Clico Cloud Control C3
Black Duck AST

Werner Obring
Cloud Security Architect
2025.11.13.

Security   Networking   Management   1

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

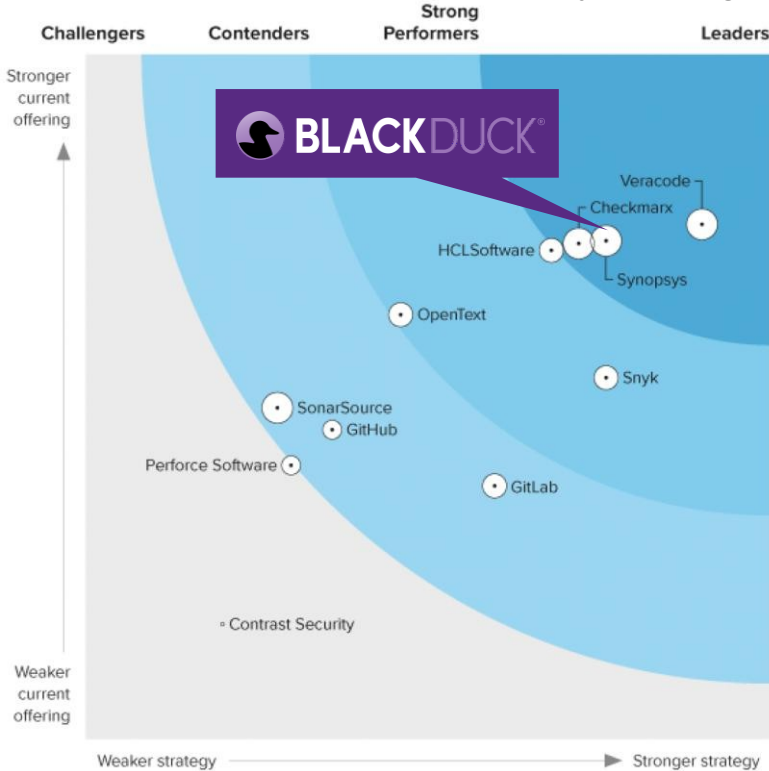# Black Duck is recognized as a leader in Application Security Testing

Gartner

**Magic Quadrant for
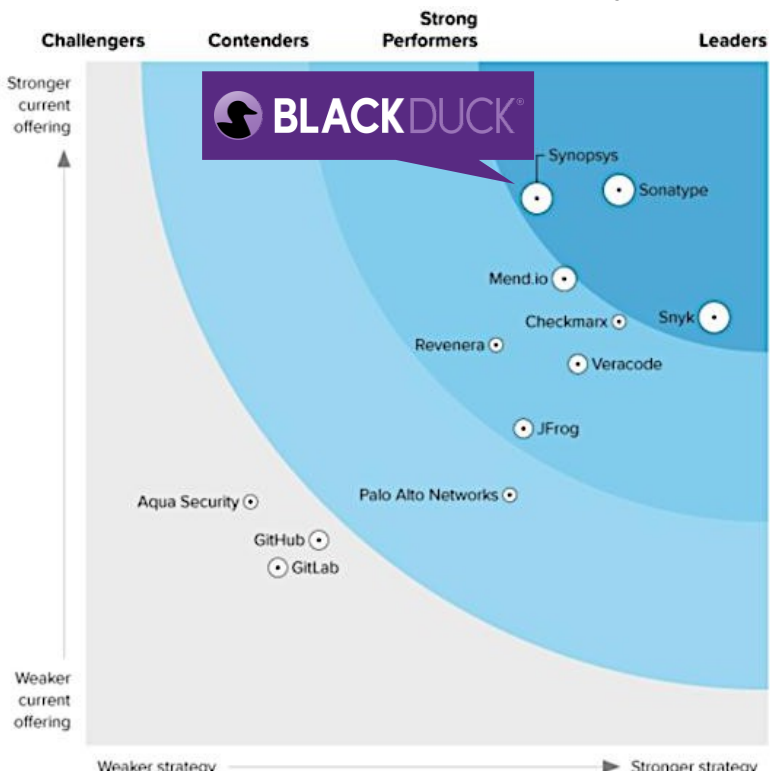Application Security Testing**

FORRESTER

Forrester Wave™:
Static Application Security Testing

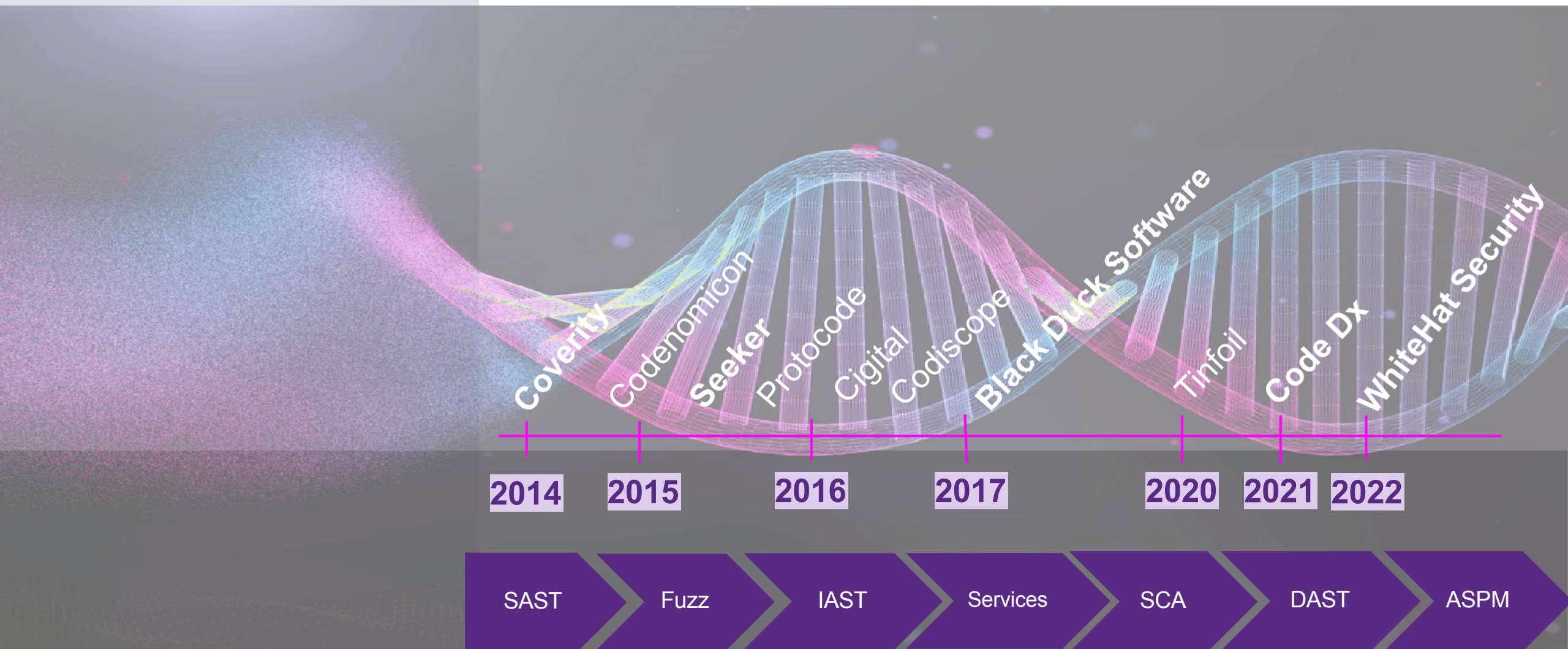Forrester Wave™:
Software Composition Analysis

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

Application velocity and volume

Increased speed, complexity, and enlarged attack surface area

Operating Model

Waterfall

Legacy, proprietary

MAINFRAME MONOLITHIC

Agile

Best-of-breed, open source

WEB CLIENT SERVER

DevOps

Automation, CI/CD

MOBILE CLOUD, CONTAINER MICROSERVICES

DevSecOps

Continuous, autonomous delivery

ARTIFICIAL INTELLIGENCE BLOCKCHAIN

Yearly releases → Monthly → Weekly / daily → Continuous

TIME
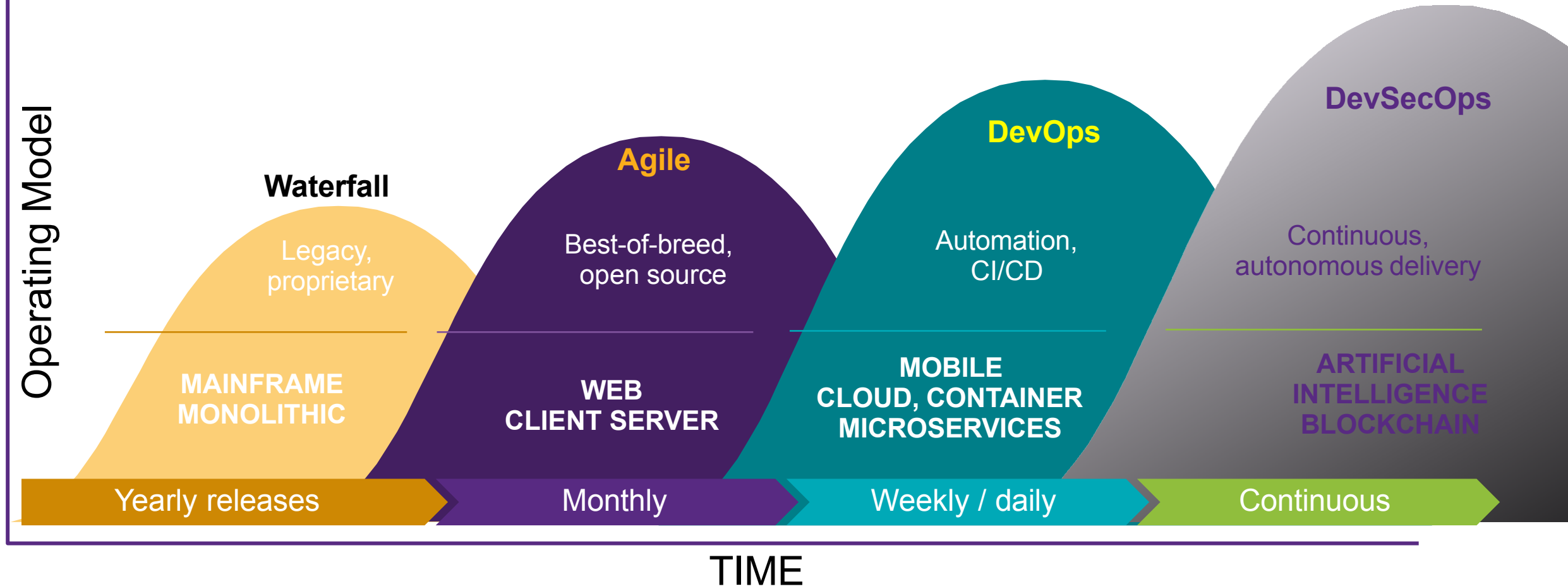
Enterprises are facing their next big challenge …

- Need for immersive experiences

- Use of open-source / 3rd party components

- Deal with attack surface expansion

- Keep up with AppSec's regulations

- Increasing use of generative AI (on both sides)

- Diversity of devices, OS types, versions

BLACK DUCK®

CLICO

Facebook delivers between **50,000** and **60,000 Android builds** each day.

Amazon reportedly deploys new software to production **every second**.

Netflix's DevOps teams deploy new releases **100 times each day**.

Etsy uses its continuous delivery practice to deploy a **single monolithic** application more than **60 times a day.**

BLACK DUCK®

CLICO

Polaris Assist
AI Application Security Assistant

Polaris
Integrated SaaS AppSec Platform

fAST Static

fAST SCA

fAST Dynamic

Software Risk Manager
ASPM

Coverity
SAST

Black Duck
*SCA &
Supply Chain*

Seeker
IAST

**Continuous
Dynamic**
DAST

Defensics
Fuzzing

Integrations

IDE   SCM   Build/CI   Workflow   3rd Party AST   Container/Cloud

Services

Program Consulting   Testing   Training   Audits   Customer Success

BLACK DUCK®

CLICO

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
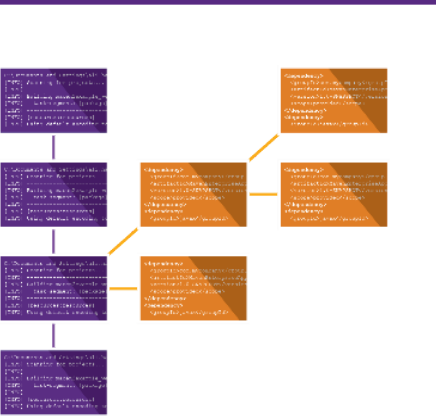- Easy triage and prioritization of results

Enterprise Scale

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

Black Duck SCA - multi-factor scanning ensures complete discovery

Dependency analysis	Codeprint analysis	Snippet matching	Binary analysis	Custom component detection
• Fast and shallow • Package managers	• Catches modified open source • C/C++	• Scans compiled code • Containers	• Identifies snippets of open source	• Non-OSS, internal, or third-party components
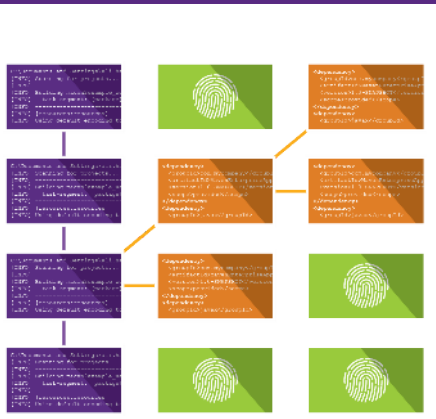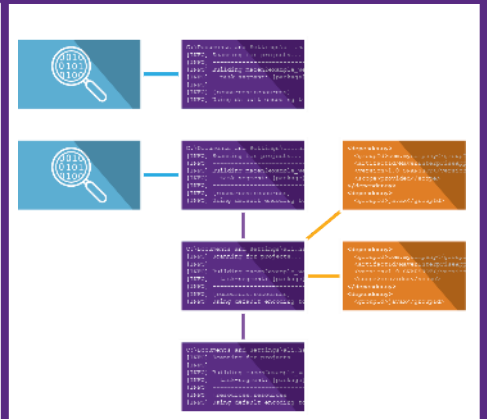
Complete Software Bill of Materials (SBOM)

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

CLICO

Seeker – IAST, Interactive Application Security Testing

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

INTEGRATED

Integrates with CI/CD workflows

———————

Extensive set of Web APIs and out-of-the-box integrations with bug-tracking systems, Slack, email

AUTOMATED

Security testing automatically performed during functional tests

———————

Highly scalable and easily deployed

ACCURATE

Highly accurate – identifies the most severe vulnerabilities

———————

Patented verification engine + sensitive data tracking

ACTIONABLE

Gives developers prioritized critical specific remediation guidance

———————

Traces vulnerability down to line of code

BLACKDUCK®

CLICO

For effective fuzzing, use better test cases

Random

101010101010
101010101010

Mutational

10101010**18**10
10**3**010101010

Generational

1010 1010 1010
3001 8101 1038

Hit or miss　　　　　　　　　　　**RESULTS**　　　　　　　　　　　**Comprehensive**

Polaris Assist
AI Application Security Assistant

Polaris
Integrated SaaS AppSec Platform

fAST Static

fAST SCA

fAST Dynamic

Software Risk Manager
ASPM

Coverity
SAST

Black Duck
*SCA &
Supply Chain*

Seeker
IAST

Continuous Dynamic
DAST

Defensics
Fuzzing

Integrations

IDE   SCM   Build/CI   Workflow   3rd Party AST   Container/Cloud
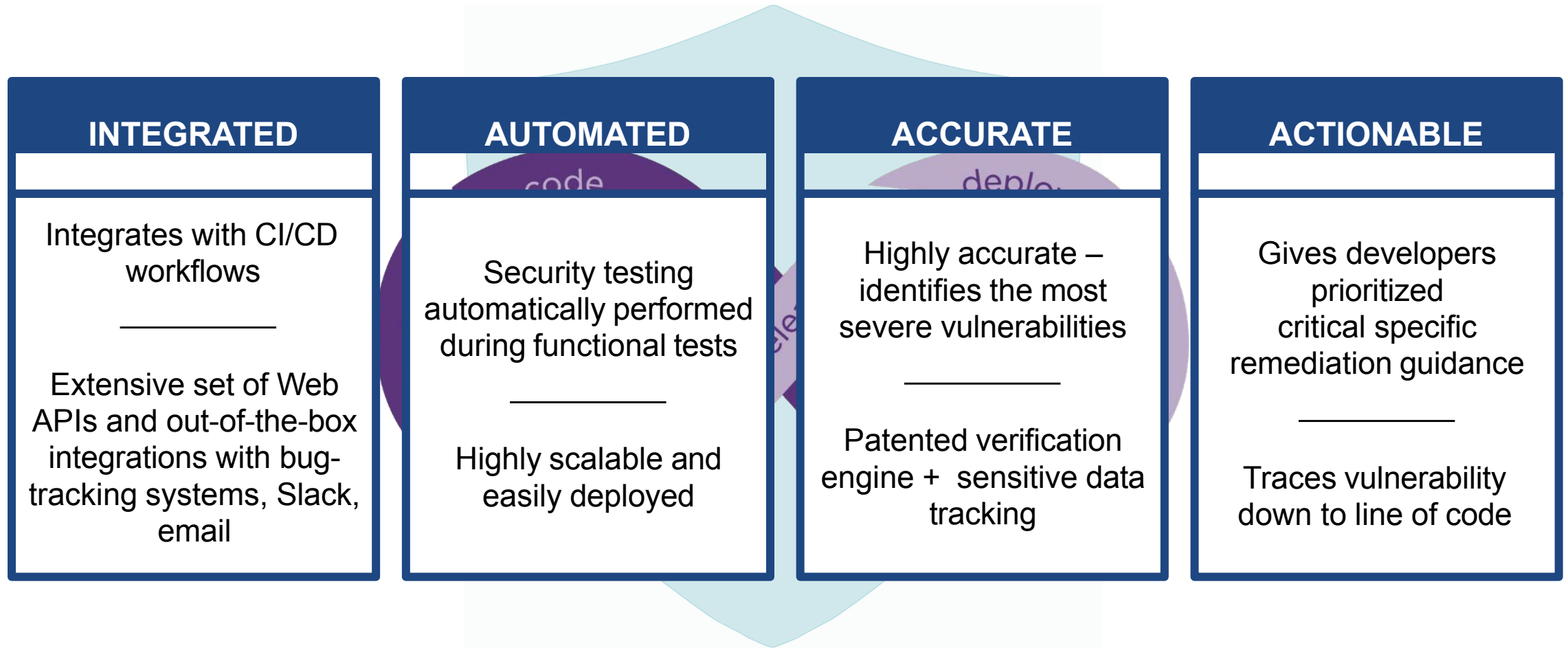
Services

Program Consulting   Testing   Training   Audits   Customer Success

BLACK DUCK®

© 2024 Black Duck Software, Inc.

CLICO

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

Polaris provides a holistic view into your risk posture

*f*AST Static ANALYSIS

Find and fix security vulnerabilities in your code as it is being developed
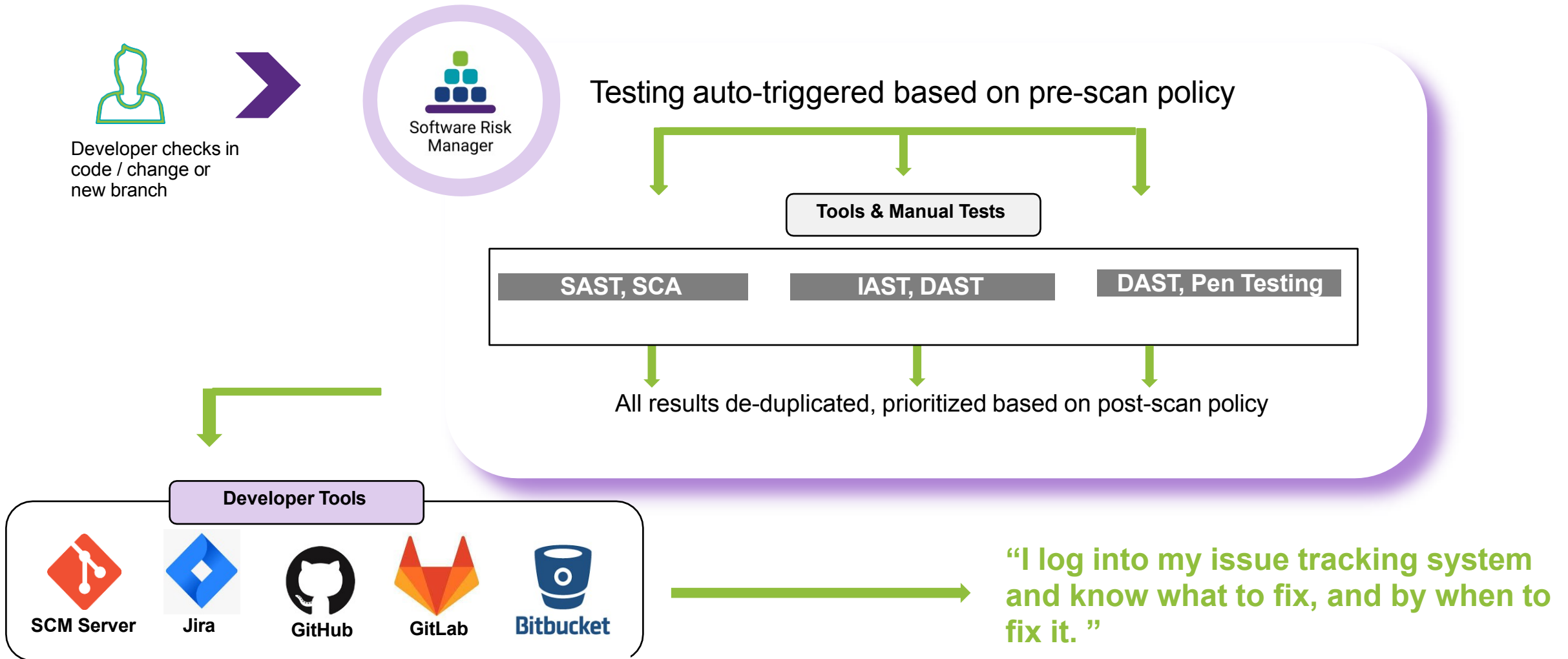
*f*AST SCA ANALYSIS

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

*f*AST Dynamic ANALYSIS

Test-running apps for common security weaknesses and vulnerabilities

BLACKDUCK®

CLICO

The Developer Dream with **Software Risk Manager**

Software Risk Manager

Developer checks in code / change or new branch

Testing auto-triggered based on pre-scan policy

Tools & Manual Tests

SAST, SCA	IAST, DAST	DAST, Pen Testing

All results de-duplicated, prioritized based on post-scan policy

Developer Tools

SCM Server   **Jira**   **GitHub**   **GitLab**   **Bitbucket**

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

Integrate Coverity scans into the SDLC
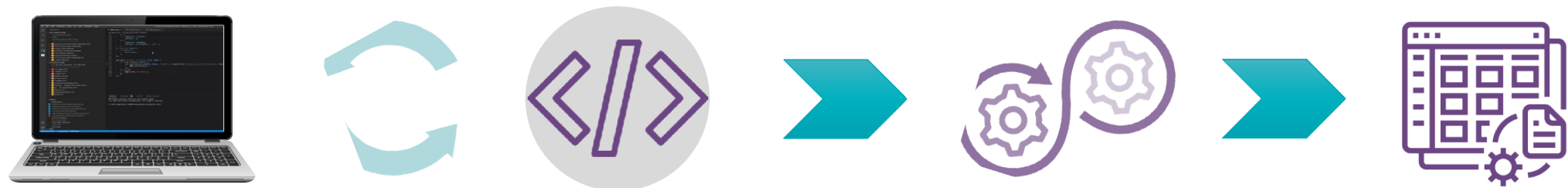
IDE	**Code Repository**	**CI / Build tools**	**Issue Tracking**
Identify issues before code is committed	*Trigger incremental scans on pull requests*	*Get a complete view of defects across your projects*	*Export scan results with configurable field values*
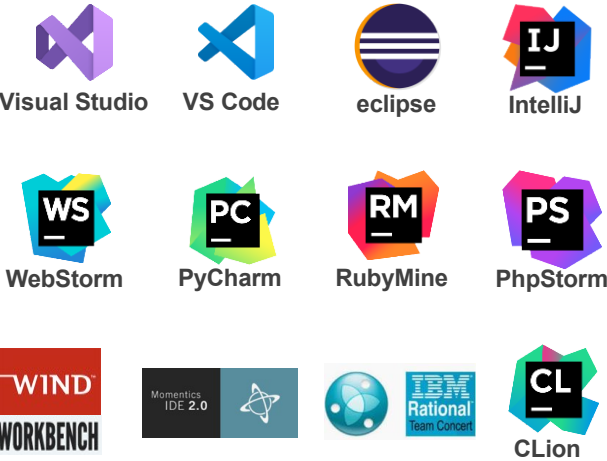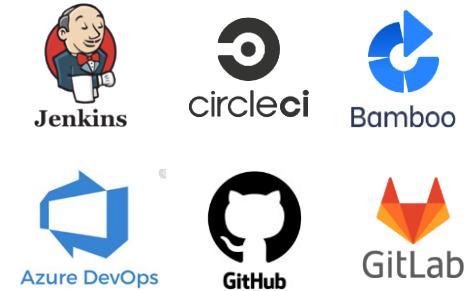
IDE: Visual Studio, VS Code, eclipse, IntelliJ, WebStorm, PyCharm, RubyMine, PhpStorm, WIND WORKBENCH, Momentics IDE 2.0, IBM Rational Team Concert, CLion

Code Repository: GitHub, GitLab, Azure DevOps, Bitbucket, SUBVERSION, plastic scm, PERFORCE Version everything.

CI / Build tools: Jenkins, circleci, Bamboo, Azure DevOps, GitHub, GitLab

Issue Tracking: JIRA, Bugzilla

BLACK DUCK®

CLICO

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++

BLACK DUCK®

CLICO

Deploy cloud environments with confidence

IaC scans identify misconfigurations to prevent vulnerabilities in cloud environments

Infrastructure-as-Code

HashiCorp Terraform

Kubernetes

Google Cloud

docker

AWS CloudFormation

ANSIBLE

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.

Analyze the context of code usage and frameworks

Poorly understood frameworks and APIs lead to false positives and missed vulnerabilities
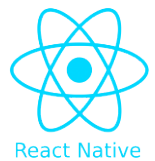
10 Most Popular Web Application Frameworks

node.js · React · jQuery · express · Angular

Vue.js · ASP.NET Core · Microsoft ASP.NET · python django · Flask

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

Support for 200+ Frameworks in All

Android · MySQL · React Native

NEXT.js · Flutter

Sequelize · RAILS

EJB Enterprise Java Beans · Bootstrap · spring

BLACK DUCK

CLICO

Köszönöm a figyelmet!

blackduck@clico.hu