ALIBABA CLOUD

阿里云

云安全中心（安骑士）

产品简介

文档版本：20220113

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

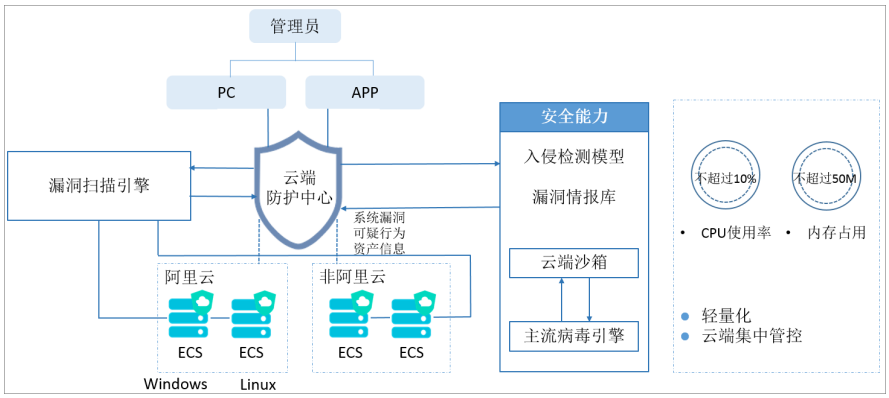
格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**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

1.什么是安骑士？

阿里云安骑士是一款经受百万级主机稳定性考验的主机安全加固产品，支持自动化实时入侵威胁检测、病毒查杀、漏洞智能修复、基线一键检查、网页防篡改等功能，是构建主机安全防线的统一管理平台。

安骑士的架构图如下：



安骑士系统架构图

2.功能列表

下表列出了安骑士的详细功能和描述。

基础版和企业版之间的功能差异用以下标识标出：

X：表示不包含在服务范围中。

√：表示包含在服务范围中。

只检测：表示该版本仅提供检测功能，不提供处理或修复等其他功能。

> **说明** ：2018年12月20日起，安骑士**基础版**将不支持**主机异常**检测功能，基础版用户将无法查看主机异常检测事件。

功能	功能项	描述	基础版	企业版
安全预防	漏洞管理	Linux软件漏洞：对标CVE官方漏洞库，自动检测并提供修复方案。	只检测	√
		Window漏洞：同步微软官网补丁，自动检测并支持一键修复。	只检测	√
		Web-CMS漏洞：自研漏洞补丁，支持一键修复0 day漏洞。	只检测	√
		检测周期：漏洞隔一天自动检测一次。其他漏洞：如软件配置型漏洞、系统组件型漏洞，都支持自动检测。	√	√
	基线检测（需开通企业版）	账号安全检测：检测服务器上是否存在黑客入侵后留下的账户、对影子账户、隐藏账户、克隆账户，同时对密码策略合规、系统及应用弱口令进行检测。	X	√
		系统配置检测：组策略、登录基线策略、注册表配置风险。	X	√
		数据库风险检测：Redis数据库高危配置。	X	√
		合规对标检测：CIS-Linux Centos7系统基线。	X	√
		检测周期：可自定义检测1天、3天、7天和30天内的基线数据。	X	√
	异常登录	异地登录提醒：对非常用登录地的事件进行告警。	√	√
		非白名单IP登录提醒：配置白名单IP后，对非白名单IP的事件进行告警。	X	√
		非法时间登录提醒：配置合法登录时间后，对非合法时间登录的事件进行告警。	X	√
		非法账号登录提醒：配置合法登录账号后，对非合法登录账号事件进行提醒。	X	√
		暴力破解登录拦截：对密码进行暴力破解的行为进行联动防御。	√	√

功能	功能项	描述	基础版	企业版
入侵检测	网站后门查杀	Webshell查杀：自研网站后门查杀引擎，拥有本地查杀加云查杀体系，同时兼有定时查杀和实时防护扫描策略，支持常见的php、jsp等后门文件类型。	只检测	√
	主机异常（含云查杀）**基础版**用户不支持**主机异常**检测和修复	进程异常行为：反弹Shell、JAVA进程执行CMD命令、Bash异常文件下载等。	X	√
		异常网络连接：C&C肉鸡检测、恶意病毒源连接下载等。	X	√
		病毒木马云查杀：常见DDoS木马、挖矿木马及病毒程序检测，支持云端一键隔离（自研沙箱+中国及中国以外地域主流杀毒引擎）。	X	√
	敏感数据篡改	系统及应用的关键文件被黑客篡改。	X	√
	异常账号	黑客入侵后创建隐藏账号、公钥账号等。	X	√
精准防御	病毒自动查杀	安骑士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	√
资产指纹	主机管理	分组和标签：支持四级资产分组和子分组、支持资产标签管理。	X	√
	资产清点：端口、账号、进程、软件	端口监听：对端口监听信息收集和呈现，并对变动进行记录、便于清点端口进行开放。	X	√
		账号管理：收集账户及对应权限信息，可清点特权账户、发现提权行为。	X	√
		进程管理：收集和呈现进程快照信息，便于自主清点合法进程及发现异常进程。	X	√
		软件管理：清点软件安装信息，同时在高危漏洞爆发时可快速定位受影响资产。	X	√
网页防篡改	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。 **说明** 网页防篡改为增值服务，需单独购买，价格详见包年包月计费方式。	X	√

3.产品优势

阿里云安骑士集网络、主机、云产品安全于一体，对云上系统的所有安全进行风险监控。

轻量级

经受百万级Windows、Linux主机稳定性验证，对业务影响小，资源消耗不超过10% CPU、50MB内存。

便捷的统一安全管控

一键开通，即开即用。服务器上无软件操作界面，所有数据展示和操作均在云盾安骑士控制台中完成，天然支持批量管理。

精准防御

多病毒检测引擎结合阿里云多年安全经验，支持主流病毒自动查杀。

安全闭环

既可检测安全问题和威胁，又能解决安全问题。支持漏洞一键修复、病毒一键查杀和基线一键检测；支持网页防篡改。

多引擎实时检测

实时全量采集数据。采用多病毒检测引擎、机器学习算法和150+关联检测模型来提升主机入侵检测效率。

大数据防御

提供威胁情报库，覆盖恶意攻击源、恶意文件库、漏洞补丁库，每天共拦截数亿次攻击，防御模型精准快速。

4.新功能发布动态

本文档介绍了安骑士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
2019-01-08	上线日志分析	企业版	无
2018-12-26	告警自动化关联分析上线	企业版	主机异常告警自动化关联分析
2018-11-20	网页防篡改上线	企业版	网页防篡改概述
2018-11-01	病毒自动隔离功能上线	企业版	病毒自动隔离
2018-03-20	主机访问控制&安全运维功能下线	企业版	主机访问控制&安全运维功能下线说明

5.【下线通知】2020年08月15日下线日志分析（公测）功能

为了给您带来更优质的产品体验，安骑士将于2020年08月15日起下线日志分析（公测）功能。

背景信息

安骑士下线日志分析（公测）功能后，不再支持日志数据的查询和分析。2021年3月将不再支持安骑士保有用户续费。

下线时间

2020年08月15日

下线内容

云安全中心（安骑士）提供的日志分析功能，即在安骑士控制台无法使用日志分析功能。

下线影响

安骑士下线日志分析后，您将无法在安骑士控制台使用日志分析功能。如果您需要查看日志数据，建议您升级到云安全中心。云安全中心在安骑士现有功能的基础上，还支持全方位的主机防护、威胁检测与处理、日志分析等功能。更多信息请参见什么是云安全中心。

给您带来的不便敬请谅解，有任何问题，请通过提交工单联系售后服务。