SYNOPSYS®

Coverity
静态分析解决方案

主要优点

高性能。快速增量扫描能够识别出新增代码或修改代码中存在的问题，不会像完整扫描那样耗时，但又兼备完整扫描的精准度。这样，开发者可以在每次提交或拉取请求时轻松进行频繁的扫描，而不会减慢开发速度。

企业级。Coverity能够扫描世界上最大的应用，包括那些涉及数千名开发者和数千万行代码的应用。

可扩展性。您可以轻松创建自定义检查器，以支持专有框架或不支持的语言。

灵活部署。Coverity可以根据您的需要，在本地或私有云环境中运行。这样，您就可以享受最优质的静态分析扫描，同时确保数据安全。

最全面的静态分析

Coverity®是市场上最准确且最具扩展能力的静态分析软件，能够帮助开发者和安全团队大规模地交付安全、高质量的应用。通过为每个应用构建深入的模型，然后将其与对所有依赖项、编译器，以及对20多种编程语言和200多种框架的深入了解相结合，Coverity能够对世界上最大的应用进行分析，发现跨越多个文件和库的复杂问题。

在开发生命周期中及早进行快速扫描

Coverity扫描可以在SDLC的早期阶段执行，以便在破坏性最小且最容易解决的时候发现安全和质量问题。

在IDE中实时运行

开发者在编写代码时会收到有关漏洞和代码质量问题的通知，从而防止问题被提交到代码仓库中。

在拉取请求时触发

增量扫描能够识别任何新增或修改代码中的问题，并集成到常用的源代码管理系统中。

在CI/CD管道中自动运行

全面的应用扫描可以识别出尚未解决的安全或质量问题，并在发现策略违规时中断构建过程。

最准确的结果

Coverity可以生成高度准确的扫描结果，从而减轻开发者的负担，使他们能够专注于处理真正的缺陷，而不是浪费时间来处理误报。

- **对每个应用构建深度模型**，以针对其运行方式提供关键洞察，包括所有的依赖项和编译器，以及数据流和控制流路径。
- **针对20多种编程语言和200多个框架提供深入洞察**，为区分误报和真正的问题提供背景信息。
- 将**背景信息**应用于初始扫描结果，以验证每个结果，并评估漏洞利用的可能性。
- **可配置的安全和质量检查器**，默认设置为“高精度”，但可根据业务或应用的风险情况进行调整。

广泛覆盖安全和行业标准

Coverity具有一流的代码质量问题识别能力，并覆盖最全面的安全性和行业标准，包括：

- **网络安全：**OWASP Top 10、SANS CWE Top 25和PCI DSS
- **功能安全：**MISRA®、CERT C/C++、CERT Java、DISA STIG、ISO 26262、ISO 23434、ISO/IEC TS 17961、AUTOSAR®和Hyundai安全编码标准

报告可以PDF格式下载，方便审计人员对每个标准保留详细的合规记录。趋势报告可以提供额外的洞察，显示漏洞严重程度随时间变化的情况，以及单个开发者和开发团队在清除重大问题方面取得的进展。

此外，Coverity Qualification Kit (Q-Kit)可以确保Coverity针对安全关键项目进行正确配置，以符合ISO 26262和DO-330等行业安全标准。

主要特性

- **易于上手。**通过Point and Scan桌面应用，用户只需指定源代码的位置，便可以轻松开始使用Coverity。对于更喜欢使用命令行界面(CLI)的开发团队，Coverity的CLI 提供类似的功能。
- **与开发者工作流无缝集成。**Synopsys Bridge提供了一种简单、可预测的方法，可通过CLI将任何新思科技应用安全测试解决方案（包括Coverity）集成到常用的CI/CD工具中。
- **实时发现缺陷。**Code Sight™ IDE插件可在开发者编写代码时提供准确的静态分析洞察。每个问题都在IDE中显示问题描述、类别、严重程度、CWE数据、缺陷位置和具体的修复指导。
- **可操作的修复指导。**详细的建议和特定于上下文的远程学习，可以帮助开发者了解如何快速修复问题，不必成为安全专家。
- **详细的报告。**仪表板可以显示Coverity根据行业公认的列表、问题类型和技术风险指标而预先生成的报告，以帮助开发者优先考虑并集中精力处理对贵组织最重要的问题。过滤器允许您按照不同的方式对问题进行轻松分组，如CWE、标准分类、优先级列表、风险指标、路径和个人开发者等。

有关支持技术的详细列表，请访问“Coverity语言和框架”(Languages and Framework)页面。

新思科技与众不同

新思科技提供的集成解决方案，可以改变您构建和交付软件的方式，在应对业务风险的同时加速创新。与新思科技同行，您的开发人员可以在编写代码的时候快速兼顾安全。您的开发和DevSecOps团队可以在不影响速度的情况下在开发管道中自动进行安全测试。您的安全团队可以主动管理风险并将补救工作聚焦在对贵组织最重要的事情上。我们无与伦比的专业知识可以帮助您规划和执行所需安全计划。只有Synopsys能够满足您构建可信软件的一切需求。

如想了解有关Synopsys Software Integrity Group的更多信息，请访问：www.synopsys.com/software.