

支付卡行业数据安全标准，PCI DSS

Klocwork提供领先的静态源代码分析技术帮助您实现企业软件的安全目标。

PCI DSS标准由PCI安全标准协会制定，该协会制定了一系列标准和惯例用来保护支付卡用户数据的安全。该标准制定一系列方式用来保护客户的数据——来源于安全的网络，包括开发和设计安全、漏洞管理和访问控制。

Klocwork可以协同该标准的应用，由于该标准与开发和维护安全软件应用相关。Klocwork静态源代码分析工具可以帮助开发团队实现遵循PCI DSS标准的一致、策略性的路径，来确保清除软件代码中的漏洞。

// 生产更加安全的代码

Klocwork Insight是一种开创性的源代码分析工具，其有效性已经在世界上某些代码要求苛刻的软件开发环境中得到了验证。Klocwork Insight能够通过以下方式帮助公司解决软件安全问题：

- 将关键性漏洞检测提前到开发过程的初始阶段
- 为开发者提供关键性漏洞检测和修复能力
- 允许开发者在代码测试之前进行漏洞修复
- 帮助安全专家将安全和构建规范发布给每一个开发者

通过在开发早期清除代码漏洞，Klocwork Insight可以帮助企业加快开发进程，降低成本，创建更好的执行过程并交付更清洁和安全的代码。

// 领先的源码分析工具

Klocwork源代码分析工具

- 分析C、C++和Java代码
- 支持主流Java框架，包括：J2EE，J2ME，J2SE，Google Web工具以及Hibernate实体
- 可以在问题形成前检测和修复代码中的漏洞
 - » 在开发者本地IDE、文本编辑器或命令行环境运行Klocwork工具
 - » 漏洞报告包括风险实质的解释和修复建议
- 在更短时间内检测更多的代码
 - » 在软件构建过程中自动运行源代码分析工具
 - » 通过架构可视化工具更好的理解软件
- 使用一套软件即可发现安全和质量缺陷

// PCI DSS 支持

Klocwork支持PCIDSS标准的三个具体部分：

PCI 兼容性需求	Klocwork 支持
6.3 基于行业最佳惯例和软件生命周期的信息安全开发软件产品。	基于行业最佳实践和软件生命周期的信息安全开发软件产品。
6.5 基于安全编码方针，例如开放式Web 应用安全方案 (OWASP)，进行Web应用开发。检测自定义应用代码来发现编码漏洞。预防软件开发过程中的常见漏洞，主要有： <ul style="list-style-type: none"> 6.5.1 未经验证的输入 6.5.2 破坏访问控制（例如：恶意使用用户ID） 6.5.3 破坏授权和会话管理（帐号信任度和会话工具的使用） 6.5.4 跨站点脚本（XSS）攻击 6.5.5 缓冲区溢出 6.5.6 注入缺陷（例如：SQL语言的注入） 6.5.7 出错处理不当 6.5.8 非法存储 6.5.9 拒绝服务 6.5.10 不安全的配置管理 	Klocwork Insight能够用来检测上百种不同的在C、C++和Java代码中的安全漏洞。为了组织能够配置与PCI DSS标准兼容的Klocwork，所有的漏洞都由Klocwork以一种与PCI兼容的格式上报给开发者、安全经理和审计人员，便于跟踪和报告组织在针对与PCI DSS兼容目标的状态。（如图一）。
6.6 使用诸如源代码分析工具等推荐技术来确保Web应用软件不受已知攻击的侵害。	Klocwork Insight静态分析工具已被应用于全球超过300家组织，并应用在需要严格编写安全代码的组织中，证明是一个有效的解决方式。

// 全面的安全研究

Klocwork的漏洞分析能力建立在先进的静态代码分析技术中，并整合为一套漏洞检查能力，用来保证自身研究的顺利进行，并与以下安全计划合作：

- 美国国家标准技术研究院(NIST)
 - » 软件保证度量 and 工具评估标准 (SAMATE) 提供了一份包含1000多个关于C/C++和Java漏洞和缺陷的参考数据。
 - » 整个SAMATE参考数据中90%以上在Klocwork的测试系列中。
- 国土安全部 (DHS)
 - » 软件缺陷通用词典 (CWE) 这一计划根据来自学术和行业资源的软件代码缺陷创建一个包含所有已知缺陷的列表。
 - » Klocwork是这个项目第一阶段的贡献者之一。
- 支持十大OWASP标准

图一：Klocwork漏洞分析报告可以以一种PCI兼容的形式显示

