SYNOPSYS® + aws

# Secure Your Application Development Workload in the AWS Cloud

## The challenge

AWS Infrastructure allows software development customers to run tools of their choice (Jenkins, Artifactory, etc.). However, customers are responsible for managing the virtual machines (VMs) that the tools run, as well as the tools themselves. This includes application security (AppSec) tools.

Because AppSec vulnerabilities are the top attack target in mobile and web apps, it's essential to integrate AppSec tools into the development pipeline on the cloud for quicker remediation. With AWS, you can deploy Synopsys AppSec tools, including Coverity, Black Duck, and Seeker, close to where you need them in CI/CD, much as if you were using an on-premises datacenter. In this way, you can manage products while renting infrastructure from AWS.

## The solution

While Synopsys tools can be used to scan within any CI/CD system, AWS has recently moved to providing hosted CI/CD and release orchestration tooling (CodePipeline, CodeStar) to remove much of the administrative overhead involved with scaling Jenkins and other CI/CD environments.

Synopsys partners with AWS to ensure that customers using AWS Developer Tools can add Coverity SAST, Black Duck SCA, and Seeker IAST to their pipelines with these integrations:

| Synopsys tool | Integration |
|---|---|
| **Coverity (on Polaris)** | Polaris CLI / Synopsys Detect |
| **Black Duck** | Synopsys Detect |
| **Seeker** | Seeker Agent for Web Applications |

For applications hosted on AWS, Synopsys works to ensure that you can use Seeker IAST with applications hosted on Elastic Beanstalk PaaS or AWS EC2. Integrating Seeker into PaaS gives Synopsys–AWS joint customers the benefits of IAST on top of those realized by AWS PaaS, with minimal management and configuration overhead.

## Solutions

AWS CodeBuild

AWS CodePipeline

AWS CodeStar

Coverity Static Application Security Testing

Black Duck Software Composition Analysis

Polaris Software Integrity Platform

## Benefits

- Synopsys tools bring SAST and SCA to AWS CodeBuild.
- Scan with Black Duck using a CodePipeline Custom Action.
- Black Duck will monitor your code and alert you to newly reported vulnerabilities associated with open source in use.
- Black Duck is available for purchase on AWS Marketplace.

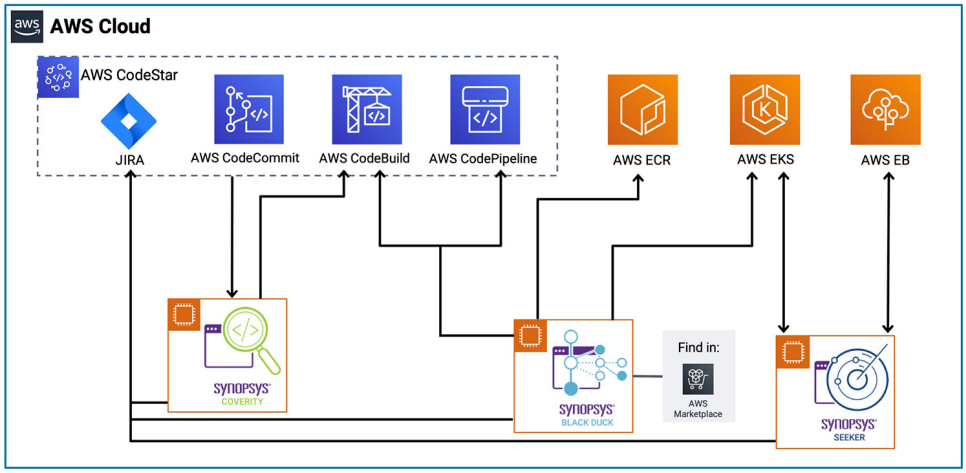
## About AWS

For 13 years, Amazon Web Services has been the world's most comprehensive and broadly adopted cloud platform. AWS offers over 165 fully featured services for compute, storage, databases, networking, analytics, robotics, machine learning and artificial intelligence (AI), Internet of Things (IoT), mobile, security, hybrid, virtual and augmented reality (VR and AR), media, and application development, deployment, and management from 69 Availability Zones (AZs) within 22 geographic regions, with announced plans for 13 more Availability Zones and four more AWS Regions in Indonesia, Italy, South Africa, and Spain. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—trust AWS to power their infrastructure, become more agile, and lower costs. To learn more about AWS, visit aws.amazon.com.

Learn how Synopsys and AWS together help customers build secure, high-quality software faster at synopsys.com/AWS.

## Synopsys and AWS Integration Architecture

Synopsys offers Black Duck and Coverity integrations with and support for AWS CI tools (CodeBuild, CodePipeline, CodeStar) and Elastic Kubernetes Service (EKS):




- **Synopsys for AWS CodePipeline.** Scan with Black Duck using a CodePipeline Custom Action. Call Synopsys product APIs to evaluate whether to continue your build.
- **Synopsys for AWS CodeBuild.** Coverity and Black Duck plug into the CodeBuild build spec, where developers direct CodeBuild on how to build the application.
- **Synopsys for AWS CodeStar.** All Synopsys tools integrate with Jira, so reported issues automatically show up in the CodeStar Dashboard alongside a view of CodePipeline.

## The benefits

- **World's leading open source KnowledgeBase™.** The Black Duck KnowledgeBase is the most comprehensive repository of open source component and vulnerability intelligence available, with information from over 19,000 data sources.
- **Enhanced vulnerability data.** The Synopsys Cybersecurity Research Center provides Black Duck Security Advisories within 24–48 hours of a vulnerability being published to help you make intelligent remediation decisions.
- **Linux patches.** Black Duck understands open source forks and Linux backports and marks vulnerabilities as patched when appropriate, significantly reducing the number of vulnerabilities you need to investigate.

## The Synopsys difference

Synopsys helps development teams build secure, high-quality software, minimizing risks while maximizing speed and productivity. Synopsys, a recognized leader in application security, provides static analysis, software composition analysis, and dynamic analysis solutions that enable teams to quickly find and fix vulnerabilities and defects in proprietary code, open source components, and application behavior.

For more information about the Synopsys Software Integrity Group, visit us online at www.synopsys.com/software.

**Synopsys, Inc.**
185 Berry Street, Suite 6500
San Francisco, CA 94107 USA

U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com