开源治理服务

产品介绍

文档版本 01

发布日期 2024-11-21

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是开源治理服务

开源治理服务（CodeArts Governance）是针对软件研发提供的一站式开源软件治理服务，凝聚华为在开源治理上的优秀实践经验，提供开源软件元数据及软件成分分析、恶意代码检测等能力，从合法合规、网络安全、供应安全等维度消减开源软件使用风险，助力企业更加安全、更加高效地使用开源软件。

检测能力

- 二进制成分分析

  对用户提供的二进制软件包/固件进行全面分析，通过解压获取包中所有待分析文件，基于组件特征识别技术、静态检测技术以及各种风险检测规则，获得相关被测对象的组件BOM清单和潜在风险清单，并输出一份专业的分析报告。

- 源码成分分析

  对用户提供的源码进行全面分析，通过解压获取源码包中所有待分析源码文件，基于源码特征识别技术，获得相关被测对象的开源软件清单和潜在风险清单，并输出一份专业的分析报告。

2 功能特性

开源治理服务提供端到端的专项安全检测能力和开源软件元数据管理能力，功能特性如下：

- 开源知识库

  提供开源软件统一管理能力，通过对开源软件元数据、开源软件制品及源码的统一管理，提供可信的开源软件来源。

  - 开源元数据中心

    提供已治理（元数据完整性、依赖信息、恶意软件扫描等）的开源数据资产信息，包含元数据信息、漏洞信息、依赖信息等内容。

- 二进制成分分析
  - 全方位风险检测

    对软件包/固件进行全面分析，基于各类检测规则，检测相关被测对象的开源软件漏洞和许可证合规、敏感信息（弱口令、硬编码密码等）、安全配置、安全编译选项等存在的潜在风险。

  - 支持各类应用

    支持对桌面应用（Windows和Linux）、移动应用程序（APK、IPA、Hap等）、嵌入式系统固件等的检测。

  - 专业分析指导

    提供全面、直观的风险汇总信息，并针对不同的扫描告警提供专业的解决方案和修复建议。

  - 恶意代码检查

    提供病毒木马等恶意软件的扫描，支持开源软件中敏感信息外发、木马下载执行、反弹shell、恶意命令执行恶意行为检测。

- 源码成分分析
  - 全方位风险检测

    对软件源码进行全面分析，基于源码特征识别检测规则，检测相关被测对象的开源软件漏洞和许可证合规等潜在风险。

  - 漏洞分析指导

    提供全面、直观的漏洞汇总信息，并提供专业的解决方案和修复建议。

3 产品优势

- 二进制成分分析
  - 无源码、无侵入快速检测
    只需要上传产品发布包或固件，无需构建运行环境或运行程序。
  - 多语言、多文件格式、多架构平台
    支持多语言，多构建场景下的制品检测，场景覆盖不遗漏。
  - 恶意代码检测，确保供应安全
    基于AI开源软件恶意代码检测能力，恶意行为早发现。
  - 敏感信息检测防泄露
    支持安全配置和密码密钥等敏感信息检测，发现潜在的安全风险。
- 源码成分分析
  - 代码克隆检测
    提供代码片段级别的代码克隆（TYPE1、TYPE2）检测分析服务，发现潜在的开源软件使用合规风险。
  - 漏洞风险检测
    提供已知漏洞安全检测分析服务，发现潜在的开源软件安全风险。
  - 许可证合规检测
    提供开源软件许可证风险等级评估体系，发现潜在的开源软件兼容性以及篡改等风险。

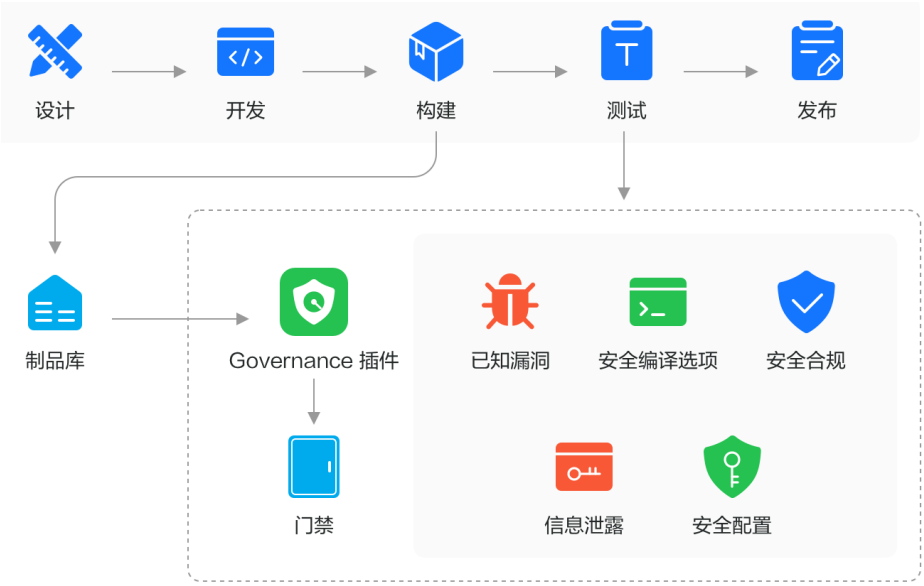
4 应用场景

- 二进制成分分析

  二进制成分分析主要用于以下场景。

  - 开源软件使用风险评估

    二进制成分分析服务提供开放API，并与CI/CD融合，完善DevSecOps安全能力。

  - 开源/第三方软件引入评估

    二进制成分分析服务提供页面和开放API，提供风险快速评估能力。

- 源码成分分析
  源码成分分析主要用于以下场景。
  - 源代码级成分分析
    识别项目源码中包含的开源成分，精确至代码片段级。
  - 开源漏洞识别与解决建议
    识别项目源码中引入的开源漏洞，并给出专业的修复建议。

5 约束与限制

介绍开源治理服务的使用限制。

控制台使用限制

表 5-1 控制台使用限制说明

指标类别	指标项	限制说明
浏览器	类型	目前适配的主流浏览器类型包括： ● Chrome浏览器：支持最新的3个稳定版本。 ● Firefox浏览器：支持最新的3个稳定版本。 ● Microsoft Edge浏览器：Win10默认浏览器，支持最新的3个稳定版本。 推荐使用Chrome、Firefox浏览器，效果会更好。
分辨率	分辨率大小	推荐使用1280*1024以上。

二进制成分分析使用限制

表 5-2 二进制成分分析使用限制说明

指标类别	指标项	限制说明
任务管理	语言类型	支持C/C++/Java/Go/JavaScript/Python/Rust/Swift/C#/PHP等语言开源软件已知漏洞检测。
	扫描包格式	支持上传的文件格式有.7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war等，以及支持上传Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot等固件。
	扫描包上传大小限制	5GB。

源码成分分析使用限制

表 5-3 源码成分分析使用限制说明

指标类别	指标项	限制说明
任务管理	语言类型	支持C/C++、Java、Python、JS、Go、TypeScript、PHP、C#等语言开源软件已知漏洞检测。
	扫描包格式	支持.zip、.tar.gz格式的文件。
	扫描包上传大小限制	1GB。

6 与其他服务的关系

- 与代码检查服务的关系

  开源治理服务中的代码检查功能由独立的代码检查（CodeArts Check）云服务提供，用户可以通过超链接跳转至代码检查的页面进行使用。当前代码检查是CodeArts云服务下的子服务，用户需开通CodeArts服务方可使用。

- 与漏洞管理服务的关系

  开源治理服务中的主机和Web漏洞扫描功能由独立的漏洞管理（CodeArts Inspector）云服务提供，用户可以通过超链接跳转至漏洞管理服务页面执行相关主机和Web的漏洞扫描。

- 与制品仓库服务的关系

  开源治理服务中的开源软件制品资产管理由制品仓库（CodeArts Artifact）云服务提供，用户可以通过超链接跳转至制品仓库服务页面进行查询。

7 计费说明

开源治理服务（CodeArts Governance）包含多个安全检测原子服务，支持单独购买，按需模式进行计费。

开源治理服务二进制成分分析定价包含以下两种套餐，详细内容请参见表7-1。

表 7-1 版本说明

套餐	主要功能	规格	量纲	目录价
二进制成分分析1次按需套餐包	• 针对Linux软件包、安卓部署包、鸿蒙部署包、Windows安装包、IoT固件包的安全检测。 • 支持开源组件漏洞分析和开源许可证分析能力。 • 支持敏感信息、安全配置、安全编译选项检查。	1次	个	3000元
二进制成分分析20次按需套餐包		20次	个	30000元

开源治理服务源码成分分析定价为包周期套餐，详细内容请参见表7-2。

表 7-2 版本说明

套餐	套餐类型	主要功能	规格	量纲	目录价
源码成分析-专业版	包周期	• 针对源文件片段进行风险扫描。 • 支持Java/Go/Js/Python/C语言。支持漏洞预警。	1个	并发数	30000元/月