ALIBABA CLOUD

阿里云

云安全中心（态势感知）

云安全中心（态势感知）公共云合集

文档版本：20220711

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.动态与公告

1.1. 功能发布记录

本文介绍了云安全中心产品功能和文档的最新动态。

2022年06月

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
应用安全	新增	新增应用安全功能，您无需修改应用代码，只需在实例中安装应用安全探针，即可为应用提供强大的安全防护能力，并抵御绝大部分未知漏洞所利用的攻击手法。	高级版、企业版、旗舰版	2022-06-14	应用安全
基线检查	更新	基线检查内容更新。	高级版、企业版、旗舰版	2022-06-14	基线检查内容
网页防篡改	更新	网页防篡改支持操作系统和内核列表更新。	高级版、企业版、旗舰版	2022-06-16	操作系统和内核版本限制
旗舰版计费模式调整	更新	云安全中心旗舰版调整计价方案为：150元/台/月+5元/核/月。	旗舰版	2022-06-24	计费模式
镜像安全扫描	更新	镜像安全扫描设置中harbor镜像仓支持设置扫描限速，以提升扫描效率。	高级版、企业版、旗舰版	2022-06-28	管理镜像仓

2022年05月

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
全局日志过滤	新增	新增全局日志过滤功能，在保障您的安全效果防护的同时，有效使用日志存储空间，保障日志采集质量，提升您的运营效率。	所有版本	2022-05-19	全局日志过滤
恶意行为防御	迭代	恶意行为防御功能开放至高级版。	高级版、企业版、旗舰版	2022-05-19	恶意行为防御
多云配置管理	迭代	多云配置管理支持接入腾讯云、亚马逊云等厂商的服务器。	所有版本	2022-05-19	多云配置管理

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
基线检查	优化	基线检查功能的基线检查项更新。更新后，基线检查项分为以下几类： • 弱口令 • 未授权访问 • 容器安全 • 最佳安全实践 • CIS合规 • 等保合规 • 自定义基线	高级版、企业版、旗舰版	2022-05-19	基线检查项目
资产中心	优化	容器资产页面交互变更。变更后按照镜像和集群两个维度展示容器资产的信息。	所有版本	2022-05-19	查看容器安全状态
安全报告	迭代	安全报告功能报告发送时间支持自定义。	高级版、企业版、旗舰版	2022-05-19	安全报告
基线检查	迭代	基线修复功能新增支持快照备份功能。	高级版、企业版、旗舰版	2022-05-05	查看和处理基线检查结果

2022年04月

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
云蜜罐	迭代	云蜜罐产品正式上线，可在控制台购买开通使用。此功能可以为您提供云内外的攻击发现、攻击溯源等能力。您可以在阿里云VPC、已接入云安全中心的服务器实例上创建云蜜罐实例，来防御您服务器在云内外受到的真实攻击，为您提供有效的主动防御能力。	所有版本	2022-04-26	云蜜罐概述、开通云蜜罐服务、配置云蜜罐、查看和处理告警事件
容器主动防御	新增	新增容器主动防御功能。容器主动防御功能可在集群内使用镜像创建资源时，对镜像进行安全风险校验，对命中容器主动防御策略的镜像执行拦截、告警或放行动作，确保集群内启动的镜像符合您的安全要求。	旗舰版	2022-04-19	概述、创建防御策略、管理防御策略、查看和处理告警事件
镜像安全扫描	迭代	新增支持导出镜像安全扫描结果列表的功能。	高级版、企业版、旗舰版	2022-04-12	查看镜像安全扫描结果

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
日志分析	迭代	进程日志和网络连接日志新增日志字段。	防病毒版、高级版、企业版、旗舰版	2022-04-08	日志字段说明
新手任务	迭代	新手任务交互页面优化。	防病毒版、高级版、企业版、旗舰版	2022-04-08	新手任务
资产中心	迭代	新增资产采集功能，用于同步资产的详细信息。您可以使用此功能，采集服务器资产的详细信息，如资产的MAC地址、内核版本等信息。	所有版本	2022-04-08	查看服务器信息
攻击分析	迭代	攻击分析功能新增WebShell拦截及规则关闭引导。	企业版、旗舰版	2022-04-01	攻击分析

2022年03月

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
基线检查	优化	基线问题修复页面交互优化。	所有版本	2022-03-11	查看和处理基线检查结果
客户端问题排查	优化	客户端问题排查功能优化。	所有版本	2022-03-18	客户端问题排查
防勒索	优化	服务器防勒索最多支持配置的防护目录由8条修改为20条。	防病毒版、高级版、企业版、旗舰版	2022-03-25	创建防护策略

2022年02月

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
资产中心	优化	资产指纹调查功能移入资产中心的服务器页签下，并新增数据库、Web服务等其他资产指纹。	企业版、旗舰版	2022-02-22	概述、查看服务器信息、资产指纹调查、查看资产指纹数据
总览	优化	云安全中心**总览**页面重新设计，突出需要重点关注数据。	所有版本	2022-02-22	总览

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
CI/CD	新增	新增CI/CD功能。在Jenkins的Freestyle模式、Pipeline模式和Github Actions中集成云安全中心CI/CD插件之后，可在项目构建阶段发现镜像中存在的高危系统漏洞、应用漏洞、恶意病毒、WebShell、恶意执行脚本、配置风险以及敏感数据进行检测和识别，并提供漏洞修复建议。	旗舰版	2022-02-22	CI/CD概述、接入配置、Jenkins-Freestyle模式集成、Jenkins-Pipeline模式集成、GitHub Actions集成、查看镜像扫描结果
恶意行为防御	优化	恶意行为防御的系统防御规则页签新增**ATT&CK攻击阶段**功能，通过此功能可按照ATT&CK攻击阶段查找系统防御规则。	企业版、旗舰版	2022-02-26	恶意行为防御
微步威胁情报	下线	微步威胁情报功能下线。	防病毒版、高级版、企业版、旗舰版	2022-02-26	无

2022年01月

功能名称	变更类型	动态说明	影响的版本	发布时间	相关文档
漏洞修复	优化	漏洞修复功能页面的漏洞列表右上方新增**仅显示真实风险漏洞**功能。开启该功能，下方漏洞公告列表中会为您展示修复紧急度较高的漏洞，关闭该功能则会显示所有漏洞。	所有版本	2022-01-11	漏洞修复概述
镜像安全扫描	优化	镜像安全扫描页面改版。取消**DockerHub安全扫描**页签和**镜像安全扫描**页签。新版页面直接显示镜像安全扫描的信息，**DockerHub安全扫描**功能移动到页面右上角。	旗舰版、企业版	2022-01-07	接入镜像仓库、执行镜像安全扫描、查看镜像安全扫描结果

功能迭代历史记录

云安全中心2022年之前的功能迭代记录，请参见功能发布记录（2022年之前）。

1.2. 历史公告

1.2.1. 【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。

2.设置
2.1. 功能设置
2.1.1. 概述

云安全中心支持设置主动防御、网站后门查杀、容器K8s威胁检测、安全管控、访问控制、防护模式管理等功能，帮助您更好地管理云安全中心提供的各项功能。

设置页面支持配置以下功能：

- 主动防御
- 网站后门查杀
- 容器K8s威胁检测
- 自适应威胁检测能力
- 自动化告警关联分析
- 安全管控
- 访问控制
- 防护模式管理
- 客户端自保护

2.1.2. 主动防御

云安全中心的主动防御能力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。本文介绍如何设置主动防御支持的功能。

功能介绍

云安全中心的主动防御能力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。以下表格是各功能的详细介绍。

功能	支持的版本	描述

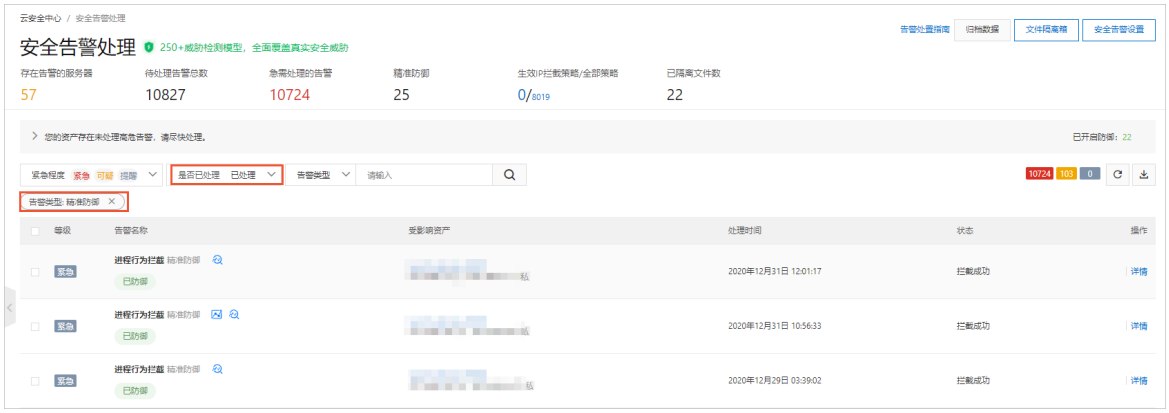
功能	支持的版本	描述
防病毒	防病毒版、高级版、企业版、旗舰版	防病毒能够帮助您自动隔离并查杀常见网络病毒，包括主流勒索病毒、DDoS木马、挖矿和木马程序、恶意程序、后门程序和蠕虫病毒等。所有支持自动隔离的病毒都经过了阿里云安全专家的测试和验证，确保零误杀。 **说明** • 您购买云安全中心防病毒版及以上版本后，云安全中心默认为您开启**防病毒**功能，并将您的所有服务器添加到防病毒的检测范围内。 • 感染型病毒是一类高级恶意程序，由病毒本体将恶意代码写入正常程序文件执行，因此往往有大量原本正常程序被感染后作为宿体被检出。感染型病毒可能会危害系统进程，终止系统进程会造成系统稳定性风险。因此云安全中心不会自动隔离感染型病毒，您需要手动处理此类病毒。
防勒索（诱饵捕获）	高级版、企业版、旗舰版	防勒索（诱饵捕获）提供了捕捉新型勒索病毒的诱饵，并通过病毒行为分析，为您自动启动新型勒索病毒的防御。云安全中心在您服务器中设置的勒索捕获诱饵文件仅用于捕获新型勒索病毒，不会对您的业务产生任何影响，请您放心使用该功能。您可以在**安全告警处理**页面，将告警类型设置为**精准防御**，以便查看云安全中心为您隔离的防勒索病毒。 **说明** 开启**防勒索（诱饵捕获）**开关前，您需要先购买并开通防勒索服务。更多信息，请参见防勒索开通服务。
网站后门连接防御	企业版、旗舰版	开启该功能后，云安全中心会自动拦截黑客通过已知网站后门进行的异常连接行为，并隔离相关文件。您可以在**安全告警处理**页面查看相应告警和被隔离的文件。更多信息，请参见查看和处理告警事件和文件隔离箱。 **说明** 您购买了企业版或旗舰版后，云安全中心默认为您开启**网站后门连接防御**功能，并将您的所有服务器添加到网站后门连接防御的检测范围内。
恶意网络行为防御	企业版、旗舰版	开启该功能后，云安全中心将拦截您的服务器和已披露的恶意访问源的之间的网络行为，为您的服务器增强安全防护。

功能	支持的版本	描述
主动防御体验优化	企业版、旗舰版	开启该功能后，如果服务器异常关机或安全防御能力缺失时，云安全中心将采集服务器Kdump数据进行安全防护分析，不断提升云安全中心的安全防御能力。

> **说明**
>
> - 如果您开启了**防病毒**、**防勒索（诱饵捕获）**、**网站后门连接防御**或**恶意网络行为防御**中的任意功能，云安全中心会为您自动开启病毒云查杀，同时云安全中心将为新购服务器默认开启该功能和病毒云查杀。病毒云查杀可以帮您自动隔离常见网络病毒。病毒云查杀的更多信息，请参见病毒云查杀。
> - 如果您**主动防御**区域的所有功能都为关闭状态，云安全中心将以安全告警的形式向您展示在您服务器上检测出的病毒，您需要在控制台手动处理病毒相关告警。建议您开启**主动防御**区域所有的功能，加固服务器安全防线。如何处理告警，请参见查看和处理告警事件。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**主动防御**区域，开启**防病毒**、**防勒索（诱饵捕获）**、**网站后门连接防御**或**恶意网络行为防御**的开关。



开启**防病毒**、**防勒索（诱饵捕获）**、**网站后门连接防御**和**恶意网络行为防御**开关后，云安全中心将从防病毒、防勒索、防网站后门异常连接和防恶意源访问等多方位为您的服务器提供安全防护。建议您打开这四个开关。

4. 单击**防病毒**、**防勒索（诱饵捕获）**、**网站后门连接防御**或**恶意网络行为防御**右侧的**管理**，管理防病毒、防勒索（诱饵捕获）、网站后门连接防御或恶意网络行为防御自动隔离、拦截病毒或恶意行为生效的服务器范围。

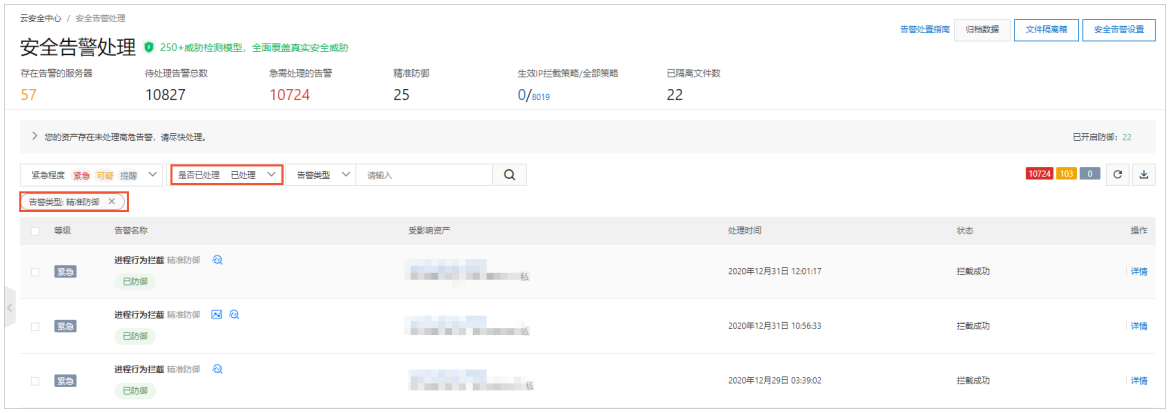
   开启对应功能开关后，云安全中心会自动为加入隔离范围内的服务器隔离、拦截病毒或恶意行为。

5. 在**主动防御-防病毒**、**主动防御-防勒索（诱饵捕获）**、**主动防御-网站后门连接防御**或**恶意网络行为防御**对话框中设置需要检测的服务器。

   从左侧**未检测服务器**列表中选择要开启检测的服务器，单击 > 图标，将其移入右侧**已检测服务器**列表中，为该服务器开启检测；将服务器从右侧框移入左侧框，为该服务器关闭检测功能。

> **注意** **防勒索（诱饵捕获）**只支持为Windows系统的服务器提供新型勒索病毒诱捕服务。您的服务器操作系统必须是Windows 2003及以上版本才能添加到防勒索（诱饵捕获）的检测范围中。

6. 单击**确定**。
   开启防病毒、防勒索（诱饵捕获）、网站后门连接防御和恶意网络行为防御服务后，云安全中心将自动隔离检测出的主流病毒类型或异常连接。
7. 在**安全告警处理**页面**精准防御**类型告警列表中，查看被主动防御功能自动隔离的病毒。



您需要将搜索条件置为**已处理**，并且**告警类型**选择**精准防御**。

> **说明** 主动防御功能的防病毒、防勒索（诱饵捕获）和网站后门连接防御功能开通后，可能会存在部分程序误报或未隔离成功的情况。
>
> - 部分误报导致文件被隔离时，您可以从文件隔离箱中恢复被误隔离的文件。具体内容请参见文件隔离箱。
> - 未隔离成功的事件可以在**安全告警处理**页面手动隔离。具体内容请参见查看和处理告警事件。

8. （可选）选中**主动防御体验优化**复选框。
   选中**主动防御体验优化**有助于云安全中心获取服务器异常情况下安全防护数据，为您提升安全防护能力。建议您选中该项。

2.1.3. 网站后门查杀

网站后门查杀功能会定期检测网站服务器、网页目录中的网站后门及木马程序。只有为服务器开启网站后门查杀后，云安全中心安全告警才会触发网站后门检测，并向您展示相关告警记录。本文介绍如何为您的服务器开启网站后门查杀。

背景信息

网站后门查杀功能使用自主查杀引擎检测常见后门文件，支持定期查杀和实时防护，并提供一键隔离功能。

以下是网站后门查杀功能的说明：

- Web目录中文件发生变动会触发动态检测，每日凌晨扫描整个Web目录进行静态检测。
- 支持针对网站后门检测的资产范围配置。
- 对发现的木马文件支持隔离、恢复和忽略。

版本限制

仅云安全中心的企业版和旗舰版支持该功能，其他版本不支持。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。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**设置**页签下的**网站后门查杀**区域，单击**管理**。
4. 在**网站后门查杀范围**面板上，选中需要开启网站后门查杀的服务器。
5. 单击**确定**。

后续步骤

为服务器开启网站后门查杀后，您可以在**安全告警处理**页面查看告警类型为**网站后门**的告警。待处理的网站后门告警可能会对您的资产安全造成严重威胁，建议您及时处理此类告警。具体操作，请参见查看和处理告警事件。

2.1.4. 容器K8s威胁检测

云安全中心旗舰版支持容器K8s威胁检测能力，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。本文介绍如何为您的服务器开启容器K8s威胁检测能力及云安全中心支持的容器威胁检测项。

前提条件

已购买或升级至云安全中心旗舰版。具体操作，请参见购买云安全中心和升级与降配。各版本支持的功能详情，请参见功能特性。

背景信息

开启容器K8s威胁检测能力后，您无需进行其他设置，云安全中心将为您开启**容器集群异常**类型告警的检测。云安全中心支持的检测项详情，请参见容器K8s威胁检测项。

开启容器K8s威胁检测

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**容器K8s威胁检测**区域，打开威胁检测开关。
   开启容器K8s威胁检测能力后，如果检测到K8s容器集群中存在安全风险，会在**安全告警处理**页面向您展示相关告警，建议您及时查看并处理相关告警。具体操作，请参见查看和处理告警事件。

容器K8s威胁检测项

类型	检测项
容器集群异常	K8s API Server执行异常指令
	Pod异常目录挂载
	K8s Service Account横向移动

类型	检测项
	恶意镜像Pod启动
异常网络连接	反弹Shell网络外连
	可疑网络外连
	疑似内网横向移动
恶意进程（云查杀）	DDoS木马
	可疑矿机通信
	可疑程序
	可疑端口爆破扫描工具
	可疑黑客程序
	后门程序
	恶意漏洞扫描工具
	恶意程序
	挖矿程序
	木马程序
	自变异木马
	蠕虫病毒
网站后门	Webshell
	Apache-CouchDB执行异常指令
	FTP应用执行异常指令
	Hadoop执行异常指令
	Java应用执行异常指令
	Jenkins执行异常指令
	Linux异常账号创建
	Linux计划任务执行异常指令
	MySQL执行异常指令
	Oracle执行异常指令

类型	检测项
进程异常行为	PostgreSQL应用执行异常指令
	Python应用执行异常指令
	SSH远程非交互式一句话异常指令执行
	Webshell执行可疑探测指令
	Windows-3389-RDP配置被修改
	Windows异常下载指令
	Windows异常账号创建
	crontab计划任务被写入恶意代码
	Linux可疑命令序列
	Linux可疑命令执行
	动态植入可疑脚本文件
	反弹Shell
	反弹Shell命令
	可疑HTTP隧道信息泄露
	可疑SSH Tunnel端口转发隧道
	可疑Webshell写入行为
	可疑特权容器启动
	可疑端口监听异常进程
	启动恶意容器
	存在风险的Docker远程调试接口
	异常操作指令
	容器内部提权或逃逸
	启动恶意容器

2.1.5. 自适应威胁检测能力

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开启重大活动保护模式。该模式开启所有安全防护规则和安全引擎，可以更全面地检测黑客的入侵行为。本文介绍如何开启自适应威胁检测能力。

前提条件

已购买或升级至云安全中心企业版、旗舰版。具体操作，请参见购买云安全中心和升级与降配。各版本支持的功能详情，请参见功能特性。

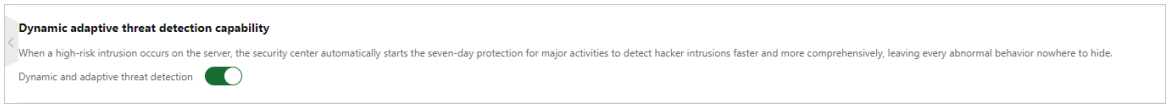
背景信息

自适应威胁检测能力默认为关闭状态，您需要手动开启该功能。开启该功能后，如果云安全中心在您的服务器中检测到高危风险（即高危告警），会自动为您的服务器Agent开启期限为7天的重大活动保护模式。重大活动保护模式会对任何可疑的入侵行为和潜在的威胁进行告警。重大活动保护模式的更多信息，请参见防护模式管理。

> **说明** 云安全中心自动为您的服务器开启了期限为7天的重大活动保护模式时，如果您在这7天中，手动设置了该服务器的防护模式，7天到期后云安全中心将不会自动为该服务器关闭重大活动保护模式，该服务器会一直保持您手动设置的防护模式。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**自适应威胁检测能力**区域，打开**动态自适应威胁检测**开关。

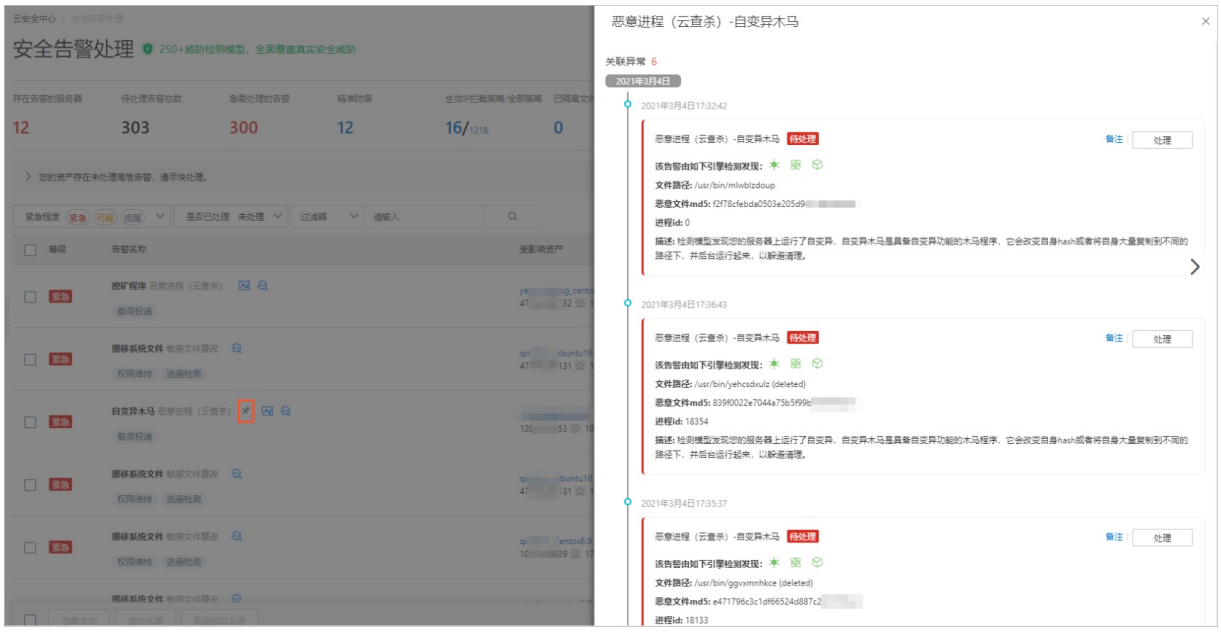


2.1.6. 自动化告警关联分析

云安全中心提供自动化告警关联分析功能，帮助您自动关联同一黑客入侵活动产生的多条告警。开启该功能后，您可以一键处理具有同一类型特征的告警，提升告警处理的效率。本文介绍如何开启自动化告警关联分析功能。

背景信息

自动化告警关联分析功能通过分析告警产生的链路，将来自同一IP、同一服务或同一个用户的多条恶意告警聚合为一个告警。云安全中心的企业版和旗舰版该功能默认为关闭状态，您需要手动开启该功能。开启该功能后，云安全中心会在**安全告警处理**页面，聚合特征相同的告警并重新统计**待处理告警总数**、**急需处理的告警**和各告警类型告警的数量。聚合后的告警右侧会产生 图标，您可以单击聚合后的告警名称查看该告警自动化关联分析的结果。更多信息，请参见查看告警自动化关联分析。



关闭自动化告警关联分析功能后，云安全中心会将已聚合的告警拆分成单条告警，并重新统计**待处理告警总数**、**急需处理的告警**和各告警类型告警的数量。

版本限制

仅云安全中心的企业版和旗舰版支持该功能，其他版本不支持。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。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**设置**页签下的**告警聚合开关**区域，打开**告警关联**开关。

> **注意** 只有告警数据（包括已处理和未处理告警）少于或等于1万条时，您才能打开**告警关联**开关。如果您的告警多于1万条，您可以在**安全告警处理**页面归档数据，减少告警数据量。具体操作，请参见归档告警数据。

2.1.7. 全局日志过滤

云安全中心提供全局日志过滤能力，在保障您的安全效果防护的同时，有效使用日志存储空间，保障日志采集质量，提升您的运营效率。

原理说明

全局日志过滤功能基于以下两个维度对云安全中心客户端的日志进行过滤。

- 基于特定字段，在时间维度聚合的过滤

  将数据采集的特定字段，例如cmdline命令行，username用户名，pcmdline父进程命令行等等字段，按一定顺序组合成key，并在单位时间内聚合过滤相同key的事件，统计相同特征的事件出现次数，次数未超过设置的阈值，正常上报，次数超过阈值即过滤掉。

- 基于进程链的过滤

  将采集事件的进程链做归一化处理，提取特征作为过滤的key。在一个过滤周期内，统计相同特征的事件出现次数，次数未超过设置的阈值，正常上报，次数超过阈值即过滤掉。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**设置**页签下的**全局日志过滤**区域，切换**日志过滤**开关的状态。

> **注意** 日志过滤开关默认为开启状态。如果您未开通日志分析服务，日志过滤开关为置灰状态且不支持关闭。只有开通了日志分析服务，才可以关闭此开关。

2.1.8. 安全管控

安全管控功能支持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，避免云安全中心拦截正常的流量。本文介绍如何使用安全管控功能。

背景信息

如果云安全中心将正常访问的IP地址识别为风险IP并对其进行拦截，导致部分业务受影响，可通过安全管控功能设置IP白名单，放行因误判被拦截的IP地址。云安全中心不会对添加至IP白名单的IP地址进行告警或拦截。

> **注意** 将某个IP地址加入IP白名单后，该IP地址在访问您的（部分或所有）服务器时将不受任何限制。添加IP白名单时请谨慎操作。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**安全管控**区域，单击**配置**，跳转至**安全管控**控制台。

4. 在左侧导航栏，选择**白名单管理 > IP白名单**。
5. 配置IP白名单。

   具体操作，请参见IP白名单。

2.1.9. 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、系统或应用程序），并可以控制这些RAM用户对资源的操作权限。当您的企业存在多用户协同操作资源的场景时，RAM可以让您避免与其他用户共享云账号密钥，按需为用户分配最小权限，从而降低企业的信息安全风险。本文介绍云安全中心访问控制模块的主要功能。

背景信息

如果您的企业存在多用户协同操作云上资源的场景，为了避免给企业用户授予过多不必要的权限，给企业的资产安全带来较大的风险，建议您定期前往RAM控制台确认企业用户的权限授予情况。设置企业用户权限时建议遵从最小授权原则。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**访问控制**区域，查看访问控制提供的权限策略管理、用户管理、角色管理功能并进行相应的操作。

您可以进行以下操作：

- 单击**权限策略管理**后的**管理**，跳转至RAM控制台，管理您当前账号下所有权限策略。具体操作，请参见权限策略管理。
- 单击**用户管理**后的**管理**，跳转至RAM控制台，管理您账号下已创建的用户。具体操作，请参见用户管理。
- 单击**角色管理**后的**管理**，跳转至RAM控制台，管理您账号下已创建的RAM角色。具体操作，请参见角色管理。

2.1.10. 防护模式管理

云安全中心Agent是云安全中心提供的本地插件，您必须在服务器操作系统上安装云安全中心Agent插件才能使用云安全中心提供的安全防护服务。防护模式管理功能提供多种Agent运行模式，可以满足您不同应用场景下的安全需求。本文介绍如何设置Agent防护模式。

背景信息

要使用云安全中心，您必须在服务器上安装Agent插件。关于Agent插件的说明，请参见Agent说明；关于如何安装Agent插件，请参见安装Agent。

防护模式说明

Agent插件在服务器上运行时，会占用少量服务器资源。您可以调整Agent的运行模式，限制其资源占用量。为服务器选择适合的防护模式，可以获得更好的安全防护效果。以下表格描述了Agent支持的运行模式。

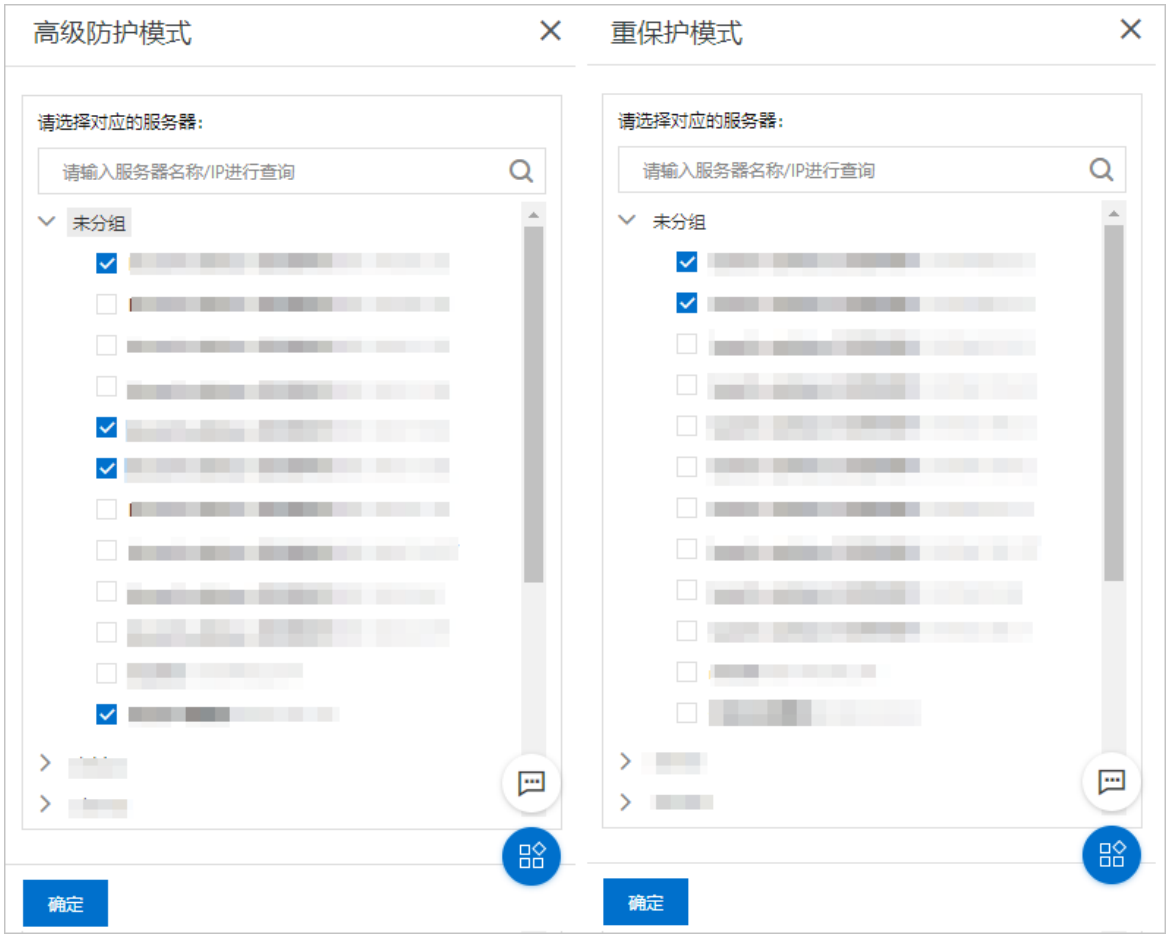
防护模式	最高内存或CPU占用	支持的版本	应用场景
基础防护模式	• 内存占用：最高200 MB • CPU占用：单核最高10%	所有版本	基础防护模式适用于所有业务场景，极低的资源消耗对业务零影响。 **说明** 新购买的ECS默认开启基础防护模式。
高级防护模式	• 内存占用：最高300 MB • CPU占用：单核最高30%	防病毒版、高级版、企业版、旗舰版	高级防护模式适用于关键业务的安全防护场景。该模式开启大数据分析引擎、机器学习、深度学习引擎，可以挖掘更多可疑的入侵行为和潜在的威胁。
重大活动保护模式	• 内存占用：最高500 MB • CPU占用：整体最高60%	企业版、旗舰版	重大活动保护模式适用于重大活动的安全保障。该模式开启所有安全防护规则和安全引擎，通过智能化的规则提升告警检测引擎的敏感度，对任何可疑的入侵行为和潜在的威胁都会进行告警。

说明 选择任一防护模式时，当Agent占用资源超过限制峰值（具体峰值，请参见以上表格**最高内存或CPU占用**列）时，Agent将会暂停工作，直至CPU使用率或内存占用下降到合理范围内，Agent会自动重启。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**防护模式管理**区域，单击**高级防护模式**或**重大活动保护模式**区域的**管理**。

4. 在**高级防护模式**或**重大活动保护模式**面板，选中需要配置**高级防护模式**或**重大活动保护模式**的服务器。



> **说明** 每台服务器Agent的运行模式只能选择**高级防护模式**或**重大活动保护模式**中的一种。例如某服务器当前是**高级防护模式**，如果您将该服务器设置为**重大活动保护模式**，该服务器的防护模式会变为**重大活动保护模式**。

5. 单击**确定**。
6. 在**重大活动保护模式**区域，在**CPU阈值**右侧设置CPU占用的阈值。

重大活动保护模式支持设置CPU占用的阈值，阈值越高，防护更精准。可设置范围：5%~60%。默认取值5%。

> **说明** **重大活动保护模式**下告警检测类型多并且检测引擎的敏感度更高，会检测出更多的告警，可能会导致误报率增加。建议您及时关注并处理告警。

2.1.11. 客户端自保护

客户端自保护功能可以主动拦截恶意卸载云安全中心Agent的行为，保障云安全中心防御机制稳定运行。本文介绍如何为服务器开启客户端自保护。

背景信息

开启客户端自保护后，不是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，与此同时云安全中心会对您服务器Agent目录下的进程文件提供默认保护，防止攻击者入侵服务器后卸载云安全中心Agent或您服务器中的其他进程误杀Agent，导致云安全中心对您服务器的防护失效的情况发生。建议您为所有服务器开启客户端自保护。

客户端自保护功能支持的操作系统版本和内核版本有限。如果服务器操作系统版本和内核版本不在客户端自保护功能支持的操作系统版本和内核版本范围内，该服务器将无法使用客户端自保护功能。该功能支持的操作系统及内核版本详细信息，请参见支持的操作系统版本和内核版本。

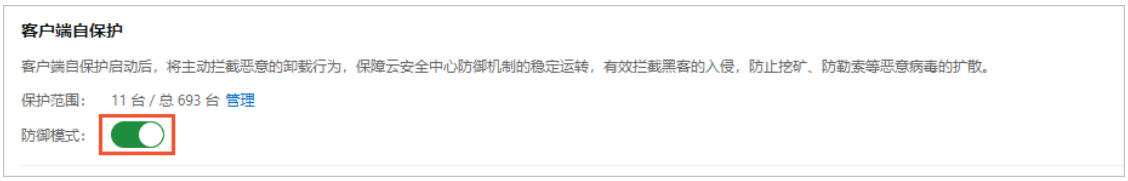
> **说明** 为服务器开启客户端自保护功能后，您只能通过以下两种方式卸载云安全中心Agent。
> - 关闭服务器的客户端自保护状态后，在服务器上卸载Agent。
> - 在云安全中心控制台上卸载Agent。具体操作，请参见卸载Agent。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

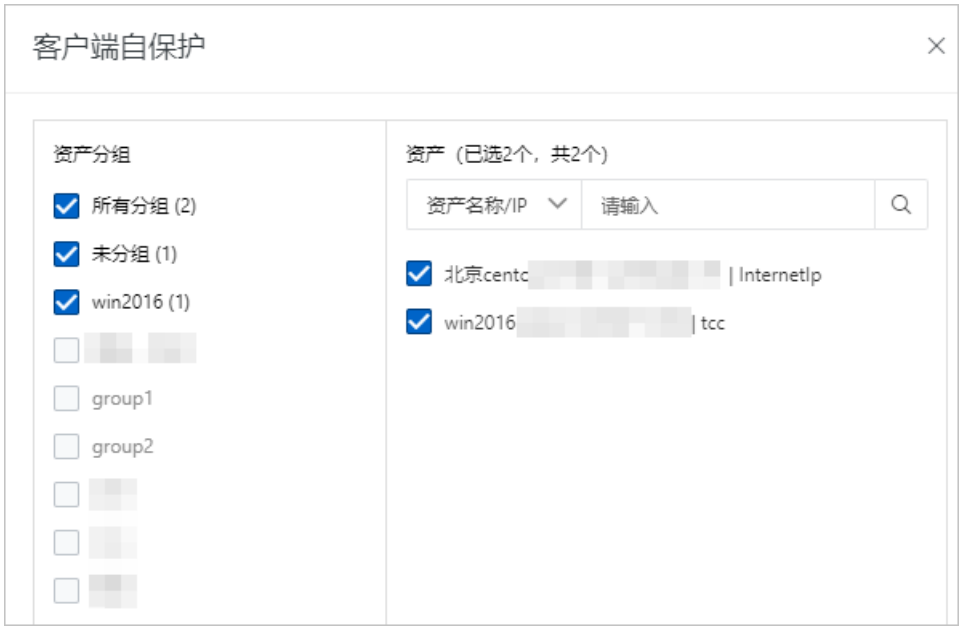
为服务器开启客户端自保护

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**设置**页签的**客户端自保护**区域，打开**防御模式**开关。



客户端自保护防御模式开启后，您已安装了Agent并属于客户端自保护**保护范围**内的服务器会自动开启客户端自保护。

4. 单击**保护范围**右侧的**管理**。
5. 在**客户端自保护**面板上，选中需要开启客户端自保护的服务器。



选中的服务器将开启客户端自保护功能，取消选中的服务器将关闭客户端自保护功能。

6. 单击**确定**。

> **说明** 您的服务器开启**客户端自保护**后，自保护机制会立即生效。您的服务器关闭**客户端自保护**5分钟后，自保护机制才会关闭。

支持的操作系统版本和内核版本

操作系统	支持的操作系统版本	支持的内核（Kernel）版本
Windows（64位）	• Windows Server 2008 R2 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019	所有版本
		• 4.18.0-240.22.1.el8_3.x86_64 • 4.18.0-240.15.1.el8_3.x86_64 • 4.18.0-193.28.1.el8_2.x86_64 • 4.18.0-193.14.2.el8_2.x86_64 • 4.18.0-147.8.1.el8_1.x86_64 • 4.18.0-147.5.1.el8_1.x86_64 • 3.10.0-1160.36.2.el7.x86_64 • 3.10.0-1160.31.1.el7.x86_64 • 3.10.0-1160.25.1.el7.x86_64 • 3.10.0-1160.24.1.el7.x86_64 • 3.10.0-1160.21.1.el7.x86_64 • 3.10.0-1160.15.2.el7.x86_64 • 3.10.0-1160.11.1.el7.x86_64 • 3.10.0-1160.6.1.el7.x86_64

操作系统	支持的操作系统版本	支持的内核（Kernel）版本
CentOS（64位）	• CentOS 6.3 • CentOS 6.4 • CentOS 6.5 • CentOS 6.6 • CentOS 6.7 • CentOS 6.8 • CentOS 6.9 • CentOS 6.10 • CentOS 7.0 • CentOS 7.1 • CentOS 7.2 • CentOS 7.3 • CentOS 7.4 • CentOS 7.5 • CentOS 7.6 • CentOS 7.7 • CentOS 7.8 • CentOS 7.9 • CentOS 8.0 • CentOS 8.1 • CentOS 8.2 • CentOS 8.3 • CentOS 8.4	• 3.10.0-1160.2.2.el7.x86_64 • 3.10.0-1127.19.1.el7.x86_64 • 3.10.0-1127.18.2.el7.x86_64 • 3.10.0-1127.13.1.el7.x86_64 • 3.10.0-1127.10.1.el7.x86_64 • 3.10.0-1127.8.2.el7.x86_64 • 3.10.0-1127.el7.x86_64 • 3.10.0-1062.18.1.el7.x86_64 • 3.10.0-1062.12.1.el7.x86_64 • 3.10.0-1062.9.1.el7.x86_64 • 3.10.0-1062.4.3.el7.x86_64 • 3.10.0-1062.4.2.el7.x86_64 • 3.10.0-1062.4.1.el7.x86_64 • 3.10.0-1062.1.2.el7.x86_64 • 3.10.0-1062.1.1.el7.x86_64 • 3.10.0-1062.el7.x86_64 • 3.10.0-957.27.2.el7.x86_64 • 3.10.0-957.21.3.el7.x86_64 • 3.10.0-957.12.2.el7.x86_64 • 3.10.0-957.10.1.el7.x86_64 • 3.10.0-957.5.1.el7.x86_64 • 3.10.0-957.1.3.el7.x86_64 • 3.10.0-957.el7.x86_64 • 3.10.0-862.14.4.el7.x86_64 • 3.10.0-862.9.1.el7.x86_64 • 3.10.0-693.21.1.el7.x86_64 • 3.10.0-693.11.1.el7.x86_64 • 3.10.0-693.5.2.el7.x86_64 • 3.10.0-693.2.2.el7.x86_64 • 3.10.0-693.el7.x86_64 • 3.10.0-514.26.2.el7.x86_64 • 3.10.0-514.21.1.el7.x86_64 • 3.10.0-514.10.2.el7.x86_64 • 3.10.0-514.6.2.el7.x86_64 • 2.6.32-754.35.1.el6.x86_64 • 2.6.32-754.33.1.el6.x86_64 • 2.6.32-754.31.1.el6.x86_64 • 2.6.32-754.30.2.el6.x86_64 • 2.6.32-754.29.2.el6.x86_64 • 2.6.32-754.28.1.el6.x86_64 • 2.6.32-754.27.1.el6.x86_64 • 2.6.32-754.23.1.el6.x86_64 • 2.6.32-754.17.1.el6.x86_64 • 2.6.32-696.16.1.el6.x86_64

操作系统	支持的操作系统版本	支持的内核（Kernel）版本
		• 2.6.32-696.10.1.el6.x86_64 • 2.6.32-696.6.3.el6.x86_64 • 2.6.32-696.3.2.el6.x86_64 • 2.6.32-642.13.1.el6.x86_64 • 2.6.32-642.6.2.el6.x86_64 • 2.6.32-573.22.1.el6.x86_64 • 2.6.32-431.23.3.el6.x86_64 • 2.6.32-431.el6.x86_64
Ubuntu（64位）	• Ubuntu 14.04 • Ubuntu 16.04 • Ubuntu 18.04 • Ubuntu 20.04	• 5.4.0-77-generic • 5.4.0-74-generic • 5.4.0-73-generic • 5.4.0-54-generic • 4.15.0-147-generic • 4.15.0-144-generic • 4.15.0-143-generic • 4.15.0-128-generic • 4.15.0-124-generic • 4.15.0-91-generic • 4.15.0-52-generic • 4.15.0-45-generic • 4.15.0-42-generic • 4.4.0-210-generic • 4.4.0-154-generic • 4.4.0-151-generic • 4.4.0-146-generic • 4.4.0-142-generic • 4.4.0-117-generic • 4.4.0-105-generic • 4.4.0-96-generic • 4.4.0-93-generic • 4.4.0-63-generic • 4.4.0-62-generic
AliyunLinux（64位）	AliyunLinux 2.1903	• 4.19.91-23.al7.x86_64 • 4.19.91-22.2.al7.x86_64 • 4.19.91-21.al7.x86_64 • 4.19.91-19.1.al7.x86_64 • 4.19.81-17.2.al7.x86_64

2.1.12. 多云配置管理

云安全中心支持对非阿里云服务器（包括第三方云服务器和IDC服务器）进行防护和管理。使用云安全中心对您的非阿里云服务器进行防护前，您需要先将非阿里云服务器资产接入云安全中心，才能将服务器资产信息同步到云安全中心进行安全防护。

支持的云安全中心版本

云安全中心免费版和所有付费版都支持多云配置管理功能。

接入多云资产

接入第三方服务器资产后，该服务器信息会同步到资产中心，便于云安全中心进行统一防护和管理。

> **说明** 目前，支持接入腾讯云、亚马逊云等厂商的服务器。

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**，在**设置**页面，单击**多云配置管理**页签。
3. 在**多云配置管理**页签中，单击**多云资产**，然后单击**新增授权**。
4. 在**接入云外资产**抽屉面板中，选择需要接入的多云服务商，单击**下一步**。
5. 按照指引完成腾讯云子账号的创建。

   支持选择**快速配置方案**和**手动配置方案**。

   - **快速配置方案**：通过获取到的第三方云服务器主账号AK，由云安全中心自动为您创建子账号AK，建立第三方服务器和云安全中心服务之间的连接。选择该方案后，接入步骤如下：
     a. 登录第三方服务器的管理控制台。
     b. 获取第三方云服务器主账号的AccessKey ID和Access Secret。

        您可以根据云安全中心控制台的**多云配置管理**页签，查看具体的操作引导。

        > **说明** 云账号默认不提供主账号AK信息，需要您手动创建AK。

     c. 返回云安全中心控制台，打开**接入云外资产**抽屉面板，并选择**快速配置方案**。
     d. 单击**下一步**。
     e. 在**提交AK**向导页面，粘贴在步骤b中获取的主账号AK信息。
     f. 单击**确定**。

        完成此步骤后，您的第三方云服务器会接入到云安全中心。后续该主账号AK所子账号下新增的第三方云服务器将自动同步到云安全中心。

     g. 单击**同步最新资产**，立即将资产同步到云安全中心。

        如果您未手动**同步最新资产**，云安全中心会在一小时后自动同步。

        > **说明** 执行同步资产的操作后，资产同步需要一段时间完成。请您耐心等待，并无需再次点击**同步最新资产**。按钮。

   - **手动配置方案**：由您手动创建第三方云服务器的子账号AK，建立第三方云服务器和云安全中心服务之间的连接。选择该方案后，接入步骤如下：
     a.

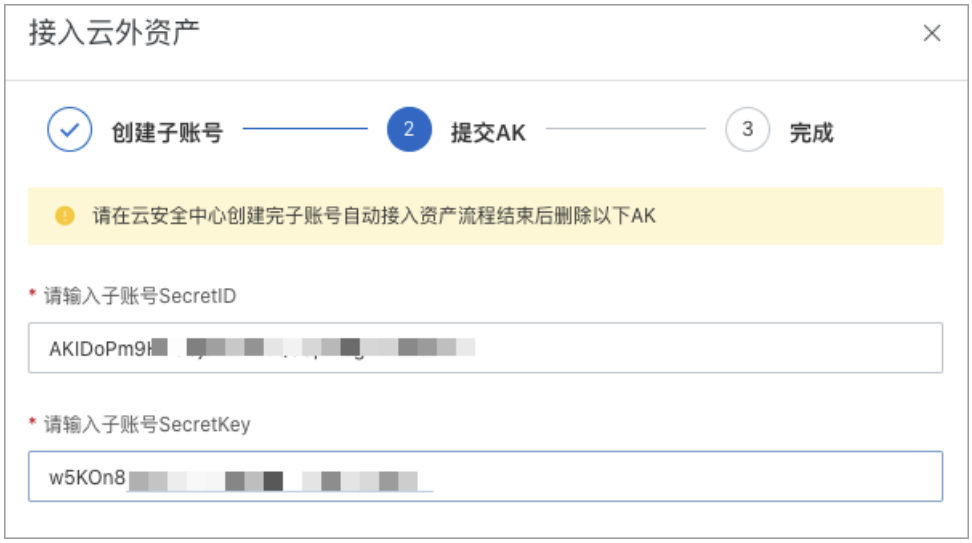
b. 获取第三方云服务器子账号的AccessKey ID和Access Secret。

> **说明** 子账号默认不提供AK信息，需要您手动创建AK。

c. 返回云安全中心控制台，打开**接入云外资产**抽屉面板，并选择**手动配置方案**。

d.

e. 在**提交AK**向导页面，粘贴在步骤b中获取的子账号AK信息。



f. 单击**确定**。

完成此步骤后，您的第三方云服务器会接入到云安全中心。

g. 单击**同步最新资产**。

> **说明** 执行同步资产的操作后，资产同步需要一段时间完成。请您耐心等待，并无需再次点击**同步最新资产**按钮。

IDC探针

您可以通过创建IDC探针，检测并发现的IDC服务器资产，并将发现的IDC服务器同步到云安全中心的资产中心模块中进行统一管理。

> **说明** 目前，IDC探针服务器仅支持已安装了云安全中心Agent的IDC服务器。

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**，在**设置**页面，单击**多云配置管理**页签。
3. 在**多云配置管理**页签中，单击**IDC探针**，然后单击**新增探针**。
4. 在**接入云外资产**抽屉面板中，设置IDC探针的信息，然后单击**下一步**。

设置项说明：

- **IDC机房**：IDC探针扫描的服务器所在的机房。
- **网段设置**：IDC探针需要扫描的网段。仅支持C类网段地址，即 `192.168.0.0` ~ `192.168.255.255` 。
- **周期设置**：IDC探针扫描的间隔时间。
- **Linux端口**：IDC探针扫描的Linux服务器的SSH端口。支持设置非标端口。
- **Windows端口**：IDC探针扫描的Windows服务器的RDP端口。支持设置非标端口。
- **地域**：该IDC服务器所在的地域信息，填写城市即可。此处填写的地域信息会展示在**资产中心**页面的服务器信息里。

5. 在**选择资产**抽屉面板中，选择需要执行扫描任务的服务器，然后单击**确定**。

   此处，您可以指定服务器来扫描和发现IDC资产。支持选择多台服务器。

   完成此步骤后，您将成功创建IDC探针。IDC探针将在您设置的扫描周期内，对指定网段范围内的IDC服务器进行扫描。探针扫描并发现了IDC服务器后，会将该服务器自动添加到云安全中心**资产中心**页面的服务器列表中。

停用IDC探针

如果您后续无需再使用该探针服务器，您可以单击**操作**列的**停用**。停用探针服务器后，该服务器将不再检测IDC服务器的状态。

> **说明** 停用IDC探针后，如果有新增的IDC服务器，将不会再自动同步资产信息到云安全中心。

后续步骤

您可以打开**资产中心**页面，在**服务器**页签和**IDC探针发现**页签，查看同步到云安全中心的非阿里云服务器资产详情和客户端安装状态。

2.2. 通知

云安全中心支持通过短信、邮件、站内信和钉钉机器人的方式向您发送通知。您可根据业务需要配置漏洞、基线检查、网页防篡改等告警通知。本文介绍如何配置通知和添加钉钉机器人。

背景信息

默认情况下，告警信息接收人为您的账号联系人。您可以前往消息中心，在**基本接收管理 > 安全消息 > 云盾安全信息通知**区域，单击**修改**新增更多消息接收人。更多信息，请参见告警通知邮箱的接收人可以在哪里修改。

仅云安全中心企业版支持使用钉钉机器人的通知方式。基础版、基础杀毒版和高级版用户需要升级到企业版，才能使用钉钉机器人的通知方式。

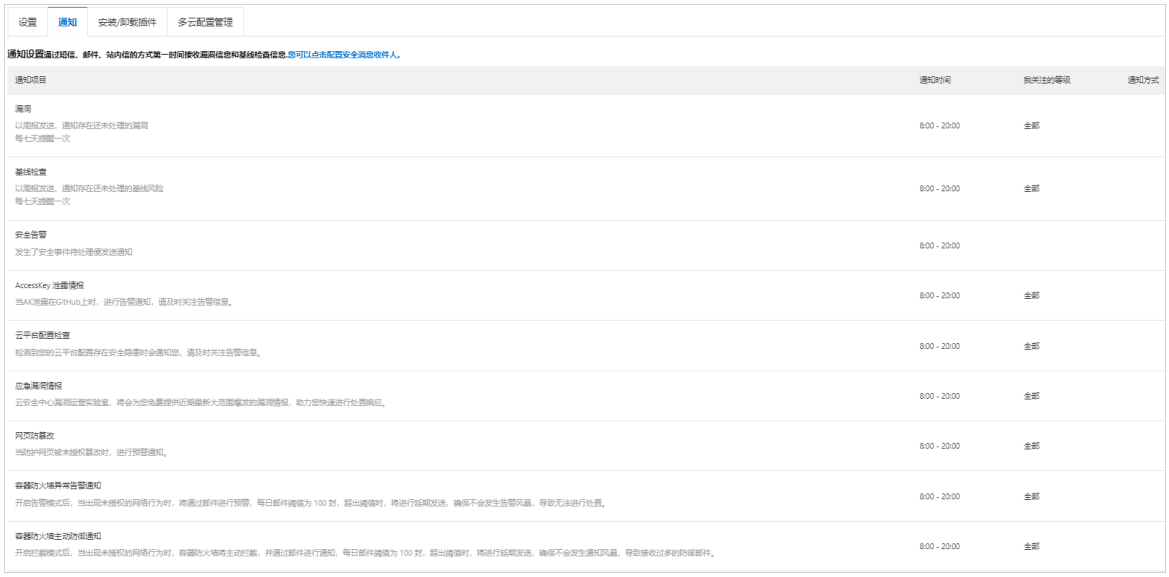
通知项目

项目	通知频率	通知发送时间	支持的通知方式	说明
漏洞	每七天发送一次	8:00~20:00	邮件	每七天向您发送一次主题为**阿里云服务器待处理漏洞周报**的通知。通知内容为您资产中未处理的漏洞数量和漏洞修复建议。
基线检查	每七天发送一次	8:00~20:00	短信 邮件 站内信	每七天向您发送一次主题为**云安全中心待处理基线配置风险周报**的通知。通知内容为您资产中未处理的基线风险数量。
安全告警	实时发送	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	检测到安全告警时发送通知。每天最多发送5条通知。同一服务器，每天最多发送1条通知。
精准防御	实时发送	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	每天最多2条短信、5条站内信、20封邮件，支持您配置的精准防御的告警通知。
AccessKey泄露情报	实时发送	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	检测到AccessKey泄露时发送通知。每天最多发送5条通知。
云平台配置检查	每七天发送一次	8:00~20:00	短信 邮件 站内信	检测到云平台配置检查风险项时发送通知。每7天发送一次通知。
应急漏洞情报	实时发送	8:00~20:00	短信 邮件 站内信	检测到未修复的应急漏洞时发送通知。每天最多发送10条通知。

项目	通知频率	通知发送时间	支持的通知方式	说明
网页防篡改	实时发送	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	检测到网页防篡改告警时发送通知。每天最多发送5条通知。
容器防火墙异常告警通知	实时发送	可选以下时段： • 24小时 • 8:00~20:00	邮件	检测到未授权的网络行为时发送通知。每天最多发送100条通知。
容器防火墙主动防御通知	实时发送	可选以下时段： • 24小时 • 8:00~20:00	邮件	检测到未授权的网络行为时主动拦截并发送通知。每天最多发送100条通知。
恶意IP拦截告警通知	实时发送	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	针对恶意IP的爆破攻击进行拦截，拦截后将为您发送通知。每天最多发送10条通知。
病毒扫描通知	按照病毒防御的扫描周期发送	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	按照您配置的病毒防御的扫描周期，在病毒扫描完成后通知扫描结果。
日志超量	每两天一次	可选以下时段： • 24小时 • 8:00~20:00	短信 邮件 站内信	每两天一次，当您的日志存储量超过了购买的日志容量的90%时，为您发送日志超量通知。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，单击**设置**。
3. 在**设置**页面，单击**通知**页签。
4. 在**通知**页面的通知项目列表中，定位到您需要配置的通知，分别配置该通知的**通知时间**、**我关注的等级**和**通知方式**。



如果需要修改安全消息接收人，您可单击通知项目列表上方的**您可以点击配置安全消息收件人**前往**基本接收管理**页面，修改**云盾安全信息通知**接收人。具体操作，请参见告警通知邮箱的接收人可以在哪里修改。

> **说明**
>
> - 在该页面修改的设置会即时生效。
> - 如果您选择了多种通知方式，云安全中心会在同一时间使用您选择的多种通知方式发送通知。

5. （可选）配置钉钉机器人通知。

> **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。基础版、基础杀毒版和高级版用户需要升级到企业版，才能使用钉钉机器人的通知方式。
> - 配置钉钉机器人通知前，请先安装钉钉并建立相关的钉钉群。

如果您已安装钉钉并建立了相关钉钉群，可按照以下步骤配置钉钉机器人通知。

i. 定位到您需要添加机器人通知的钉钉群，单击右上角**群设置 > 智能群助手 > 添加机器人 > 自定义（机器人） > 添加**。

ii. 配置机器人。具体操作，请参见配置钉钉机器人。

> **说明** 添加机器人时，将**安全设置**选择为**自定义关键词**，并将**自定义关键词**设置为**云安全中心**。无需选择**加签**和**IP地址（段）**。

iii. 复制**webhook地址**，并单击**完成**机器人的设置。

iv. 在云安全中心控制台**设置 > 通知**页面的**钉钉机器人通知**区域，单击**添加新的机器人**。

v. 在**添加钉钉机器人**面板，参考以下表格配置云安全中心钉钉机器人参数。

参数	说明	配置方法
机器人名称	为钉钉机器人自定义名称。	手动输入机器人名称，建议输入便于识别的名称。
Webhook地址	机器人的接入地址。	在要应用该钉钉机器人的钉钉群中，找到机器人的Webhook链接，复制粘贴到**Webhook地址**输入栏中。 注意 请保管好此Webhook地址，不要公布在外部网站上，泄露后可能会产生安全风险。
资产分组	您可以选择在云安全中心**资产中心**中创建的资产分组。选中后，钉钉机器人将会发送该资产分组中资产相关的告警通知。	单击下拉列表，选择钉钉机器人通知涉及的资产分组。

参数	说明	配置方法
通知范围	需要钉钉机器人通知的告警类型。	单击下拉列表，选择需要钉钉机器人通知的告警类型。 **说明** 目前，钉钉机器人通知范围覆盖漏洞、基线检查、安全告警和AK泄露检测。
通知频率	钉钉机器人发送通知的间隔周期，可选1分钟、5分钟、10分钟、30分钟或无限制（每检测到一条告警实时发送通知）。 **说明** 选择无限制后，一个 Webhook，一分钟最多发送20条通知。	单击下拉列表，选择您所需的通知间隔周期。
通知语言	钉钉机器人发送通知的语言类型，可选中文或英文。	单击下拉列表，选择钉钉机器人的通知语言。

vi. 单击**添加**，完成钉钉机器人通知的创建。

新创建的钉钉机器人通知默认为**启用**状态。

说明

- 添加机器人通知后，可单击**操作**栏的**测试**，验证钉钉机器人通知是否已经和钉钉群连通。
- 钉钉机器人通知支持**编辑**和**删除**。删除通知后，您将无法收到相关告警的钉钉机器人通知，但不影响您已设置的短信、邮件或站内信通知。

配置完成后，云安全中心将按照您配置的通知策略为您发送相关通知。

2.3. 安装或卸载插件

云安全中心Agent是云安全中心提供的本地安全插件，您必须在服务器操作系统上安装云安全中心Agent，才能使用云安全中心提供的安全防护服务。本文介绍了如何安装、卸载Agent插件。

背景信息

关于Agent插件的详细介绍和相关限制说明，请参见Agent概述。

工作原理

云安全中心Agent会实时向云安全中心服务器端上报Agent在线信息。

如果云安全中心Agent没有按时上报其在线信息，云安全中心服务器端会在12小时后判定该服务器不在线，并在云安全中心控制台中将该服务器的保护状态变更为**未受保护**。

Agent支持的操作系统

操作系统类型	支持的操作系统
Windows	• Windows Server 2019 • Windows Server 2016 • Windows Server 2012 • Windows Server 2008 • Windows Server 2003
Linux	• CentOS 5、6、7、8（32位或64位） • Ubuntu 9.10~20.10（32位或64位） • Debian 6、7、8、9（32位或64位） • RHEL 5、6、7、8（32位或64位） • Gentoo（32位或64位） • OpenSUSE（32位或64位） • SUSE（32位或64位） • Aliyun Linux

一键自动安装Agent（仅阿里云服务器支持）

执行一键安装前，需确定您的服务器已满足以下条件：

- 服务器为阿里云服务器，非阿里云服务器需进行手动安装。
- 该服务器已安装云助手。云助手安装的相关内容，请参见云助手。
- ECS服务器在支持一键安装功能的地域内。具体地域信息，请参见一键安装功能支持的地域。
- 服务器已在运行中。
- 网络已正常连接。
- 如果您的服务器上安装了第三方安全软件，云安全中心Agent可能无法正常安装。在安装Agent前，请确认您的服务器上是否存在这类安全软件。如果存在，建议您先关闭或卸载该安全软件后，再安装云安全中心Agent。

操作步骤

1. 登录云安全中心控制台，在左侧导航栏，单击**设置**。
2. 在**设置**页面的**安装/卸载插件**页签下，单击**待安装客户端**页签。
3. 在**待安装客户端**页签下的未安装Agent插件的服务器其列表中，单击要安装Agent插件的服务器**操作**列的**安装客户端**，为该服务器安装Agent

   您也可以选中多台服务器，单击左下角**一键安装**，批量安装Agent。
4. 在**安装/卸载插件 > 待安装客户端**页签，定位到待安装服务器，单击**操作**栏的**安装客户端**，为单台服务器安装Agent。
   Agent插件安装完成约5分钟后，您即可在**资产中心**中查看您服务器的**客户端**在线情况：阿里云服务器**客户端**状态将会从**离线**变成**在线**。

> **说明** 一键安装后如果客户端状态显示为**安装失败**并提示**未安装云助手**，请先安装云助手。云助手安装的相关内容，请参见云助手。

在服务器中手动安装Agent

以下情况不支持一键自动安装，必须在您的服务器中手动安装Agent：

- 您的服务器为非阿里云服务器（包括第三方云服务器、IDC服务器）和暂未安装云助手的阿里云服务器。云助手安装的相关内容，请参见云助手。
- 网络类型为经典网络。
- ECS不在支持一键安装功能的地域内。具体地域信息，请参见一键安装功能支持的地域。
- 服务器操作系统为Windows 2019、Windows 2016、Windows 2012、Windows 2008、Windows 2003。
- 通过专线连接、内网通信的非阿里云服务器，需要在服务器*host*文件中添加云安全中心的DNS解析地址。如果未添加DNS解析地址，无法一键自动安装Agent。

  添加云安全中心DNS解析地址的步骤如下：

  i. 通过以下路径找到服务器的*host*文件：
     - Linux系统：*/etc/hosts*
     - Windows系统：*C:\windows\system32\drivers\etc\hosts*

  ii. 将以下DNS解析地址添加到*host*文件中：
     - `106.11.248.209 jsrv.aegis.aliyun.com`
     - `106.11.248.90 update.aegis.aliyun.com`

> **说明**
> - 请不要对无需保护的服务器（例如：线下测试机器、您自己的工作电脑等）安装Agent，否则会消耗对应的授权数。
> - 手动安装Agent前，请确认该服务器已正常运行，并且网络已连通。
> - 建议您不要在*/usr/local/aegis/*的子目录执行Agent安装命令，否则命令运行时会清空这个目录。建议您在服务器的根目录执行该操作。

操作步骤

1. 登录云安全中心控制台，在左侧导航栏，单击**设置**。
2. 在**设置**页面的**安装/卸载插件**页签下，单击**客户端安装指南**页签，查看手动安装Agent插件的命令。
   - 使用默认命令

     客户端安装指南页面查为您提供4条默认命令。如果您无需生成命令镜像或不需要应用该命令的服务器自动添加到指定的资产分组中，您可以按照自己服务器和操作系统类型选择对应的安装命令，直接使用该默认命令安装到服务器中。
   - 新增安装命令

     如果您需要生成命令镜像或需要将应用该命令的服务器自动添加到指定的资产分组中，你可以通过新增安装命令，手动创建安装Agent的命令。

> **说明** 您可以通过新增安装命令，实现以下两个目的：
>
> - 创建命令镜像，使用该命令镜像批量预装到服务器中。
> - 为新增的安装命令绑定资产分组，后续使用该命令安装Agent插件的服务器会自动加到该资产分组中。

单击**新增安装命令**，在**新增安装命令**对话框中，配置命令的基本信息，然后单击**确定**生成一条Agent安装命令，并复制该命令。

配置项	说明
过期时间	该命令过期的时间。
服务商	服务器所属的服务提供商。
默认分组	该安装命令生效的服务器分组。
操作系统	命令应用的操作系统类型。可选操作系统类型为Windows、Linux、Windows 2003。
制作镜像系统	是否需要制作镜像文件。可选项说明： - 选择**是**：云安全中心会创建命令的镜像文件，您无需在每台服务器中重复执行Agent安装命令，就可批量预装到其他服务器中。 > **说明** 在服务器中运行了该镜像命令后，将仅下载Agent文件，不启动Agent进程。如果您需要对该服务器进行防护，必须重启服务器，Agent进程才能启动，该服务器才能受到云安全中心的防护。 - 选择**否**：直接生成安装命令。

您可以在**客户端安装指南**页签中，查看已创建的Agent安装命令。

3. 使用有管理员权限的账号登录需要安装Agent的服务器，根据服务器的操作系统类型，执行安装命令。
   - **Windows系统**：在命令提示符（CMD）中，执行已复制的安装命令，即可完成Agent文件的下载及安装。
   - **Linux系统**：在服务器的命令行界面，执行已复制的安装命令，即可完成Agent文件的下载及安装。

> **注意** 该安装命令执行过程中会从阿里云站点下载最新的Agent插件，如您使用的是非阿里云服务器请确认您的服务器已连接公网。

Agent插件安装完成约五分钟后，您即可在云安全中心管理控制台中查看您服务器的**客户端**在线情况：

- 阿里云服务器**客户端**会从**离线**变成**在线**。
- 非阿里云服务器将会被添加至您的服务器列表中。

> **注意** 由于网络环境的原因，非阿里云服务器安装Agent后服务器信息同步可能会出现延迟，导致云安全中心控制台**资产中心**页面不会及时展示服务器的信息。这种情况下，您需要在**资产中心**的**服务器**页签下单击**同步最新资产**，将该服务器的信息手动同步到资产中心。

卸载Agent

如果您无需再使用云安全中心保护您的服务器，您可以单击页面右上角的**卸载客户端**，卸载Agent。详细内容，请参见卸载Agent。第三方云服务器和IDC服务器都必须到服务器中手动卸载。

> 注意
>
> - 如果您是在服务器上手动卸载Agent（即服务器管理员通过应用程序在服务器上卸载Agent等方式），执行卸载操作前，您必须先在云安全中心控制台的**设置**页面关闭服务器的客户端自保护开关，才能成功卸载Agent。关闭客户端自保护开关的具体步骤，请参见客户端自保护。
> - 如果您是在云安全中心控制台上卸载Agent，无需关闭服务器的客户端自保护状态，可直接卸载Agent。

2.4. 资产管理规则

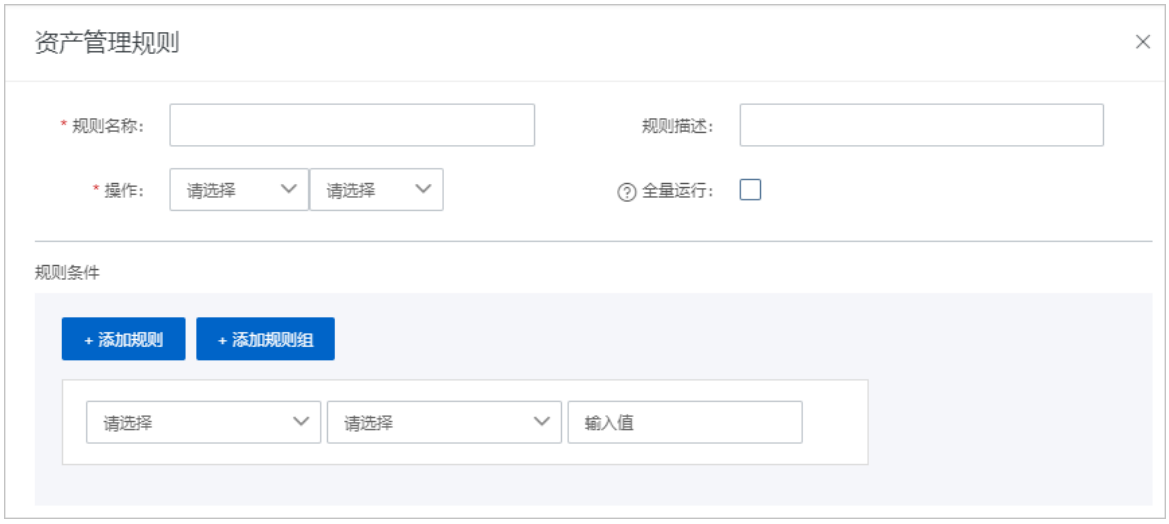
使用云安全中心的资产管理规则功能，可以通过设置不同资产管理规则的条件，将满足同一条件的服务器进行分组或者标签管理，帮助您提升资产管理的效率。本文介绍如何使用资产管理规则功能。

限制条件

创建资产管理规则时，选择的分组或者标签为已有分组或标签，资产管理规则执行时不会影响该分组或标签下已有的服务器，只对不在该分组或标签下的服务器生效。如果您不想使用已有的分组或者标签，您可以新建分组或标签，在创建资产规则是选择新建的分组或标签。创建分组或标签的具体操作，请参见管理服务器的分组、重要性及标签、管理资产标签。

创建资产管理规则

1. 登录云安全中心控制台。
2. 在左侧导航栏中单击**设置**。
3. 在**设置**页面，单击**多云配置管理**页签。
4. 在**多云配置管理**页签下，单击**资产管理规则**页签。
5. 在**资产管理规则**页签下，单击**新增规则**。
6. 在**资产管理规则**面板上，进行如下配置。



配置项说明如下：

配置项	说明
规则名称	设置该资产管理规则的名称。
规则描述	设置该资产管理规则的描述。
操作	设置规则的类型。支持选择： ○ **分组**。规则类型选择分组时，执行该规则时会对满足条件的服务器自动进行分组管理。 ○ **标签**。规则类型选择标签时，执该规则时会对满足条件的服务器自动进行标签管理。
全量运行	设置该资产管理规则对那些服务器生效。 ○ 选中此配置项表示该规则对现有服务器生效。 ○ 未选中此配置项表示该规则对后续新增的服务器生效。
规则条件	设置资产管理规则的规则条件。支持通过规则或者规则组来设置规则条件。

7. 单击**确定**。
   您可以在资产管理规则列表中查看您新建的资产管理规则。资产管理规则执行后，您可以在**资产中心**的**服务器**页签下的**服务器组**或者**标签**下查看规则执行的结果，满足资产管理规则条件的服务器将被移动到对应的服务器分组或者标签下。

修改资产管理规则

1. 登录云安全中心控制台。
2. 在左侧导航栏中单击**设置**。
3. 在**多云配置管理**页签下，单击**资产管理规则**页签。
4. 在**多云配置管理**页签下的资产管理规则列表中，定位到您要修改的资产管理规则。
5. 单击操作列的**修改**。
   您可以对该资产管理规则的**规则名称**、**规则描述**、**操作**、**全量运行**、**规则条件**进行修改。
6. 单击**确定**。
   云安全中心将按照您修改后的资产管理规则管理资产。

删除资产管理规则

如果不再需要某个资产管理规则，您可以删除该规则。具体操作如下：

1. 登录云安全中心控制台。
2. 在左侧导航栏中单击**设置**。
3. 在**多云配置管理**页签下，单击**资产管理规则**页签。
4. 在**多云配置管理**页签下的资产管理规则列表中，定位到您要删除的资产管理规则。
5. 单击操作列的**删除**。
6. 在弹出的确认对话框中单击**确认**。

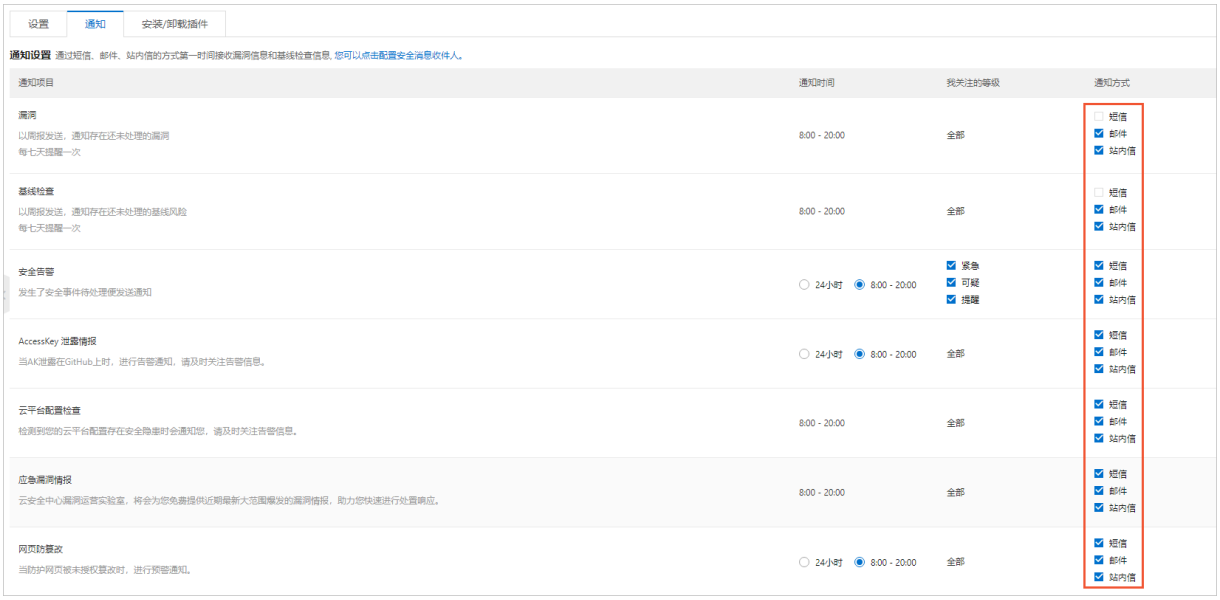
> **说明** 删除资产管理规则不会影响此资产管理规则执行已产生的分组或者标签。

2.5. 常见问题

本文介绍了使用云安全中心设置功能的常见问题。

告警通知邮箱的接收人可以在哪里修改？

云安全中心支持通过短信、邮件、站内信的方式第一时间向您发送漏洞、基线检查、安全告警等安全信息。您可以执行以下步骤修改消息接收人或消息接收人的基本信息：



1. 登录阿里云消息中心。
2. 在**基本接收管理**页面定位到**云盾安全信息通知**，并单击**消息接收人**列下的**修改**。

   消息接收人列为您展示了各消息类型的接收人。
3. 在**修改消息接收人**对话框中修改消息接收人。

您需要选中对应的接收人，只有被选中的接收人才能接收云安全中心为您发送的通知。您可以根据需要执行以下操作：

- 如果您需要新增消息接收人，您可以单击**新增消息接收人**并填写接收人的姓名、邮箱等信息，信息填写完成后单击**确定**。
- 如果要修改已有信息接收人的信息，您需要单击**基本接收管理**页面右上角的**消息接收人管理**修改相应联系人的信息。具体操作，请参见消息接收管理设置。

> **说明**
>
> - 您至少需要设置一位消息接收人。如果您未更改过消息设置，消息接收人默认为您的账号联系人（即您注册账号时填写的联系人）。
> - 未验证过的联系人邮箱和手机号码需要进行验证操作才能正常接收消息。系统将自动发送验证消息到所填手机号和邮箱，您可以根据短信或邮箱中的提示及时进行验证。

4. 单击**保存**。
   该操作完成后，更改后的消息接收人配置会立即生效。

如果设置告警通知时，我没有勾选任何关注等级能收到告警通知吗？

不能。

如果您在安全告警的**我关注的等级**列没有勾选任一等级（如下图所示），云安全中心不会向您发送任何告警通知。这种情况下，您可以在**安全告警处理**页面查看您资产中检测到的安全告警事件。

3.应用市场

3.1. 概述

应用市场展示了云安全中心提供的扩展能力和您已购买的安全产品概况。您可以在应用市场页面申请或开通云安全中心提供的扩展能力，例如：应用白名单、安全大屏、自定义告警、网页防篡改等。

申请或开通云安全中心扩展能力

在云安全中心控制台的**应用市场 > 概况**页面的**云安全中心扩展能力**区域，查看云安全中心提供的扩展能力。

您可以申请或开通以下扩展能力：

- 应用白名单

  应用白名单功能可防止您的服务器上有未经过认证或授权的程序运行，为您提供可信的资产运行环境。目前应用白名单功能处于邀测阶段，您可以单击**应用白名单**区域的**申请**，提交使用白名单功能的申请。申请审批会在5个工作日内完成。

- 安全大屏

  安全大屏为云安全中心基础杀毒版、高级版和企业版提供的增值服务，可从您资产的当前安全情况、外部攻击情况、威胁情况三个维度为您全面展现当前资产的网络安全态势。您可以单击**安全大屏**区域的**开通**，前往云安全中心购买页购买安全大屏服务。

- 自定义告警

  云安全中心支持配置自定义的告警规则，帮助您更全面和深入地获取您服务器中存在的威胁信息。自定义告警功能目前处于公测阶段，您可以单击**自定义告警**区域的**申请**，提交自定义告警开通的申请。完成申请审批一般需要5~7个工作日。

- 网页防篡改

  网页防篡改为云安全中心的增值服务，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。您可以单击**网页防篡改**区域的**开通**，前往云安全中心购买页购买防篡改服务。

查看云盾产品概况

在云安全中心控制台的**安全运营 > 应用市场**页面的**云盾产品**区域，您可以查看已购买的安全产品概况，包括已开通产品购买的实例数量、到期日期等信息。如果需要了解该产品的更多信息，您可以单击需要查看的云产品名称跳转至该产品控制台。

3.2. 合规检查

3.2.1. 等保合规检查

等保合规检查（全称为等级保护合规检查）为您提供了全面覆盖通信网络、区域边界、计算环境和管理中心的网络安全检查。您可以使用该功能检查系统是否符合等保合规要求，及时发现和处理安全风险。本文介绍如何查看等保合规检查结果。

背景信息

- 2019年12月01日起，*网络安全等级保护基本要求（GB/T 22239-2019信息安全技术）*等系列标准正式实施，落实网络安全等级保护制度是每个企业和单位的基本义务和责任。阿里云在确保云平台自身满足基本要求的基础上，提供了等保合规检查功能，帮助您更快速、高效和持续地落实网络安全等级保护制度，提升云上业务系统的安全防护能力。
- 您访问**等保合规检查**页签时，云安全中心会自动执行等保合规检查并为您提供最新的等保合规检查结果。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

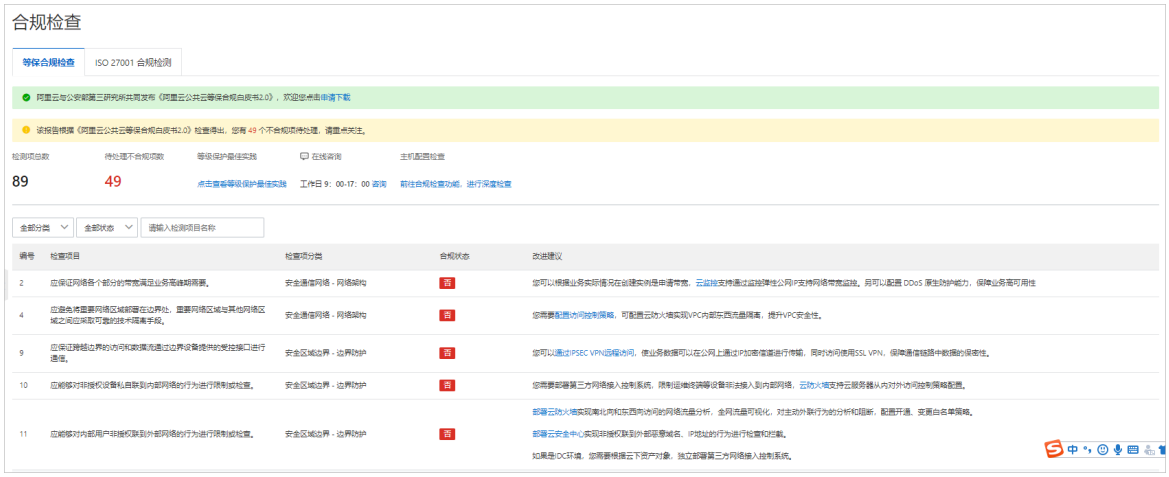
操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**应用市场 > 合规检查**。
3. （可选）在**等保合规检查**页签上方*阿里云公共云等保合规白皮书2.0*提示信息右侧单击**申请下载**，申请下载云安全中心为您提供的等保2.0解决方案材料包。

   在**等保2.0解决方案材料包**页面，请根据提示填写您的信息并提交。您的申请审核通过后（预计2~4个工作日），您的邮箱将会收到等保2.0解决方案材料包。

> **说明** 等保2.0解决方案材料包含以下内容：
>
> - 阿里云安全架构师免费专业指导
> - 等保2.0解决方案PPT
> - 安全产品的销售许可证
> - 阿里云平台等保备案证明
> - 等保测评报告
> - 阿里云公共云等保合规白皮书2.0（介绍阿里云如何助力云服务客户构建基于网络安全等级保护的安全合规体系）

4. 在**等保合规检查**页签，查看检查结果的统计数据。



您可以执行以下操作。

- **查看检测项总数和不合规项数**

  在**检测项总数**和**待处理不合规项数**查看等保合规支持的检测项总数量和不合规项的数量。单击**待处理不合规项数**可直接查看不合规的检查项列表。

- **查看等级保护最佳实践**

  阿里云为您提供了等保合规2.0安全解决方案，可以帮助您顺利通过等保合规2.0的等保测评。您可以单击**点击查看等级保护最佳实践**，了解等保合规2.0安全解决方案的更多信息。

- **等保问题在线咨询**

  单击**在线咨询**右侧的**咨询**，跳转到聊天窗口咨询等保相关问题。咨询时间为工作日09:00~17:00，请您在此时间内进行咨询。

- **主机配置检查**

  单击**前往合规检查功能，进行深度检查**，前往**基线检查**页面，查看并处理您资产中的基线问题。更多信息，请参见查看和处理基线检查结果。

- **搜索指定检测项**

  在搜索框设置检查项分类和是否合规，或输入检测项目名称，查看符合条件的检测项。

5. 处理不合规的检查项目。

   根据**改进建议**下的说明，处理不合规的检查项目。

> **说明** 云安全中心等保合规检查检测您的系统是否具备等保合规检查要求的安全能力，例如访问控制、日志审计等。您在确保具备等保合规检查的能力，并处理完发现的问题后，才可以通过等保测评。等保更多信息请参见等保合规2.0安全解决方案。

3.2.2. ISO 27001合规检测

ISO 27001是国际信息安全管理体系的认证标准。企业通过ISO 27001认证，表示国际权威组织认可企业的信息安全体系，证明企业有能力为客户提供安全可靠的信息服务。云安全中心提供ISO 27001合规检测功能，可以帮助您通过ISO 27001认证。本文介绍ISO 27001合规检测支持的检测项以及如何查看检测结果。

背景信息

您无需手动执行ISO 27001合规检测，每次访问**ISO 27001合规检测**页面时，云安全中心会自动执行ISO 27001合规检测并为您提供最新的ISO 27001合规检测结果。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

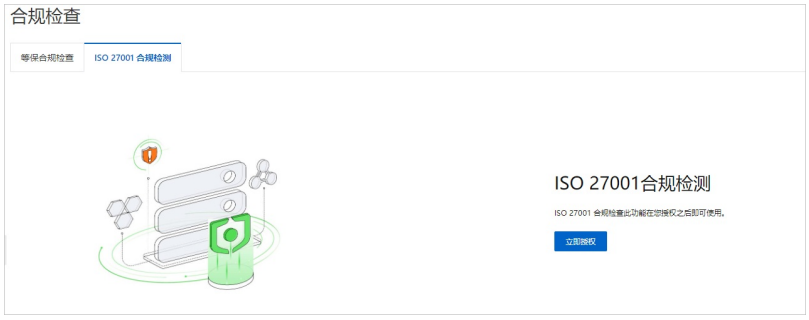
支持的检测项

条款	章节
A.8 资产管理	A.8.1.1 资产清单
	A.8.1.2 资产所有权
	A.8.2.1 信息的分级
	A.8.2.2 信息的标记
A.9 访问控制	A.9.1.2 网络和网络服务的访问
	A.9.2.1 用户注册及注销
	A.9.2.2 用户访问开通
	A.9.2.3 特殊访问权限管理
	A.9.2.4 用户秘密鉴别信息管理
	A.9.2.5 用户访问权限的复查
	A.9.2.6 撤销或调整访问权限

条款	章节
	A.9.4.1 信息访问限制
	A.9.4.2 安全登录规程
	A.9.4.3 口令管理系统
	A.9.4.4 特殊权限实用工具软件的使用
A.10 密码学	A.10.1.1 使用密码控制的策略
	A.10.1.2 密钥管理
A.12 操作安全	A.12.1.3 容量管理
	A.12.2.1 控制恶意软件
	A.12.3.1 信息备份
	A.12.4.1 事态记录
	A.12.4.2 日志信息的保护
	A.12.4.3 管理员和操作员日志
	A.12.6.1 技术脆弱性的控制
	A.12.7.1 信息系统审计控制措施
A.13 通信安全	A.13.1.1 网络控制
	A.13.1.2 网络服务安全
	A.13.1.3 网络隔离
A.16 信息安全事件管理	A.16.1.4 评估和确定信息安全事态
A.17 业务连续性管理的信息安全方面	A.17.2.1 信息处理设施的可用性

查看ISO 27001合规检测结果

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**应用市场 > 合规检查**。
3. 在**合规检查**页面，单击**ISO 27001合规检测**页签。
4. 单击**立即授权**。



首次使用云安全中心时，云安全中心需要获取您的授权后，才能访问您的云资源并进行ISO 27001合规检测。

完成授权后，您将在控制台看到**授权成功**的提示信息。

5. 在**ISO 27001合规检测**页签，查看检查结果的统计数据和检查结果列表。

您可以执行以下操作：

- **查看检测项总数和不合规项数**

  在**检测项总数**和**待处理不合规项数**区域，查看ISO 27001合规检测支持的检测项总数量和不合规项的总数量。

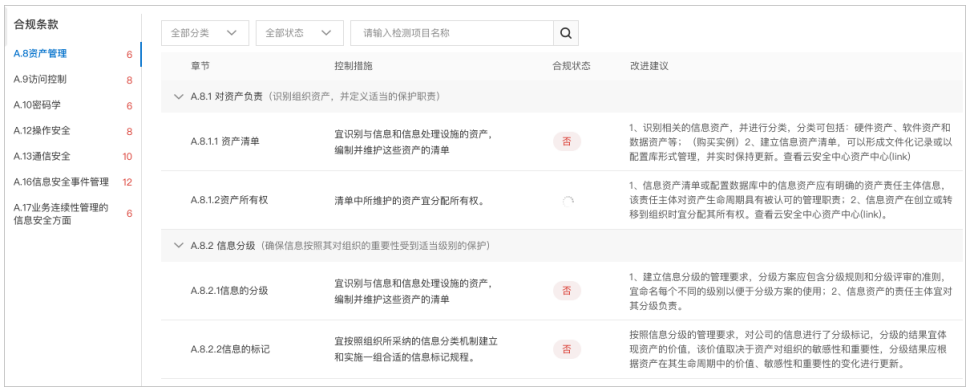
- **查看合规、不合规或检测中的检查项**

  在搜索框将搜索条件设置为合规、不合规或检测中，可查看合规、不合规或检测中的检测项列表。

6. 处理不合规的检查项目。

   根据**改进建议**下的说明，处理不合规的检查项目。

   云安全中心ISO 27001合规检测可以检测您的系统是否符合ISO 27001认证的要求，例如资产管理、访问控制、密码学、操作安全等。建议您及时处理不合规的检测项。



3.3. 安全组检查

安全组规则设置不当可能会引起严重的安全事故。安全组检查功能为您检查ECS服务器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。本文介绍如何在云安全中心控制台使用安全组检查功能。

背景信息

安全组是一种虚拟防火墙，仅适用于阿里云ECS服务器。安全组检查功能支持对普通安全组和企业级安全组进行安全检查。安全组更多信息，请参见安全组概述。

安全组检查功能由云防火墙提供，您可前往云防火墙控制台体验更多网络安全功能。安全组检查支持的检查项详情，请参见安全组配置检查项列表。

版本限制

云安全中心所有版本用户都可使用该功能。各版本支持的功能详情，请参见功能特性。

操作步骤

1. 登录云安全中心控制台。
2. 在左侧导航栏，选择**应用市场 > 安全组检查**。
3. （可选）首次使用安全组检查功能，请在**云防火墙为您提供安全组配置检查服务**对话框中，单击**授权并检查**。
4. 在**安全组检查**页面，单击**获取最新检查结果**。

   安全组检查预计需要1~5分钟，请您耐心等待。

> **说明** 此处获取的最新检查结果只是针对安全规则的静态分析得出，可能无法覆盖全部的端口风险情况。您可以在云防火墙互联网访问活动页面查看端口相关的全部检查结果，了解端口的实际暴露情况。

5. 在**检查结果详情**区域，查看检测出安全风险的规则详细信息。

您可以查看规则**风险等级**、**检查项**名称、**风险安全组/服务器数**和**检查项状态**信息。

> **说明** 检查项默认为开启状态。如果需要关闭某个检查项，您可以单击该检查项的**检查项状态**列下的图标，关闭该检查项。检查项关闭后，云防火墙将不会对该检查项中的安全风险进行检查。

6. 修复高危安全组规则。
   i. 定位到指定检查项，单击其**操作**列下的**修复详情**。
   您也可以单击指定检查项**风险安全组数/服务器数**下的数字跳转至**安全组修复详情**页面。
   ii. 在**安全组修复详情**页面，定位到需要修复的安全组，单击其**操作**列下的**去安全组修复**。

安全组规则设置不当可能会引起严重的安全事故。**安全组修复详情**页面针对风险安全组提供了**修复建议**，您需要根据**修复建议**尽快修改存在风险的安全组规则。

- 如果您是云防火墙高级版及以上版本用户，您将跳转到**安全组列表**页面。您需要根据**修复建议**手动修复高危安全组规则。更多信息，请参见修改安全组规则。
- 如果您是云防火墙免费版用户，您需要执行子步骤III中的内容。

iii. （可选）在**推荐使用云防火墙智能修复**对话框，单击**立即升级**或**去安全组手动修复**。
可选择的修复方式说明如下：

- **立即升级**：购买云防火墙高级版本，使用云防火墙提供的**安全组配置检查**功能修复安全组高危规则。云防火墙可统一管理安全组和公网IP访问控制策略，及时缩小安全风险暴露面，提高安全管理效率。推荐您使用该方式。
- **去安全组手动修复**：跳转到**安全组列表**页面，手动修复高危安全组规则。更多信息，请参见修改安全组规则。

安全组配置检查项列表

检查项名称	安全风险	修复建议
Linux远程运维端口暴露	22端口允许任意IP访问，关联的Linux服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器22端口的访问。如果业务需要访问服务器22端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息，请参见什么是堡垒机。
Windows远程运维端口暴露	3389端口允许任意IP访问，关联的Windows服务器可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3389端口的访问。如果业务需要访问服务器3389端口，建议您限制可访问该端口的公网IP，或使用堡垒机进行远程运维。更多信息，请参见什么是堡垒机。

检查项名称	安全风险	修复建议
DB2远程运维端口暴露	50000端口允许任意IP访问，关联的DB2数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50000端口的访问。
ECS加入的安全组数量过多	ECS实例加入了3个及以上安全组，会增加运维难度，提高错误配置风险。	建议一台ECS实例加入的安全组数量小于等于2个。更多信息，请参见安全组概述。
Elasticsearch远程运维端口暴露	9200、9300端口允许任意IP访问，关联的Elasticsearch可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器9200、9300端口的访问。
Hadoop YARN远程运维端口暴露	8088端口允许任意IP访问，关联的Hadoop YRAN可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器8088端口的访问。
Hadoop远程运维端口暴露	50070、50030端口允许任意IP访问，关联的Hadoop可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器50070、50030端口的访问。
MongoDB远程运维端口暴露	27017端口允许任意IP访问，关联的Mongo DB数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器27017端口的访问。
MySQL远程运维端口暴露	3306端口允许任意IP访问，关联的MySQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器3306端口的访问。
Oracle远程运维端口暴露	1521端口允许任意IP访问，关联的Oracle数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器1521端口的访问。
PostgreSQL远程运维端口暴露	5432端口允许任意IP访问，关联的PostgreSQL数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器5432端口的访问。
Redis远程运维端口暴露	6379端口允许任意IP访问，关联的Redis数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器6379端口的访问。
SQL Server远程运维端口暴露	1433端口允许任意IP访问，关联的SQL Sever数据库可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器1433端口的访问。
Spark远程运维端口暴露	6066端口允许任意IP访问，关联的Spark可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器6066端口的访问。
Splunk远程运维端口暴露	8089、8090端口允许任意IP访问，关联的Splunk可能被暴力破解入侵。	建议您在ECS管理控制台的**安全组列表**页面配置拒绝公网IP对服务器8089、8090端口的访问。
访问源过度开放	检查到安全组配置为入方向允许任意IP访问任意端口，关联服务器被入侵风险极大。	建议仅开放业务所需端口，并限制访问源IP范围。

4.常见问题

本文档介绍了阿里云云安全中心各类常见问题和对应的解决方案。

云安全中心按照以下分类为您提供常见问题和解决方案。

新功能动态

功能发布记录

售前常见问题

我已经免费试用过，是否可以再次申请免费试用？

7天免费试用如何开通？

云安全中心是否支持按月购买？

云安全中心各个版本有区别吗？

为什么定价为60元9.5 USD/月，但在购买页面实际显示的金额不止60元9.5 USD？

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？

云安全中心是否可以防护其他厂商提供的云服务器？

线下IDC和其他云服务器如何使用云安全中心？

常见问题

云安全中心能杀毒吗？

漏洞自动修复需要使用云安全中心哪个版本？

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？

安骑士、态势感知和云安全中心的区别

安骑士企业版升级到云安全中心功能说明

购买、续费相关问题

云安全中心提示即将到期续费如何处理？

为什么在云安全中心看不到DDoS攻击的告警数据了？

接入云安全中心

如何查看云安全中心Agent的日志文件

如何在非阿里云服务器中使用云安全中心

不支持一键安装云安全中心Agent的场景

云虚拟主机和轻量级服务器中无法安装云安全中心Agent

安骑士升级到云安全中心后如何授权开通云安全中心功能

Linux实例中手动安装云安全中心的Agent插件时出现“Permission denied”报错

控制台操作问题

控制台提示“token校验失败”

RAM用户登录时提示“当前操作未被授权”

进入控制台存在浏览器兼容性问题

实例的最大授权数小于当前拥有的实例总数量

安全评分相关问题

安全评分中处理事件优先级是怎样的？

企业版、旗舰版、免费版、防病毒版和高级版的安全评分扣分项有什么不同？

如何开通防暴力破解功能？

常见告警处理方法有哪些？

修改漏洞关注等级与提高安全评分有什么关系？

修改基线关注等级与提高安全评分有什么关系？

解绑、释放资产相关问题

如何解绑（释放）非阿里云资产？

云安全中心如何解绑阿里云ECS服务器？

病毒防御相关问题

怎么购买防勒索容量？

防勒索是什么功能？为什么要单独付费？

购买病毒防御后，之前购买的其他服务是否受影响？

云安全中心防勒索功能和阿里云混合云备份服务有什么关系？

怎么使用云安全中心病毒防御功能？

购买防勒索数据保护容量后数据备份会自动启动吗？

防勒索客户端占用服务器CPU或内存资源过多怎么办？

网页防篡改相关问题

Linux软件漏洞问题

漏洞修复问题

漏洞扫描问题

基线检查问题

安全告警问题

高危敏感信息泄露后处理方法

云安全中心基础版处理网站后门告警

支持线上手动隔离操作的安全告警类型

ECS实例被暴力破解了登录密码

提示异常登录的告警信息时如何在Windows实例中查看登录失败的用户名

如何处理“异常网络连接-主动连接恶意下载源”告警

如何处理“异常网络链接-访问恶意域名”告警

修改SSH服务的默认端口后仍然收到密码暴力破解提示

暴力破解问题

常见问题

被暴力破解成功之后该怎么处理？

为什么修改22端口后仍然出现密码暴力破解提示？

为什么安全组或者防火墙规则已经屏蔽了RDP服务的3389端口，但RDP还是有被暴力破解的记录？

ECS登录弱口令是指系统层面的RDP或者SSH扫描吗？

如何处理SSH、RDP远程登录被拦截？

AK泄露检测问题

高危敏感信息泄露处置方案

通知

告警通知邮箱的接收人可以在哪里修改？

5.历史文档

5.1. 功能发布记录（2022年之前）

本文介绍了云安全中心产品功能发布的动态。

更多阿里云最新产品动态，请订阅云产品动态。

2021年12月

发布时间	动态说明	影响的版本	相关文档
2021-12-23	多账号安全管控功能开放到所有版本都可以使用。	所有版本	多账号安全管控
2021-12-23	服务器防勒索自定义策略的防护目录最多新增8条。	防病毒版、高级版、企业版、旗舰版	创建防护策略
2021-12-15	服务器防勒索功能的备份数据保留时间支持自定义时间。	防病毒版、高级版、企业版、旗舰版	创建防护策略
2021-12-15	漏洞一键扫描功能取消了对扫描基线问题和云平台配置的检测。	高级版、企业版、旗舰版	扫描漏洞
2021-12-01	容器防火墙功能更新。防御规则支持设置对访问流量放行、告警或拦截。端口号支持8组端口范围等。	旗舰版	新增网络对象、创建防御规则、防御状态与规则管理、查看防护状态、集群防御规则可拦截状态异常排查
2021-12-01	容器网络拓扑功能全面更新。 • 集群、应用拓扑图新增下载功能。 • 拓扑数据默认搜索时间范围由原来的1天变更为7天。 • 对于超大集群，进入集群应用拓扑图为默认收起状态 。 • 集群应用拓扑图新增仅显示有连接的应用、显示端口信息、隐藏连接线、隐藏或显示、收起或展开的功能。 • 集群面板上支持查看集群信息、集群风险、镜像信息和防护策略。	旗舰版	容器网络拓扑

2021年11月

发布时间	动态说明	影响的版本	相关文档
2021-11-26	多账号安全管控功能新增对成员账号下的资产的客户端、漏洞扫描、基线检查策略进行配置。	旗舰版、企业版	多账号安全管控
2021-11-25	漏洞管理设置取消**扫描方式**配置项。	所有版本	漏洞管理设置
2021-11-25	服务器防勒索功能在创建防勒索策略时，取消每个策略仅可添加100台服务器的限制。	所有版本	创建防护策略
2021-11-19	云蜜罐功能支持的地域更新，已支持全部地域。	旗舰版、企业版	云蜜罐（公测中）
2021-11-04	镜像安全扫描的扫描配置新增**漏洞保留时长**配置项，您可按照业务需要通过该配置项，设置漏洞扫描结果的保留时长。漏洞扫描结果在超过保留时长时才会自动删除。	旗舰版、企业版	执行镜像安全扫描

2021年10月

发布时间	动态说明	影响的版本	相关文档
2021-10-30	服务器防勒索支持的服务器的操作系统版本更新。数据库防勒索支持的地域、支持的数据库版本及操作系统版本更新。	防病毒版、高级版、企业版、旗舰版	防勒索概述
2021-10-30	服务器防勒索功能更新，1.0策略不再支持编辑，1.0策略可一键升级至2.0策略。	防病毒版、高级版、企业版、旗舰版	创建防护策略
2021-10-21	通知功能新增病毒扫描通知和日志超量两个通知项。	所有版本	通知

发布时间	动态说明	影响的版本	相关文档
2021-10-19	多账号安全管控新增添加委派管理员功能。您可为云安全中心添加委派管理员账号，委派管理员账号将获得企业管理账号的授权，获取在云安全中心中访问和管理资源目录中的组织、成员信息以及查看管控账号安全风险的权限。	旗舰版、企业版	多账号安全管控

2021年09月

发布时间	动态说明	影响的版本	相关文档
2021-09-29	防病毒版一键扫描漏洞的支持扫描项修改为与免费版相同。	防病毒版	扫描漏洞
2021-09-16	资产指纹列表中增加进程PID信息。	所有版本	查看服务器信息
2021-09-06	资产中心新增客户端排查功能。当云安全中心客户端出现离线、安装或卸载失败、进程CPU占有率高等问题时，可以使用客户端问题排查功能进行排查。	所有版本	客户端问题排查
2021-09-06	新加坡中心增加AK泄漏和云产品基线两个功能。	所有版本	AK泄露检测、云平台配置检查概述
2021-09-06	恶意行为防御功能发布。可使用恶意行为防御功能根据业务需要启用、停用某个系统防御规则以及管理该规则中的资产。	旗舰版、企业版	恶意行为防御
2021-09-06	基线检查策略新增支持添加自定义策略功能。使用此功能可根据业务需求自定义基线检查策略。	高级版、企业版、旗舰版	无
2021-09-06	资产管理规则新增支持用户自定义规则配置主机分组和标签。	所有版本	资产管理规则

2021年08月

发布时间	动态说明	影响的版本	相关文档
2021-08-19	数据库防勒索功能发布。支持为安装在阿里云ECS的MySQL数据库、Oracle数据库和SQL Server数据库创建勒索病毒的防护策略。	所有付费版本	• 创建防护策略 • 预检数据库 • 管理防护策略 • 创建恢复任务
2021-08-12	镜像漏洞扫描的漏洞列表支持导出。	旗舰版	查看镜像安全扫描结果
2021-08-12	主动防御新增恶意行为防御功能。支持针对不同的恶意防护规则选择需要防护的服务器。	企业版	无

2021年07月

发布时间	动态说明	影响的版本	相关文档
2021-07-22	支持Docker Hub镜像扫描。可监控Docker Hub中所有镜像的安全态势，免费为您提供基础镜像的安全情报。	免费版	无
2021-07-22	支持容器南北向网络（即容器与互联网流量）连接状态的可视化展示。	旗舰版	无
2021-07-22	混合云场景支持腾讯云资产、IDC资产接入。	免费版	概述

2021年05月

发布时间	动态说明	影响的版本	相关文档
2021-05-21	支持容器防火墙。	旗舰版	新增网络对象
2021-05-13	攻击详情列表新增**端口**列。攻击类型为**SSH暴力破解**时，将显示被暴力破解的端口号。	企业版、旗舰版	攻击分析

2021年04月

发布时间	动态说明	影响的版本	相关文档
2021-04-25	发布云安全中心免费版简介文档，为您提供免费版的详细介绍和使用指导。	免费版	云安全中心免费版简介

发布时间	动态说明	影响的版本	相关文档
2021-04-22	存在弱口令风险的资产，支持在该资产的暴露分析链路图中展示弱口令风险图标。	企业版、旗舰版	资产暴露分析
2021-04-22	Linux软件漏洞详情页新增**选择全部**按钮，使用该按钮可以一次性选择所有存在该漏洞的资产，为您提升处理漏洞的效率。	所有版本	Linux软件漏洞
2021-04-15	安全报告中应用漏洞列表支持展示软件成分分析类型的漏洞。	企业版、旗舰版	安全报告
2021-04-08	资产暴露分析功能进行了以下使用体验优化： • 在资产暴露分析的**网关资产**面板，支持单击网关资产名称跳转至对应资产详情页。 • 在资产暴露分析的**暴露端口**面板，支持单击暴露端口名称筛选存在该暴露端口的资产列表。 • 在资产暴露分析的**暴露组件**面板，支持单击暴露组件名称筛选存在该暴露组件的资产列表。 • 暴露资产的详情页面，支持单击安全组ID跳转至安全组配置页面。	企业版、旗舰版	资产暴露分析
2021-04-08	资产中心**容器**页签新增**存在风险的镜像**功能项。	所有版本	查看容器安全状态
2021-04-01	网页防篡改防护模式支持设置**告警模式**或**拦截模式**。	所有付费版本	启用网页防篡改保护
2021-04-01	云平台配置检查增加检查项：云效-Codeup代码安全。	高级版、企业版、旗舰版	云平台配置检查概述
2021-04-01	**通知**页面新增通知项目：**容器防火墙异常告警通知**和**容器防火墙主动防御通知**。	旗舰版	通知
2021-04-01	在**容器网络拓扑**页面，支持单击页面左侧**集群**、**应用**、**容器**、**节点**、**镜像**跳转至资产中心对应容器资产列表。	旗舰版	容器网络拓扑

2021年03月

发布时间	动态说明	影响的版本	相关文档
2021-03-30	云安全中心支持ISO 27001合规检查功能。	所有版本	ISO 27001合规检测

发布时间	动态说明	影响的版本	相关文档
2021-03-30	在任务中心创建任务时，自定义时间支持设置**起始日期**和**结束日期**。	企业版、旗舰版	创建任务
2021-03-25	**资产暴露分析**页面支持展示暴露资产中检测出的弱口令数据。	企业版、旗舰版	资产暴露分析
2021-03-25	**镜像安全扫描**支持展示近7天扫描量。	高级版、企业版、旗舰版	镜像安全扫描概述
2021-03-25	漏洞修复支持展示云防火墙可以防护的漏洞。针对云防火墙可以防护的漏洞，云安全中心提供**云防火墙虚拟补丁支持防护**联动功能，您可以单击**云防火墙虚拟补丁支持防护**标签跳转到云防火墙控制台修复该漏洞。	所有版本	• Web-CMS漏洞 • 应用漏洞 • 应急漏洞
2021-03-18	防勒索**恢复任务**面板恢复任务列表，增加**恢复目标目录**列。	所有付费版本	创建恢复任务
2021-03-09	**设置**页面**主动防御体验优化**功能仅支持企业版和旗舰版用户使用。	免费版、防病毒版、高级版	主动防御
2021-03-09	支持将**精准防御**类型的告警加入白名单，您可以根据告警实际情况自定义加白规则。此类告警加入白名单后，再次发生此类告警时云安全中心将不再向您发送通知。	所有付费版本	查看和处理告警事件
2021-03-09	**总览**页面增加**关于我们**页签，为您提供云安全中心产品的产品架构、安全能力及安全专家的介绍，欢迎访问。	所有版本	无

2021年02月

发布时间	动态说明	影响的版本	相关文档
2021-02-25	**设置**页面新增自动化告警关联分析功能，支持聚合同类告警，提高您处理安全告警的效率。	防病毒版、高级版、企业版、旗舰版	自动化告警关联分析
2020-02-25	安全评分新增镜像安全扫描范围配置的扣分项。	高级版、企业版、旗舰版	安全评分
2021-02-04	镜像基线检查AccessKey泄露风险项详情中的**检查提示**支持展示发现AK泄露的文件路径，帮助您快速处理AK泄露事件。	高级版、企业版、旗舰版	查看镜像安全扫描结果

发布时间	动态说明	影响的版本	相关文档
2021-02-04	**镜像安全扫描**页面支持展示镜像安全扫描次数的使用情况。	高级版、企业版、旗舰版	镜像安全扫描概述
2021-02-04	镜像安全扫描设置支持选择扫描时间范围，您可以根据实际需要扫描指定时间范围内变更过的镜像。	高级版、企业版、旗舰版	执行镜像安全扫描
2021-02-04	设置安全报告内容时，支持全选所有安全数据。	高级版、企业版、旗舰版	安全报告
2021-02-04	**AccessKey泄露检测**页面支持展示AccessKey信息泄露的来源平台。	所有版本	AK泄露检测

2021年01月

发布时间	动态说明	影响的版本	相关文档
2021-01-28	应急漏洞功能优化： • 未检测到应急漏洞时禁用导出漏洞功能。 • 支持分页展示应急漏洞。	所有版本	应急漏洞
2021-01-26	支持在镜像安全扫描的**扫描配置**面板中管理基线相关配置。	企业版、旗舰版	执行镜像安全扫描
2021-01-26	镜像安全扫描支持接入私有镜像仓库。	企业版、旗舰版	接入镜像仓库
2021-01-21	**总览**页面新增云资产全景（即荷鲁斯之眼功能）的访问入口。	企业版、旗舰版	荷鲁斯之眼
2021-01-21	镜像安全扫描支持修复镜像系统漏洞，帮助您创造更安全的镜像运行环境。 **说明** 目前，仅中国香港地域支持修复镜像系统漏洞。	企业版、旗舰版	查看镜像安全扫描结果
2021-01-21	**总览**页面全新改版，功能分区设置更合理，欢迎体验。	所有版本	总览
2021-01-14	下线Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞和应急漏洞详情页保存筛选条件功能。	所有版本	Linux软件漏洞
2021-01-14	**资产暴露分析**页面支持查看网关资产、暴露端口、暴露组件的列表信息。	企业版、旗舰版	资产暴露分析

发布时间	动态说明	影响的版本	相关文档
2021-01-14	攻击分析支持查看攻击来源的详细信息，并支持跳转到威胁情报控制台查看攻击来源的威胁情报数据。	企业版、旗舰版	攻击分析
2021-01-14	镜像安全扫描支持对容器镜像服务中的默认实例进行安全检测。	企业版、旗舰版	执行镜像安全扫描
2021-01-12	镜像安全扫描支持镜像基线检查功能。	企业版、旗舰版	查看镜像安全扫描结果
2021-01-12	**镜像安全扫描**页面新增风险总览信息。	企业版、旗舰版	镜像安全扫描概述
2021-01-07	基线检查支持自定义弱口令字典，帮助您提升登录口令的安全性。	高级版、企业版、旗舰版	设置基线检查策略

2020年12月

发布时间	动态说明	影响的版本	相关文档
2020-12-30	任务中心支持取消进程状态为等待中的任务。	企业版、旗舰版	创建任务
2020-12-24	云安全中心新增**旗舰版**，为您的服务器和容器资产提供统一安全管控平台、全面的运行时威胁检测、容器网络可视化、镜像安全扫描、漏洞修复、基线检查等功能。	旗舰版	功能特性
2020-12-24	**资产暴露分析**支持导出暴露在公网中的资产列表。	企业版	资产暴露分析
2020-12-24	**设置**页面新增**自适应威胁检测**功能。	所有版本	主动防御
2020-12-17	云安全中心云蜜罐功能公测中，帮助您快速识别并防御云上攻击威胁，欢迎体验。	企业版	云蜜罐（公测中）
2020-12-17	**漏洞修复**页面优化了搜索条件样式，展开了常用搜索项。	所有版本	• 漏洞修复概述 • 安全告警概述
2020-12-17	安全告警详情页透出告警原因和处理建议，方便您获取发生告警的原因并及时处理告警。	所有版本	查看告警自动化关联分析
2020-12-17	镜像安全扫描接入私有镜像仓时支持限制接入速度和网络带宽，保障不影响您的正常业务。	企业版	查看镜像安全扫描结果

发布时间	动态说明	影响的版本	相关文档
2020-12-17	安全评分扣分规则优化，无ECS服务器用户去掉未检测应急漏洞的扣分项。	所有付费版本	安全评分扣分项目表
2020-12-17	应用市场入口调整至左侧导航栏。	所有版本	概述
2020-12-17	等保合规检查、安全组配置检查和数据安全的入口调整至左侧导航栏**应用市场**目录下。	所有版本	• 等保合规检查 • 安全组检查
2020-12-17	云安全中心新增**资产暴露分析**功能，为您暴露在公网中的资产提供统一的管理入口和安全风险统计功能。	企业版	资产暴露分析
2020-12-17	资产中心服务器列表增加资产暴露列，为您展示服务器在公网中的暴露情况。	企业版	查看服务器信息
2020-12-17	云安全中心控制台左下角提供钉钉技术支持群入口。	所有付费版本	无
2020-12-17	病毒防御支持一键处理和按照告警名称批量处理告警事件。	所有付费版本	病毒防御
2020-12-17	病毒防御一键扫描功能支持选择资产分组下的部分服务器执行病毒扫描。	所有付费版本	病毒防御
2020-12-17	**总览**页面支持按月自动续费。	所有付费版本	总览

2020年11月

发布时间	动态说明	影响的版本	相关文档
2020-11-26	**漏洞修复**和**安全告警处理**页面优化了搜索条件格式。	所有版本	• 漏洞修复概述 • 安全告警概述
2020-11-26	应急漏洞详情页支持按照资产分组筛选受影响资产。	所有版本	应急漏洞
2020-11-26	**设置**页面新增**主动防御体验优化**能力，帮助您提升主动防御的体验和质量。	所有版本	主动防御
2020-11-26	安全评分新增K8s威胁检测配置的扣分项。	企业版	安全评分扣分项目表
2020-11-19	资产指纹调查支持一键立即采集所有资产的最新指纹数据。	企业版	资产指纹调查
2020-11-12	安全评分新增病毒查杀周期扫描配置的扣分项。	所有付费版本	安全评分扣分项目表

发布时间	动态说明	影响的版本	相关文档
2020-11-09	云安全中心已接入阿里云双11上云狂欢节，欢迎访问安全分会场获取更多产品优惠。	所有版本	无

2020年10月

发布时间	动态说明	影响的版本	相关文档
2020-10-26	云安全推出**仅采购增值服务**版本，基础版用户可以直接采购所需的增值服务，体验更灵活的功能搭配。	仅采购增值服务	购买云安全中心
2020-10-22	防勒索功能入口调整至**主动防御**目录下，您可以直接在左侧导航栏访问**通用防勒索解决方案**页面。	防病毒版、高级版、企业版	防勒索概述
2020-10-22	**安全告警处理**页面优化容器相关资产的展示方式，受影响资产提供容器组、应用、集群和服务器信息。	企业版	安全告警概述
2020-10-22	**资产指纹调查**页面的**中间件**页签删除了重复的**名称**列。	企业版	查看资产指纹数据
2020-10-22	漏洞修复在修复进度为99%时，增加提示信息：由于该补丁较大，修复所需时间较长，请您耐心等待。为您提供更好的漏洞修复体验。	高级版、企业版	Linux软件漏洞
2020-10-22	执行忽略漏洞操作后，支持查看忽略漏洞时填写的备注信息，方便您管理已忽略的漏洞。	高级版、企业版	
2020-10-22	镜像安全扫描功能在漏洞详情页面提供漏洞或恶意样本的**首次/最新扫描时间**帮助您了解镜像漏洞的更多详细信息。	企业版	查看镜像安全扫描结果
2020-10-22	镜像安全扫描支持接入私有镜像仓库。私有镜像仓库接入后，云安全中心可以深度检测您的私有镜像仓库中的安全漏洞和恶意样本，为您的私有镜像提供安全可信的运行环境。	企业版	接入镜像仓库
2020-10-22	镜像安全立即扫描功能支持选择镜像类型进行安全检测，您可以选择容器镜像服务中的镜像和私有镜像进行安全检测。	企业版	执行镜像安全扫描
2020-10-15	资产中心**容器**页签支持展示您资产中的所有应用、存在风险的应用、集群和命名空间信息。	所有版本	查看容器安全状态

发布时间	动态说明	影响的版本	相关文档
2020-10-15	漏洞修复功能支持对部分Linux和Windows漏洞修复进行前置检查。例如因为Windows Update服务正在运行中而无法修复漏洞时，在修复按钮处提供漏洞无法修复原因和处理方法的提示信息，并禁用修复按钮。	高级版、企业版	• Linux软件漏洞 • Windows系统漏洞
2020-10-15	云安全中心支持周期性扫描应用漏洞中扫描方式为**软件成分分析**的漏洞。	企业版	漏洞管理设置

2020年09月

发布时间	动态说明	影响的版本	相关文档
2020-09-25	**通知**页面增加配置安全消息接收人的链接，方便您快速跳转到消息接收人修改页面。	所有版本	通知
2020-09-25	**客户端安装指南**页面非阿里云Windows服务器地域增加**命令有效期**信息。	所有版本	安装或卸载插件
2020-09-25	控制台总览页面增加到新功能发布记录的入口，方便您了解和使用云安全中心发布的最新功能。	所有版本	总览
2020-09-25	仅支持高级版和企业版在**漏洞管理设置**页面选择应急漏洞扫描周期。	高级版、企业版	漏洞管理设置
2020-09-25	批量修复Windows 2008服务器上的漏洞会导致服务器无法启用，云安全中心已禁用Windows 2008服务器漏洞的批量修复功能，并在修复按钮处提供修复说明。	高级版、企业版	Windows系统漏洞
2020-09-25	云安全中心在异地登录告警详情页提供查看当前告警相关日志的入口，您可以单击**日志分析**跳转到**日志分析**页面，查看该告警的相关日志。	所有付费版本	查看和处理告警事件
2020-09-24	云安全中心下线RDS SQL注入威胁检测功能。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。	企业版	【下线通知】2020年09月24日下线RDS SQL注入威胁检测
2020-09-22	病毒防御功能支持配置病毒扫描周期。您可以为指定服务器自定义病毒扫描周期，云安全中心会根据您设置的周期自动扫描指定服务器中是否存在病毒。	所有版本	病毒防御

发布时间	动态说明	影响的版本	相关文档
2020-09-22	安全镜像扫描功能支持配置镜像漏洞扫描周期。您可以自定义镜像漏洞扫描周期，云安全中心会根据您设置的周期自动扫描镜像漏洞。	企业版	查看镜像安全扫描结果
2020-09-22	漏洞管理设置支持配置应急漏洞扫描周期。您可以自定义应急漏洞扫描周期，云安全中心会根据您设置的周期自动扫描应急漏洞。	高级版、企业版	漏洞管理设置
2020-09-22	**设置**页面主动防御地域支持开启**恶意网络行为防御**能力，帮助您管理需要拦截恶意网络行为的服务器。	所有付费版本	主动防御
2020-09-16	**设置**页面病毒查杀功能升级为**主动防御**，增加防病毒、防勒索（诱饵捕获）和网站后门连接防御开关，帮助您管理防病毒和恶意网络行为防御生效的服务器。	所有付费版本	主动防御
2020-09-16	在您资产详情的漏洞页面，批量修复Linux软件漏洞时，不支持选择需要手动升级才能修复的漏洞。在**漏洞修复**页面进行批量修复漏洞时，云安全中心会自动忽略需要手动升级才能修复的漏洞，帮助您提高修复漏洞的效率。	高级版、企业版	Linux软件漏洞
2020-09-03	防勒索数据备份支持的地域新增西南1（成都）、美国（弗吉尼亚）和印度（孟买）。	所有付费版本	防勒索概述
2020-09-03	防勒索支持批量安装、卸载防勒索客户端和删除防护策略下的服务器，提升您同时管理多台服务器上防勒索客户端的效率。	所有付费版本	创建防护策略
2020-09-03	单个勒索防护策略最多支持添加100台服务器，防止单个勒索防护策略下添加过多服务器增加管理难度。	所有付费版本	创建防护策略
2020-09-03	应急漏洞支持通过检测方式（版本检测、网络扫描）筛选指定类型的应急漏洞列表，方便您查看并修复通过软件版本或网络扫描检测出的应急漏洞。	所有版本	应急漏洞
2020-09-03	基础版用户支持使用一键扫描功能检测应急漏洞，为您提升检测应急漏洞的效率。	免费版	应急漏洞

发布时间	动态说明	影响的版本	相关文档
2020-09-03	**设置**页面**容器威胁检测**变更为**容器K8s威胁检测**，并支持配置**威胁检测**开关，为您提供打开或关闭K8s集群安全风险检测的能力。	企业版	容器K8s威胁检测
2020-09-02	防勒索客户端新增支持的操作系统类型为：Ubuntu 18.04、Ubuntu 20.04和CentOS 8.2。	所有付费版本	防勒索概述

2020年08月

发布时间	动态说明	影响的版本	相关文档
2020-08-27	云平台配置检查支持通过未启用和已启用检查项的统计值查看未启用和已启用的检查项，方便您快速查看未启用或已启用的云平台配置检查项。	高级版、企业版	云平台配置检查概述
2020-08-27	**网站安全报告**页面**存在风险的网站**地域增加网站SSL证书配置状态，提升您管理资产中所有网站证书的效率。	企业版	查看网站信息
2020-08-27	在漏洞修复执行重启操作前增加必要的校验操作。如果需要重启的服务器在修复或验证漏洞中，则不允许进行重启操作，并提供对应的提示信息。为您避免重启操作造成该服务器上其他漏洞修复或验证失败。	高级版、企业版	Linux软件漏洞
2020-08-27	**需紧急修复的漏洞(CVE)**页面的**应急漏洞**页签优化分页展示样式，为您提供更好的漏洞管理体验。	高级版、企业版	漏洞修复概述
2020-08-27	安全评分基线问题模块新增数据库安全风险提示信息，建议您使用阿里云RDS数据库（阿里云RDS数据库有更强的数据库安全防护机制）。	所有版本	总览
2020-08-27	安全告警设置常用登录地支持选择海外地域，方便您将业务涉及到的海外地域设置为常用登录地。	所有版本	安全告警设置
2020-08-26	资产中心**容器**页面全新升级，支持显示容器组和容器的统计数据和风险信息，为您一站式展示容器资产中的安全风险，欢迎体验。	所有版本	查看容器安全状态
2020-08-20	云安全中心针对需升级操作系统才能修复的Linux软件漏洞，在修复时提供升级操作系统的提示，方便您更高效地修复漏洞。	高级版、企业版	Linux软件漏洞

发布时间	动态说明	影响的版本	相关文档
2020-08-19	防勒索客户端版本升级，修复防勒索客户端备份数据时占用CPU或内存资源过高问题，为您提供更好的勒索防护体验。	所有付费版本	创建防护策略
2020-08-13	云安全中心支持镜像应用漏洞扫描功能，帮助您扫描镜像相关中间件上的漏洞并提供修复建议，为您的镜像运行创造更安全的环境。	企业版	查看镜像安全扫描结果
2020-08-13	**安全告警处理**页面新增Web应用威胁检测、恶意脚本检测、DDoS攻击检测能力。	高级版、企业版	安全告警概述
2020-08-13	**安全告警处理**支持归档历史告警数据，您可以随时归档并下载历史告警，方便您回溯历史告警数据。	所有版本	归档告警数据
2020-08-06	支持批量修复Linux软件漏洞和Web-CMS漏洞，帮助您提升漏洞管理效率。	高级版、企业版	• Linux软件漏洞 • Web-CMS漏洞
2020-08-06	基线检查功能开放至高级版，高级版用户可以使用基线检查功能检查服务器的安全配置，欢迎体验。	高级版	基线检查概述
2020-08-06	资产中心服务器页面，新增基线列。方便您查看服务器中存在的基线检查风险项数量。	高级版、企业版	查看服务器信息
2020-08-06	支持设置网页防篡改通知方式。当已防护的网页被非法篡改时，云安全中心将根据您设定的方式，为您发送网页防篡改告警通知。	所有付费版本	通知
2020-08-06	**漏洞管理设置**页面变更**扫描方式**时增加弹框提示，并提供扫描方式应用场景的说明，帮助您更便捷地选择扫描方式。	所有付费版本	漏洞修复概述
2020-08-06	创建勒索防护策略时，推荐策略的**数据备份开始时间**由00：00~05：00变更为00：00~03：00，为您降低数据备份对业务产生的影响。	所有付费版本	创建防护策略
2020-08-06	需紧急修复的漏洞（CVE）中应用漏洞和应急漏洞展示需要修复的漏洞数量，为您提供更好的漏洞修复体验。	高级版、企业版	漏洞修复概述

2020年07月

发布时间	动态说明	影响的版本	相关文档
2020-07-30	需紧急修复的漏洞支持应用漏洞和应急漏洞，帮助您快速查看和修复所有高紧急程度的漏洞。	高级版、企业版	漏洞修复概述
2020-07-30	Windows软件漏洞根据微软官方漏洞等级展示漏洞修复紧急度，方便您查看漏洞等级并修复漏洞。	所有版本	Windows系统漏洞
2020-07-30	安全评分新增网页防篡改扣分项，建议您为网站服务器开启网页防篡改保护，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。	所有付费版本	总览
2020-07-29	资产中心支持网站安全体检功能，并提供网站安全报告，帮助您快速查看网站中存在的安全风险并提供安全建议，避免黑客对网站进行篡改或注入恶意外链，确保网站的正常运行。	企业版	查看网站信息
2020-07-23	计算漏洞修复紧急度得分时增加资产重要性因子。重要资产的重要性因子为1.5，即重要资产上的漏洞修复紧急度得分更高，方便您优先修复重要资产上的漏洞。	所有版本	漏洞修复优先级
2020-07-23	在**安全告警处理**页面，选择已处理告警后，支持筛选状态为**拦截成功**的告警。帮助您一键查看云安全中心已为您自动隔离的常见网络病毒。	所有版本	查看和处理告警事件
2020-07-23	在**任务中心**页面创建自动化批量修复漏洞任务时，最多支持选择修复200个漏洞。	企业版	创建任务
2020-07-16	新增**安全组配置检查**页面，帮助您查看所有存在高危风险的安全组规则，并提供修复建议。	所有版本	安全组检查
2020-07-16	云安全中心支持镜像安全扫描功能，可**一键扫描**您资产中存在的容器镜像漏洞和镜像恶意样本，为您大幅降低使用容器的安全风险。 **说明** 在容器镜像服务购买企业版实例后，才能使用云安全中心镜像安全扫描功能。	企业版	执行镜像安全扫描
2020-07-16	等保合规检查报告全新升级，新增在线咨询入口，为您提供更便捷的咨询服务和更权威的等保合规检查报告。	所有版本	等保合规检查

发布时间	动态说明	影响的版本	相关文档
2020-07-16	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。	所有版本	漏洞管理设置
2020-07-16	漏洞修复页面支持按VPC筛选漏洞，方便您查看并统一处理不同VPC下的漏洞。	所有版本	Linux软件漏洞
2020-07-09	应用市场功能开放至基础版，基础版用户可以申请使用应用白名单、自定义告警等扩展功能，欢迎体验。	免费版	概述
2020-07-09	荷鲁斯之眼Beta功能入口调整至左侧导航栏安全运营下，在左侧导航栏单击**安全运营 > 荷鲁斯之眼Beta**可直接访问该功能。	企业版	荷鲁斯之眼
2020-07-09	安全告警处理支持查看威胁检测模型，威胁检测模型为您提供全链路的威胁检测能力，让黑客无处遁形。	所有版本	安全告警概述
2020-07-09	安全告警支持在告警事件上标记攻击阶段，例如攻击入口、横向移动等，帮助您快速掌握资产受到网络攻击的阶段。	所有版本	查看和处理告警事件
2020-07-09	安全告警加白名单方式支持基于告警详情字段进行加白，例如异常登录告警处理方式选择白名单时，支持将当前登录地加入常用登录地。帮助您更方便地进行加白名单的运维工作。	所有付费版本	查看和处理告警事件

2020年06月

发布时间	动态说明	影响的版本	相关文档
2020-06-23	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。	高级版、企业版	漏洞管理设置
2020-06-11	防勒索支持删除已备份的数据版本，您可以更灵活地管理备份数据，更充分地使用已购买的防勒索容量。	所有付费版本	删除已备份数据
2020-06-11	资产中心支持资产重要性标签功能，帮助您快速标记重要资产、一般资产和测试资产，提升您管理资产的效率。	所有版本	管理资产标签

发布时间	动态说明	影响的版本	相关文档
2020-06-09	云安全中心针对中小企业抵御恶意病毒入侵的迫切需求，推出**防病毒版**，为您提供扫描、告警和一键式处理资产中顽固型病毒的能力。	防病毒版	功能特性
2020-06-04	资产指纹调查支持采集服务器的中间件信息，帮助您更全面地了解资产的运行状态。	企业版	概述
2020-06-04	防勒索防护策略配置参数更新，推荐策略支持从00:00进行数据备份，避开业务高峰，降低数据备份给您业务带来的影响。	所有付费版本	创建防护策略
2020-06-02	安全大屏新增荷鲁斯之眼，为您提供云上资产安全态势全景、网络拓扑和安全风险处理入口，帮助您统一管控云上资产并进行安全运营。	高级版、企业版	荷鲁斯之眼

2020年05月

发布时间	动态说明	影响的版本	相关文档
2020-05-15	安全评分新增防勒索扣分项，建议您为核心服务器开启防勒索保护，提高资产安全评分。	所有付费版本	总览

2020年04月

发布时间	动态说明	影响的版本	相关文档
2020-04-30	支持病毒防御功能，针对挖矿程序等持久化、顽固型病毒提供扫描、告警、深度查杀和数据备份能力，实现逐层递进的纵深式防御。	所有付费版本	病毒防御
2020-04-23	云安全中心支持自定义弱口令规则，您可以基于业务需求，自定义弱口令规则。	所有付费版本	自定义弱口令规则
2020-04-23	支持客户端自保护功能，为您主动拦截恶意的Agent卸载行为，保障云安全中心防御机制稳定运行。	所有付费版本	客户端自保护
2020-04-17	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。	企业版	多账号安全管控
2020-04-03	支持紧急漏洞修复，提供建议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。	所有付费版本	漏洞修复概述

发布时间	动态说明	影响的版本	相关文档
2020-04-02	Agent客户端防护支持基础防护模式、高级防护模式和重保护模式，覆盖多场景下的Agent使用需求，更好地保护您的资产安全。	所有版本	防护模式管理

2020年03月

发布时间	动态说明	影响的版本	相关文档
2020-03-19	支持容器签名，确保容器镜像在未获得可信授权的情况下无法应用，从根本上提升资产的安全性。	企业版	容器签名
2020-03-12	容器镜像漏洞扫描服务公测中，为您提供120,000+历史漏洞的识别能力和最新突发漏洞的检测能力，并提供漏洞修复方案，让漏洞修复更简单。	企业版	查看镜像安全扫描结果
2020-03-06	设置功能调整至控制台左侧导航栏，登录控制台后可一键使用设置功能。	所有版本	概述

2020年02月

发布时间	动态说明	影响的版本	相关文档
2020-02-28	资产中心支持查看容器安全状态，帮助您更全面地分析容器中存在的安全风险，打造更安全的云环境。	所有版本	查看容器安全状态
2020-02-11	基线检查支持将检查项加入白名单。	企业版	加入白名单
2020-02-10	防篡改支持Linux服务器进程加入白名单。	所有付费版本	加入白名单

2020年01月

发布时间	动态说明	影响的版本	相关文档
2020-01-16	病毒自动查杀开关更名为病毒拦截。2020年1月16号后新购用户将默认开启该功能。	所有付费版本	功能介绍
2020-01-13	Linux软件漏洞和Windows系统漏洞支持自动创建快照修复漏洞。创建快照后支持系统回滚，让修复漏洞更安全。	所有付费版本	Linux软件漏洞 Windows系统漏洞
2020-01-08	任务中心功能上线，支持创建自动化批量修复漏洞的任务，帮助您更高效地实施系统安全加固。	企业版	任务中心概述

发布时间	动态说明	影响的版本	相关文档
2020-01-02	云安全中心支持通过设置IP拦截策略达到防止暴力破解的目的。根据业务场景需要您可以创建自定义IP拦截策略，防止您的服务器密码被恶意IP暴力破解。	所有版本	设置IP拦截策略

2019年

发布时间	动态说明	影响的版本	相关文档
2019-12-25	支持在免费试用云安全中心7天后生成试用报告。	免费版	总览
2019-12-20	支持等保合规检查功能。	所有版本	等保合规检查
2019-12-10	支持运行状态下的容器安全威胁检测。	企业版	容器K8s威胁检测
2019-10-17	云安全中心安全告警设置模块新增自定义防暴力破解功能。	所有版本	安全告警设置
2019-10-17	云安全中心新增Linux CentOS 6基线风险项修复和回滚功能，包括单项或多项基线风险项批量修复。针对Linux CentOS 6系统，云安全中心基线检查功能提供从检测、告警、修复和回滚的全链路闭环操作。	企业版	查看和处理基线检查结果
2019-09-17	云安全中心上线产品专家服务功能。	所有付费版本	购买云安全中心
2019-08-30	云安全中心全新发布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。	所有版本	2019年上半年云上企业安全指南
2019-08-08	云安全中心上线RDS SQL注入检测功能。	企业版	无
2019-08-02	**AK和账密泄露检测**页面全新改版为**AK泄露检测**。	企业版	AK泄露检测
2019-08-01	资产管理页面全新改版为资产中心页面，提供资产和指纹视角的资产数据，帮助您更全面地分析潜在风险影响的范围；资产指纹模块支持手动触发资产指纹信息的采集。	所有版本	资产中心总览
2019-07-31	云安全中心支持容器安全威胁检测功能。	企业版	容器K8s威胁检测

发布时间	动态说明	影响的版本	相关文档
2019-07-26	设置页面的通知功能新增AccessKey泄露情报和云安全配置检查两项。	所有版本	通知
2019-07-16	开启安全日报功能从设置页面下线。	所有付费版本	主动防御
2019-06-20	云平台配置检查支持导出检测结果。	所有版本	云平台配置检查概述
2019-06-20	应急漏洞功能优化，支持展示应急漏洞修复进度。	所有版本	应急漏洞
2019-06-19	云平台最佳实践功能更名为**云产品配置检查**。	所有版本	云平台配置检查概述
2019-06-19	安全报告上线，通过自定义报告内容、报告展示的数据类型和接收人邮箱地址，实现安全报告的自定义，更好地满足您对于您资产安全状况数据的需求。	所有付费版本	安全报告
2019-06-16	设置页面全新改版，登录IP拦截加白功能从设置页面下线。	所有版本	概述
2019-06-05	支持应用漏洞检测功能。	企业版	应用漏洞
2019-05-21	云产品最佳实践新增18项检测项，包括常用数据库白名单配置检测、OSS日志记录和跨地域复制功能检测、SLB白名单配置检测、ECS自动镜像配置检测和ECS存储加密检测。	所有版本	云平台配置检查概述
2019-05-21	网页防篡改功能升级，支持查看防护总览信息、支持目录防护黑名单和白名单模式。	所有付费版本	启用网页防篡改保护
2019-04-19	新版安全大屏已正式上线。新版安全大屏支持自定义选配多个安全大屏，并支持所有旧版大屏的功能，帮助您更好地监控资产的安全态势并及时提供安全情况报告。欢迎您试用体验。 **说明** 旧版安全大屏功能于2019年05月07日正式下线。	所有付费版本	安全大屏
2019-03-30	支持漏洞关联进程。	所有付费版本	Linux软件漏洞
2019-03-30	支持应用白名单。	所有付费版本	应用白名单
2019-03-21	态势感知全新升级为云安全中心。新增高级版功能。升级后，云安全中心支持基础版、高级版和企业版3个版本。	所有版本	什么是云安全中心

发布时间	动态说明	影响的版本	相关文档
2019-03-21	日志检索功能下线。	所有付费版本	无
2019-01-17	支持新版可视化大屏。	企业版	安全大屏

2018年

发布时间	动态说明	影响的版本	相关文档
2018-12-28	攻击、访问、威胁功能下线。	企业版	无
2018-12-20	基础版威胁检测能力只支持**异常登录**和**其他-DDoS**类型安全告警；企业版不受影响。	免费版	功能特性说明
2018-12-15	支持攻击分析和溯源。	企业版	攻击分析
2018-12-10	支持告警自动化关联分析。	企业版	告警自动化关联分析
2018-10-25	支持自定义告警。	企业版	自定义告警