

Finastra and Synopsys SIG:

Partnering to bring world-class security to Finastra's app ecosystem



Company Overview

Finastra (www.finastra.com) provides the broadest portfolio of financial services software in the world today—spanning retail banking, transaction banking, lending, and treasury and capital markets. Finastra solutions enable customers to deploy mission-critical technology on-premises or in the cloud.

A leader in application security testing, Synopsys (<https://www.synopsys.com/software-integrity.html>) helps customers build secure, high-quality software faster with solutions that manage code quality and security risks throughout the application life cycle.

The challenge: Ensuring the security of FinTech apps from design through deployment

In the world of digital banking apps, security is paramount. That's why Finastra, one of the largest FinTech companies in the world, partnered with the Synopsys Software Integrity Group (SIG) to bring world-class security to applications offered through Finastra's FusionFabric.cloud, an open platform for developing, deploying, and consuming financial applications.

Benefits for FinTechs

"With its stringent regulation and rigorous legal requirements, the financial services industry is not an easy one to satisfy, especially with dozens—even hundreds—of other FinTech vendors clamoring for attention," said Paul Andrusyshyn, GM, financial services at Kore.ai. "Financial institutions are demanding secure digital services with a quality of experience equal or superior to person-to-person interactions."

"Finastra's FusionFabric.cloud gives Kore.ai the opportunity to market our BankAssist.ai product to potentially thousands of financial institutions," Andrusyshyn said. "Finastra's partnership with Synopsys provides the added benefit of a thorough security validation that only has to be done once to ready us to work with any of Finastra's FSI clients. This not only saves valuable time but assures Finastra and our joint customers [of] the level of trust they need."

The partnership ensures that applications offered via FusionFabric.cloud are vetted by the Synopsys application security validation program—rigorous software security assessments that include [static application security testing](#), [software composition analysis](#), [penetration testing](#), and [code reviews](#).

The solution: The Synopsys application security validation program

FusionFabric.cloud is designed to give FinTechs, financial institutions, students, independent developers, system integrators, and consultants access to a global marketplace of financial applications. A key requirement of making that marketplace viable is creating trust among all the parties involved.

"Security is a requisite in the FinTech space," said Nir Valtman, VP and head of product and data security at Finastra. "Synopsys' application validation program leverages Synopsys' security testing technology and expertise to ensure that applications published on the FusionFabric.cloud platform are designed, developed, and deployed with the highest standards for security."

Benefits for banks

"FinTechs are defining change across almost every financial services sector," said Jayson Callies, EVP and chief technology officer of Seattle Bank. "FinTechs are vital links in the financial services value chain and represent a great partnership opportunity for smart FSIs. Finastra's App Store ecosystem (FusionStore) is a veritable supermarket of FinTech capabilities, allowing us to choose and deploy new FinTech offerings via the cloud and APIs."

"We need to be 100% certain of any app's security before we commit to it. Finastra's partnership with Synopsys provides us with confidence that apps in the FusionStore have been vetted and are secure."

The Synopsys application security validation program provides rigorous software security assessments, including Coverity® static application security testing (SAST), Black Duck® software composition analysis (SCA), penetration testing, and code reviews. Coverity identifies critical software quality defects and security vulnerabilities to ensure code that is secure, higher quality, and compliant with standards. Black Duck SCA provides a comprehensive solution for managing security, quality, and license compliance risk that comes from the use of open source and third-party code in applications and containers. Synopsys managed penetration testing systematically finds and eliminates business-critical vulnerabilities in running web applications and web services.

"The net result is a win-win for both FinTech providers and their financial services customers," said Nir Valtman. "FinTech app providers get third-party validation from an industry-leading application security company, and their customers can rely on the applications with confidence."

The results: Security validation for FinTechs and their customers

"We have more than 20 apps today in the store, all of which went through the SIG vetting process before going live on FusionStore," Nir Valtman said. "With the easily understood reports that the Synopsys security validation program provides, it's a relatively simple process for me to make a 'go/no-go' decision and provide any needed feedback to the FinTechs."

Results

- A total of 18 FinTechs have used the application security validation program for more than 20 separate apps. The security validation program includes Black Duck software composition analysis, Coverity static application security testing, and security controls analysis.
- A full 65% of the FinTechs that used the Synopsys security validation program were able to correct minor missing security controls.
- FinTechs quickly addressed the missing security controls with a corrective action plan.

"An added benefit is that FinTechs see the value of the program for themselves through these reports," added Nir Valtman. "Their code is scanned and validated by a third party. And not just a third party, but Synopsys, one of the leaders in [application security testing](#). Even the most sophisticated FinTechs may lack the expertise to review their own security posture. But they still need to assure customers that they've tested for security issues in their code. From their perspective, being able to produce the Synopsys report and say to customers, 'yes we've had a security scan,' is a major plus."

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