

开源治理服务

# 产品介绍

文档版本 01  
发布日期 2024-07-17



版权所有 © 华为云计算技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

## 商标声明



HUAWEI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.....	1
2 功能特性.....	2
3 产品优势.....	3
4 应用场景.....	4
5 约束与限制.....	6
6 与其他服务的关系.....	7
7 计费说明.....	8

# 1 什么是开源治理服务

开源治理服务（CodeArts Governance）是针对软件开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。

# 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，功能特性如下：

- 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。

# 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秘钥等敏感信息检测，发现潜在的安全风险。

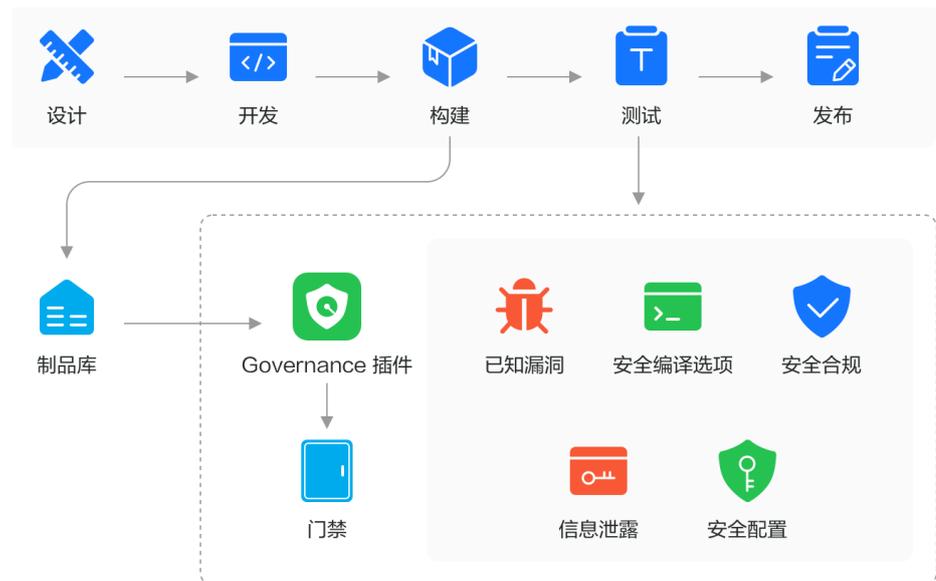
# 4 应用场景

- 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。



# 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： <ul style="list-style-type: none"><li>• Chrome浏览器：支持最新的3个稳定版本。</li><li>• Firefox浏览器：支持最新的3个稳定版本。</li><li>• Microsoft Edge浏览器：Win10默认浏览器，支持最新的3个稳定版本。</li></ul> 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.7z、.arj、.cpio、.phar、.rar、.tar、.xar、.zip、.jar、.apk、.war等格式文件，以及Android OTA Images、Android sparse、Intel HEX、RockChip、U-Boot等固件。
	扫描包上传大小限制	5GB。

# 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。

# 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	<ul style="list-style-type: none"><li>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。</li><li>支持开源组件漏洞分析和开源许可证分析能力。</li><li>支持敏感信息、安全配置、安全编译选项检查。</li></ul>	1次	个	3000元
二进制成分分析20次按需套餐包		20次	个	30000元