Black Duck AST

© 2024 Black Duck Software, Inc.

Black Duck offers the most comprehensive, powerful, and trusted portfolio of application security testing solutions in the industry.

- On October 1, 2024, Black Duck was created as an independent company
  - Carve out of the Software Integrity Group, a business unit of Synopsys Inc.
  - Purchased by Clearlake and Francisco Partners

© 2024 Black Duck Software, Inc.

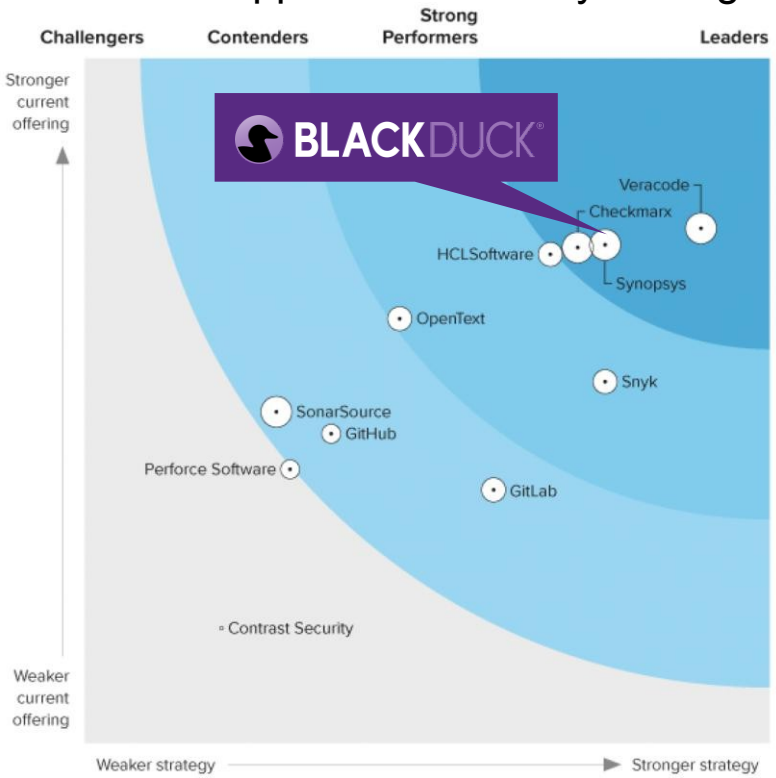
Black Duck is recognized as a leader in Application Security Testing

Gartner®

Magic Quadrant for Application Security Testing

FORRESTER

Forrester Wave™: Static Application Security Testing



Forrester Wave™: Software Composition Analysis

Note: Black Duck was Synopsys Software Integrity Group at the time of these reports.

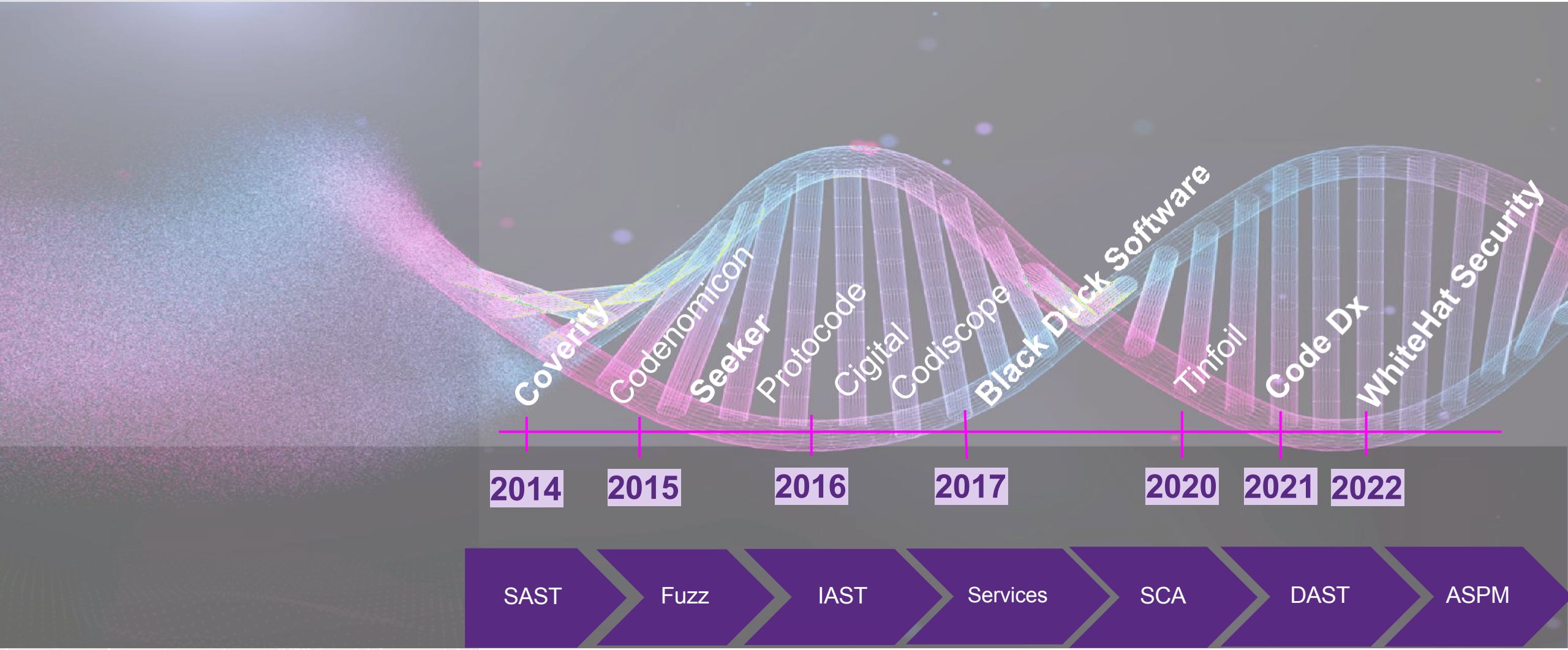
© 2024 Black Duck Software, Inc.

BLACKDUCK®

CLICO

Strength in Security and Quality

The most comprehensive AppSec portfolio evolution



© 2024 Black Duck Software, Inc.

Why AI-assisted development changes the AppSec landscape

Teams are not only writing code faster. They are compressing security decisions across the SDLC.

Speed

The same team can now produce much more code in much less time.

Risk

Defects, unsafe patterns and problematic dependencies can spread earlier and further.

Reaction

Security must move closer to code generation without losing depth later in the pipeline.

In AI-assisted development, the biggest challenge is not running scans. It is getting useful feedback to the right team quickly enough.

AI coding agents compress the SDLC — and amplify software risk

What changes when code is generated faster?

- Human review time per change shrinks, while code volume grows.
- Security defects, unsafe patterns, and bad dependencies can be introduced earlier and more often.
- License and copyright exposure becomes harder to spot when generated snippets move quickly into repos.
- Traditional AppSec gates still matter — but they must keep pace with AI-assisted delivery.

Speed

Code lands faster than security review cycles can traditionally handle.

Noise

Generic AI guidance often produces too many low-value findings and weak prioritization.

Context

Teams need issue context, exploitability signal, and remediation guidance in workflow.

Governance

Portfolio controls still need SAST, SCA, DAST, IAST, fuzzing, and policy-based orchestration.

Black Duck positions Signal as the new AI-native front line, with the established portfolio enforcing depth across the SDLC.

BLACKDUCK®

© 2026 Black Duck Software, Inc.

Black Duck Signal™

Agentic AI AppSec for AI-powered software development

Signal combines ContextAI™ with 20+ years of human-curated AppSec intelligence to help teams find and fix issues without the usual noise or AI hallucinations.

MCP + coding assistant

Real-time analysis

• Analyze new code instantly and fix issues before code is committed.

AI-powered development fit

• Run security scans with natural language prompts in coding assistants and IDEs.

Agentic investigation

• Route and prioritize issues so teams focus on the code that matters most.

Language coverage

• Built for modern languages, frameworks, and AI-assisted development workflows.

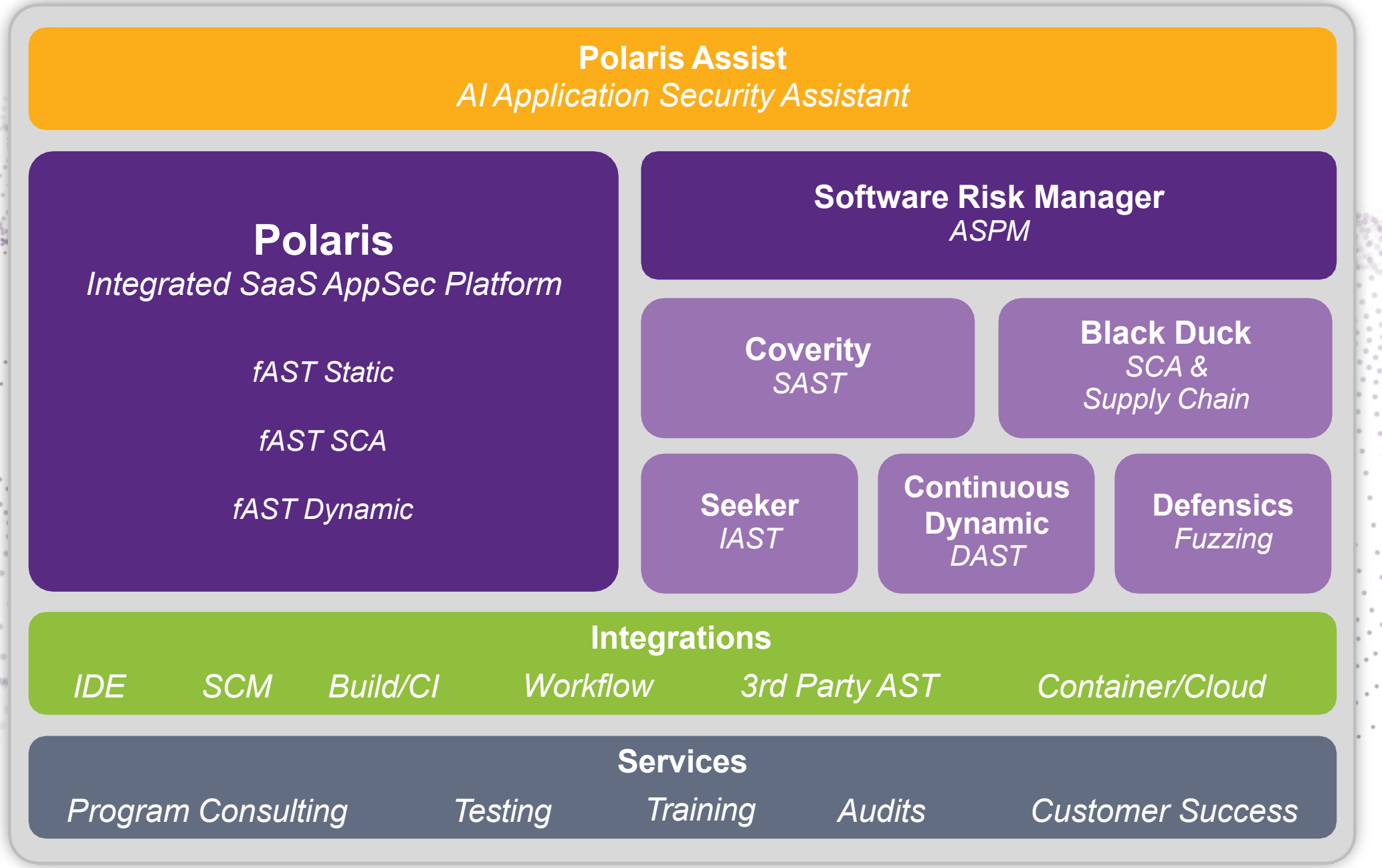
Operational role

• Signal secures the earliest AI-generated code path; the broader Black Duck portfolio validates, governs, and scales trust across the rest of the SDLC.

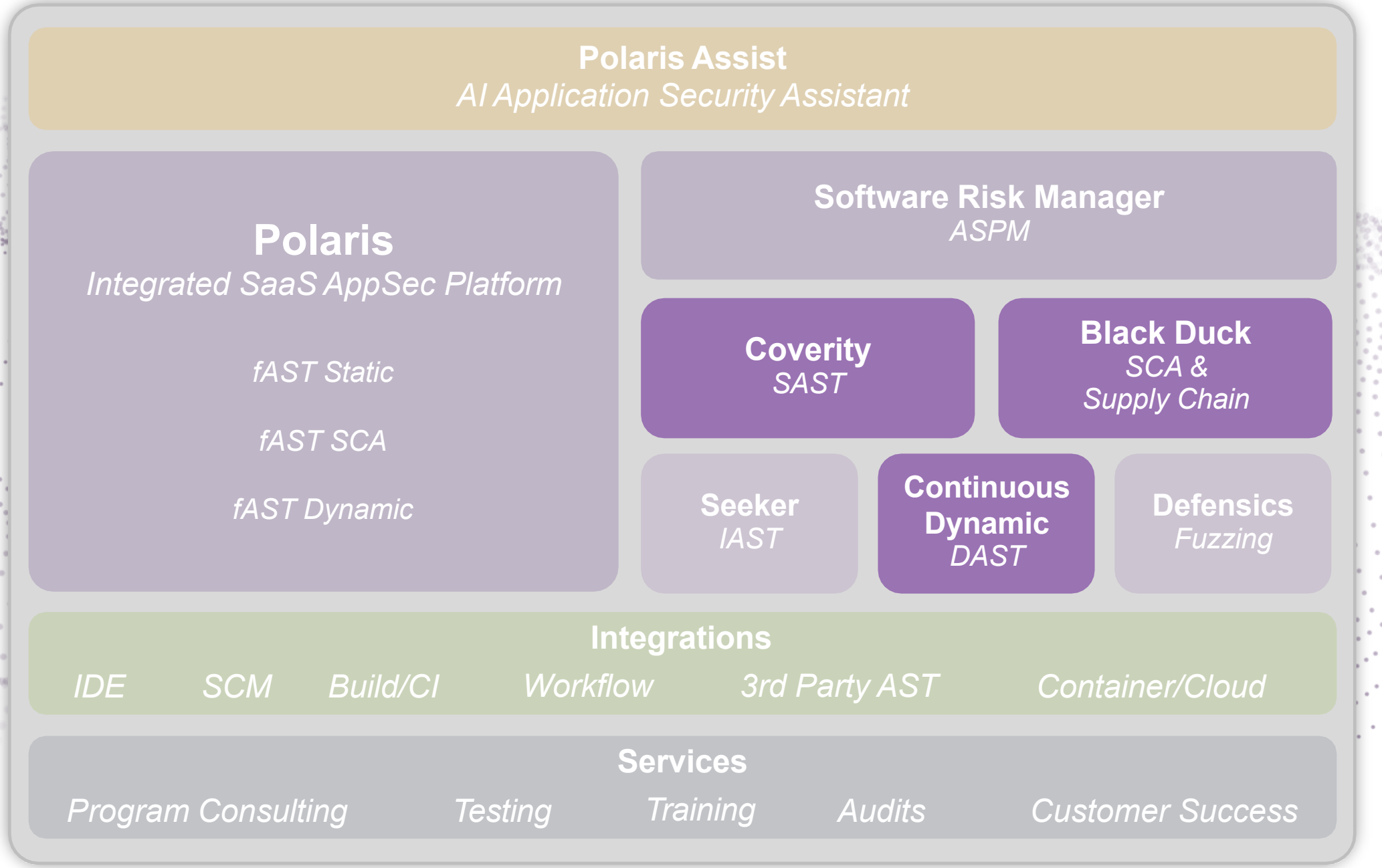
BLACKDUCK®

© 2026 Black Duck Software, Inc.

CLICO



© 2024 Black Duck Software, Inc.



© 2024 Black Duck Software, Inc.

SAST - Coverity

In-depth static analysis for secure code that's free of defects

Comprehensive Analysis

- Identifies both code quality and security issues
- Uncovers complex issues that span files and libraries
- Broad and deep language and framework support

Developer Velocity

- Accurate results let developers focus on business value
- Fast scans on PR/MR to find defects early in the SDLC
- Easy triage and prioritization of results

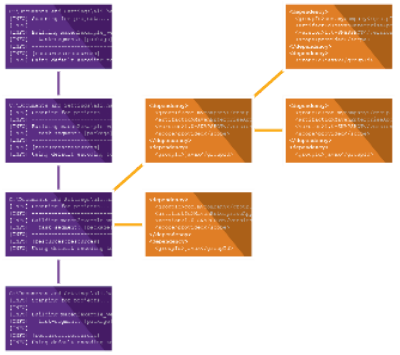
Enterprise Scale

- Thousands of developers
- Thousands of projects
- Apps with millions of lines of code

© 2024 Black Duck Software, Inc.

Black Duck SCA - multi-factor scanning ensures complete discovery

Dependency analysis



- Fast and shallow
- Package managers

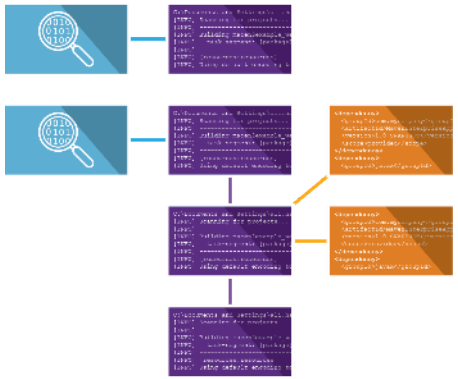
Codeprint analysis

- Catches modified open source
- C/C++

Snippet matching

- Scans compiled code
- Containers

Binary analysis



- Identifies snippets of open source

Custom component detection

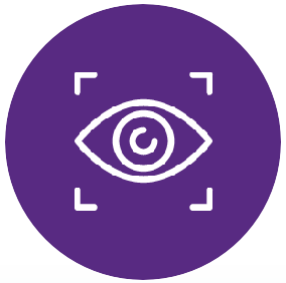
- Non-OSS, internal, or third-party components

Complete Software Bill of Materials (SBOM)

© 2024 Black Duck Software, Inc.

DAST - Continuous Dynamic

Continuous Dynamic provides industry-proven web application security testing for modern and traditional websites, web applications, and frameworks.



Full Visibility

Delivers full visibility and the front line of defense for secure DevSecOps

Intelligent Prioritization

Automates the prioritization of results based on machine learning

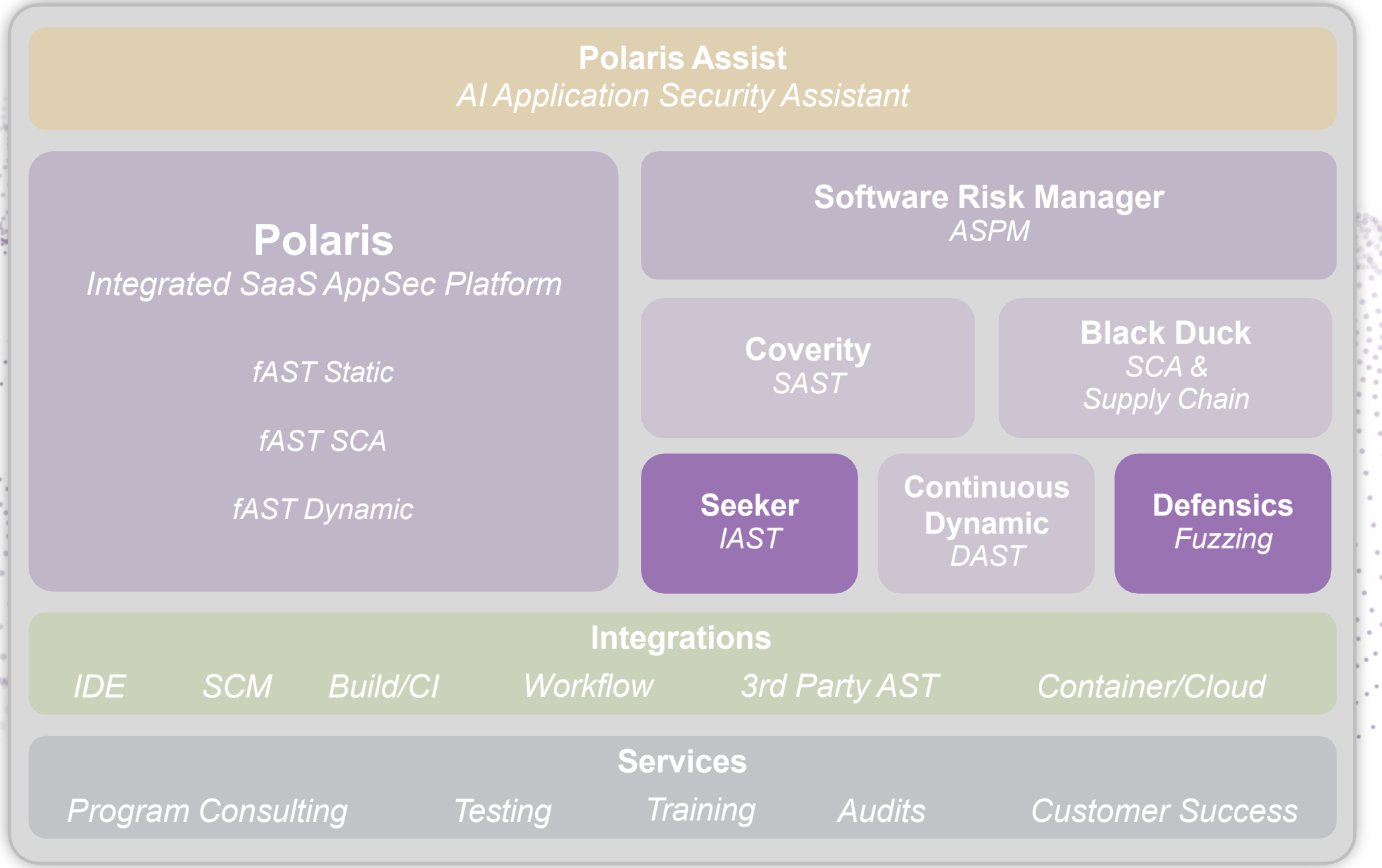
Continuous and On-Demand Risk Assessments

Provides continuous and on-demand scanning to automatically check for vulnerabilities

Production-Safe

Scans production servers safely and without causing any downtime - saving valuable time, resources, and cost

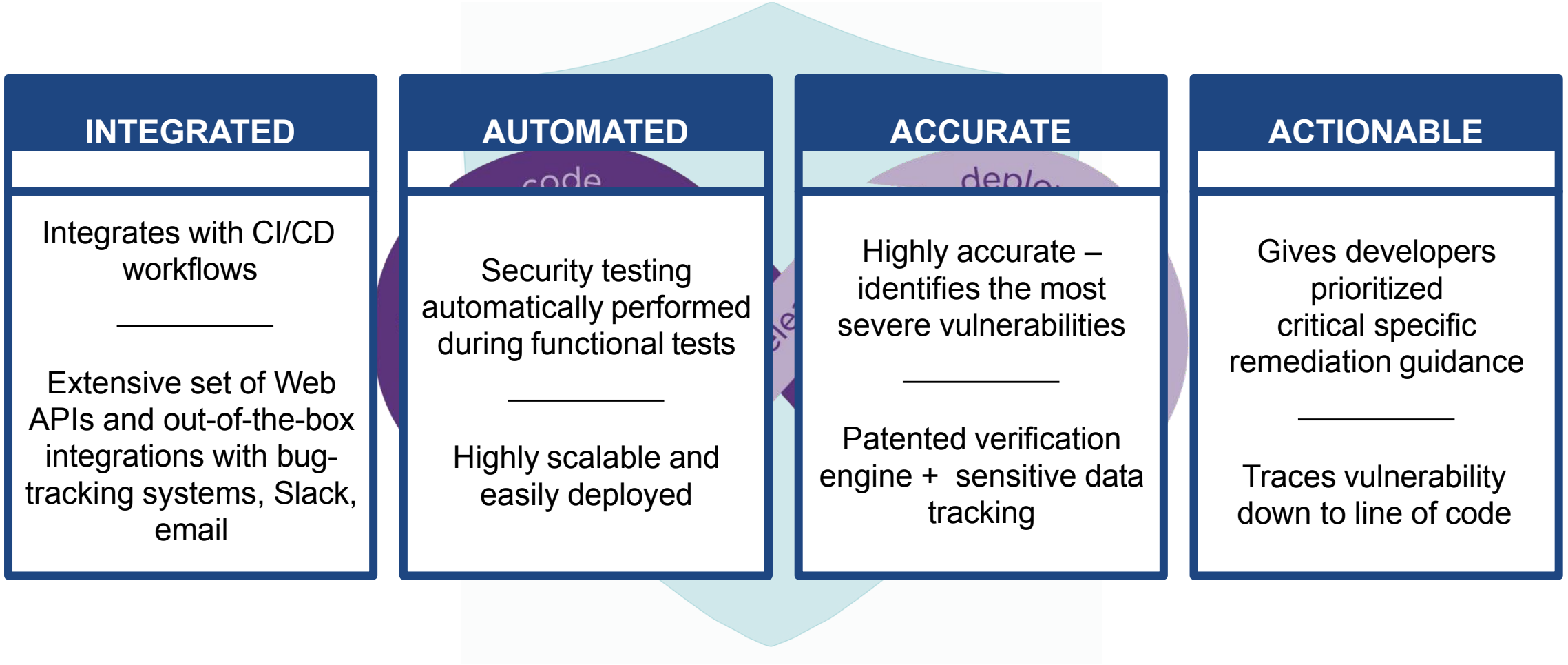
© 2024 Black Duck Software, Inc.



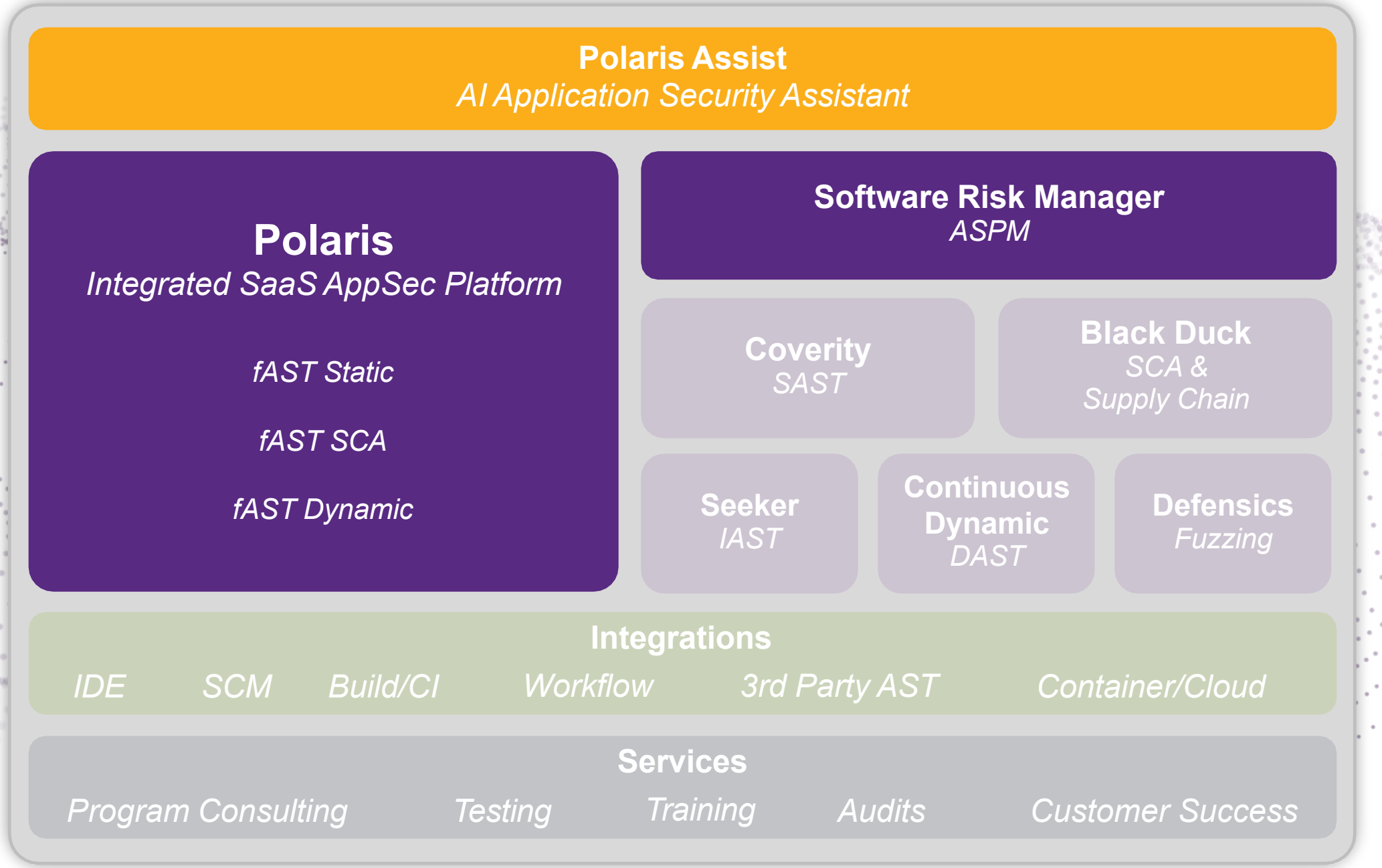
© 2024 Black Duck Software, Inc.

Seeker – IAST, Interactive Application Security Testing

*Accurate, easy-to-use enterprise-scale IAST that identifies **and** verifies web application vulnerabilities in real time*



© 2024 Black Duck Software, Inc.



© 2024 Black Duck Software, Inc.

POLARIS

An integrated cloud-based application security testing solution that is optimized for the needs of development and DevSecOps teams

- Easy to onboard and use
- Concurrent scan types, scalable and cost-effective SaaS delivery
- Market leading SAST, SCA & DAST engines
- Seamless integration with popular SCM and DevOps tools
- Built-in policy management, reporting, and analytics with AI-enabled remediation assistance
- Expert onboarding, triage, and support services

© 2024 Black Duck Software, Inc.

Polaris provides a holistic view into your risk posture

fAST Static ANALYSIS

Find and fix security vulnerabilities in your code as it is being developed

fAST SCA ANALYSIS

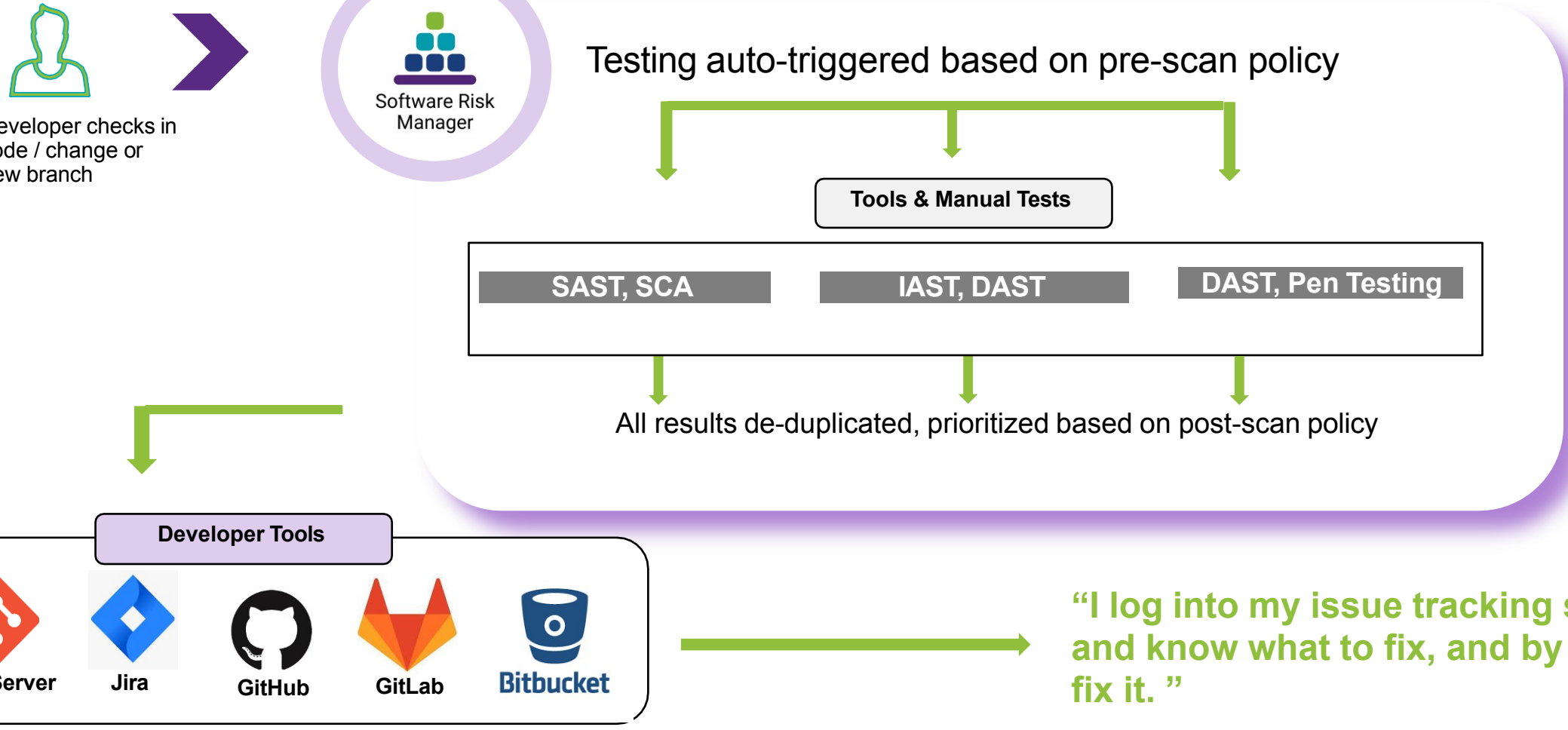
Detect and manage open source and third-party component risks in development and production

fAST Dynamic ANALYSIS

Test-running apps for common security weaknesses and vulnerabilities

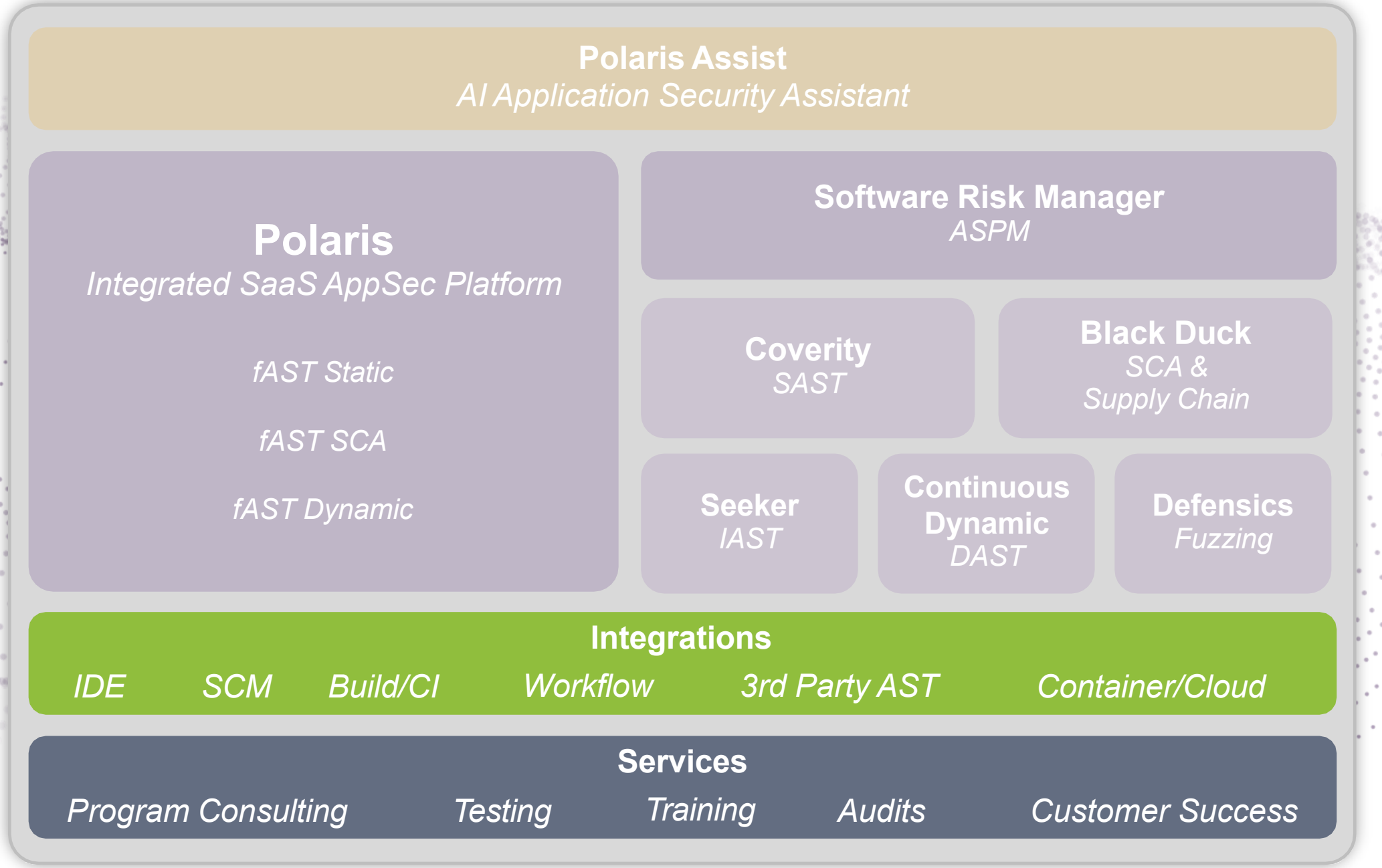
© 2024 Black Duck Software, Inc.

The Developer Dream with **Software Risk Manager**



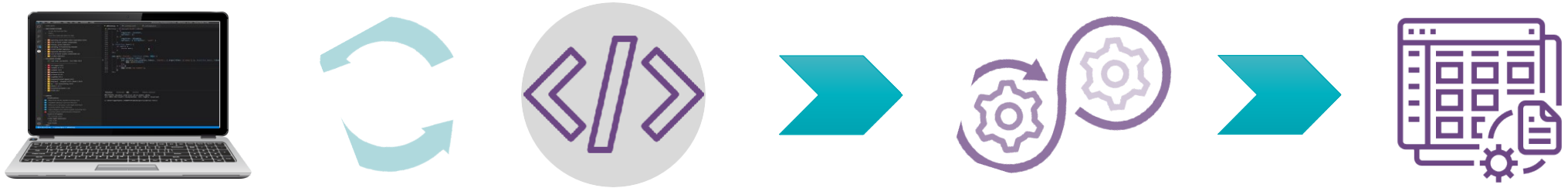
"I log into my issue tracking system and know what to fix, and by when to fix it. "

© 2024 Black Duck Software, Inc.



© 2024 Black Duck Software, Inc.

Integrate Coverity scans into the SDLC



IDE

Identify issues before code is committed

Visual Studio
VS Code
eclipse
IntelliJ
WebStorm
PyCharm
RubyMine
PhpStorm
WIND WORKBENCH
Momentics IDE 2.0
IBM Rational Team Concert
CLion

Code Repository

Trigger incremental scans on pull requests

GitHub
GitLab
Azure DevOps
Bitbucket
SUBVERSION
plasticscm
PERFORCE Version everything.

CI / Build tools

Get a complete view of defects across your projects

Jenkins
circleci
Bamboo
Azure DevOps
GitHub
GitLab

Issue Tracking

Export scan results with configurable field values

JIRA
Bugzilla

© 2024 Black Duck Software, Inc.

Uncover vulnerabilities across all your languages

Broad and deep support for more than 20 languages

Language Coverage

Support for Popular Compilers

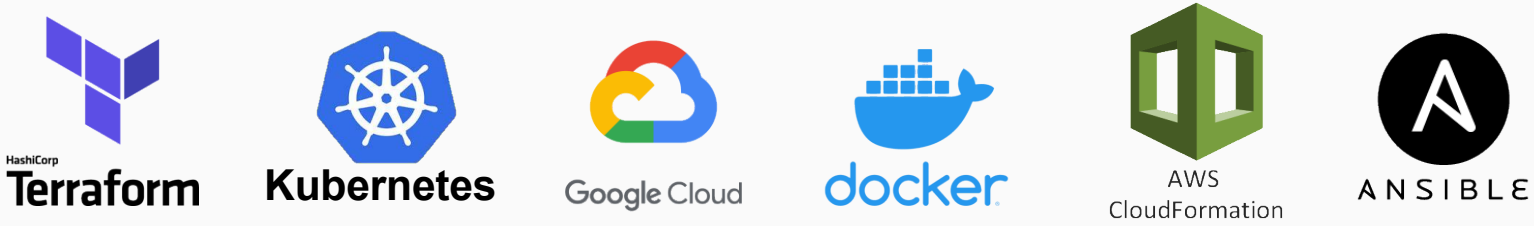
- ARM C/C++
- Clang
- GNU GCC/G++
- Intel C++ for Windows
- JDK for Mac OS X
- Microsoft Visual C++
- Nvidia CUDA (NVCC)
- Renesas C/C++
- SONY PS4 SDK
- Sun (Oracle) CC
- Sun/Oracle JDK
- Wind River C/C++

© 2024 Black Duck Software, Inc.

Deploy cloud environments with confidence

IaC scans identify misconfigurations to prevent vulnerabilities in cloud environments

Infrastructure-as-Code



File formats:

JSON	YAML	HCL	HTML	XML	plist
TOML	Properties	Vue template	JSX	TSX	

Supports CIS Benchmarks for Cloud Environment

- Access controls
- Data protection
- Hardcoded secrets
- Network settings
- Infrastructure configuration
- Software settings

CIS Center for Internet Security®
Creating Confidence in the Connected World.™

© 2024 Black Duck Software, Inc.

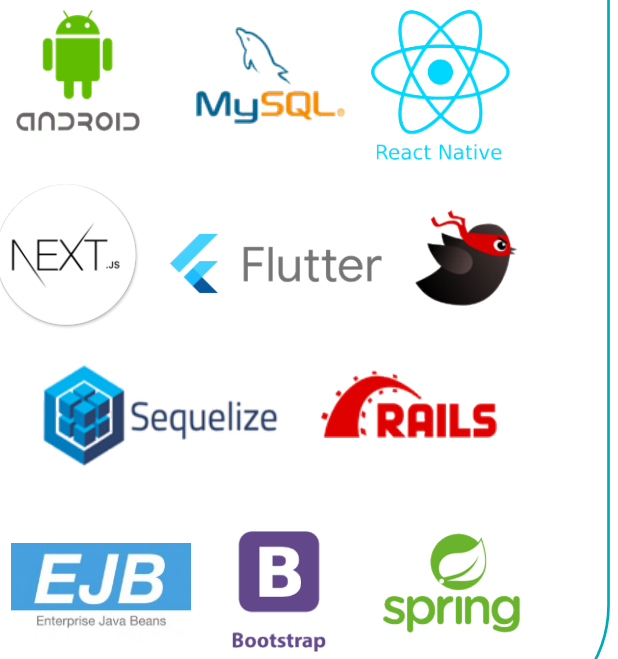
Analyze the context of code usage and frameworks

Poorly understood frameworks and APIs lead to false positives and missed vulnerabilities

10 Most Popular Web Application Frameworks

Source: *Stack Overflow, [2022 Developer Survey] (58,743 responses)*

Support for 200+ Frameworks in All



© 2024 Black Duck Software, Inc.

Köszönöm a figyelmet!

blackduck@clico.hu

© 2024 Black Duck Software, Inc.