

The Synopsys logo is displayed in white, uppercase letters on a dark purple rectangular background. The background of the entire page is a complex, low-poly geometric pattern of triangles in various shades of gray, white, and purple, creating a modern, abstract aesthetic.

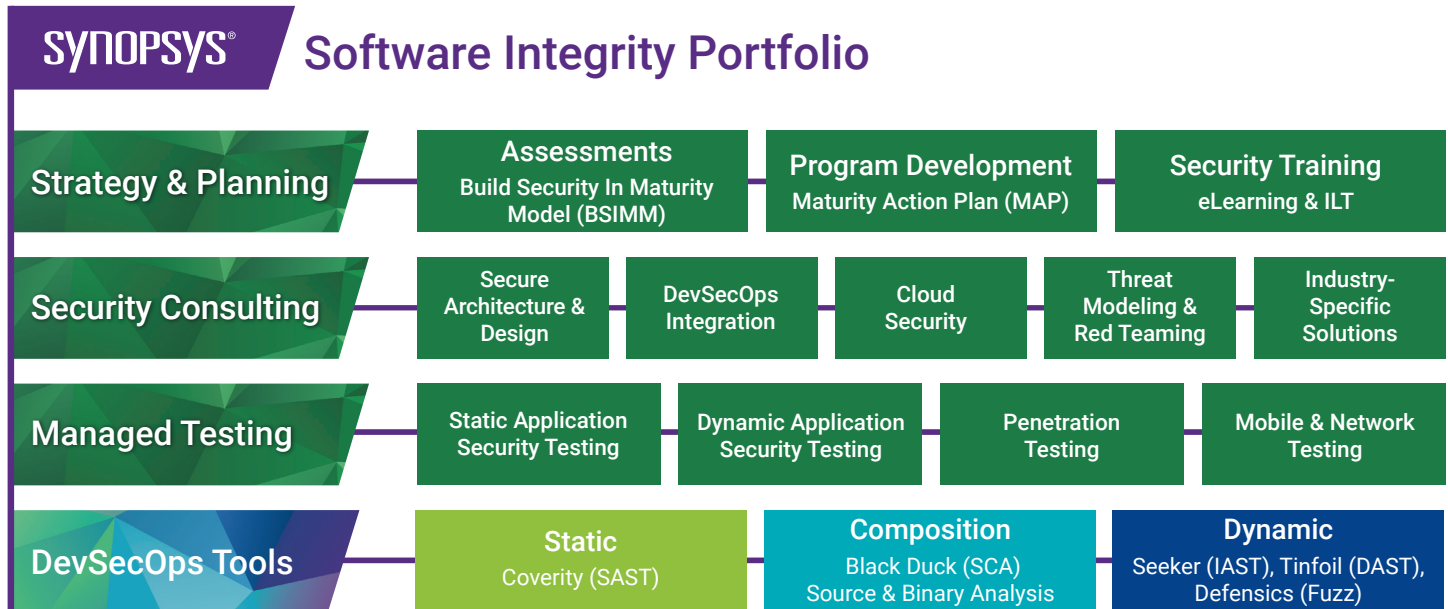
SYNOPSYS®

Software Security Portfolio

Build Secure, High-Quality Software Faster

A full spectrum of tools and services

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. With a combination of industry-leading tools, services, and expertise, only Synopsys helps organizations optimize security and quality in DevSecOps and throughout the software development life cycle.



Strategy & Planning

Our experts draw on experiences working with hundreds of organizations to help you build a strong foundation for your software security initiative (SSI), communicate security and quality requirements across teams, and measure the results that matter.

- **Building Security In Maturity Model (BSIMM).** Measure the effectiveness of your SSI by assessing your current state.
- **Maturity Action Plan (MAP).** Get clear directions for establishing or maturing your software security program.
- **Security Training.** Develop the skills to create and maintain secure, high-quality software across every role in your development organization, with a variety of training methods to fit your learning goals and schedule:
 - **eLearning.** On-demand, online application security training classes based on real-world experience and taught by industry-leading security practitioners.
 - **Instructor-Led Training.** A hands-on, technically rich training experience delivered on your own premises.
 - **IDE-Based Training.** The ideal way to learn secure coding best practices as you code.

Security Consulting

Synopsys provides access to hundreds of industry-leading experts to help you integrate quality and security best practices, tools, and strategies into your organization's unique technology stack.

- **Secure Architecture & Design.** Identify missing or weak security controls, understand secure design best practices, and mitigate security and quality defects that increase your risk of a breach.
- **DevSecOps Integration.** Inject security and quality analysis into your development workflow at the right time, at the right level, with the right tools and processes.
- **Cloud Security.** Develop a sustainable software integrity initiative for applications deployed to the cloud.
- **Threat Modeling & Red Teaming.** Adopt an attacker's perspective to identify the types of threat agents facing your software and systems, and measure how well your organization can withstand a real-life attack.
- **Industry-Specific Solutions.** Access software security, quality, and compliance solutions tailored to your industry, from automotive to retail, financial services, healthcare, embedded and IoT, critical infrastructure, government, and energy.

Managed Testing

Our security-as-a-service (SaaS) model enables security teams to accelerate security, quality, and compliance testing for any application, at any depth, to rapidly respond to changing testing requirements and evolving threats. Our premium automated testing services include:

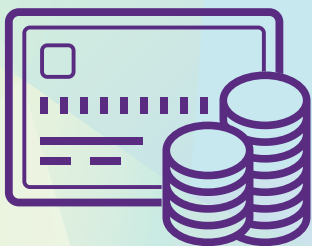
- **Static Application Security Testing.** Scan source code to systematically identify and eliminate software security weaknesses and quality defects.
- **Dynamic Application Security Testing.** Identify security vulnerabilities while web applications are running, without the need for source code.
- **Penetration Testing.** Perform exploratory risk analysis and business logic testing to reveal vulnerabilities in web applications and web services.
- **Mobile & Network Testing.** Uncover vulnerabilities in your mobile applications and your external network and systems.

DevSecOps Tools

Modern applications are built with a mix of proprietary code, open source components, and runtime behavior and configuration. We offer industry-leading tools to secure all three:

- **Coverity.** Identify critical quality defects and security weaknesses early in the SDLC, when it's least expensive to remediate, with our comprehensive static analysis solution.
- **Black Duck Source & Binary Analysis.** Detect and manage open source and third-party component risks in development and production with our industry-leading software composition analysis tools.
- **Seeker.** Discover real, exploitable vulnerabilities in web-based applications during QA and other testing, with near-zero false positives, using interactive application security testing.
- **Tinfoil.** Integrate developer-friendly dynamic application security testing for APIs and web apps into your CI and bug-tracking tools and minimize the noise of false positives.
- **Defensics.** Fuzz test software and devices for security weaknesses and vulnerabilities with flexible, scalable, automated negative testing that integrates into nearly any development workflow.

To date, Synopsys, with a market cap over \$15 billion, has invested over \$1 billion into building the ultimate software security solution. We currently work with:



17 of the top 25
commercial
banks



9 of the top 10
software
companies



4 of the top 5
managed
healthcare firms



3 of the top 4
U.S. wireless
providers

**Our mission is to help you build secure,
high-quality software faster for years to come.**

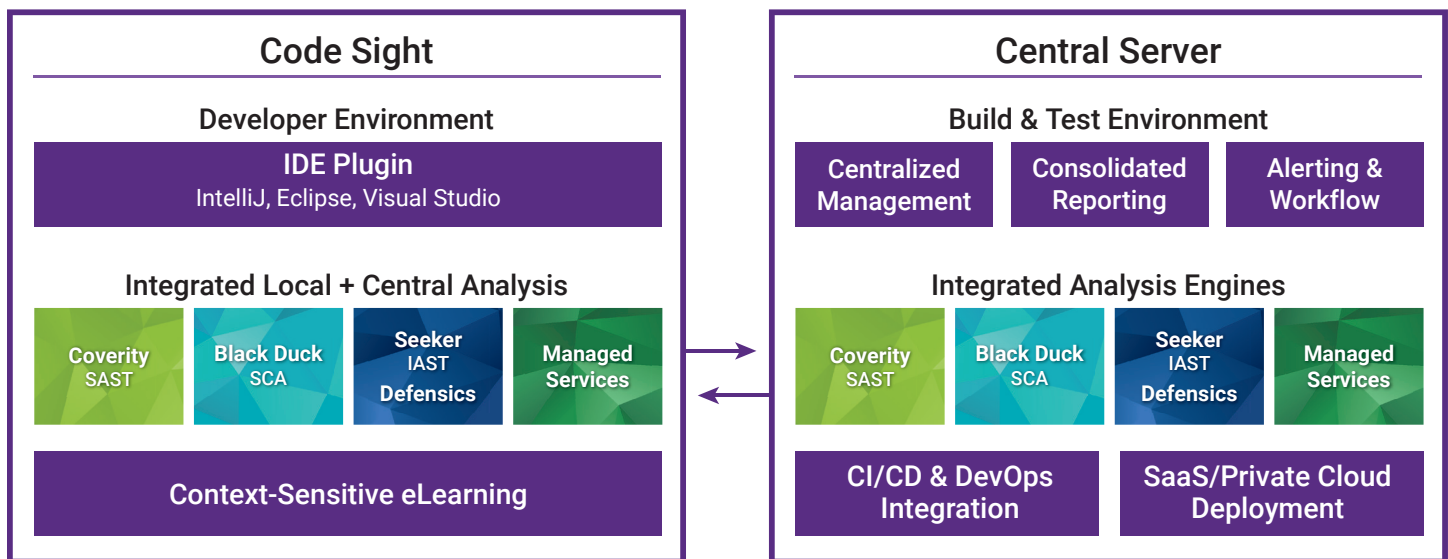
9 common goals we help you achieve

1. Mitigate and manage risk
2. Accelerate security programs and testing
3. Manage compliance
4. Create internal/operational efficiencies
5. Reduce time to market
6. Minimize costs
7. Improve business process agility and outcomes
8. Elevate customer relations and service
9. Drive innovation

Polaris Software Integrity Platform

The **Polaris Software Integrity Platform™** brings the power of Synopsys Software Integrity products and services together into one integrated solution. Unlike other platforms, Polaris enables security and development teams to use the same security analysis engines in both the developer and build/test environments, ensuring consistency of results throughout the development process. In turn, the vulnerabilities found can be fixed earlier in the SDLC, minimizing downstream delays and costs.

- Automate static, dynamic, and software composition analysis with the tools your developers already use.
- Integrate application security analysis seamlessly into your IntelliJ, Eclipse, or Visual Studio IDE with the Polaris Code Sight™ IDE plugin.
- Get combined results from multiple Synopsys analysis engines, including Coverity and Black Duck, in consolidated reports and dashboards.
- Automate security testing and policy enforcement with Jenkins, Travis, Kubernetes, Red Hat OpenShift, and other DevOps orchestration



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