ALIBABA CLOUD

阿里云

云安全中心（态势感知）

产品简介

文档版本：20210115

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
Courier字体	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.什么是云安全中心

云安全中心是一个实时识别、分析、预警安全威胁的统一安全管理系统，通过防勒索、防病毒、防篡改、镜像安全扫描、合规检查等安全能力，帮助您实现威胁检测、响应、溯源的自动化安全运营闭环，保护云上资产和本地服务器并满足监管合规要求。

云安全中心可帮助您收集并呈现10余种类型的日志和云上资产指纹，并结合网络实体威胁情报进行安全态势分析，扩大安全可见性。

云安全中心提供基础版、防病毒版、高级版和企业版多个版本供您选择。各版本详细信息，请参见功能特性。以下是各版本的介绍。

- **基础版**

  免费为您提供基础的**安全加固**能力，可检测服务器异常登录、DDoS攻击、服务器主流类型的漏洞以及云产品安全配置。您在购买ECS实例时选择**安全加固**即可开通基础版。

  云安全支持7天免费试用旗舰版功能。只有购买了ECS实例并且以前未试用过云安全中心的用户，才可以免费试用旗舰版的功能。如果您已具有试用资格，在登录云安全中心控制台后，会有弹窗提示您已获得云安全中心旗舰版7天免费试用资格。

- **防病毒版**

  采用包年包月的计费方式，提供安全告警、病毒防御等服务。

- **高级版**

  采用包年包月的计费方式，提供安全告警、病毒防御、漏洞检测及修复、安全报告等服务。

- **企业版**

  采用包年包月的计费方式，提供安全告警、病毒防御、漏洞检测及修复、基线检查、资产指纹、攻击分析等全面的安全服务。

- **旗舰版**

  采用包年包月的计费方式，提供镜像安全扫描、容器K8s威胁检测、天机镜、安全告警、病毒防御、漏洞检测及修复、基线检查、资产指纹、攻击分析等全面的安全服务。

云安全中心已通过ISO 9001、ISO 20000、ISO 22301、ISO 27001、ISO 27017、ISO 27018、ISO 29151、ISO 27701、BS1 0012、CSA STAR、PCI DSS等多项国际权威认证。

参考文档

云安全中心已发布2019年上半年云上企业安全指南。阿里云基于对云安全中心检测到的威胁情况进行了详细地分析，为您的云上安全建设提供建议，帮助您打造更健全的云上安全体系。详细内容请参见云上企业安全指南。

2.产品优势

云安全中心通过安全告警实时抵御恶意入侵，使用漏洞和基线配置检测消除系统弱点、预防恶意攻击，提供安全态势分析和安全可视化界面、满足事后追溯和分析需求，帮助您建立完整的安全体系。

云安全中心具有以下优势：

- **安全事件告警和检索**

  实时监控安全事件并提供处理建议，对告警事件进行分析和检索，抵御恶意入侵。

- **漏洞和基线配置检测**

  自动检测并呈现服务器资产的漏洞和风险配置，提供修复建议，帮助您巩固系统安全。

- **安全风险量化和预测**

  通过机器学习，量化分析威胁，预测潜在的安全风险。

- **安全可视化界面**

  提供安全可视化界面，帮助您全面并实时地感知安全问题。

- **支持病毒云查杀**

  病毒云查杀为您提供全面和实时的病毒检测和防护服务。从数据的采集、脱敏、识别、分析、隔离到恢复已形成安全闭环，同时支持您在云安全中心控制台中对病毒云查杀结果进行隔离和恢复处理。详细内容，请参见病毒云查杀。

- **符合多项国际安全认证标准**

  云安全中心已通过ISO 9001、ISO 20000、ISO 22301、ISO 27001、ISO 27017、ISO 27018、ISO 29151、ISO 27701、BS1 0012、CSA STAR、PCI DSS等多项国际权威认证。

3.功能特性

云安全中心提供基础版、防病毒版、高级版、企业版和旗舰版多个版本，本文介绍各版本的功能差异。

- **基础版**

  免费为您提供基础的**安全加固**能力，可检测服务器异常登录、DDoS攻击、服务器主流类型的漏洞以及云产品安全配置。您在购买ECS实例时选择**安全加固**即可开通基础版。

  云安全支持7天免费试用旗舰版功能。只有购买了ECS实例并且以前未试用过云安全中心的用户，才可以免费试用旗舰版的功能。如果您已具有试用资格，在登录云安全中心控制台后，会有弹窗提示您已获得云安全中心旗舰版7天免费试用资格。

- **防病毒版**

  采用包年包月的计费方式，提供安全告警、病毒防御等服务。

- **高级版**

  采用包年包月的计费方式，提供安全告警、病毒防御、漏洞检测及修复、安全报告等服务。

- **企业版**

  采用包年包月的计费方式，提供安全告警、病毒防御、漏洞检测及修复、基线检查、资产指纹、攻击分析等全面的安全服务。

- **旗舰版**

  采用包年包月的计费方式，提供镜像安全扫描、容器K8s威胁检测、天机镜、安全告警、病毒防御、漏洞检测及修复、基线检查、资产指纹、攻击分析等全面的安全服务。

> **说明** 以下是介绍云安全中心不同版本的功能差异时用到的标识说明：
>
> - X：表示云安全中心不支持该特性。
> - √：表示云安全中心支持该特性。
> - 增值：表示您在购买云安全中心服务时需要额外选择的特性，或购买云安全中心后需要使用升级功能单独购买的特性。
> - 需申请：表示您需要向云安全中心提交开通申请并经过审批才能使用的特性。

版本定价对比

计费项		基础版	基础杀毒版	高级版	企业版	旗舰版	仅采购增值服务
基础费用		免费	30元/台/月	60元/台/月	150元/台/月	19.5元/核/月	免费
	网页防篡改	不支持	980元/台/月	980元/台/月	980元/台/月	980元/台/月	980元/台/月
	防勒索病毒	不支持	0.3元/GB/月	0.3元/GB/月	0.3元/GB/月	0.3元/GB/月	0.3元/GB/月
	日志分析	不支持	500元/TB/月	500元/TB/月	500元/TB/月	500元/TB/月	不支持

增值功能费用项		基础版	基础杀毒版	高级版	企业版	旗舰版	仅采购增值服务
	容器镜像安全扫描	不支持	不支持	不支持	0.5元/镜像	0.5元/镜像	0.5元/镜像
	安全大屏	不支持	8000元/月	8000元/月	8000元/月	8000元/月	不支持
	产品专家服务	不支持	2000元/阿里云账户/月	2000元/阿里云账户/月	2000元/阿里云账户/月	2000元/阿里云账户/月	2000元/阿里云账户/月
购买时长		不限时间	支持按月购买（保有服务器台数大于10台时）	支持按月购买（保有服务器台数大于10台时）	支持按月购买（保有服务器台数大于10台时）	支持按月购买	支持按月购买

容器安全

注意 云安全中心仅支持对以下阿里云服务中的容器集群或容器实例进行安全检测：

- 容器服务Kubernetes版：支持所有模板创建的Kubernetes集群的安全检测。
- 容器镜像服务：仅支持对企业版实例进行安全检测，不支持对默认实例进行安全检测。

功能模块	功能详情	基础版、防病毒版、高级版	企业版	旗舰版	相关文档
	为容器Kubernetes版提供运行时刻安全监控和告警，包括在容器中或在主机层面发生的病毒和恶意程序攻击、容器内部的入侵行为、容器逃逸和高风险操作预警等主要的容器侧攻击行为。	X	X	√	使用运行时刻安全监控

容器运行时威胁检测功能模块	功能详情	基础版、防病毒版、高级版	企业版	旗舰版	相关文档
	支持容器风险项检测和告警。检测范围如下： • **恶意镜像启动** 对DockerHub等公开的镜像源进行实时监控，当含有后门或者挖矿行为的恶意镜像被安装到服务器时及时进行预警。 • **病毒和恶意程序** 检测容器中是否存在病毒、木马、挖矿程序、恶意脚本以及Webshell。 • **容器内部入侵行为** 检测是否存在黑客通过应用层漏洞成功入侵容器，以及在容器中进行后续渗透利用和横向传播的行为。 • **容器逃逸** 检测是否存在黑客利用容器配置不当或者Docker、操作系统自身漏洞进行的容器逃逸攻击。 • **高风险操作预警** 检测是否存在宿主机敏感目录挂载、Docker或者K8s API泄露、以及可疑的特权容器启动行为，避免攻击者轻易对这些风险点发起攻击。	X	X	√	查看和处理告警事件
容器K8s威胁检测	实时检测正在运行的容器集群安全状态，帮助您及时发现容器中的安全隐患和黑客入侵行为。支持以下检测项： • K8s API Server执行异常指令 • Pod异常目录挂载 • K8s Service Account横向移动 • 恶意镜像Pod启动	X	X	√	容器K8s威胁检测
镜像签名	支持对容器镜像的可信签名，确保只允许部署您认可的容器镜像，防止未经签名授权的镜像启动，从根本上帮助您提升资产的安全性。目前，仅部署在中国香港的Kubernetes集群支持镜像签名。	X	X	√	容器签名

功能模块	功能详情	基础版、防病毒版、高级版	企业版	旗舰版	相关文档
镜像安全扫描	支持检测以下类型的镜像漏洞或恶意样本： • **镜像系统漏洞** 提供镜像系统漏洞扫描功能，为您提供安全可信的镜像。 • **镜像应用漏洞** 提供镜像应用漏洞扫描功能，为您扫描容器相关中间件上的漏洞并提供修复建议，为您创造安全的镜像运行环境。 • **镜像恶意样本** 提供容器恶意样本的检测能力，为您展示资产中存在的容器安全威胁，大幅降低您使用容器的安全风险。 **说明** 目前云安全中心仅支持检测容器镜像漏洞和恶意样本，暂时不提供一键修复的功能。如果您的容器镜像中检测到了漏洞，请您根据云安全中心提供的漏洞修复方案或恶意样本路径信息加固镜像。	X	增值	增值	镜像安全扫描概述
容器配置安全	针对容器的配置提供安全检测和告警，基于阿里云容器最佳安全实践对Kubernetes Master和Node节点针对容器基线配置提供风险检查。检测范围如下： • **阿里云标准-Docker安全基线检查** 基于阿里云最佳实践安全实践的Docker基线标准，从Docker的安全审计、服务配置和文件权限等方面进行风险排查和及时预警。 • **阿里云标准-Kubernetes-Master安全基线检查** 基于阿里云容器最佳安全实践的Kubernetes Master节点的基线检查。 • **阿里云标准-Kubernetes-Node安全基线检查** 基于阿里云容器最佳安全实践的Kubernetes Node节点的基线检查。	X	X	√	基线检查概述
容器安全状态可视化	支持实时检测容器的安全状态，并在资产中心页面展示。	√	√	√	查看容器安全状态

试用报告

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
试用报告	在免费试用云安全中心旗舰版后生成试用报告。	√	X	X	X	X	总览

安全评分

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
安全评分	云安全中心总览页面根据您资产整体的安全状态展示当前的安全评分。安全评分越高说明您系统的安全隐患越少。	√	√	√	√	√	• 安全评分 • 提高安全评分最佳实践 • 安全评分FAQ

资产中心

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
服务器	资产中心提供了所有服务器的安全状态相关信息，例如服务器的防护状态、分组、地域、专有网络VPC等统计信息。	√	√	√	√	√	查看服务器安全状态
容器	资产中心提供了所有容器组、容器、镜像的安全状态相关信息，主要包括容器组、容器、镜像的统计数据和风险状态信息。	X	X	X	√	√	查看容器安全状态
网站	资产中心提供了所有网站的安全状态相关信息，主要包括网站根域名、子域名及其资产的风险状态和告警数量统计。	√	√	√	√	√	查看网站安全状态
云产品	资产中心提供了云产品安全状态的相关信息，包括存在风险云产品信息及云产品分类（负载均衡、NAT网关、RDS数据库和MongoDB数据库）统计等。	√	√	√	√	√	查看云产品安全状态

资产暴露分析

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
资产暴露分析	支持自动分析您的ECS服务器在互联网上的暴露情况，可视化呈现ECS与互联网的通信链路，并集中展示您暴露在公网的ECS的漏洞信息，帮助您快速定位您资产在互联网上的异常暴露情况并提供相应漏洞的修复建议。	X	X	X	√	√	资产暴露分析

病毒防御

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
病毒查杀	云安全中心安全专家团队通过对海量病毒样本、持久化、攻击方式的自动化分析，正式推出阿里云机器学习病毒查杀引擎，实现一键式病毒查杀。	X	√	√	√	√	病毒防御概述
防病毒	病毒自动查杀功能可隔离主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒。	X	√	√			
防勒索	支持使用诱饵捕获勒索病毒，支持文件的备份还原。	X	增值	增值	增值	增值	防勒索概述

漏洞修复

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
Linux软件漏洞	**Linux软件漏洞检测**对标CVE官方漏洞库，采用OVAL匹配引擎进行软件版本比对，对当前使用的软件版本中存在的漏洞进行告警。 **说明** 基础版只支持漏洞自动检测，不支持漏洞**一键扫描**和漏洞修复操作。如需使用云安全中心手动**一键扫描**资产是否存在漏洞，需要升级到防病毒版、高级版、企业版和旗舰版。如需使用云安全中心对漏洞进行修复，需要升级到高级版、企业版或旗舰版。	√	√	√	√	√	Linux软件漏洞
	漏洞修复支持系统漏洞一键修复，同时自动化快照能力实现一键回滚，更安全地修复漏洞。	X	X	√	√	√	

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
Windows系统漏洞	**Windows系统漏洞检测**同步微软官网补丁源，对高危及有影响的漏洞进行检测和提醒。 **说明** 基础版只支持漏洞自动检测，不支持漏洞**一键扫描**和漏洞修复操作。如需使用云安全中心手动**一键扫描**资产是否存在漏洞，需要升级到防病毒版、高级版、企业版和旗舰版。如需使用云安全中心对漏洞进行修复，需要升级到高级版、企业版或旗舰版。	√	√	√	√	√	Windows系统漏洞
	漏洞修复自动化识别漏洞修复所需的前置补丁包，解决服务器因无前置补丁而无法修复漏洞的问题，实现您一键修复Windows漏洞。对需要重启系统修复的漏洞会进行提醒，提升修复Windows系统漏洞的效率。	X	X	√	√	√	
Web-CMS漏洞	**Web-CMS漏洞检测**监控网站目录，识别通用建站软件，通过漏洞文件比对方式检测建站软件中的漏洞。 **说明** 基础版只支持漏洞自动检测，不支持漏洞**一键扫描**和漏洞修复操作。如需使用云安全中心手动**一键扫描**资产是否存在漏洞，需要升级到防病毒版、高级版、企业版和旗舰版。如需使用云安全中心对漏洞进行修复，需要升级到高级版、企业版或旗舰版。	√	√	√	√	√	Web-CMS漏洞
	漏洞修复自研漏洞补丁，支持一键修复，通过文件替换、修改等方式从源代码级别修复漏洞。	X	X	√	√	√	
应急漏洞	临时提供针对网络上突然出现的紧急漏洞的检测服务。应急漏洞不支持一键修复，您可以根据提供的修复建议，手动修复服务器上的应急漏洞。	√	√	√	√	√	应急漏洞
应用漏洞	提供系统服务弱口令、系统服务和应用服务的漏洞检测服务。 **说明** 应用漏洞为企业版和旗舰版功能，基础版、防病毒版和高级版不支持。如需使用云安全中心检测您的资产中是否存在应用漏洞，需要升级到企业版或旗舰版。	X	X	X	√	√	应用漏洞

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
一键扫描	云安全中心支持对您的资产进行手动**一键扫描**、实时检测您的资产中是否存在漏洞。 **说明** 应用漏洞属于企业版和旗舰版功能，基础版、防病毒版和高级版不支持，只有企业版或旗舰版才可使用**一键扫描**功能。各版本**一键扫描**功能支持的漏洞类型详情，请参见一键扫描支持的项目列表。	√（基础版仅支持扫描应急漏洞）	√（防病毒版不支持应用漏洞）	√（高级版不支持应用漏洞）	√	√	一键扫描漏洞
需紧急修复的漏洞	云安全中心支持修复紧急漏洞，提供需紧急修复的漏洞聚合页面，帮助您快速查看和修复所有高紧急程度的漏洞。	X	X	√	√	√	漏洞修复概述
YUM/APT源配置	漏洞管理设置支持选择**YUM/APT源配置**，在修复Linux软件漏洞时自动使用阿里云提供的YUM或APT源，帮助您有效提高漏洞修复的成功率。	X	X	√	√	√	漏洞管理设置
扫描方式	漏洞管理支持设置扫描方式，您可以通过选择**真实风险模式**或**全面规则扫描模式**，更灵活地进行漏洞扫描。	√	√	√	√	√	漏洞管理设置

基线检查

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
服务器基线检查	**服务器基线检查**通过任务下发模式，对服务器进行安全配置扫描，对不符合标准的项目进行告警提示。 支持自定义检测策略，设置检测项目、检测周期、应用的服务器组等。暂不支持自定义检测脚本。 支持自定义弱口令规则。根据您配置的基线策略定期检测您的云产品基线是否存在这些弱口令，命中后提供告警。 支持的检测范围如下： • **高危风险利用** 检测CouchDB、Docker等未授权访问漏洞风险。 • **容器安全** 检测Docker、Kubernetes Master节点、Kubernetes Node存在的风险。 • **等保合规** 检测是否符合等保三级、等保二级和CIS标准的安全基线要求。 • **最佳安全实践** 检测是否满足Linux操作系统、Windows操作系统、Redis等的安全基线要求。 • **弱口令** 检测是否登录MongoDB、FTP、Linux系统等时存在弱口令。	X	X	√（仅支持检测弱口令）	√	√	基线配置检查
基线修复	支持阿里云安全基线、等级保护合规基线一键修复。	X	X	X	√	√	处理风险检查项

云平台配置检查

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
云平台配置检查	检测ECS、RDS等云产品的安全配置是否存在安全隐患。 检测范围如下： • **ECS** 检测安全组端口访问策略是否过于宽松。 • **SLB** 检测是否转发不必要的端口至公网，增加系统受攻击风险。 • **RDS** 检测数据库是否公开在外网，以及是否配置访问白名单。 • **Actiontrail** 检测是否开启了操作日志审计，便于日志回溯。 • **MFA** 检测是否开启了双因素认证登录，防止阿里云账号被破解。 • **其他** 检测SLB白名单、RDS加密通信等。	X	X	√	√	√	云平台配置检查概述

安全告警

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
进程异常行为	通过云上真实的攻防场景对入侵链路还原，建立进程行为白名单，对于进程的非法行为、黑客的入侵过程进行告警。 **异常行为检测能力**为数百个进程建立了近千个行为模型，通过比对模型分析异常行为。 检测范围如下： • **反弹Shell** 检测Bash进程执行可疑指令，服务器被远程控制执行任意命令等。 • **数据库异常指令执行** 检测MySQL、PostgreSQL、SQL Server、Redis、Oracle等数据库的异常指令。 • **应用进程非法操作** 检测Java、FTP、Tomcat、Docker容器、Lsass.exe等应用进程的非法操作。 • **系统进程非法行为** 检测Powershell、SSH、RDP、SMBD共享、SCP文件拷贝等系统进程的非法行为。 • **其他可疑进程行为** 检测Vbscript被访问、Host被访问、Crontab被写入、Webshell写入等可疑进程行为。	X	√	√	√	√	
网站后门	支持服务器+网络双重检测机制，检测PHP、ASP、JSP等类型的网站脚本文件。 检测范围如下： • **服务器检测** 实时监控服务器上网站目录文件变化。 • **网络检测** 通过还原后门文件及分析网络协议进行检测。	√（基础版仅支持部分类型Webshell检测）	√	√	√	√	
	Webshell查杀支持在控制台一键隔离检测出来的Webshell文件。已隔离文件可在30天内恢复。	X	√	√	√	√	

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
异常登录	提供基础登录检测功能。 检测范围如下： • **非常用登录地登录** 系统自动记录ECS常用登录地（支持手动添加）。如果在非常用登录地进行登录，则触发告警。 • **暴力破解** 检测ECS在多次尝试登录失败后最终登录成功的情况。这类情形很有可能是密码被暴力破解。	√	√	√	√	√	
	提供高级登录检测功能。 检测范围如下： • **非合法IP登录** 开启后，允许用户配置ECS合法登录IP（例如：堡垒机IP、办公网IP等）。如果使用非指定的IP登录，则触发告警。 • **非合法账号登录** 开启后，允许用户配置ECS合法登录账号。如果使用非合法账号登录，则触发告警。 • **非合法时间登录** 开启后，允许用户配置合法登录时间（例如：工作时间）。如果在非合法登录时间登录，则触发告警。	X	X	√	√	√	

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
敏感文件篡改	实时监控敏感目录及文件，对异常的读取、写入、删除等敏感操作进行告警。 检测范围如下： • **系统文件篡改** 检测Bash、ps命令进程是否被恶意替换，隐藏的非法进程运行等。 • **网站核心文件删除** 检测是否有黑客非法登录服务器，恶意删除网站文件。 • **网站挂马篡改** 检测网站是否被加入恶意代码，造成访问者自动下载木马病毒。 • **其他可疑事件** 检测是否存在Linux、MySQL等被勒索软件篡改登录界面、留下邮箱或比特币钱包地址等情形。	X	√	√	√	√	安全告警

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
恶意进程（云查杀）	定期扫描进程并监控进程启动事件，通过云查杀机制检测恶意病毒和木马进程。支持在控制台一键结束进程和隔离恶意文件。 云查杀病毒库有以下特点： • **更新机制** 病毒库部署在云端，由阿里云统一控制，实时更新，避免因病毒库更新不及时而造成的损失。 • **病毒样本能力** 基本覆盖全种类病毒，在云端集成中国及中国以外地域主流杀毒引擎、阿里云自研沙箱和机器学习引擎等。 检测范围如下： • **勒索病毒** WannaCry、CryptoLocker等加密文件型勒索软件。 • **恶意攻击** 对外DDoS攻击木马、对外恶意扫描木马、垃圾邮件发送木马等。 • **挖矿软件** 占用服务器非法挖掘虚拟货币的资源消耗型软件。 • **傀儡机程序** 中控木马、恶意中控连接、黑客工具等。 • **其他病毒** 蠕虫病毒、Mirai病毒、感染型病毒等。	X	√	√	√	√	

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
异常网络连接	在服务器中和网络层对网络连接进行监控，识别非法的连接行为，并进行告警。 检测范围如下： • **主动外连** 可疑Shell反弹、Bash主动外连等主动外连到可疑IP。 • **恶意攻击** 被种植恶意软件，对外发动SYN-Flood、UDP-Flood、ICMP-Flood等恶意攻击。 • **可疑通信** 检测后门程序通信、可疑Webshell通信行为等。 • **异常TCP发包** 您的服务器上有进程对其他设备发起了疑似扫描行为。	X	√	√	√	√	
其他	检测范围如下： • 云安全中心客户端异常离线。 • DDoS攻击行为。	X	X	√	√	√	
异常账号	基于用户行为分析，对异常账号登录系统进行检测。	X	√	√	√	√	
应用入侵事件	对通过应用入侵的行为进行检测，如：SQLServer。	X	√	√	√	√	
云产品威胁检测	基于用户行为分析，对云产品的异常使用进行检测。例如黑客调用AccessKey异常购买大量ECS服务器进行挖矿等行为。	X	√	√	√	√	
精准防御	自动隔离常见网络病毒，包括主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等。所有支持自动隔离的病毒都经过了阿里云安全专家的测试和验证，确保零误杀。	X	√	√	√	√	
持久化后门	检测服务器中是否存在持久化后门。 当入侵者通过某种手段获取服务器的控制权之后，通过在服务器上放置一些后门（脚本、进程、链接等），来方便后续执行持久化的入侵。常见的持久化后门有Crontab计划任务、自启动任务、替换系统文件等。	X	√	√	√	√	

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
Web应用威胁检测	检测通过Web应用入侵的行为。	X	√	√	√	√	
恶意脚本	检测服务器中是否存在恶意脚本。 恶意脚本分为有文件脚本和无文件脚本。攻击者在获取到服务器权限后，使用脚本作为载体来达到进一步攻击利用的目的。利用方式包括植入挖矿程序、添加系统后门、添加系统账户等操作。恶意脚本的语言包括Bash、Python、Perl、Powershell、Bat、Vbs。	X	√	√	√	√	
威胁情报	提供第三方威胁情报源。	X	增值	增值	增值	增值	
恶意网络行为	通过流量内容、主机行为等日志综合判断是否存在异常的网络行为，包括攻击者通过开放的网络服务入侵服务器，以及服务器沦陷后对外发起的异常网络行为。	X	√	√	√	√	
归档告警数据	提供30前的历史告警数据归档并下载功能。方便您对历史数据进行回溯和审计。	√	√	√	√	√	归档告警数据

攻击分析

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
攻击分析	支持查看系统遭受的Web攻击详情和ECS遭受的暴力破解攻击等攻击信息，溯源出攻击IP和入侵弱点。	X	X	X	√	√	攻击分析

AK泄露检测

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
AK泄露检测	实时监控Github代码托管网站，捕获并判定被公开的源代码（包含企业员工私自上传并不小心公开的源代码）中是否含有阿里云资产的AccessKey信息。	√	√	√	√	√	AK泄露检测

日志分析

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
全量日志分析	基于日志服务功能，提供服务器进程启动、对外网络连接、系统登录、五元组、DNS请求、安全日志和报警日志等原始日志的检索和分析。 **说明** 仅企业版和旗舰版用户支持查看网络日志，防病毒版和高级版用户不支持。防病毒版和高级版用户在云安全中心控制台**日志分析**页面仅能查看安全日志和主机日志。	X	增值	增值	增值	增值	日志分析

资产指纹调查

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
资产指纹	支持实时检测服务器的以下指纹信息： • **端口** 收集和呈现端口监听信息，便于清点开放的端口信息。 • **账号** 收集服务器账号及对应权限信息，可清点特权账号，检测提权行为。 • **进程** 收集和呈现进程快照信息，便于自主清点合法进程，检测异常进程。 • **软件** 清点软件安装信息，在高危漏洞爆发时可快速定位到受影响资产。 • **计划任务** 收集计划任务信息，便于您及时清点资产的任务路径信息。 • **中间件** 收集中间件信息，便于您了解资产中存在的中间件信息。	X	X	X	√	√	资产指纹调查概述

安全运营

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
安全报告	对安全日报进行配置。开启安全日报后，云安全中心以邮件形式向您指定的收件人发送每日安全统计信息。	X	X	√	√	√	安全报告
任务中心	任务中心提供任务管理功能。通过执行任务，可以自动化、批量地在多台资产上修复漏洞。	X	X	X	√	√	任务中心概述
荷鲁斯之眼Beta	支持查看云上资产全景图、网络拓扑、安全评分和资产的安全风险，为您管控云上资产安全提供全景视图和统一入口。	X	X	X	√	√	荷鲁斯之眼Beta
多账号安全管控	支持统一管控企业内多个云账号和资源账号，帮助您实时获取企业内所有账户的安全风险信息。	X	X	X	√	√	多账号安全管控

应用市场

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
自定义告警	支持用户自定义告警规则，实时检测威胁，支持对第三方日志导入进行实时分析。	需申请	需申请	需申请	需申请	需申请	自定义告警
应用白名单	支持将需要重点防御的服务器加入到白名单中，通过检测白名单中指定的应用程序区分可信、可疑或恶意程序，防止未经白名单授权的程序运行。	需申请	需申请	需申请	需申请	需申请	应用白名单
安全大屏	支持查看业务运营监控、安全应急响应中心、安全感知体系、安全防御体系大图、业务访客概览等多种数据大屏，并支持组件自定义。	X	增值	增值	增值	增值	安全大屏
网页防篡改	可实时监控网站目录并通过备份恢复被篡改的文件或目录，保障重要系统的网站信息不被恶意篡改，防止出现挂马、黑链、非法植入恐怖威胁、色情等内容。 支持对Windows和Linux进程添加白名单。网页防篡改功能将不对加入白名单的进程进行拦截。	X	增值	增值	增值	增值	网页防篡改
微步威胁情报	提供第三方威胁情报源。	x	增值	增值	增值	增值	微步威胁情报
等保合规检查	云安全中心提供覆盖通信网络、区域边界、计算环境和管理中心的等级保护合规检查功能，并提供等保合规检查报告。	√	√	√	√	√	等保合规检查

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
安全组配置检查	安全组配置检查功能为您检查安全组中存在高危风险的规则，并提供修复建议，帮助您更安全高效地使用安全组功能。	√	√	√	√	√	安全组配置检查

设置

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
设置	【主动防御】 为您自动拦截常见病毒、恶意网络连接和网站后门连接，并设置诱饵捕获勒索病毒。支持设置以下开关： • 防病毒 • 防勒索（诱饵捕获） • 网站后门连接防御 • 恶意网络行为防御 • 主动防御体验优化	X	√	√	√	√	主动防御
	【网站后门查杀】 为您定期检测网站服务器、网页目录中的网站后门及木马程序。	X	√	√	√	√	网站后门查杀
	【容器K8s威胁检测】 实时为您检测正在运行的容器集群安全状态，帮助您及时发现容器集群中的安全隐患和黑客入侵行为。	X	X	X	√	√	容器K8s威胁检测
	【自适应威胁检测】 开启自适应威胁检测能力后，如果服务器发生高危入侵事件，云安全中心会自动为您服务器的Agent开启重保护模式，更快更全地检测黑客的入侵行为。	X	X	X	√	√	自适应威胁检测能力
	【安全管控】 支持IP地址白名单配置，可对加入到白名单中的IP地址进行放行，避免正常的流量被拦截。	√	√	√	√	√	安全管控

功能模块	功能详情	基础版	防病毒版	高级版	企业版	旗舰版	相关文档
	【访问控制】 使用访问控制（RAM），您可以创建、管理RAM用户（例如员工、系统管理员或应用程序管理员），并可以控制这些RAM用户对资源的操作权限。	√	√	√	√	√	访问控制
	【防护模式管理】 为服务器提供多种防护模式，满足多业务场景下您服务器的防护需求。支持设置以下防护模式： • 基础防护模式（所有版本都支持） • 高级防护模式（仅防病毒版、高级版、企业版和旗舰版支持） • 重保护模式（仅企业版和旗舰版支持）	√	√	√	√	√	防护模式管理
	【客户端自保护功能】 开启客户端自保护后，未通过云安全中心控制台卸载Agent的行为将被云安全中心主动拦截，防止攻击者直接入侵服务器恶意卸载Agent或Agent进程被其他程序误杀。	√	√	√	√	√	客户端自保护
通知	对告警通知进行自定义设置，通过告警设置调整云安全中心向您发送告警通知的方式和要关注的风险等级。支持通过短信、邮件、站内信和钉钉机器人的方式向您发送告警通知。支持设置以下通知项目： • 漏洞 • 基线检查 • 安全告警 • AccessKey泄露情报 • 云平台配置检查 • 应急漏洞情报 • 网页防篡改 说明 仅云安全中心企业版支持使用钉钉机器人的通知方式。	√	√	√	√	√	通知
安装/卸载插件	支持Agent插件的安装和卸载。	√	√	√	√	√	安装或卸载插件

安全威胁防御限制说明

云安全中心支持安全告警实时检测与处理、漏洞检测与一键修复、攻击分析、云平台安全配置检查等功能，结合告警关联分析和攻击自动化溯源，帮助您全面加固系统和资产的安全防线。在云安全中心提供的防御能力以外，建议您定期更新服务器安全系统补丁、配合使用云防火墙、Web应用防火墙等产品缩小网络安全威胁的攻击范围，实时预防，不让黑客有任何可乘之机。

> **说明** 由于网络攻击手段、病毒样本在不断演变，实际的业务环境也有不同差异，因此无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查、云平台配置检查等安全能力，提升整体安全防线，预防黑客入侵、盗取或破坏业务数据。

4.应用场景

云安全中心的典型应用场景包括：

- 对于拥有数十个账号和上千台ECS服务器的场景，统一管控所有资产并实时监控云上业务整体安全，让上千台服务器中的漏洞、威胁和攻击情况一目了然。有效避免每一个漏洞演变成为整个网络被攻击的入口，帮助企业轻松应对运维工作和资产管控。
- 定期对云上服务进行漏洞扫描和基线配置核查，针对检测到的漏洞和风险配置项提供监控与修复服务。
- 对多种网络和主机日志进行检索，调查访问量，统计和分析各维度的原始日志信息。
- 监控AK泄露、网络入侵事件、DDoS攻击事件、ECS恶意肉鸡等行为，并对ECS开放的端口进行实时监控。
- 对ECS中发生的入侵事件（例如：Webshell、恶意软件、核心数据被加密勒索等）进行回溯，发现入侵的原因和全过程。

5.限制说明

本文档介绍了云安全中心使用的限制说明。

安全威胁防御限制说明

云安全中心支持安全告警实时检测与处理、漏洞检测与一键修复、攻击分析、云平台安全配置检查等功能，结合告警关联分析和攻击自动化溯源，帮助您全面加固系统和资产的安全防线。在云安全中心提供的防御能力以外，建议您定期更新服务器安全系统补丁、配合使用云防火墙、Web应用防火墙等产品缩小网络安全威胁的攻击范围，实时预防，不让黑客有任何可乘之机。

> **说明** 由于网络攻击手段、病毒样本在不断演变，实际的业务环境也有不同差异，因此无法保证能实时检测防御所有的未知威胁，建议您基于安全告警处理、漏洞、基线检查、云平台配置检查等安全能力，提升整体安全防线，预防黑客入侵、盗取或破坏业务数据。

日志库限制说明

云安全中心的日志库属于专属日志库。

- 您无法通过API/SDK等方式在日志库中写入数据，或者修改日志库的属性（例如存储周期等）。
- 其他日志库功能，例如查询、统计、报警、流式消费等均支持，与一般日志库无差别。
- 日志服务对专属日志库不进行任何收费，但日志服务本身需处于可用状态（不超期欠费）。
- 内置的报表可能会在以后更新并升级。

6.检测范围说明

云安全中心通过安装在您服务器上的Agent和云端防护中心的联动，为您提供服务器的安全告警、漏洞管理、病毒防御、基线检查、攻击分析等功能。

关于云安全中心检测范围说明，请仔细阅读以下内容：

> **说明** 以下收集的服务器相关信息的内容如发生变动，阿里云将提前在阿里云官网的适当版面公告向您提示修改内容；如您不同意阿里云所做的修改，您有权停止使用阿里云云安全中心服务。这种情况下，您可以卸载您云服务器上的Agent。具体操作，请参见卸载Agent。如您继续使用阿里云云安全中心服务，则视为您接受阿里云所做的相关修改。

可疑文件信息

云安全中心为您提供恶意文件检测功能。系统在检测到可疑文件后会上传该文件的相关信息（包括但不限于文件的路径、MD5值、创建时间等）到云端防护中心，以便进行最终核查。确认为恶意文件后，云安全中心会向您发送安全告警通知。

可疑进程信息

云安全中心为您提供恶意进程检测功能。系统在检测到可疑进程后会上传该进程的相关信息（包括但不限于进程名、进程启动参数、进程对应文件的路径、进程启动时间等）到云端防护中心，以便进行最终核查。确认为恶意进程后，云安全中心会向您发送安全告警通知。

账户信息

云安全中心为您提供登录审计、疑似帐号提醒、暴力破解拦截等功能。系统会定期分析和上传服务器的帐号信息（包括但不限于用户名、用户权限等）和登录日志信息（包括但不限于登录名、登录IP等）。如果发生异常登录事件，云安全中心会向您发送安全告警通知。

异常连接信息

云安全中心为您提供异常网络连接检测功能。系统在检测到可疑网络连接后，会上传该网络连接的相关信息（包括但不限于访问源IP、源端口、访问目的IP、目的端口等）到云端防护中心，以便进行最终核查。确认为异常连接后，云安全中心会向您发送安全告警通知。

服务器资产信息

云安全中心为您提供资产管理功能。系统将定期收集服务器的相关资产信息（包括但不限于安装的软件信息、监听的端口信息、运行的网站信息等），并在云安全中心控制台**资产中心**页面为您统一展示所有资产。

容器镜像安全

云安全中心为您提供镜像安全扫描功能。系统将定期扫描容器中是否存在漏洞和恶意文件，并在云安全中心控制台**镜像安全扫描**页面为您展示容器中检测出的所有漏洞和恶意文件信息。

容器运行时安全

云安全中心为您提供容器运行时威胁检测功能，实时检测运行中的容器是否存在病毒文件、恶意程序、内部入侵行为、容器逃逸、高风险操作等威胁。如果在容器运行时检测出了安全风险，云安全中心会向您发送安全告警通知。

7.售前常见问题

本文档介绍了购买云安全中心前的常见问题。

我已经免费试用过旗舰版，是否可以再次申请免费试用？

不可以。

每个阿里云账号用户仅享有一次免费试用旗舰版的机会。

7天免费试用如何开通？

开通旗舰版的7天免费试用前，请先确保您已符合以下条件，否则将无法成功试用旗舰版：

- 云安全中心基础版用户。

  未购买过云安全中心服务（包括防病毒版、高级版、企业版和旗舰版）的阿里云账号默认为基础版。基础版无需开通，默认所有云账号都可以使直接使用。

  > **说明** 如果您之前购买过付费版服务，但是服务到期后未续费，您的付费版将自动变成基础版。由于您已购买过云安全中心服务，此种情况下，您无法开通免费试用。

- 未参加过云安全中心7天免费试用活动。
- 至少有一台阿里云ECS服务器。

确认符合条件后，您可以执行以下步骤开通企业版7天免费试用：

1. 访问云安全中心产品详情页。
2. 单击**免费试用**并登录您的阿里云账号。
3. 在**7天免费试用**的对话框中，单击**免费试用旗舰版**。

> **说明** 每个阿里云账号用户仅享有一次免费试用旗舰版的机会。开通企业版7天免费试用的更多信息，请参见开通免费试用。

如果我有100台ECS服务器，可以只买10台授权数吗？

不可以。

使用云安全中心付费版时，需要为您账号下的所有服务器购买授权数，不支持仅购买部分服务器授权数。

云上安全需要从整体上进行防护，如果未对所有服务器进行整体防护，会存在防护漏洞，黑客入侵一台服务器后会尝试突破其他服务器，从而导致您业务的整体安全受损。

您在购买云安全中心付费版时，需要选择您当前**保有服务器台数**。保有服务器台数是您当前阿里云账号下所拥有的服务器台数的总和（购买页默认显示您的阿里云ECS服务器和已安装了云安全中心Agent的非阿里云服务器总数）。

完成购买后，如果您出于防护需求，对不包含在购买授权数范围内的服务器（即非阿里云服务器、线下IDC服务器和新购买的ECS）安装了Agent，云安全中心会统计出您实际已安装Agent的服务器数量是超出了购买时选择的授权数的。那么云安全中心会提示您补齐差价，即补交预支给您使用的授权数费用。

云安全中心是否支持按月购买？

支持。

云安全中心支持按月购买和按月续费。不同的资产规模可选择的购买时长有区别：

- 您的资产规模大于1台且小于或等于10台时，最小购买时长为6个月。
- 您的资产规模大于10台时，最小购买时长为1个月。

> **说明** 资产规模等于1台时，不支持按月购买，最小购买时长为1年。

更多云安全中心的价格信息，请参见计费模式。

云安全中心各个版本有区别吗？

有区别。

云安全中心提供基础版、防病毒版、高级版、企业版和旗舰版多个版本，以下是不同版本的功能差异：

- **基础版**

  免费为您提供基础的**安全加固**能力，可检测服务器异常登录、DDoS攻击、服务器主流类型的漏洞以及云产品安全配置。您在购买ECS实例时选择**安全加固**即可开通基础版。

  云安全支持7天免费试用旗舰版功能。只有购买了ECS实例并且以前未试用过云安全中心的用户，才可以免费试用旗舰版的功能。如果您已具有试用资格，在登录云安全中心控制台后，会有弹窗提示您已获得云安全中心旗舰版7天免费试用资格。

- **防病毒版**

  采用包年包月的计费方式，提供安全告警、病毒防御等服务。

- **高级版**

  采用包年包月的计费方式，提供安全告警、病毒防御、漏洞检测及修复、安全报告等服务。

- **企业版**

  采用包年包月的计费方式，提供安全告警、病毒防御、漏洞检测及修复、基线检查、资产指纹、攻击分析等全面的安全服务。

- **旗舰版**

  采用包年包月的计费方式，提供镜像安全扫描、容器K8s威胁检测、天机镜、安全告警、病毒防御、漏洞检测及修复、基线检查、资产指纹、攻击分析等全面的安全服务。

为什么防病毒版定价为30元/月，但在购买页面实际显示的金额不止30元？

购买页面实际购买金额主要受以下两个因素的影响：

- 保有服务器台数

  保有服务器台数是指云安全中心保护的服务器总数，包括已购买的阿里云ECS服务器和安装了云安全中心Agent的非阿里云服务器，默认值是当前账号下拥有的ECS服务器和安装了云安全中心Agent的非阿里云服务器总数。如果您的保有服务器台数超过了1台，那么购买页面显示的实际订单金额将会超过30元/月。

- 开通的增值功能

  云安全中心还为您提供了网页防篡改、日志分析、防勒索等增值服务。下单购买时，购买页面会自动选择日志和防勒索的默认容量。如果您无需使用日志分析和防勒索功能，购买防病毒版时将日志和防勒索的容量设置为0 GB即可。

我没有阿里云ECS服务器，只有线下IDC服务器，是否能使用云安全中心？

可以使用。

云安全中心可以防护阿里云ECS服务器、线下IDC服务器和其他厂商提供的云服务器。只要在您的服务器上安装云安全中心Agent插件，即可受到云安全中心的防护。详细内容，请参见安装Agent和线下IDC使用云安全中心最佳实践。

云安全中心是否可以防护其他厂商提供的云服务器？

可以。

云安全中心可以对其他厂商提供的云服务器（例如：AWS、腾讯云、青云、UCloud等）提供安全防护。只要在您的服务器上安装云安全中心Agent插件，您的服务器即可受到云安全中心的防护。详细内容，请参见非阿里云服务器安装Agent。

线下IDC和其他云服务器如何使用云安全中心？

在您的IDC服务器或非阿里云服务器上安装云安全中心Agent插件后，即可受到云安全中心的防护。相关内容请参见下表。

服务器类型	如何使用云安全中心
阿里云ECS服务器	如果购买ECS时选择了**安全加固**，会自动安装云安全中心Agent并开通云安全中心基础版（即免费版），无需您再手动安装Agent。 **说明** 云安全中心基础版（免费版）仅提供服务器异常登录和应急漏洞检测，适用于个人用户。

服务器类型	如何使用云安全中心
	如果购买ECS时未选择**安全加固**或者云安全中心提示**Agent已离线**，您需要执行以下操作，才能使您的服务器受到云安全中心的保护。 1. 开通云安全中心防病毒版、高级版、企业版或旗舰版。详细内容，请参见购买云安全中心。 **说明** 云安全中心基础版（免费版）仅提供服务器异常登录和应急漏洞检测，适用于个人用户。 2. 登录云安全中心控制台。 3. 在控制台为该服务器安装Agent。详细内容，请参见手动安装Agent。
其他云服务器（非阿里云ECS服务器） 线下IDC服务器	完成以下操作后，您的非阿里云服务器才能受到云安全中心的保护。 1. 开通云安全中心防病毒版、高级版、企业版或旗舰版。详细内容，请参见购买云安全中心。 **说明** 云安全中心基础版（免费版）仅提供服务器异常登录和应急漏洞检测，适用于个人用户。 2. 登录云安全中心控制台。 3. 在控制台为该服务器安装Agent。详细内容，请参见手动安装Agent。 4.

云安全中心能杀毒吗？

可以的。

云安全中心防病毒版、高级版、企业版和旗舰版支持对常见的网络病毒进行检测和自动查杀。详细内容，请参见功能介绍。

漏洞自动修复需要使用云安全中心哪个版本？

高级版、企业版和旗舰版都支持漏洞自动修复（即一键修复功能）。您可以购买或升级至云安全中心高级版、企业版或旗舰版使用漏洞自动修复功能。购买和升级云安全中心服务的具体操作，请参见购买云安全中心和升级与降配。

信息安全等级保护测评（等保）需要使用云安全中心哪个版本？

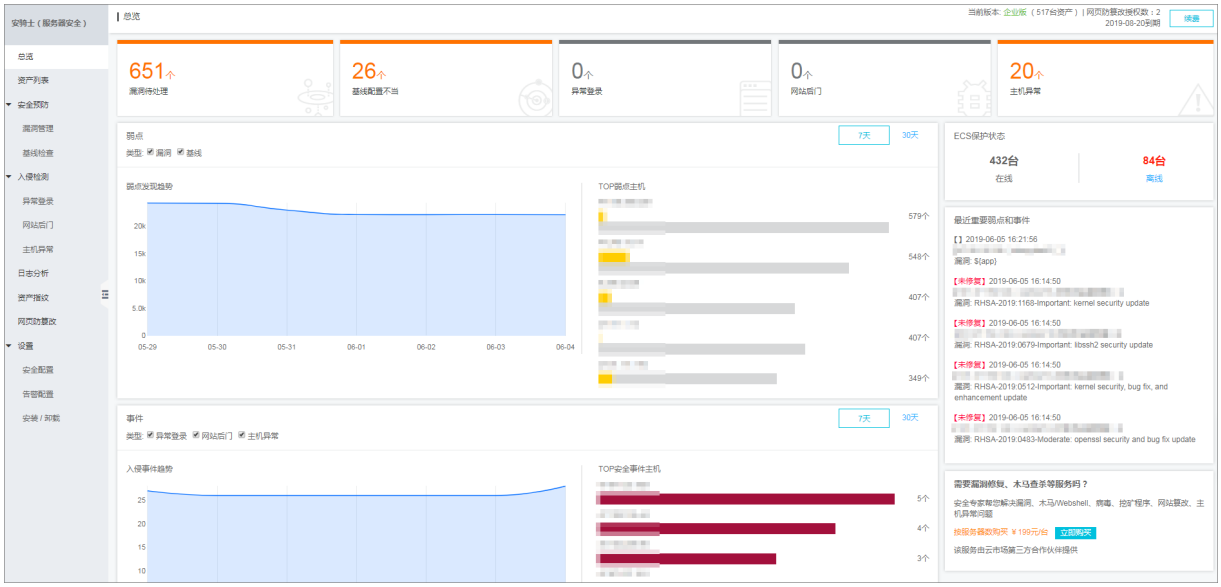
需要使用云安全中心**企业版**或**旗舰版**并单独开通日志分析增值服务。如何开通日志分析服务，请参见开通日志分析。

说明 云安全中心企业版和旗舰版提供基线检查的功能（等保必备功能），结合日志分析提供180天的日志存储，可以帮助您顺利通过等保测评。

安骑士、态势感知和云安全中心的区别

阿里云提供安骑士和云安全中心（态势感知全新升级版产品名称），帮助用户全面从主机以及系统层面防御风险和威胁，提升安全指数。

安骑士是阿里云提供的服务器安全服务产品，为您的主机提供实时防护。安骑士支持基础版（免费版）和企业版。基础版和企业版功能差异，请参见功能列表。



云安全中心是由态势感知全新升级而来，继承了态势感知的所有功能，并新增了安全评分总览、镜像安全扫描、防勒索、网页防篡改、病毒查杀、攻击分析、安全大屏等功能，是实时检测、分析和预警安全威胁的统一安全管理平台。云安全中心提供基础版、防病毒版、高级版、企业版和旗舰版，各个版本的功能详情，请参见功能特性。

安骑士企业版升级到云安全中心高级版功能说明

安骑士企业版升级到云安全中心高级版后，会在原有安骑士企业版基础上增加云产品配置检查、安全评分、等保合规检查等功能；相比原有的安骑士企业版，云安全中心高级版不支持资产指纹和基线检查的功能。

标识说明：

- √：支持
- X：不支持

功能	安骑士企业版升级到云安全中心高级版
安全评分	√（新增功能）

功能	安骑士企业版升级到云安全中心高级版
病毒防御	√（新增功能）
安全告警	√
资产中心	√
漏洞修复	√
基线检查	√ **说明** 原安骑士企业版支持；云安全中心高级版仅支持检测弱口令。
云平台配置检查	√（新增功能）
安全报告	√（新增功能）
资产指纹调查	X **说明** 原安骑士企业版支持；云安全中心高级版不支持，企业版、旗舰版支持。
设置	√
等保合规检查	√（新增功能）
安全组配置检查	√（新增功能）
日志分析	增值服务（高级版支持主机日志和安全日志）
防勒索	增值服务
微步威胁情报	增值服务
网页防篡改	增值服务

说明 其他增值功能，例如防勒索、网页防篡改、安全大屏、产品专家服务、应用白名单和自定义告警等，需升级到对应支持的版本才可开通并使用。更多信息，请参见云安全中心功能特性。

8.常见术语

本文档介绍了云安全中心相关的技术术语。

本地提权

本地提权漏洞是指攻击者在实施网络攻击时获得了系统最高权限，从而取得对网站服务器的控制权。 黑客利用该漏洞可突破安全防御系统，直接威胁用户的系统和数据安全。

代码执行

代码执行是指攻击者可能会利用漏洞，在服务器上执行恶意代码，从而实现对服务器的攻击或控制。

CVSS

通用安全弱点评估系统（Common Vulnerability Scoring System），用于评估安全漏洞的严重性。

DDoS

分布式拒绝服务DDoS（Distributed Denial of Service）指借助于客户机或服务器模式，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。

Web-CMS

Web内容管理系统（Web Content Management System），使用内容存储库或数据库来存储系统所需的页面内容、元数据或其他信息资产。

漏洞

漏洞是指在操作系统实现或安全策略上存在的缺陷，例如操作系统软件或应用软件在逻辑设计上存在的缺陷或在编写时产生的错误。攻击者可以对这类缺陷或错误进行利用，从而能够在未获得授权的情况下访问和窃取您的系统数据或破坏系统。系统漏洞需要系统管理员及时处理并修复，否则将带来严重的安全隐患。

基线

基线一般指配置和管理系统的详细描述，或者说是最低的安全要求，包括服务和应用程序设置、操作系统组件的配置、权限和权利分配、管理规则等。

9.历史公告

9.1. 【下线通知】2020年09月24日下线RDS SQL注入威胁检测

为了给您带来更优质的产品体验，云安全中心将于2020年09月24日起下线RDS SQL注入威胁检测功能。

下线内容

云安全中心将于2020年09月24日下线RDS SQL注入威胁检测功能。

下线时间

2020年09月24日

下线影响

- 从2020年09月24日起，您将无法申请开通RDS SQL注入威胁检测功能。
- 如果您已申请开通RDS SQL注入威胁检测，2020年09月24日起云安全中心将不再为您检测和展示RDS SQL注入告警事件。
- 对于该功能下线前检测出的RDS SQL注入告警事件，即使该功能下线后，您仍可以在云安全中心控制台**安全告警处理**页面查看和处理此类告警。

该功能下线后，如果您有检测RDS SQL注入的需求，可以使用数据库自治服务的安全审计功能。更多信息请参见安全审计。

给您带来的不便敬请谅解。有任何问题，请提交工单联系售后服务。