SYNOPSYS® + Google Cloud

Secure Your Application Development Workload in Google Cloud

The challenge

Are you aware that 84% of cyber attacks occur at the application layer? Application security is critical but can be challenging in the cloud. Hybrid infrastructures, container technologies, and open source are just a few of the obstacles that can stand in the way of developing secure apps and mitigating vulnerabilities.

Organizations developing in the cloud must manage an array of tools, technologies, and methodologies, including agile, DevOps, and continuous integration and continuous deployment (CI/CD), while increasingly relying on open source and delivering secure software faster. But they don't have to do it alone.

Using a cloud platform is like being in a partnership. Cloud providers protect the infrastructure from DDoS and other attacks and can offer managed open source platforms-as-a-service (PaaS). But your organization is still responsible for securing your web applications, including any open source capabilities they take advantage of.

Synopsys helps accelerate the development of cloud applications without sacrificing security, offering tools that integrate at various points throughout the application life cycle to help customers shift left and streamline application security.

The solution

Thanks to the Google-Synopsys partnership, developers can develop secure applications faster in Google Cloud Platform. GCP provides the environment for developing and deploying applications, and Synopsys provides the tools to automate and streamline application security testing for code moving through the Google Cloud Build process toward deployment. Synopsys helps integrate application security end-to-end in the development life cycle, with the flexibility to mix integrated tools and managed services to meet your needs so your developers can focus on coding.

Find issues in code and open source packages in development pipelines. Automate application security testing with Coverity and Black Duck as part of your CI/CD pipelines. Add the Synopsys Detect scan client to your Cloud Build pipelines using the Google Cloud Build worker. Coverity uses Git metadata from Cloud Source Repositories to assign issues to the developers who committed them.

Scan container images with Black Duck for open source security and compliance. Using build triggers from Google Container Registry, the Black Duck worker for Google Cloud Build can scan images as they're pushed into GCR. Optionally, the scan can sign the image in Binary Authorization to prevent it from being deployed to Google Kubernetes Engine (GKE) in case of policy violations.

Solutions

- Google Cloud Source Repositories
- Google Cloud Build
- Google Container Registry
- Google Kubernetes Engine (GKE)

- Coverity Static Application Security Testing
- Black Duck Software Composition Analysis
- Seeker Interactive Application Security Testing
- Polaris Software Integrity Platform

Benefits

- Develop apps using tools and platforms you're comfortable with
- Integrate application security seamlessly for streamlined deployment
- Write scan information directly to container images in Google Binary Authorization via Grafeas

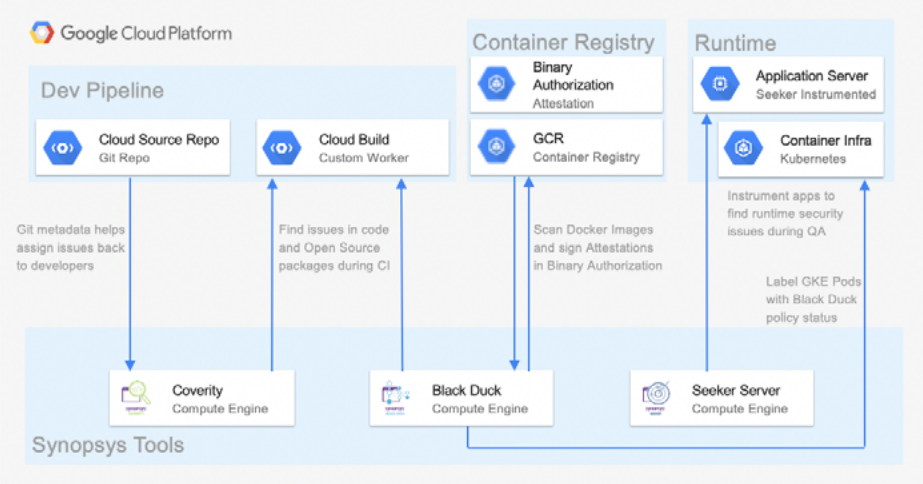
About Google Cloud

Google Cloud is widely recognized as a global leader in delivering a secure, open, intelligent, and transformative enterprise cloud platform. Google Cloud's technology is built on Google's private network and is the product of nearly 20 years of innovation in security, network architecture, collaboration, artificial intelligence, and open source software. Google Cloud offers a simply engineered set of tools and unparalleled technology across Google Cloud Platform and G Suite that help bring people, insights, and ideas together. Customers across more than 150 countries trust Google Cloud to modernize their computing environment for today's digital world.

Find vulnerabilities in web applications at runtime with IAST. Use Seeker to instrument Node.js, PHP, .NET Core, and other flavors of web applications running on GKE, Compute Engine, or an App Engine flexible environment to find security issues and sensitive-data leakage.

Get notified of new vulnerabilities reported against the open source in your applications. Black Duck keeps you updated about new open source vulnerabilities in your applications. With the Black Duck Connector for Kubernetes, Black Duck can add labels with vulnerability counts and policy status to Pods in GKE for consumption with other third-party tools.

Synopsys and Google Cloud integration architecture



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

The benefits

- Easily install and deploy from Google Cloud Platform.
- Monitor code and identify open source vulnerabilities.
- Seamlessly add notifications to images in Container Registry.
- Integrate and automate scans in CI/CD pipelines to streamline development without sacrificing security.

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