

Finastra和Synopsys SIG:

携手为Finastra的应用生态系统带来世界一流的安全性



公司介绍

Finastra (www.finastra.com) 提供当今世界上最广泛的金融服务软件组合，涵盖零售银行、交易银行、借贷、债券和资本市场。Finastra解决方案使客户能够在本地或云端部署关键任务技术。作为应用安全测试领域的领导者，Synopsys软件质量与安全部门 (www.synopsys.com) 提供可在整个应用程序生命周期中管理代码质量和安全风险解决方案，从而帮助客户更快地构建安全、高质量的软件。

挑战：确保金融科技应用程序从设计到部署的端到端安全性

对数字银行应用程序来说，安全性是至关重要的。鉴于此，世界上规模最大的金融科技公司之一Finastra与Synopsys软件质量与安全部门 (SIG) 建立了合作关系，为通过FusionFabric.cloud提供的应用程序带来世界一流的安全性。FusionFabric.cloud由Finastra提供，是用于开发、部署和消费金融应用的开放平台。

对金融科技公司的益处

通用汽车金融服务有限公司 (GM Financial Services) 的Paul Andrusyshyn在Kore.ai表示：“金融服务业的法律法规非常严格，因此，满足金融服务业的要求并非易事，尤其是在数十甚至数百家金融科技供应商都在竭力抢夺客户的情况下。金融机构需要体验质量至少等同于人与人之间互动的安全的数字服务。”

“Finastra的FusionFabric.cloud使Kore.ai有机会向潜在的数千家金融机构推广我们的BankAssist.ai产品。Finastra与Synopsys的合作还带来了一个额外好处，即只需进行一次全面的安全验证，我们便可与Finastra的任何FSI客户进行合作。这不仅能够节省宝贵的时间，而且还能确保赢得Finastra和我们的共同客户的信任。”

该计划可确保凡是通过FusionFabric.cloud提供的应用程序，均需接受Synopsys应用程序安全验证解决方案的审查 — 严格的软件安全评估解决方案，涵盖静态应用程序安全测试 (SAST)、软件组成分析 (SCA)、渗透测试和代码审查等组件。

Synopsys应用程序安全验证解决方案

FusionFabric.cloud旨在使金融科技公司、金融机构、学生、独立开发商、系统集成商和顾问均能访问全球金融应用程序市场。开通该市场的一个关键前提是在所有相关方之间建立信任。

Finastra的产品和数据安全主管Nir Valtman表示：“安全是金融科技领域的必要条件。Synopsys的应用程序验证解决方案利用了Synopsys的安全测试技术和专业知识，可确保在FusionFabric.cloud平台上发布的应用程序是采用最高安全标准来设计、开发和部署的。”

对银行的好处

西雅图银行 (Seattle Bank) 副总裁兼首席技术官Jayson Callies表示：“金融科技正在定义几乎每个金融服务领域的变革。金融科技是金融服务价值链中至关重要的一环，给智能金融服务机构带来了绝佳合作机会。Finastra的‘App Store’生态系统 (FusionStore) 是名副其实金融科技能力超级市场，使我们能够通过云和API来选择和部署新的金融科技产品。”

“我们首先需要100%确定任何应用程序的安全性，然后才会做出承诺。Finastra与Synopsys的合作为我们提供了信心，因为我们知道FusionStore中的应用程序均已经过审查，是安全的。”

Synopsys应用程序安全验证解决方案提供严格的软件安全评估，包括Coverity静态应用安全测试 (SAST)、Black Duck软件组成分析 (SCA)、渗透测试和代码审查等组件。Coverity可识别出重大的软件质量缺陷和安全漏洞，以确保代码是安全的、高质量的、符合标准的。Black Duck SCA为管理因应用程序和容器中使用开源代码和第三方代码而带来的安全性、质量及许可证合规风险提供了全面解决方案。Synopsys托管的渗透测试能够系统地发现并消除因运行web应用和web服务而带来的关键业务安全漏洞。

Nir Valtman表示：“最终结果是金融科技提供商及其金融服务客户取得双赢。金融科技应用程序提供商将能够获得业界领先的应用程序安全公司提供的第三方验证，而他们的客户则可以放心地依赖这些应用程序。”

结果：为金融科技及其客户提供安全验证

Nir Valtman表示：“我们的FusionStore中目前有20多个应用程序，所有这些应用程序在上线之前均已经过SIG审查。Synopsys安全验证解决方案提供易于理解的报告，使我能够相对简单地做出‘放行/不放行’决定，并向金融科技客户提供他们所需的任何反馈。”

结果

- 共有18家金融科技公司对20多个独立应用使用了这个应用程序安全验证解决方案。该解决方案中包括Black Duck软件组成分析 (SCA)、Coverity静态应用安全测试 (SAST) 和安全控件分析 (SCDA) 等组件。
- 在使用Synopsys安全验证解决方案的金融科技公司中，有65%能够纠正因安全控件稍有缺失而带来的问题。
- 金融科技公司通过适当的纠正计划迅速解决了安全控件缺失带来的问题。

Nir Valtman补充道：“另一个好处是，金融科技公司可以通过这些报告看到该解决方案对他们的价值。他们的代码将由第三方扫描和验证。不仅仅是第三方，还有应用安全测试领域的领导者之一Synopsys。即使是最成熟的金融科技公司，也可能并不具备对安全态势进行自我审查的专业知识。但他们仍需向客户保证已对代码中的安全问题进行了测试。从他们的角度来看，能够生成Synopsys报告并对客户说‘是的，我们已经进行了安全扫描’，这将是一个重要的附加优势。”

Synopsys 的与众不同之处

Synopsys 公司帮助开发团队构建安全、高质量的软件，最大限度地提高速度和生产力，同时将风险降至最低。Synopsys 是静态分析、软件组成分析和应用安全测试领域公认的领导者，定位于将最佳实践应用于私有代码、开源软件以及运行时环境。

有关Synopsys Software Integrity Group的
详细信息，请访问
www.synopsys.com/software。

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

美国销售：800.873.8193
国际销售：+1 415.321.5237
电子邮件：sig-info@synopsys.com

©2020 Synopsys, Inc. All rights reserved. Synopsys is a trademark of Synopsys, Inc. in the United States and other countries. A list of Synopsys trademarks is available at www.synopsys.com/copyright.html. All other names mentioned herein are trademarks or registered trademarks of their respective owners. December 2020