

# 阿里云 云安全中心（态势感知）

## 新功能发布记录

文档版本：20190911

# 法律声明

---

阿里云提醒您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
	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。	 <b>禁止：</b> 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	 <b>警告：</b> 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 <b>说明：</b> 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	设置 > 网络 > 设置网络类型
<b>粗体</b>	表示按键、菜单、页面名称等UI元素。	单击 <b>确定</b> 。
<code>courier</code> 字体	命令。	执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。
<code>##</code>	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
<code>[ ]</code> 或者 <code>[a b]</code>	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
<code>{ }</code> 或者 <code>{a b}</code>	表示必选项，至多选择一个。	<code>swich {stand   slave}</code>

# 目录

---

法律声明.....	I
通用约定.....	I
1 新功能发布记录.....	1
2 云安全中心文档概览.....	4

# 1 新功能发布记录

本文档介绍了云安全中心产品功能和文档的最新动态。

发布时间	动态说明	影响的版本	相关文档
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。	-	<a href="#">2019年上半年云上企业安全指南</a>
2019-08-08	云安全中心上线RDS SQL注入检测功能	企业版	<a href="#">#unique_4</a>
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	<a href="#">#unique_5</a>
2019-08-01	资产管理页面全新改版为资产中心。	基础版、高级版、企业版	<a href="#">#unique_6</a>
2019-07-31	云安全中心支持容器安全威胁检测功能。	企业版	<a href="#">#unique_7</a>
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。	基础版、高级版、企业版	<a href="#">#unique_8</a>
2019-07-16	开启安全日报功能从设置页面下线。	高级版、企业版	<a href="#">#unique_9</a>
2019-06-20	云平台配置检查支持导出检测结果。	基础版、高级版、企业版	<a href="#">#unique_10</a>
2019-06-20	应急漏洞功能优化，支持展示应急漏洞修复进度。	基础版、高级版、企业版	<a href="#">#unique_11</a>
2019-06-19	云平台最佳实践功能更名为云产品配置检查。	基础版、高级版、企业版	<a href="#">#unique_12</a>

发布时间	动态说明	影响的版本	相关文档
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。	高级版、企业版	<a href="#">#unique_13</a>
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。	基础版、高级版、企业版	<a href="#">#unique_14</a>
2019-06-05	支持应用漏洞检测功能。	企业版	<a href="#">#unique_15</a>
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日志记录和跨区域复制功能检测、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。	基础版、高级版、企业版	<a href="#">#unique_10</a>
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。	高级版、企业版	<a href="#">#unique_16</a>
2019-04-19	新版安全大屏已正式上线, 并支持所有旧版大屏的功能。  说明: 旧版安全大屏功能将于5月7日正式下线。	高级版、企业版	<a href="#">#unique_17</a>  说明: 新版大屏支持自定义选配多个安全大屏, 帮助您更好地监控您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。
2019-03-30	支持漏洞关联进程。	高级版、企业版	<a href="#">#unique_18</a>
2019-03-30	支持应用白名单。	高级版、企业版	<a href="#">#unique_19</a>

发布时间	动态说明	影响的版本	相关文档
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。	基础版、高级版、企业版	<a href="#">#unique_20</a>
2019-03-21	日志检索功能下线。	高级版、企业版	<a href="#">#unique_21</a>
2019-01-17	支持新版可视化大屏。	企业版	<a href="#">#unique_22</a>
2018-12-28	攻击、访问、威胁功能下线。	企业版	-
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。	基础版	<a href="#">功能特性说明</a>
2018-12-15	支持攻击分析和溯源。	企业版	<a href="#">攻击分析</a>
2018-12-10	支持告警自动化关联分析。	企业版	<a href="#">告警自动化关联分析</a>
2018-10-25	支持自定义告警。	企业版	<a href="#">自定义告警</a>

## 2 云安全中心文档概览

---

本文档介绍了如何使用云安全中心的服务和进行相关的操作。

### 前提条件

云安全中心Agent是云安全中心提供的本地插件，只有Agent处于在线状态时才能使用云安全中心提供的安全防护服务。

使用云安全中心服务前，请确保您服务器的Agent处于在线状态。详情参见[Agent说明](#)。

### 查看安全概览信息

[#unique\\_29](#)

### 查看资产保护状态

[#unique\\_30](#)

[#unique\\_31](#)

[#unique\\_32](#)

[#unique\\_33](#)

[#unique\\_34](#)

[#unique\\_35](#)

[#unique\\_36](#)

[#unique\\_37](#)

[#unique\\_38](#)

[#unique\\_39](#)

### 查看与处理告警事件

[#unique\\_40](#)

[#unique\\_41](#)

[#unique\\_42](#)

[#unique\\_43](#)

[#unique\\_44](#)

[#unique\\_45](#)



[#unique\\_46](#)

[#unique\\_47](#)

#### 检测与管理漏洞

[#unique\\_48](#)

[#unique\\_49](#)

[#unique\\_50](#)

[#unique\\_51](#)

[#unique\\_52](#)

[#unique\\_53](#)

[#unique\\_54](#)

[#unique\\_55](#)

[#unique\\_56](#)

#### 检测与查看云产品安全配置

[#unique\\_57](#)

#### 配置与执行基线检测

[#unique\\_58](#)

[#unique\\_59](#)

[#unique\\_60](#)

#### 网页防篡改

[网页防篡改概述](#)

[#unique\\_62](#)

[#unique\\_63](#)

[#unique\\_64](#)

#### 分析日志

[#unique\\_65](#)

[#unique\\_66](#)

[#unique\\_67](#)

### 查询实时日志分析

- [#unique\\_69](#)
- [#unique\\_70](#)
- [#unique\\_71](#)
- [#unique\\_72](#)
- [#unique\\_73](#)
- [#unique\\_68](#)

[#unique\\_74](#)

[#unique\\_75](#)

[#unique\\_76](#)

[#unique\\_77](#)

### 查看安全报告

[#unique\\_78](#)

### 查看攻击分析信息

[#unique\\_79](#)

### 检测AK和账号密码泄露

[#unique\\_5](#)

### 管理资产指纹

[#unique\\_80](#)

### 开通和访问可视化大屏

[#unique\\_81](#)

### 配置应用白名单

[#unique\\_82](#)

### 配置自定义告警规则

[#unique\\_83](#)

[#unique\\_84](#)

[#unique\\_85](#)

## 设置

[安全配置](#)

[告警通知设置](#)

[安装/卸载Agent插件](#)

## 常见问题

[#unique\\_88](#)