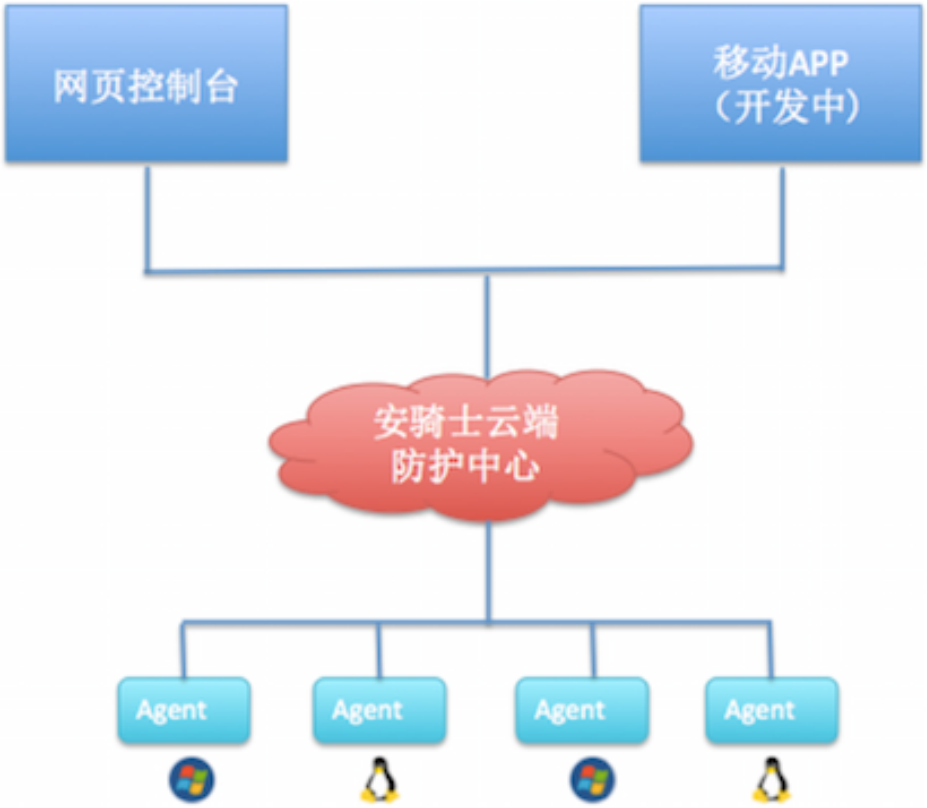
安骑士

产品简介

产品简介

安骑士是云盾推出的一款服务器安全运维管理产品。通过安装在服务器上的轻量级Agent插件与云端防护中心的规则联动，实时感知和防御入侵事件，保障服务器的安全。

安骑士的架构，如下图所示。



功能及版本参数

下表是服务器安全(安骑士)的功能列表和版本参数。

模块	功能	功能详情	基础版	企业版
弱点	漏洞管理	**系统软件漏洞** 对标CVE官方漏洞库，可检出软件版本、组件型、配置型漏洞；另外对Windows主机可进行一键批量修复	X	√
		CMS漏洞 共享漏洞获取的威胁情报，自研漏洞补丁，可一键修复CMS如WordPress、phpcms等CMS漏洞	只检测	√
	基线检查	**高危风险配置检测** 自动化检测系统、账号、权限、数据库、Web服务器的风险配置，典型问题如：弱口令、可疑自启动项等	X	√
事件	异常登录	**异地登录&暴力破解** 对于在非常用登录地的登录行为进行告警，同时可检测密码暴力破解行为，并联动实时防御	√	√
	Webshell检测	**网站后门查杀** 本地+云端多引擎检测网站后门文件，并提供一键隔离能力	只检测	√
	主机异常	**异常行为分析** Bash反弹、异常进程运行CMD命令等非法行为识别 **异常网络连接** C&C肉鸡检测、恶意源下载等非法连接	X	√

功能说明

漏洞管理：

- 系统软件漏洞
  - 软件版本扫描：通过检测服务器上安装软件的版本信息，与CVE官方的漏洞库进行匹配，检测出存在漏洞的软件并给您推送漏洞信息（可检测如：SSH、OpenSSL、Mysql等软件漏洞）
  - Windows系统漏洞：通过订阅微软官方更新源，若发现您服务器存在高危的官方漏洞未修复，将为您推送微软官方补丁（如“SMB远程执行漏洞”，另外系统将只推送高危漏洞，安全更新和低危漏洞需要您手动更新）
  - 配置型、组件型的漏洞：无法通过版本匹配和文件判断的漏洞（如：redis未授权访问漏洞等）
  - Web漏洞：通过网络端Web扫描完成，可检测SQL注入、XSS等业务逻辑漏洞；
- CMS漏洞：共享阿里云安全情报源，通过目录及文件的检测方案，检出Web-CMS软件漏洞，并给您提供云盾自研补丁（可修复如：Wordpress、Discuz等软件漏洞）

基线检查：

- 账户安全检测：深度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、克隆账户进行提醒
- 弱口令检查：收集了常用的弱口令字典，检测您SSH、RDP等服务是否使用了弱密码
- 配置风险检测：对常见登录配置、进程配置、注册表配置进行检查，以达到企业级服务器安全准入标准

入侵检测：

- 异地登录提醒：记录所有登录记录，对于非常用登录的行为进行实时提醒，可自由配置常用登录地
- 暴力破解联动：对非法破解密码的行为进行识别，并上报到阿里云处罚中心进行拦截，避免被黑客多次猜解密码而入侵

- 网站后门查杀：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
- 异常进程检测：实时监控进程启动行为，检测Bash反弹、挖矿进程检测、DDoS木马等恶意进程和进程的异常行为

历史版本功能（不再提供，即将下线）

主机访问控制：

- TCP、UDP、HTTP：支持这三种协议的自定义访问控制
- 协同防御：共享云盾恶意IP库，直接将恶意IP进行拦截
- Web攻击拦截策略自定义：支持URL、Referer、User-Agent等HTTP常见字段的条件组合，自定策略可支持盗链防护等场景；
- 记录4层和7层的策略的命中情况，支持近1个月的记录查看和数据导出。

安全运维：

- 支持Shell命令（Linux）、BAT命令（Windows），非交互式命令
- 批量下发：支持在服务器安全(安骑士)控制台一键下发脚本命令，支持运行账户切换、权限切换
- 结果在线和导出查看：对运行结果支持在线查看和导出结果查看

版本更新

2016年4月14日

上线安骑士专业版，在原有功能上增加补丁管理、安全巡检功能。

补丁管理：支持通用Web软件漏洞检测和修复，共享云盾威胁情报，一键修复0day漏洞

安全巡检：控制台批量下发安全体检，对服务器上高危基线、配置、弱口令进行检测。

安骑士 V2.0

2016年5月31日

上线安骑士增强版、企业版，在原有功能上增加主机访问控制、安全运维功能

主机访问控制：支持七层Web访问控制，自定义Web攻击拦截规则，特定场景防护

安全运维：控制台一键批量下发shell/bat脚本，并支持在线查看，白屏化运维操作

安骑士 V3.0

2016年8月9日

主机访问控制大版本更新。

支持四层TCP、UDP协议控制

可开启协同防御，共享云盾恶意IP库，实时拦截全网攻击威胁。

2016年10月8日

安全巡检更新为基线检查、主机防火墙小版本更新。

基线检查支持更多的检测项，增加合规检测等内容

主机防火墙增加DDoS防护功能，可对synflood进行精准拦截。

功能新增

漏洞管理

1、系统软件CVE漏洞

通过检测服务器上安装软件的版本信息，与CVE官方的漏洞库进行匹配，检测出存在漏洞的软件并给您推送漏洞信息
可检测如：SSH、OpenSSL、Mysql等软件漏洞

2、其他高危漏洞

可检测出配置型、组件型的漏洞，无法通过版本匹配和文件判断的漏洞
如：redis未授权访问漏洞等

资产管理

1、资产分组：支持对ECS进分组管理，便捷地通过资产的维度查看安全事件；

售卖改动

1、新增一种售卖方式：安全点（按每天保有ECS台数进行计费）

付费形态：预付费，购买“安全点”
扣费周期：每天凌晨出账扣“安全点”
计费逻辑：根据当天保有的ECS台数和选择的计费版本，进行扣费（专业版1台服务器扣1个安全点，企业版1台服务器扣5个安全点），“安全点”扣完后，将停止付费版的功能使用，自动降到基础版（免费）
计费版本限制：只能选择一个计费版本，版本支持升级，不支持降级

2、原来的售卖模式调整（按固定的使用授权ECS计费的售卖模式调整）

功能完全不变，但是老的计费模式不能转到新的计费模式（即1个账号同时只能是1种收费模式）
取消授权数的内部折扣，即专业版统一售价20元/月/个授权，企业版统一售价200元/月/个授权，再叠加其他活动计费
该售卖模式将在近期做下线处理，下线时间和处理方案将另行公告通知，故新用户建议您以“按每天保有ECS台数计费”方式进行购买

3、功能及版本调整：

增强版停止售卖，产品付费版为两个：专业版、企业版
目前的增强版主机访问控制功能、企业版安全运维功能，都将停止新购，不再开放新客户使用这两个功能
老客户若原来购买了这两个功能，即继续维护该功能
新购买企业版和原绑定企业版授权的ECS，将享有新的功能：漏洞管理

更多售卖改动，请点击链接查看

包年包月售卖策略调整

1、全量购买：即需要对账号下所有的ECS进行统一的安全保护，不再支持对部分ECS单独付费使用增值版本（即相当于原来的先购买“授权”，再去控制台绑定的逻辑将下线）；

2、老用户：在官网公告发送前，通过“包年包月购买固定授权”方式使用安骑士增值版本的客户，在调整上线后将免费升级到“全量”服务（即账号下所有的ECS都将有相应增值版功能）【公告发出后，购买授权数若小于保有ECS台数，售卖调整后需要进行升级补充差价才能正常使用】

注：按量付费（安全点）购买的售卖模式不变。

企业版价格调整：

版本	付费方式	原价格	调价后价格	折扣	调整后折扣价格
企业版	包年包月	200元/台/月	60元/台/月	无	60元/台/月
	按量付费（安全点）	5个安全点/台/天 ≈ 150元/台/月	3个安全点/台/天 ≈ 90元/台/月	6折	≈54元/台/月

版本功能调整：

1、基础版的一键隔离网站后门功能，调整到专业版才能享有（原基础版的木马检测功能不变）；

2、原Beta测试功能：系统软件漏洞及其他漏洞，于8月1日正式上线，为企业版的功能，企业版客户才能查看和处理。

新增功能

1、Dashboard页面新增“弱点趋势”、“事件趋势”图；

2、基线检查可添加白名单，对不需要检测的项目可以不进行检测；

功能优化

1、基线检查不再需要手动进行检测，对于企业版客户将自动为您周期检测；

其他

1、专业版停止售卖：原专业版享有的功能：一键修复CMS漏洞、一键隔离网站后门功能权益不变，可正常使用到合约到期；2、企业版功能调整：原基线检查功能，部分检测项可免费使用，部分检测项专业版可使用，部分检测项企业版可使用，统一调整为所有检测项目需要“企业版”才能使用；