

Black Duck Polaris™ Platform – Implementation Package

The services described in this Polaris Implementation Package (the "**Services**") are provided by Black Duck® and/or its Affiliates (collectively, "**BD**") to Customer in accordance with the terms of this Polaris Implementation Package (this "**Services Package**") and are subject to the terms and conditions of the Purchasing Agreement and the End User License and Maintenance Agreement pursuant to which this these Services have been purchased by Customer, or where no such agreement governing the Services to be provided is referenced therein, the most recent version of the End User License Agreement posted at at <https://www.blackduck.com/company/legal/end-user-licenses.html> (collectively, the "**Agreement**"), and such terms and conditions are incorporated herein by reference. All capitalized terms that are not defined in this Polaris Implementation Package will have the meaning set forth in the Agreement.

1 Overview

The Polaris Implementation Packages assist customers in getting acquainted with Polaris and its Application Security Testing (AST) capabilities, fAST Static, fAST SCA, and/or fAST Dynamic. These implementation packages provide a structured and guided approach to help with Polaris' deployment, application onboarding, and adoption.

The Polaris packages are offered in QuickStart, QuickStart Plus, and Pro tiers and include the following:

Description	QuickStart	QuickStart Plus	Pro
Curated project plan providing step-by-step deployment guide.	✓	✓	✓
Engagement Model	Webinar / Self-Service	Webinar / BD Led	BD Led
Polaris Configuration Organization, User Setup, SSO Integration application and project setup Deployment Settings and SCM integrations		✓	✓
Run initial full scan/test with the purchased AST capabilities (SCA, Static, and/or Dynamic)		1 Application / 1 Project	1 Application / 1 Project
CI/CD Integration			✓
Reporting, APIs, & Dashboards			✓
IDE Integration			✓
Enable JIRA integration			✓
End User training covering tool administration, end user, and reporting		Computer Based Training	BD Led Training

All Packages are delivered remotely. Onsite delivery for QuickStart Plus and Pro Packages can be purchased separately.

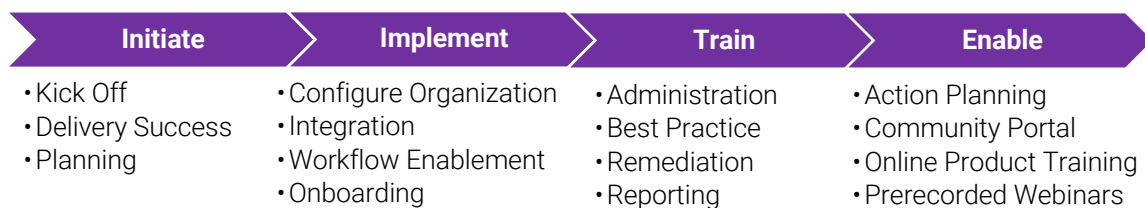
1.1 Package Delivery Success Criteria

Item	Criteria
1	Polaris is “Production Ready” • Polaris has been configured for Customer access. • End-user access provisioned and successfully tested.
2	Designated application and respective project team has been onboarded as per section 2.2.
3	In-scope product features have been enabled and demonstrated to the relevant project team.
4	Customer administrator(s) have been identified and trained in Polaris administrative functions.
5	The in-scope integrations designated in Section 2.2 are enabled and tested; members of the in-scope project team are trained on their usage.
6	Developer workflows designated in Section 2.2 have been reviewed, enabled, and tested for alignment with BD best practices and fulfillment of Customer's usage requirements.
7	Customer has been given post-implementation support, including self-paced online training, Community Portal, and Technical Support access.
8	An Action Plan to identify the completed tasks and recommended next steps have been reviewed and discussed with the Customer.

2 Implementation Approach

BD will assist Customer with onboarding users onto Polaris and will facilitate adoption. The overall process consists of the following phases, as described below.

Figure 1: Phases



2.1 Initiate

The Initiate Phase will be conducted by BD and Customer in one or more meetings with the following objectives:

- **Kick-Off** – Review Customer’s goals and organizational outcomes. Identification of Customer stakeholders for the following functions:
 - Project management.
 - Project team leader(s) – the owner of teams pioneering adoption.

- Integrated application managers – the owners of the tools/systems Polaris will be integrated.
 - Customer evangelists – members of the customer's team identified as the critical leaders for adoption and success.
- **Requirements** – Customer confirmation of what elements of the Services are applicable.
- **Success Criteria** - Confirm the success criteria as they relate to the scope:
 - Production-ready – Polaris is accessible.
 - 3rd party integrations – continuous integration/deployment, bug tracking systems.
 - The development team is trained on the best practices of the purchased application security testing capabilities (fAST SCA, fAST Static, and/or fAST Dynamic), tool usage, and remediation.
 - Administrators – trained in configuration, tool usage, and reporting.
- **Delivery Process** – Review the Polaris Implementation process:
 - Target goals: short-term, near-term, and long-term.
 - A sample project plan for the initial 90 days.
 - Establish Customer champion and implementation point of contact.
- **Plan** – Identify a plan of action designed to ensure Services are completed in a timely manner.

2.2 Implement

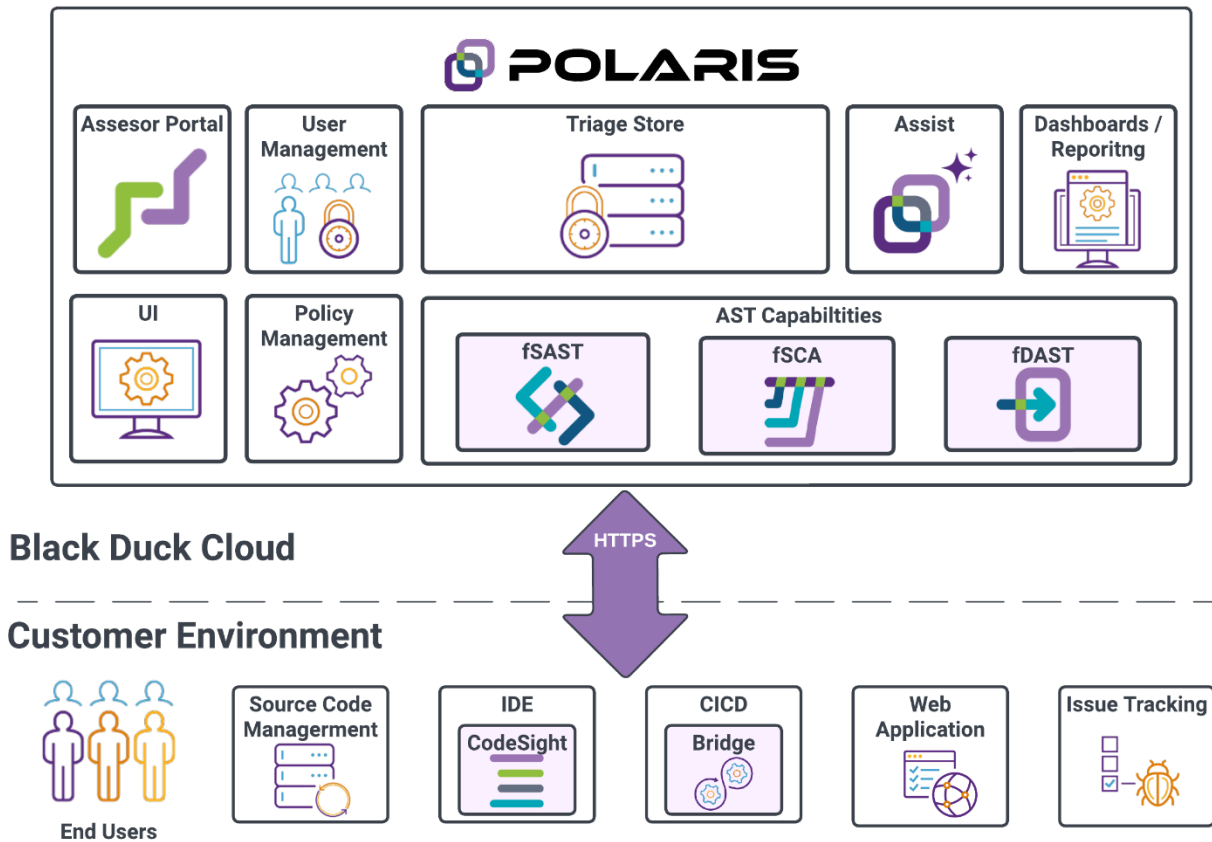
2.2.1 Configuration

BD will assist the Customer with setting up and configuring their Polaris instance. Activities include creating users, access controls, reviewing roles, and creating initial Applications and Projects.

Description	QuickStart	QuickStart Plus	Pro
Organization and User Setup		✓	✓
Enable LDAP/SAML SSO Authentication		✓	✓

The following component diagram approximates how Polaris may be integrated into a customer environment.

Figure 2 – Polaris Component Diagram



2.2.2 Application Onboarding

BD will assist with the onboarding of the in-scope Application and Project onto Polaris to meet the objectives described in the selected service package:

Description	QuickStart	QuickStart Plus	Pro
Run initial full scan/test with the licenced Application Security Testing Capabilities (SCA, Static, and/or Dynamic)		1 Application / 1 Project	1 Application / 1 Project
Results Review		✓	✓
Create Policies		✓	✓
Navigation & Workflow			✓
Reporting, APIs, & Dashboards			✓

BD defines an application as a collection of projects and subscriptions associated with it. The projects within an application are not required to align with the boundaries of a software product, but generally, all the projects in an application have the same business purpose. A subscription represents the ability to scan or use a service within Polaris. The subscription associated with the application will determine the types and quantities of available tests.

In fAST SCA and fAST Static terms, a “Project” consists of source code with the following attributes:

- Checked out from the same source code management (SCM) repository.
- Uses the same compiler for a given supported programming language.
- Utilizes the same build infrastructure and scripts.
- If multiple checkouts are required (each building a particular component or microservice), then each checkout:
 - comprises a part of a cohesive system and
 - consistently communicates with other components (e.g., direct function call, library, or REST API) to provide the required functionality.

In fAST Dynamic terms, a “Project” is the web application to be scanned is identified by a Fully Qualified Domain Name (FQDN).

For QuickStart and QuickStart Plus implementation packages, the Customer will be invited to a webinar. BD will demonstrate running an initial scan and reviewing the results in Polaris.

Initial Full Scan / Results Review – BD representatives will work with QuickStart Plus and Pro customers to enable them on their purchased AST Capabilities, which may include the following:

1. fAST Static and/or fAST SCA: complete one (1) local CLI scan with the Black Duck Bridge tool.
2. fAST Dynamic: run a scan on the web application through one (1) FQDN.

Following the scans, BD will review the scan test results in Polaris with the customer representative. Additional guidance will be provided to Pro Package customers on how to navigate tests and debug test failures. The steps to complete these tasks are:

- Install and configure Black Duck Bridge.
- Configure a Dynamic test profile.
- Complete an initial scan of the Project per Customer's service package.
- Review the scan and discuss the Static, SCA, and/or Dynamic test results with Customer representatives.
- With the Pro Package:
 - Assist in triaging the identified issues, including false-positive remediation, when the Customer has yet to purchase Triage Services.

Create Policies – BD will assist the Customer in creating Polaris Policy rules to flag vulnerabilities, notify users via email, and/or break the build.

Reporting, APIs, and Dashboards – As part of the Pro package, BD will review the Polaris reporting capabilities, which include:

- Reporting dashboards,
- Filtering and exporting project results, and
- API endpoints.

2.2.3 Workflow Integration

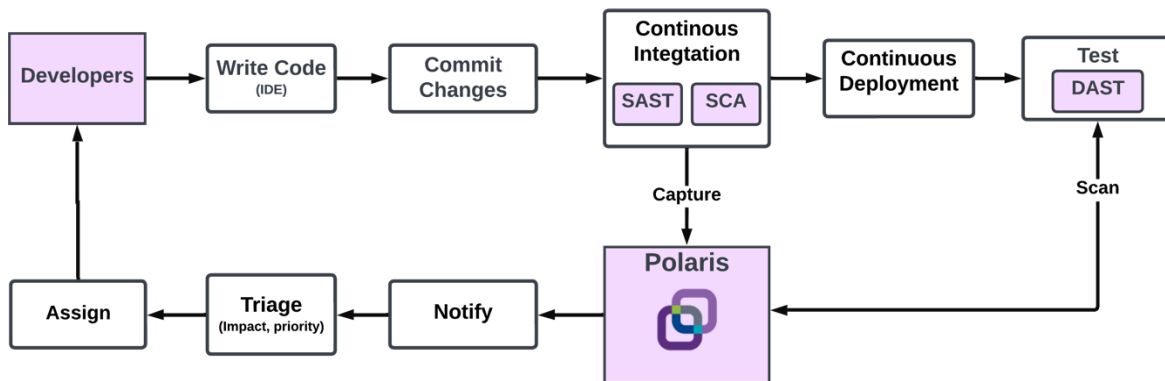
BD will assist Customer with integrating Polaris with Customer's tools and development processes. The following tasks will be completed for each in-scope application:

Description	QuickStart	QuickStart Plus	Pro
One (1) CI/CD integration onboarding (e.g., Azure, Bamboo, and Jenkins).			✓
One (1) supported 3rd party workflow system integration.			✓
One (1) supported IDE integration			✓

Issue Resolution Workflow – A best practice is the implementation of an issue resolution workflow, a standardized process whereby developers are assigned and notified of issues that must be addressed. As part of the Pro package, BD will enable the Issue Resolution Workflow by integrating Polaris with:

- CI/CD Process, which analyzes Projects regularly.
- Issue Tracking System, for critical defects to be assigned to develops for resolution.
- Integrated Development Environment (IDE).

Figure 3 - Issue Resolution Workflow



As shown in the diagram:

1. Developers write code and commit their changes to their SCM system.
2. The project is built and scanned using fAST Static and fAST SCA capabilities as part of the continuous integration process. Any vulnerabilities identified during this step are committed to Polaris for review.
3. Once the Continuous Integration process is completed, the newly built project is deployed to a test environment as part of the continuous deployment step.
4. Polaris then scans the project using its fAST Dynamic capability. Any vulnerabilities identified during the scan are captured in Polaris for review.
5. Users are notified of any newly discovered vulnerabilities.
6. The vulnerabilities are triaged using the Polaris user interface. Vulnerabilities requiring action are assigned to a developer to address.

CI/CD Integration – BD will assist in integrating the Black Duck Bridge with one (1) CI/CD process for the in-scope project. This will allow automatic and consistent scanning of your project to surface defects as they are added for a quick resolution.

Issue Tracking Integration – Users can explicitly promote an individual issue from Polaris by clicking the “Export” button in the Polaris graphical user interface (“GUI”). Based on the package tier, one (1) supported issue-tracking system will be integrated and configured.

IDE Integration – BD will host one (1) workshop to take Customer developer resources through the installation and configuration of Code Sight on one (1) supported Integrated Development Environment (IDE), allowing developers to view and address defects.

2.3 Train

Description	QuickStart	QuickStart Plus	Pro
Self-paced online training resources	✓	✓	✓
BD Hosted webinar series	✓	✓ (Optional)	✓ (Optional)
End-user training sessions (Up to 16 participants)			✓

Webinar Series – BD will invite Customer to a webinar series to provide additional support with the Implementation Phases. The topics covered in the webinar series are:

- System Architecture and User Interface Overview
- Scanning best practices and reviewing scan results
- Workflow enablement

Developer Training – For Pro packages, BD will lead an end-user training session with the Customer’s Developer team to provide general SCA/Static/Dynamic education, tool navigation, vulnerability triaging, and issue resolution.

2.4 Enable

Product	QuickStart Plus	Pro	Premier
Product Adoption Maturity Model (PAMM) assessment	✓	✓	✓
Action Plan	✓	✓	✓

This phase ensures Customer is set up for success and is ready to begin using Polaris.

PAMM – At the start of this phase, BD will work with Customer to complete a PAMM assessment to measure product adoption. The benefits of the PAMM and obtaining a maturity score is that it provides:

- A well-defined roadmap of activities that can be performed to maximize investment in BD’s tools.
- Quantitatively measure the product adoption of AppSec tools, which correlates to the security of the applications they are developing.
- A way to compare their maturity with other organizations in their industry.

Action Plan – Using the results from the PAMM assessment, BD will create an Action Plan outlining the recommended activities for Customer's continued adoption of Polaris. The **Action plan** provides Customer with the following:

- A summary of the steps completed during the execution of the service package;
- The results of Customer's maturity as it relates to BD's product adoption maturity model;
- Recommended next steps to mature Customer's implementation,
- Instructions to access:
 - The Community,
 - Online product training and
 - Webinars.

BD will review the Action Plan with the Customer for final sign-off and transition the Customer to the BD Customer Success team.

3 Prerequisites and Dependencies

Entry Criteria – The following is a list of requirements and dependencies that the Customer must meet to enable BD to perform the Services:

1. Provide a primary point of contact with a deep understanding of the requirements.
2. Review the documentation and environmental needs that meet the minimum requirements for Black Duck Bridge.
3. Review the prerequisite documentation to run a fAST Dynamic test.
4. Verify that login credentials for Polaris have been received.
5. Identify the Project Polaris will scan.
6. Ensure successful regular builds (i.e., not using Black Duck Bridge) of the codebase are completed on the build server(s).
7. Provide access to system administration assistance for any hardware or networking issues.
8. Remote access to build servers.

If the Customer does not meet the prerequisites and dependencies described above, and to the extent that BD is unable to perform the Services due to the Customer's failure to meet those prerequisites and dependencies, BD will not be obligated to perform the affected Services.

4 Purchasing Agreement

The parties shall mutually agree to the schedule for the performance of the Services, subject to the terms of the Agreement and this Service Package. All Services described within this Services Package must be used within one year of the Start Date set forth in the Purchasing Agreement pursuant to which this Services were purchased. Unused services are non-refundable and non-transferable pursuant to the terms and conditions of the Purchasing Agreement. Performance of Services is subject to scheduling and Customer availability.

End of Services Package