CodeArts Governance

Service Overview

Issue 01

Date 2025-06-30

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 What Is CodeArts Governance?

By incorporating Huawei's experience, CodeArts Governance helps enterprises use open-source software with enhanced security and efficiency. It analyzes metadata and components to eliminate risks in compliance, networks, and supply.

Capability

- Binary component analysis

  CodeArts Governance decompresses and scans your binary software or firmware packages. It performs component feature analysis and static analysis based on the bill of materials (BOM) to identify possible rule violations, and generates a report accordingly.

2 Features

CodeArts Governance safeguards your open-source software usage by preventing vulnerabilities from end to end. Specifically, it has the following features.

- Binary component analysis
  - Comprehensive scan

    CodeArts Governance analyzes software and firmware packages to identify software vulnerabilities against security rules. It also evaluates license compliance, password strength (including weak or hard-coded passwords), security configurations, and secure complier options.
  - Wide applicability

    CodeArts Governance can scan desktop applications that run on Windows and Linux, mobile applications that run on Android Application Package (APK), iOS App Store Package (IPA), and HarmonyOS Ability Package (HAP), as well as embedded system firmware.
  - Professional analysis and guide

    Risk information is presented based on thorough analysis from different perspectives, along with relevant troubleshooting suggestions.

3 Advantages

- Binary component analysis
  - Source code-free and harmless detection

    You only need to upload the product release package or firmware, without the need to build the running environment or run programs.
  - Serving multiple languages, file formats, and architectures

    Artifacts built using different languages or architectures can all be scanned.
  - Prevention of sensitive data breach

    Potential risks in security configurations, passwords, and secret keys can all be identified.

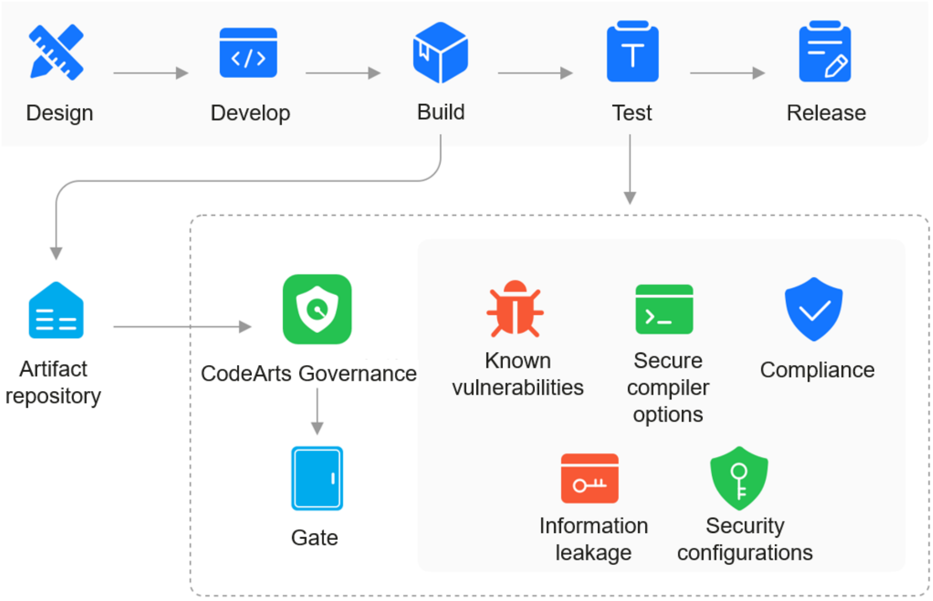
4 Application Scenarios

- Binary component analysis

  This function is opened as APIs for you to scan open-source and third-party software.

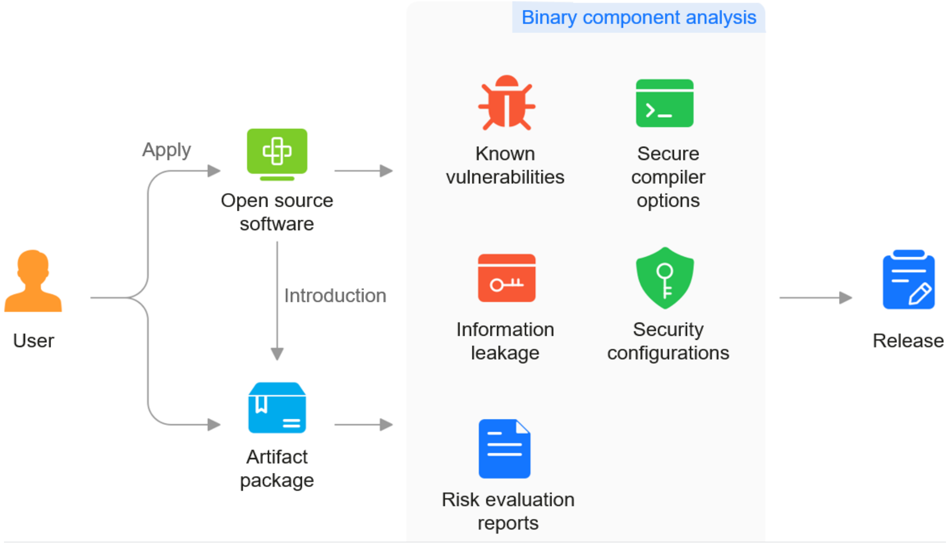
  – Usage risk evaluation

    You can call APIs in your continuous integration and continuous delivery (CI/CD) process to implement security in DevSecOps.



  – Assessment before introduction

    You can efficiently assess the risks using the APIs or on the web pages before you introduce software.


Binary component analysis
Apply
Open source software
Introduction
User
Artifact package
Known vulnerabilities
Secure compiler options
Information leakage
Security configurations
Risk evaluation reports
Release

5 Security

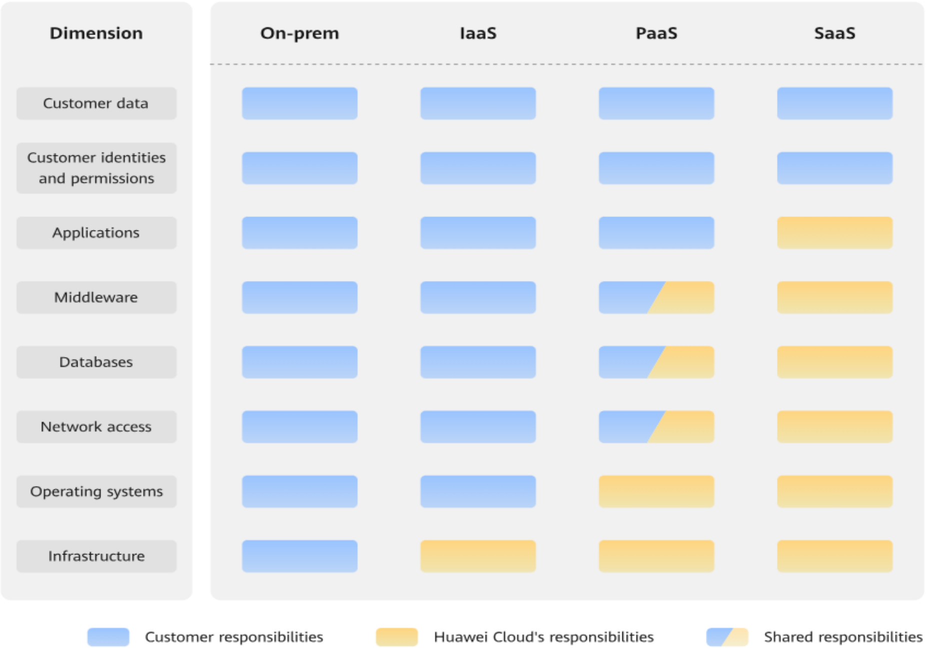
5.1 Shared Responsibilities

Huawei guarantees that its commitment to cyber security will never be outweighed by the consideration of commercial interests. To cope with emerging cloud security challenges and pervasive cloud security threats and attacks, Huawei Cloud builds a comprehensive cloud service security assurance system for different regions and industries based on Huawei's unique software and hardware advantages, laws, regulations, industry standards, and security ecosystem.

Unlike traditional on-premises data centers, cloud computing separates operators from users. This approach not only enhances flexibility and control for users but also greatly reduces their operational workload. For this reason, cloud security cannot be fully ensured by one party. Cloud security requires joint efforts of Huawei Cloud and you, as shown in **Figure 5-1**.

- **Huawei Cloud**: Huawei Cloud is responsible for infrastructure security, including security and compliance, regardless of cloud service categories. The infrastructure consists of physical data centers, which house compute, storage, and network resources, virtualization platforms, and cloud services Huawei Cloud provides for you. In PaaS and SaaS scenarios, Huawei Cloud is responsible for security settings, vulnerability remediation, security controls, and detecting any intrusions into the network where your services or Huawei Cloud components are deployed.
- **Customer**: As our customer, your ownership of and control over your data assets will not be transferred under any cloud service category. Without your explicit authorization, Huawei Cloud will not use or monetize your data, but you are responsible for protecting your data and managing identities and access. This includes ensuring the legal compliance of your data on the cloud, using secure credentials (such as strong passwords and multi-factor authentication), and properly managing those credentials, as well as monitoring and managing content security, looking out for abnormal account behavior, and responding to it, when discovered, in a timely manner.

Figure 5-1 Huawei Cloud shared security responsibility model



Dimension	On-prem	IaaS	PaaS	SaaS
Customer data	🟦	🟦	🟦	🟦
Customer identities and permissions	🟦	🟦	🟦	🟦
Applications	🟦	🟦	🟦	🟨
Middleware	🟦	🟦	🟦🟨	🟨
Databases	🟦	🟦	🟦🟨	🟨
Network access	🟦	🟦	🟦🟨	🟨
Operating systems	🟦	🟦	🟨	🟨
Infrastructure	🟦	🟨	🟨	🟨

🟦 Customer responsibilities 🟨 Huawei Cloud's responsibilities 🟦🟨 Shared responsibilities

Cloud security responsibilities are determined by control, visibility, and availability. When you migrate services to the cloud, assets, such as devices, hardware, software, media, VMs, OSs, and data, are controlled by both you and Huawei Cloud. This means that your responsibilities depend on the cloud services you select. As shown in **Figure 5-1**, customers can select different cloud service types (such as IaaS, PaaS, and SaaS services) based on their service requirements. As control over components varies across different cloud service categories, the responsibilities are shared differently.

- In on-premises scenarios, customers have full control over assets such as hardware, software, and data, so tenants are responsible for the security of all components.
- In IaaS scenarios, customers have control over all components except the underlying infrastructure. So, customers are responsible for securing these components. This includes ensuring the legal compliance of the applications, maintaining development and design security, and managing vulnerability remediation, configuration security, and security controls for related components such as middleware, databases, and operating systems.
- In PaaS scenarios, customers are responsible for the applications they deploy, as well as the security settings and policies of the middleware, database, and network access under their control.
- In SaaS scenarios, customers have control over their content, accounts, and permissions. They need to protect their content, and properly configure and protect their accounts and permissions in compliance with laws and regulations.

5.2 Identity and Access Management

Identity Authentication

You can access CodeArts Governance through its UI, APIs, and SDKs. Regardless of the access mode, your requests are sent through RESTful APIs provided by CodeArts Governance.

CodeArts Governance APIs can be accessed only after requests are authenticated.

CodeArts Governance supports two authentication modes:

- Token: Requests are authenticated using tokens. By default, token authentication is required to access the CodeArts Governance console.
- AK/SK: Requests are encrypted using an AK (Access Key ID)/SK (Secret Access Key). Authentication using AK/SK is recommended because it provides higher security than authentication using tokens.

Access Control

CodeArts Governance works with Identity and Access Management (IAM). IAM is used to validate tenant identity and control access to CodeArts Governance.

IAM is a basic service provided by Huawei Cloud for permission management. It helps CodeArts Governance control access permissions.

With IAM, you can add users to a user group and configure policies to control their access to CodeArts Governance resources. You can allow or deny access to a specific CodeArts Governance resource in a fine-grained manner.

5.3 Data Protection Controls

CodeArts Governance uses multiple methods to secure data.

Method	Description
Transmission encryption (HTTPS)	CodeArts Governance uses HTTPS to secure data transmission.
Personal data protection	The service controls access to data and records operation logs to prevent data leakage.
Privacy data protection	CodeArts Governance does not consume or store sensitive user data.
Data destruction	When you delete service data or deregister your account: ● Non-key data is physically deleted in real time. ● Key data will be marked as soft deleted and then physically deleted 15 days later.

5.4 Auditing and Logging

Auditing

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

After you enable CTS and configure a tracker, CTS can record management and data traces of CodeArts Governance for auditing.

For details about how to enable and configure CTS, see **CTS Getting Started**.

For details about CodeArts Governance operations that can be tracked by CTS, see **CodeArts Governance Operations That Can be Recorded by CTS**.

Logs

Log Tank Service (LTS) provides one-stop log collection, log search in seconds, massive log storage, log structuring and transfer. Graphical application O&M, visual analysis of network logs, and operation analysis make organization tracking easier.

For analysis, CodeArts Governance records system running logs to LTS in real time and stores the logs for three days.

5.5 Service Resilience

CodeArts Governance uses various setups to quickly recover services from faults, such as deploying multi-active, stateless applications across AZs, and implementing disaster recovery of data between AZs.

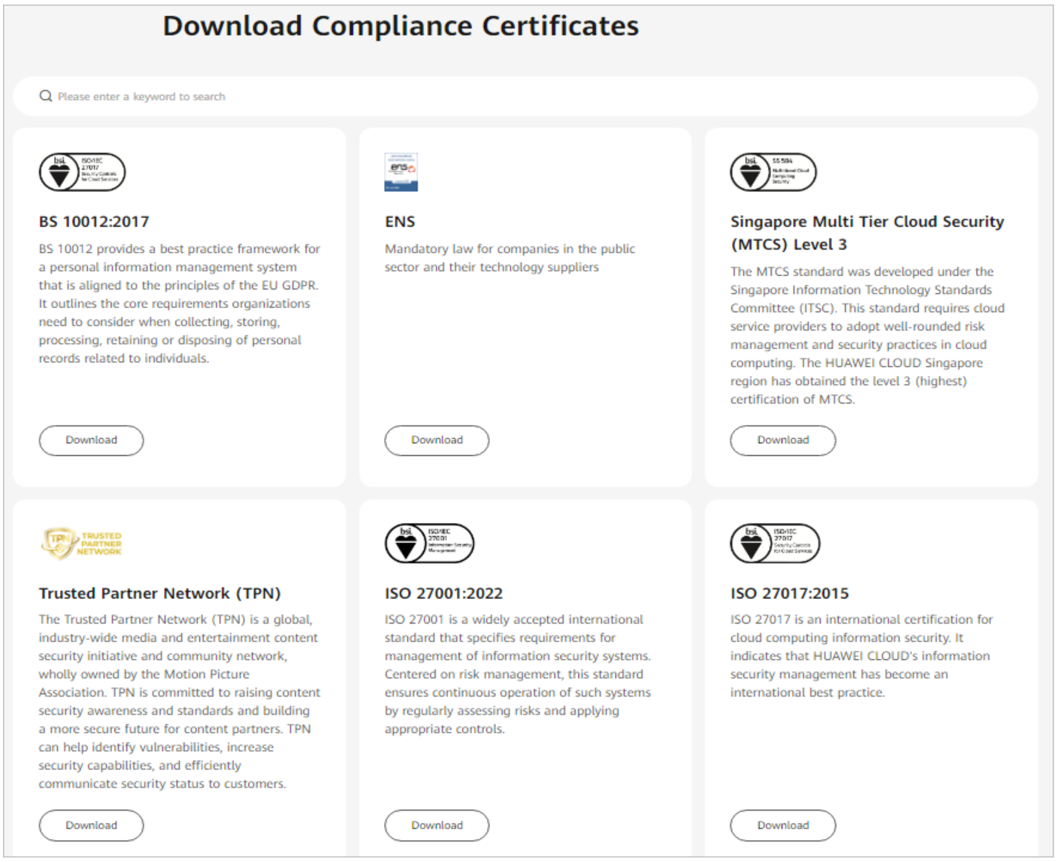
These technical solutions improve service durability and reliability.

5.6 Certificates

Compliance Certificates

Huawei Cloud services and platforms have obtained various security and compliance certifications from authoritative organizations, such as International Organization for Standardization (ISO). You can **download** them from the console.

Figure 5-2 Downloading compliance certificates



Download Compliance Certificates

Please enter a keyword to search

BS 10012:2017

BS 10012 provides a best practice framework for a personal information management system that is aligned to the principles of the EU GDPR. It outlines the core requirements organizations need to consider when collecting, storing, processing, retaining or disposing of personal records related to individuals.

Download

ENS

Mandatory law for companies in the public sector and their technology suppliers

Download

Singapore Multi Tier Cloud Security (MTCS) Level 3

The MTCS standard was developed under the Singapore Information Technology Standards Committee (ITSC). This standard requires cloud service providers to adopt well-rounded risk management and security practices in cloud computing. The HUAWEI CLOUD Singapore region has obtained the level 3 (highest) certification of MTCS.

Download

Trusted Partner Network (TPN)

The Trusted Partner Network (TPN) is a global, industry-wide media and entertainment content security initiative and community network, wholly owned by the Motion Picture Association. TPN is committed to raising content security awareness and standards and building a more secure future for content partners. TPN can help identify vulnerabilities, increase security capabilities, and efficiently communicate security status to customers.

Download

ISO 27001:2022

ISO 27001 is a widely accepted international standard that specifies requirements for management of information security systems. Centered on risk management, this standard ensures continuous operation of such systems by regularly assessing risks and applying appropriate controls.

Download

ISO 27017:2015

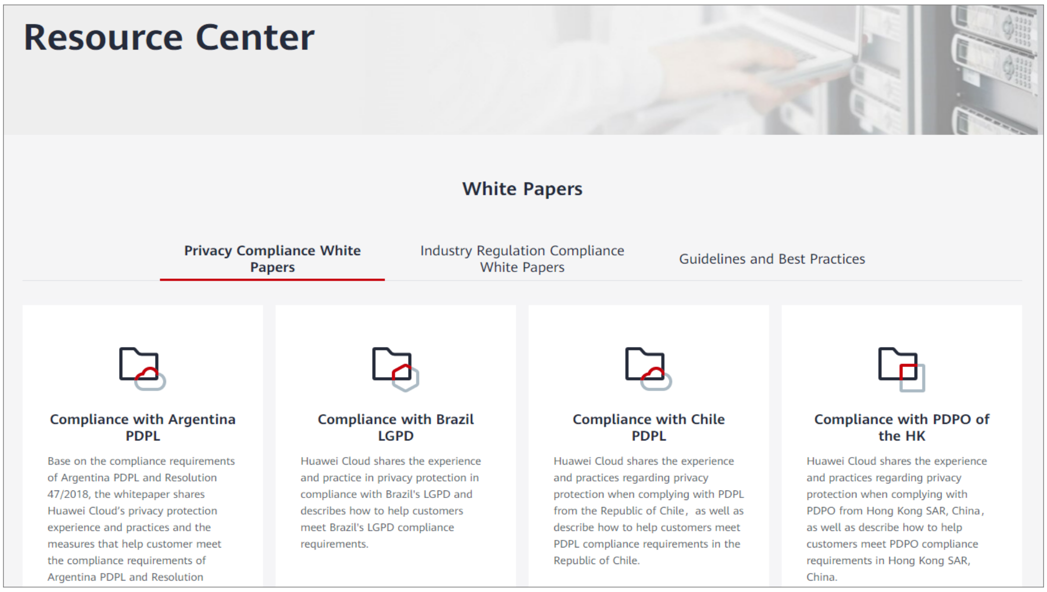
ISO 27017 is an international certification for cloud computing information security. It indicates that HUAWEI CLOUD's information security management has become an international best practice.

Download

Resource Center

Huawei Cloud also provides the following resources to help users meet compliance requirements. For details, see **Resource Center**.

Figure 5-3 Resource center



Resource Center

White Papers

Privacy Compliance White Papers | Industry Regulation Compliance White Papers | Guidelines and Best Practices

Compliance with Argentina PDPL

Base on the compliance requirements of Argentina PDPL and Resolution 47/2018, the whitepaper shares Huawei Cloud's privacy protection experience and practices and the measures that help customer meet the compliance requirements of Argentina PDPL and Resolution

Compliance with Brazil LGPD

Huawei Cloud shares the experience and practice in privacy protection in compliance with Brazil's LGPD and describes how to help customers meet Brazil's LGPD compliance requirements.

Compliance with Chile PDPL

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPL from the Republic of Chile，as well as describe how to help customers meet PDPL compliance requirements in the Republic of Chile.

Compliance with PDPO of the HK

Huawei Cloud shares the experience and practices regarding privacy protection when complying with PDPO from Hong Kong SAR, China，as well as describe how to help customers meet PDPO compliance requirements in Hong Kong SAR, China.

6 Permissions Management

If you need to grant your enterprise personnel permission to access your CodeArts Governance resources, use Identity and Access Management (IAM). IAM provides identity authentication, fine-grained permissions management, and access control. IAM helps you secure access to your cloud resources.

With IAM, you can create IAM users and grant them permissions to access only specific resources. For example, some software developers in your enterprise need to use CodeArts Governance resources but must not delete them or perform any high-risk operations. To achieve this result, you can create IAM users for the software developers and grant them only the permissions required for using CodeArts Governance resources.

If your cloud account does not require individual IAM users for permissions management, you can skip this section.

IAM is a free service. You only pay for the resources in your account. For details, see **IAM Service Overview**.

CodeArts Governance Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and then attach policies or roles to these groups. After that, users can perform operations on cloud services.

CodeArts Governance is a project-level service deployed and accessed in specific physical regions. To assign CodeArts Governance permissions to a user group, specify the scope as region-specific projects and select projects for the permissions to take effect. If **All projects** is selected, the permissions will take effect for the user group in all region-specific projects. When users access CodeArts Governance, they need to switch to a region where they have been authorized to use this service.

You can grant users permissions by using roles and policies.

- Roles: A type of coarse-grained authorization mechanism first provided by IAM to define permissions related to user responsibilities. Only a limited number of service-level roles are available for authorization. When you grant permissions using roles, you also need to attach any existing role dependencies. Roles are not ideal for fine-grained authorization and least privilege access.

- Policies: A type of fine-grained authorization mechanism lately provided by IAM to define permissions required to perform operations on specific cloud resources under certain conditions. This mechanism allows for more flexible authorization. Policies allow you to meet requirements for more secure access control. For example, you can grant ECS users only the permissions for managing a certain type of ECSs. Most policies define permissions based on APIs.

Table 6-1 lists all the system-defined permissions for CodeArts Governance.

Table 6-1 System-defined permissions

Role/Policy	Description	Type	Dependency
CodeArtsInspector Administrator	Full permissions for CodeArts Governance	System-defined role	None.
Tenant Administrator	Full permissions for CodeArts Governance	System-defined role	None.

7 Notes and Constraints

This section describes the restrictions on using CodeArts Governance.

Console

Table 7-1 Restrictions on the console

Category	Item	Description
Browser	Type	CodeArts Governance supports: - Chrome: the latest three versions - Firefox: the latest two versions - Edge: default browser of Windows 10 Chrome and Firefox are recommended.
Resolution	Resolution	1280 x 1024 or higher

Binary Component Analysis

Table 7-2 Restrictions of the binary component analysis function

Category	Item	Description
Job management	Language	C, C++, Java, Go, JavaScript, Python, Rust, Swift, C#, and PHP
	Package format	Files in .7z, .arj, .cpio, .phar, .rar, .tar, .xar, .zip, .jar, .apk, .war, .rpm, and .deb formats and firmware such as Android OTA Images, Android sparse, Intel HEX, RockChip, and U-Boot can be uploaded.
	Package size	- Professional edition: 5 GB - Free edition: 300 MB

8 Specifications

The binary component analysis function of CodeArts Governance provides two package editions: free edition and professional edition. The professional edition can be billed on a pay-per-use or yearly/monthly basis. A yearly/monthly package provides a higher discount than the pay-per-use mode does, and is recommended for long-term users.

Table 8-1 Version specifications

Edition	Feature
Free	● Each account has five free scans. ● A file up to 300 MB can be scanned each time. ● All risk items are covered. ● No report will be generated for download. ● Only the top 10 components with the most vulnerabilities are displayed.
Professional	● You can check complete scanning results and export professional reports. ● A file up to 5 GB can be scanned each time.

9 Related Services

CodeArts Artifact

CodeArts Artifact helps software development enterprises manage the software release process in a standardized, visualized, and traceable way.

There is an entry on the CodeArts Governance console for you to access CodeArts Artifact easily.

Cloud Trace Service (CTS)

Cloud Trace Service (CTS) records operations on cloud resources in your account. You can use the logs to perform security analysis, track resource changes, audit compliance, and locate faults.

With CTS, you can record operations related to CodeArts Governance for future query, audit, and backtrack.

10 Basic Concepts

Open-Source Software

Open-source software is software that is released under a license, allowing groups and individuals to use, copy, distribute, modify, and release their own versions.

Open-Source License

Open-source software is accompanied by a license that grants permissions, rights, and obligations, while also setting limitations. All behaviors related to the open-source software should adhere to the license. Common licenses include the BSD license, Apache license, Eclipse Public License (EPL), and GNU General Public License (GPL).

Reports

CodeArts Governance generates a report after the binary component analysis is complete. The report may involve the following information that requires special attention.

- **Open-Source Software Vulnerabilities**: There are vulnerabilities in the open-source software list or version. Confirm whether to fix them, and then, install patches or upgrade the software as required.
- **Key and Info Leakage**: There may be sensitive information that is prone to breaches, such as weak passwords, hard-coded secret keys, and IP addresses. Confirm whether to fix it.
- **Secure Compiler Options**: The building or compilation scripts may have risks. Add secure compiler options for specific languages like C, C++, and Go to prevent attacks like buffer overflow.
- **Security Configurations**: The credentials and authentications may involve risks. Rectify the issues according to the reports.
- **Open-Source Software Licenses**: Licenses used in your artifact may be incompatible with each other. Using such licenses may violate regulations. Fix this issue if needed.