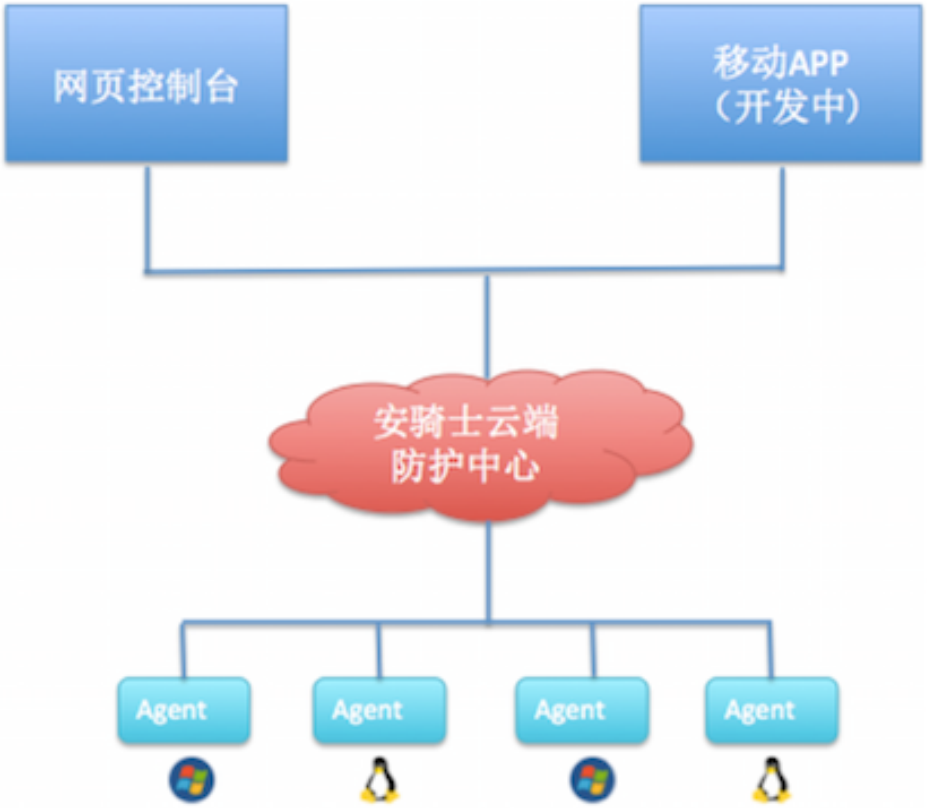
# 安骑士

## 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 | 功能点 | 功能详情 | 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 | √ |
| | | Windows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0day漏洞 | 只检测 | √ |
| | | 其他漏洞：如软件配置型漏洞、系统组件型漏洞，均支持自动检测 | √ | √ |
| | 基线检查 | 账号安全检测：密码策略合规、系统及应用弱口令 | 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 | √ |
| 入侵检测 | 异常登录 | 异地登录提醒：对在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，对非合法账号登录事件进行告警 | X | √ |
| | | 暴力破解登录拦截：对密码暴力破解的行为进行联动防御 | √ | √ |
| | 网站后门查杀 | Webshell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(含云查杀) | 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 | 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，对变动进行记录，便于清点端口开放 | 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：进程快照信息收集及呈现，便于自主清点合法进程发现异常进程 | X | √ |
| | | 软件管理：清点软件安装信息，同时在高危漏洞爆发可快速定位受影响资产 | X | √ |
| 日志检索 | 进程相关 | 进程启动：进程一旦启动，则记录下该启动事件的详细信息 | X | √ |
| | | 进程快照：某一时刻的进程全量日志抓取并存储 | X | √ |
| | 网络连接 | 主动外联：对外网络连接的五元组相关信息实时采集 | X | √ |
| | 其他日志 | 系统登录：SSH、RDP的系统登录流水日志 | X | √ |
| | | 端口监听快照：某一时刻的所有对外监听端口的快照数据 | X | √ |
| | | 账号快照：某一时刻的所有账号信息的快照数据 | X | √ |

# 功能说明

## 安全预防

**漏洞管理**：

- Linux软件漏洞：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）
- Windows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）
- 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）
- 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）

**基线检查**：

- 账户安全检测：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
- 系统配置检测：系统组策略、登录基线策略、注册表配置风险检测

- 数据库风险检测：支持对Redis数据库高危配置进行检测
- 合规对标检测：CIS-Linux Centos7系统基线合规检测

## 入侵检测

- **异常登录**：
  - 异地登录：系统记录所有登录记录，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
  - 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
  - 非法时间登录提醒：配置合法登录时间后，对非合法时间登录事件进行告警
  - 非法账号登录提醒：配置合法登录账号后，对非合法账号登录事件进行告警
  - 暴力破解登录拦截：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（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
- **主机异常 (含云查杀)**：
  - 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
  - 异常网络连接：C&C肉鸡检测、恶意病毒源连接下载等
  - 恶意进程（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+国内外主流杀毒引擎）
  - 敏感文件篡改：系统及应用的关键文件被黑客篡改
  - 异常账号：黑客入侵后创建隐藏账号、公钥账号等

## 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
- **端口、账号、进程、软件**：
  - 端口监听：对端口监听信息收集和呈现，对变动进行记录，便于清点端口开放
  - 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
  - 进程管理：进程快照信息收集及呈现，便于自主清点合法进程发现异常进程
  - 软件管理：清点软件安装信息，同时在高危漏洞爆发可快速定位受影响资产（待上线）

## 日志检索

- **进程相关**：
  - 进程启动：进程一旦启动，则记录下该启动事件的详细信息
  - 进程快照：某一时刻的进程全量日志抓取并存储
- **网络连接**：
  - 主动外联：对外网络连接的五元组相关信息实时采集
- **其他日志**：
  - 系统登录：SSH、RDP的系统登录流水日志

- 端口监听快照：某一时刻的所有对外监听端口的快照数据
- 账号快照：某一时刻的所有账号信息的快照数据

### 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；

2017年12月5日发布，该版本更新内容如下：

# 1、漏洞管理

**基础版开放所有漏洞的查看功能**：包括Linux软件漏洞、Web-CMS漏洞、Windows漏洞和其他漏洞

**增加漏洞“修复必要性”参考字段**：根据漏洞原等级、曝光时间、资产的环境因子得出，以帮助您快速评估出需尽快修复的漏洞

新增支持自定义只对部分漏洞类型和部分服务器进行检测

新增支持数据导出、批次保存、批量加入白名单、批量忽略

解决单台机器生成修复命令不合并问题

未付费客户不再进行任何漏洞告警

## 2、基线检查

该功能仅企业版可使用

支持批量加入白名单、批量忽略

新增支持自定义选择基线检查项目

新增支持自定义选择服务器是否开启检测

新增支持基线风险导出功能

## 3、异常安全

暴力破解成功事件与异地登录事件整合为“异常登录”，正常登录流水调整到“日志”模块

企业版新增功能支持：非合法IP、账号、时间的登录告警

异地登录告警及展示修正：异地登录第五次不再告警，仅第一次告警，同时第1-5次控制台均会显示异地登录

## 4、一键安全检查

- 企业版功能新增：支持一键触发安全扫描，在资产管理页批量选择机器可以一键检查，不用再等48小时自动上报

## 5、告警（发送时间段可配置）

漏洞管理：仅企业版客户告警，每周一次

基线检查：仅企业版客户告警，每周一次

主机异常：仅企业版客户告警，单ECS一天最多1条，单账号一天最多5条

异常登录：基础版&企业版均发送，单ECS一天最多1条，单账号一天最多5条

网站后门：基础版&企业版均发送，单ECS一天最多1条，单账号一天最多5条

# 6、其他更新

非阿里云机器在资产列表页面，支持强制解绑，不用先卸载再等6小时了

已失效的安全事件，如漏洞、基线、异常登录、主机异常等，系统自动设置为7天过期，部分事件再过7天自动删除，数据不再一直保留给您带来信息干扰

安装/卸载页面，若有离线服务器，则会展示离线服务器列表，同时支持离线服务器列表的导出

体验改进：增加单ECS详情页可管理单台ECS的漏洞和基线情况；增加漏洞详情和基线详情页可管理同一漏洞或基线影响的对应ECS