sonar | sonarqube

C&S 创实信息

在您的工作流程中使用{SonarQube}实现清洁代码

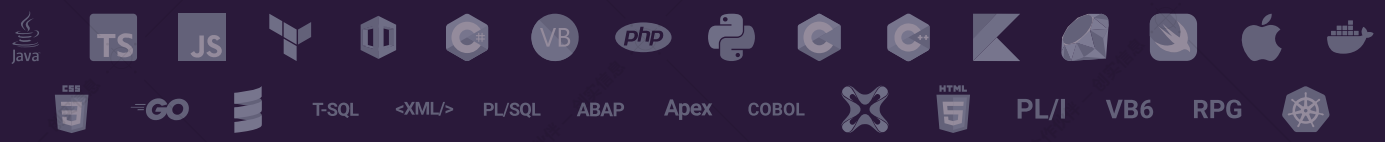
SonarQube 是一种自我管理、全面且自动化的代码分析解决方案，可系统性地帮助开发人员和组织交付清洁代码。

作为 Sonar 解决方案的核心组成部分，SonarQube 可融入您现有的开发工作流程，并在对项目进行持续代码检查的过程中，检测代码库中的错误和安全问题。

{可靠性}
· BUG · 测试覆盖率

{安全性}
· 热点 · 漏洞 · 注入缺陷检测

{可维护性}
· 代码异味 · 认知复杂度
· 重复代码



广泛的语言和规则覆盖范围
支持包括 IaC 在内的 31 种语言、框架和基础架构技术，并提供超过 5000 条编码规则，涵盖清洁代码的方方面面。

与 DevOps 平台集成
与首选的 DevOps 平台集成 – GitHub, GitLab, Bitbucket 或 Azure DevOps。

拉取请求和分支分析
拉取请求和分支分析以及开发流水线中的质量门状态，可提供早期反馈，以确保持续交付干净的代码。使用 SonarQube，每一次新的生产交付都会比上一次更好。

共享并统一代码质量定义
使团队对代码健康的定义保持统一。通过利用和自定义规则来满足质量配置文件中所设定的期望，从而在项目间实现高效协作。

项目组合管理
将项目和应用程序映射到企业层次结构中。项目组合可让领导团队即时了解和跟踪整个部门所有项目的健康状况，包括项目的可发布性。

企业报告
以 PDF 格式导出和规划报告，确保所有利益相关者都能看到关键指标。项目报告提供当前的质量门状态以及任何失败条件，以及新代码（新增或更改的代码）的主要指标值。

安全合规性
在与 PCI DSS, OWASP ASVS, OWASP Top 10 和 CWE Top 25 等报告相对应的分析过程中，检测安全漏洞和热点。

支持和社区
Sonar 提供您与我们服务团队之间的私人沟通渠道。我们的社区是一个免费且活跃的论坛，我们和社区成员每天都在这里发布内容，以解决问题和分享知识。

“在静态分析方面，市场上没有任何其他的工具能像 SonarQube 一样可靠和值得信赖。它们是软件质量分析的行业标准，任何需要对软件质量和漏洞进行审计的公司都应该使用它们。”

Daniel Anjos, TrustRadius 评论员

边编码边清洁（Clean as You Code）
Sonar 的“边编码边清洁”对于实现清洁代码（Clean Code）至关重要——当您的代码库达到无问题状态时，既适合开发也适合生产。这种方法使开发人员和组织能够仅通过关注新增或修改的代码，来优化代码库的质量。这种简单而强大的方法能够以最小的成本和努力，逐步改善整个代码库的质量。

受到 700 万开发人员和 40 万组织的信赖

IBM Microsoft BARCLAYS Alphabet FBI NASA

SonarQube 企业版

商业支持版的“清洁代码”解决方案，可帮助加速您的关键任务软件开发，同时减少技术债务。

SonarQube 企业版为大型成长型组织提供了高可用性和可扩展性。该解决方案基于 Sonar 的清洁代码（Clean Code）方法论，可对 30 多种编程语言进行深入的代码分析，并将其集成至整个组织的项目和 CI/CD 流程中。SonarQube 企业版可评估复杂的错误和漏洞，并生成关于软件可维护性、可靠性和安全性的详细报告。

此外，SonarQube 企业版还提供了代码覆盖率、重复检测和代码异味等方面的见解，使开发团队能够在整个软件开发生命周期中，提高整体代码质量和安全性。

为何升级到SonarQube 企业版?

升级到 SonarQube 企业版，可解锁专属支持、安全性、高效性、可扩展性，以及更多高级功能，将您的代码质量提升到新水平。

支持、安全、可靠：

- 提供全天候的高级支持服务
- 内置高可用性和数据完整性 *
- 符合美国国防部（DoD）标准
- 被超过 80% 的财富 100 强公司所信赖
- 提供整个组织的执行报告和项目组合管理

解锁 70% 以上的规则和其他语言，检测复杂的漏洞和 Bug：

- 污点分析追踪不受信任的用户输入（例如 SQL 注入，XSS 代码注入）
- 深入 SAST 分析开源代码使用中隐藏的问题
- 检测导致运行时错误和崩溃的高级错误
- 利用高级机密检测功能防止敏感信息泄露
- 全面的安全和合规性报告（例如 PCI DSS，OWASP，CWE）
- 专门支持 C，C++，Swift，COBOL，PL/I，PL/SQL，ABAP 等语言

通过企业级的可扩展性和可用性加速创新：

- 通过组织范围内的质量门，确保安全采用人工智能代码生成技术
- 快速、准确的分析，可扩展至数十亿行代码 *
- 分析多个 DevOps 平台上的多个分支、拉取请求和项目
- 在无缝集成的 IDE 和 CI/CD 工作流中实时应用“边编码边清洁”

SonarQube 助您掌握代码质量与安全的力量，赋予开发团队一个以代码为先的解决方案，同时可深度集成到您的企业环境中，让您能够在整个组织中部署清洁代码，以实现创新且持久的软件开发。

* 适用于数据中心版

SonarQube 安全功能

或许您已经熟悉 SonarQube 强大的代码质量功能，但可能还不了解其广泛的安全功能，这些功能都包含在许可证中。SonarQube 企业版为开发团队提供先进的安全功能，以确保您的代码稳健、安全并符合行业标准。

以下是所包含的安全功能的详细概述：

功能	描述	优势
静态应用程序安全测试 (SAST)	自动化分析，以检测代码库中的安全漏洞和编码缺陷。	尽早准确地识别并修复漏洞，确保代码部署更安全。
安全热点检测	突出显示可能存在风险但需要手动审查以确认的代码部分。	使开发人员能够专注于潜在的易受攻击区域，而不会因误报倍感压力。
深度 SAST	检测由于第一方代码与开源库（第三方代码）交互而产生的深度隐藏的复杂安全漏洞。	提供深入的安全分析，并揭示与第三方库 / 代码交互产生的深度隐藏问题。
安全引擎自定义配置	允许根据特定需求自定义安全规则和配置。	使安全分析适应项目的独特需求。
机密检测	准确识别代码中硬编码的秘密，如密码和 API 密钥。	防止敏感信息的意外暴露，保护您免受安全漏洞的威胁。
高级机密检测	允许根据特定需求自定义机密检测规则。与 SonarLint 一起使用，可防止秘密泄露及成为严重的安全漏洞。	确保检测到独特的或组织特定的机密，以降低漏洞风险。
强制执行代码质量和安全的质量门	在您的 CI/CD 工作流中定义并强制执行安全阈值。	确保只有安全且高质量的代码被部署到生产环境中。
详细的安全报告	专用报告跟踪应用程序的代码安全性，符合 OWASP Top 10、OWASP ASVS、CWE Top 25（2021、2020 和 2019）以及 PCI DSS 等标准。	关于安全问题和补救措施的综合合规报告。帮助团队有效理解并解决安全问题。

SonarQube 10.6 版本

在 SonarQube 10.6 版本中，我们进行了一些重大更改，包括 Kubernetes 中的自动扩展、C 和 C++ 项目的自动配置、支持在 FIPS 中运行、设置规则优先级以维护您的编码标准、轻松设置 monorepo、可预测的升级、为 AI/ML(机器学习) 开发人员扩展库覆盖范围等。

Kubernetes 中的 SonarQube 自动扩展

从此版本开始，在 Kubernetes 集群中运行时，SonarQube 支持应用程序 pods 的水平自动扩展。这将确保开发人员不会因资源限制而花时间等待分析完成。此外，由于应用程序 pods 可根据需求自动伸缩，因此可优化运行它们所需的资源，从而节约成本。**适用于数据中心版**

C 和 C++ 项目的 AutoConfig

随着 C 和 C++ 项目引入 AutoConfig，分析这些项目不再需要设置编译包和编译数据库。因此，大多数编译器（即使是以前不支持的编译器）无需额外配置即可运行。这大大减少了设置 C 和 C++ 项目所需的时间，分析工作也能顺利进行。**适用于开发者版、企业版、数据中心版**

SonarQube 在 FIPS 强制执行的环境中运行

Sonar 通过采用安全代码开发实践，帮助政府机构和组织满足 FIPS 要求。在 FIPS 环境中运行 SonarQube 服务器可确保用于加密、解密和数字签名的加密算法，获得美国国家标准与技术研究院（NIST）的批准。**适用于社区版、开发者版、企业版、数据中心版**

设置规则优先级以防止发布不合规的代码

开发经理或任何确定公司代码标准的人员，现在都可以在质量配置文件中配置规则的优先级，以便所有符合优先级规则的问题都无法通过质量门。这将允许公司设置策略，确定开发人员在下一个版本之前必须解决整体代码中的哪些问题，以确保该版本符合公司的清洁代码（Clean Code）标准。**适用于企业版、数据中心版**

Python 中的 Scikit-learn 库

在 10.6 中，我们增加了对 Scikit-learn 库的支持，该库是用于 AI 和机器学习开发的顶级 Python 库之一。通过此次新增，SonarQube 现在支持机器学习从业者使用的四大 Python 库：TensorFlow、Scikit-learn、NumPy 和 Pandas。**适用于社区版、开发者版、企业版、数据中心版**

为所有 DevOps 平台轻松设置 monorepo

在 10.5 中，我们为 GitHub 和 GitLab 添加了 monorepo 的简单设置。在 10.6 中，相同的 monorepo 单一流程设置在 Azure DevOps 和 Bitbucket 中同样可用，从而完善了我们在所有四个 DevOps 平台对 monorepo 的简化设置。**适用于企业版、数据中心版**

在升级期间监控升级时间和进度

SonarQube 的升级可能无法预测，尤其是对于因项目众多而拥有大型数据库的实例。现在，Sonar 通过估算执行升级所需的时间，使升级更具可预测性。这允许您将升级安排在更合适的时段，从而减少对团队的影响。此外，在升级期间，您可以监控完成升级的剩余时间，以了解 SonarQube 实例何时可以再次运行。**适用于社区版、开发者版、企业版、数据中心版**

针对 Sonar 问题提供基于 AI 的修复建议

- 我们提供基于 AI 的修复建议，以帮助开发人员在开发工作流程中更快地修复代码问题。
- 更多机器学习和数据科学规则