

# Application Security Program Assessment

Expert assessment through in-depth interviews, maturity models, and guideline comparisons

Security teams are under tremendous pressure to secure software that connects their organizations to customers, partners, and employees. Modern security developments, such as open-source components, new LLM applications, web and mobile development with rapid delivery expectations, complex outsourcing, and securing the supply chain are making that job a moving target. A comprehensive, measurable Software Security Assurance (SSA) program is necessary to ensure that current and future software releases introduce minimal risk to your business.

The OpenText Application Security Program Assessment is an expert, independent service that measures the efficacy of your SSA, comparing your capabilities and security posture against other organizations. OpenText security experts conduct in-depth interviews, observe your environment, and apply various industry standard maturity and assurance models. Their results provide insight into the strengths and potential weaknesses of your existing program, which can guide process improvements.

## Service implementation

### Scope

The assessment focuses on activities spanning the full gamut of a Software Security Initiative (SSI) and involves staff from across the software lifecycle, including legal and compliance. It concludes with a report outlining the results, highlighting key findings, and providing an organization-specific scorecard.

### Scorecard

The scorecard provides a comparison with industry peers, which is invaluable in measuring investment returns and guiding future activities.

### Outcome

Taking the assessment results and investing in secure coding practices, automated code analysis, and regular security assessments will help reduce application vulnerability density. This decreases the likelihood of successful attacks, protecting critical business operations and data.

## Service highlights

- Assess your software security maturity level
- Compare your software security with industry peers
- Improve secure coding and analysis practices
- Reduce application vulnerability density

Service planning and deployment

Scheduling

The OpenText Security Services specialist will schedule the delivery of this service at a time mutually agreed upon between OpenText and the customer. This will be during local OpenText standard business hours, excluding holidays, unless otherwise agreed by OpenText. Any services provided outside of standard business hours will be subject to added charges.

The Application Security Assessment can be repeated regularly over time to:

- Evaluate a secure SDLC integration.
- Substantiate maturity claims for compliance purposes or to address customer inquiries.
- Define a roadmap to prioritize future SSA investments.

Associated OpenText products

- OpenText™ Fortify™

Service eligibility

Prerequisites

The customer must provide the following for delivery of this service:

- Conference room with whiteboard and projector.
- Access to key staff for interviews and group discussions including:
  - Software security process leaders (e.g., “risk managers,” “security champions,” etc.) who ensure software security processes are followed by application teams.
  - Business analysts who specialize in driving non-functional security requirements into development projects.
  - Architects who specialize in driving software security into technology stacks, common libraries, coding standards, etc.
  - Development & QA managers: Note that while there might be many people in these roles, analysts only need access to a small sample, and can interview a small group at the same time.
  - Risk/Threat/Attack intelligence managers responsible for providing information to the SSG and engineering teams.
  - A security operations manager and/or incident response manager focused on application-level events and with whom the SSG interfaces with on a regular basis.
  - Compliance, legal, risk, and audit representatives, if there is someone instrumental in defining or enforcing software security-related items.
  - An audit or a PMO group representative if there is someone tasked with watching or enforcing SDLC gates specific to software security.

Service limitations

This service will be delivered as a single, continuous event. Environments requiring multiple engagements or phases over longer periods of time are not included in this service but can be accommodated at added cost through a Statement of Work.

Activities such as, but not limited to, the following are excluded from this service:

- Installation and configuration of OpenText software or appliances.
- Racking of appliances or servers.
- Delivery of standard education offerings.
- Performance testing or modeling services that, in the opinion of OpenText, are required due to unauthorized attempts by non-OpenText personnel to install, repair, maintain, or modify hardware, firmware, or software.
- Services required due to causes external to the OpenText-maintained hardware or software.
- Any services not clearly specified in this document or services beyond the license limitations of the included products.
- This service offering does not include the sale of additional OpenText products or support services, which shall require the necessary terms and conditions for such purchase by separate agreement between the parties.

## Customer responsibilities

- Contact an OpenText Security Services specialist within 90 days of the date of purchase to schedule the delivery of the service.
- Coordinate service deployment on third-party-maintained hardware/software (if applicable) with OpenText.
- Assign a designated person from the customer's staff who, on behalf of the customer, will grant all approvals, provide information, attend meetings, and otherwise be available to aid OpenText in facilitating the delivery of this service.
- Ensure that all service prerequisites as named in the Service eligibility section are met.

## Duration

Delivery of this service will not exceed a total of 80 service hours. This service will be delivered by two (2) OpenText Security Services specialists and includes one (1) on-site visit for up to three (3) days , followed by off-site compilation of findings and report generation, and remote delivery of final SSA Report and Recommendations.

## Terms

OpenText Customer Terms—Professional Services. The services described in this data sheet ("Services") are subject to the OpenText Customer Terms—Professional Services posted at **[www.microfocus.com/en-us/legal/end-user-agreement-terms](http://www.microfocus.com/en-us/legal/end-user-agreement-terms)** (the "Terms"). All capitalized terms used in this data sheet, but not otherwise defined, will have the meaning set forth in the Terms.

Rescheduling. Customer may reschedule Services by providing written notice ten (10) or more business days in advance of the scheduled delivery but only if the revised schedule results in completion of delivery within one year from the purchase date.

If Customer notifies OpenText of rescheduling less than ten (10) business days prior to the offering start date, the obligations of OpenText to deliver the Services are considered fulfilled and the rights of Customer to receipt of the Services will expire.

Change in Scope. Changes in scope to the Services are not allowed. Customer may request additional or different services, if available and at additional cost, through a mutually executed Statement of Work.

Services; Acceptance. Services do not include hardware maintenance and repair, software maintenance, or other standard support services provided by OpenText; software as a service; managed print services; or outsourcing services. Deliverables are deemed accepted upon delivery.

Any acceptance criteria or procedures set forth in this data sheet apply only to the Services specified herein and do not apply to any other products or services OpenText may supply or has supplied to Customer, regardless of whether such products or services be used in connection with the Services.

Authorization to Install Software. During the provision of Services, OpenText may be required to install copies of third-party or OpenText-branded software and may be required to accept license terms accompanying such software ("Shrink-wrap Terms") on behalf of the Customer. Shrink-wrap Terms may be in electronic format, embedded in the software, or contained within software documentation. Customer hereby acknowledges its responsibility to review Shrink-wrap Terms at or prior to installation and hereby authorizes OpenText to accept all Shrink-wrap Terms on Customer's behalf.

Existing License & Support Agreements. Services may be in support of a Customer license to software under a separate agreement and, in such case, the separate agreement shall govern all use by Customer of such software and these terms shall relate solely to the Services. These terms are not intended to modify, amend or in any way affect the licensing, warranty, or other provisions applicable to software products separately licensed by Customer from OpenText or any other party unless expressly provided for in the applicable data sheet.

Payment; Validity. The Services will be prebilled. Pricing for the offering may vary by country. Customer must schedule delivery to be completed within a period of one (1) year from the date of purchase. Notwithstanding the previous sentence, OpenText's obligations to deliver the Services are considered fulfilled and Customer's rights of receipt of the Services will expire one (1) year from the date of purchase.

Pricing for the offering may vary by country.

## Cancellation

To avoid a Cancellation Fee as defined herein, you shall notify OpenText in writing of cancellation or rescheduling at least ten (10) business days prior to the offering start date. Cancellations or rescheduling with less than ten (10) business days notification will incur 100% of the offering fee ("Cancellation Fee"). If you cancel with ten (10) or more business days in advance of scheduled delivery, you may reschedule only if delivery is complete within one year of the purchase date.

**SKU PS-AA657**

## Resource links

- [OpenText Professional Services](#)

### Learn More

- [OpenText Application Security](#)
- [OpenText™ Fortify™ Aviator](#)
- [OpenText™ Fortify™ On Demand](#)

### Download

- [Fortify SCA Quick Start Basic](#)
- [Fortify on Demand Quick Start](#)
- [Fortify SCA Health Check Services](#)
- [Fortify on Demand Health Check 5-Day Service](#)