only AppSec provider to offer SAST, SCA, DAST, and MAST as a unified service.
- Flexible consumption through the purchase of Assessment Units.
- Comprehensive support and on-demand experts to help you audit/triage results.
- Dedicated Customer Success Manager to assist in your AppSec journey.
- Automatic updates for the latest security, including Rule Packs from the Software Security Research Team.
- OpenText Core Application Security and OpenText Core Software Composition Analysis (OpenText's software composition analysis solution) are FedRamp Certified.

Built for DevSecOps

OpenText Core Application Security helps your AppSec keep pace with the "everything-as-code" era, transitioning from point of friction to enablement without sacrificing quality.

- Expand the breadth of integrations and extensibility into your ecosystem.
- Comprehensive shift-left security for next-gen architectures.
- Accurate, reliable, repeatable results.
- Real-time, centrally managed, enterprise-class reporting and dashboards.

Enterprise-grade AppSec

Regardless of your current application security situation, OpenText Core Application Security can help you mature your AppSec program, meet program goals, and integrate application security while scaling from one to hundreds, or even thousands of apps.

- Enables collaboration between the AppSec team and developers to ensure adoption.
- Ensures separation of duties and collaborative auditing, with a full audit trail.
- Supports one to thousands of scans per day.
- Supports the challenges of the modern enterprise.
- Empowers your organization for AppSec success.
- Enables headless AppSec programs through APIs.

Accelerate AppSec initiatives

Launch your application security initiative in a day. Expand your Software Security Assurance program and achieve all the advantages of security testing, vulnerability management, tailored expertise, and support—without the need for additional infrastructure or resources.

- Start immediately, scale rapidly (low barrier for adoption).
- Easy to use and consume.
- Access to security expertise (24×7 testing and support).
- Focus on your core business while maturing your AppSec program.

Key features

Static application security assessments

	Static	Static*
Application type	Web, mobile, or thick-client	Web, mobile, or thick-client
OpenText Static Application Security Testing analysis	+	+
Audit Assistant automated audit	+	+
Security Assistant	+[1]	+[1]
Security expert manual review	[2]	+
Open source analysis	+[3]	+[3]

1. Subscriptions only
2. Security expert review optional for first subscription scan only
3. Added Sonatype subscription needed

Static assessments help developers identify and eliminate vulnerabilities in source, binary, or byte code to build more secure software. Powered by OpenText Static Application Security Testing, over 1,654 vulnerability categories across 33+ languages and more than one million individual APIs.

OpenText Core Application Security static assessments can also include a review by our security experts and the Audit Assistant machine learning platform to remove false positives and ensure overall quality so that development teams can maximize their remediation efforts early in the software lifecycle. OpenText Core Application Security seamlessly fits into customers' existing agile or DevOps processes with out-of-the-box IDE, continuous integration/continuous deployment (CI/CD), and bug tracker integrations.

- Supports 33+ languages: 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, JSON/YAML and Docker (Dockerfile).
- Named Contributing Developer licensing model for modern application development.
- Real-time vulnerability identification with Security Assistant.
- Actionable results in minutes for most applications with DevOps automation.

Open source software composition assessments

Third-party components make up a significant portion of many applications' codebase and the use is growing every year. This makes software composition analysis a "must-have" AppSec capability that uses natural language processing to dynamically monitor every GitHub commit to every open source project, advisory websites, Google search alerts, OSS Index, and a plethora of vulnerability sites.

OpenText Core Application Security Software Composition Analysis is much more than a simple comparison of declared dependencies against the National Vulnerability Database (NVD). New vulnerabilities are regularly discovered by OpenText Core Software Composition Analysis's state of the art machine learning algorithms with extremely high accuracy added to the proprietary knowledgebase. This means more vulnerabilities are found and caught but it also reduces the amount of false positives providing a much better experience when remediating them. OpenText Core Application Security simplifies the onboarding and scanning process by combining static and composition analysis into a single integration point, whether that's in the IDE or CI/CD pipeline. The comprehensive bill-of-materials (including security vulnerabilities, recommendations, and license details) are delivered as a fully integrated experience for security professionals and developers alike.

- Provides code once for both SAST and software composition analysis.
- Supports Java, .NET (technologies), JavaScript, PHP, Ruby, Go, Python, Objective-C, and Swift.
- Integrated results delivered one platform for remediation, reporting, and analytics.
- Easily automate open source security, compliance, and project health.
- Detects 70 percent more vulnerabilities than the NVD database alone.

Dynamic Web Application Security Assessments

	Dynamic	Dynamic*
Application type	Website OR APIs	Website OR APIs
OpenText Dynamic Application Security Testing analysis	+	+
Verify URL & authentication	+	+
Security expert manual review	+	+
Continuous application monitoring	+[4]	+[4]
Manual vulnerability testing		+

4. Subscriptions only. Includes vulnerability and risk profile scanning.

Dynamic assessments mimic real-world hacking techniques and attacks using both automated and manual techniques to provide comprehensive analysis of complex web applications and services. Featuring OpenText Dynamic Application Security Testing for automated dynamic scanning, Fortify on Demand provides a full-service experience.

All scans include macro creation for authentication and a full audit of results by our experts to remove false positives and ensure overall quality—a level of service you don't get with other providers. Our manual testing focuses on the types of vulnerabilities that skilled hackers exploit, including authentication, access control, input validation, session management, and business logic testing.

- Scanning intranet applications is made simpler with an out of box VPN solution (OpenText Core Application Security Connect).
- Identifies over 250 unique vulnerability categories for web applications in QA, staging, or production.
- Assess public-facing and internal web sites and APIs.
- Generate virtual patches for all leading web application firewalls (WAFs).
- For APIs we asess customer provided OpenAPI JSON specification of Postman collection.

OpenText Core Application Security Connect

If your web application is internally facing, you can use OpenText Core Application Security to set up site-to-site VPN. OpenText Core Application Security Connect implements an OpenVPN server and client configuration to create secure site-to-site connections. The OpenVPN client is available as a Docker container.

DAST Automated

This expansion of OpenText Core Application Security DAST offerings enables dynamic scanning in the DevOps pipeline, where rapid turn-around time and increased scan frequency is required. This new offering enables developers to perform dynamic scanning earlier in the development lifecycle.

It does this through automated scanning of web APIs, functional test workflows, or web-site segments invoked by the customers through their CI/CD integrations, portal, or by utilizing the OpenText Core Application Security API. This self-service capability empowers customers with options such as policy selection and timeboxing to control scan speed and testing depth.

For assistance in establishing a good baseline scan, customers can request one-time per application set-up support. Our OpenText Core Application Security delivery team will create a login macro file and perform false-positive removal of scan results. Customers can then leverage the login macro file for subsequent submissions.

Mobile Application Security Assessments

	Mobile	Mobile*
Application type	Website OR APIs	Website OR APIs
Vulnerability analysis (mobile binary)	+	+
Endpoint reputation analysis	+	+
Security expert manual review	+	+
OpenText Dynamic Application Security Testing analysis (backend services)		+
Manual vulnerability testing		+

OpenText Core Application Security delivers comprehensive, end-to-end mobile security with real-world mobile application security testing across all three tiers of the mobile ecosystem: client device, network, and APIs. Similar to dynamic testing for web applications, mobile assessments utilize the compiled application binary and employ the same techniques that hackers utilize to exploit vulnerabilities in mobile applications—whether they are developed internally, outsourced, or acquired.

More than just simple reputation or behavioral analysis, OpenText Core Application Security mobile assessments provide true security testing for companies serious about securing their mobile applications.

- Supports iOS and Android mobile applications.
- Identifies over 300 unique vulnerability categories, from mobile binary to backend services.
- Emphasizes security vulnerability identification in addition to behavioral and reputation analysis.
- Delivers automated mobile binary assessments in less than five minutes for most applications.
- Performs manual testing on physical devices.

Resources

OpenText Core Application Security
Learn more ›

OpenText Core Application Security video
Watch the demo ›

OpenText Core Application Security community
Join our community ›

Assessment Units

OpenText Core Application Security static, dynamic, and mobile application security testing services are available by purchasing and redeeming Assessment Units. OpenText Core Application Security Assessment Units are prepaid credits that are redeemed for single assessments, application subscriptions or Named Contributing Developer subscriptions, offering the flexibility to allocate your investment throughout the year.

Assessment Units are valid for 12 months and may be redeemed individually. For each single assessment or subscription requested, customers choose a combination of one assessment type (dynamic, static, or mobile) and one assessment service level. An application subscription allows for one application to be assessed an unlimited number of times during the 12-month period. All assessments include one remediation validation scan within one month of the assessment.

Support

OpenText Core Application Security is designed as a self-service platform that provides in depth how-to guides covering the platform and tool usage as well as chat support and helpdesk ticketing available 24×7 through a dedicated support team. For larger customers, the service includes a CSM (customer success manager) to help drive adoption of the service and ensure customer success. The CSM is the customer's primary point of contact, proactively supporting the on-boarding of the first development team, managing support issues, and holding regularly scheduled service reviews. Additional onsite or remote support services are available for an additional charge. Customers must have internet connectivity to access OpenText Core Application Security.

opentext™