# 目录

# 产品概述

### 什么是服务器安全

服务器安全 KHS（Kingsoft Cloud Host Security）是一款针对服务器进行防护的安全产品，通过本地客户端和云端服务器的联动，实时同步最新安全数据，提供资产管理、漏洞风险管理、基线检查、病毒木马检测、入侵检测、安全监控等功能，帮助用户构建服务器安全防护体系，以及满足合规要求。

### 为什么需要服务器安全

云服务在极大地方便用户和企业廉价使用存储资源、软件资源、计算资源的同时，也面临着巨大的挑战安全挑战。

- **安全边界模糊化**：虚拟化模糊了传统的安全边界，传统的安全产品并不适合在虚拟化环境中采用。
- **汹涌的东西向流量**：虚机之间缺乏威胁隔离机制，网络威胁一旦进入云平台内部，可以肆意蔓延。
- **0Day漏洞带来的严重威胁**：针对漏洞攻击愈来愈多，不少漏洞遭纰漏，其中包括埋藏在系统中多年未被发现的漏洞，影响面非常广泛。
- **组件资产数量庞大难以维护**：企业由于业务发展迅速，变更频繁，但内部极少有人能及时了解本身的核心资产情况。尤其是资产和组织架构越来越复杂之后，管理难度也越来越高。

### 工作原理

用户通过在主机中安装Agent后，获得金山云服务安全系统对主机全方位的安全保障能力，统一查看并管理同一区域内所有主机的防护状态和主机安全风险。


# 使用限制

### 支持的云服务器类型

- 金山云云服务器（Kingsoft Cloud Elastic Compute，KEC）
- 金山云裸金属服务器（Elastic Physical Compute，EPC）*即将支持*
- 暂不支持云外服务器

### 支持的操作系统

服务器安全的Agent可运行在CentOS、EulerOS等Linux系统以及Windows 2008、Windows 2012、Windows 2016等Windows系统的主机上。

# 功能介绍与版本比较

服务器安全有基础版（免费）、企业版供您选择，版本功能差异及功能介绍如下表1所示 *基础版将于2021年末上线*

### 版本推荐说明

- 用于测试、个人用户防护主机账户安全，推荐使用基础版。
- 对需要满足等级保护合规基本要求的主机，推荐使用企业版。

### 版本功能比较

表1 不同版本功能差异说明

| 类别 | 内容 | 描述 | 基础版 | 企业版 |
| --- | --- | --- | --- | --- |
| 安全概览 | 安全概览 | 实时展示主机安全体检得分、防护状态、待处理风险、风险趋势以及主机安全的实时动态 | √ | √ |
| | 资产概览 | 支持一键搜索主机资产信息。展示主机资产和主机操作系统分布情况 | √ | √ |
| 资产管理 | 主机资产 | 查看主机资产信息、安全风险等功能，方便用户快速管理服务器 | √ | √ |
| | 资产变更分析 | 支持资产变更情况导出、分析30天内各资产数量的变更情况 | × | √ |
| | Web站点 | 展示主机包含Web站点个数、运行状态、网站域名、端口、网站路径 | × | √ |
| | Web中间件 | 展示主机包含Web中间件的名称、版本、安装路径、发现时间 | × | √ |
| | Web应用 | 展示主机包含Web应用的个数、名称、当前版本、发现时间 | × | √ |
| | Web应用框架 | 展示主机上的Web应用框架信息，包含应用框架名、框架语言、框架版本、服务类型、应用路径 | × | √ |
| | 端口 | 展示主机对内端口和对外端口的数量，使用协议、绑定IP、进程名、服务名 | × | √ |
| | 账号 | 展示主机包含账号个数、账号名称、登录方式、账号状态、上次登录时间 | × | √ |
| | 进程 | 展示主机包含进程个数、进程名称、进程路径、主机数、PID、hash值、启动时间、进程版本。支持导出进程信息 | × | √ |
| | 数据库 | 展示主机上的数据库信息，包含数据库的版本、安装路径、监听地址及端口、端口协议类型、运行权限、配置文件路径、日志文件路径、错误日志文件路径、插件路径、数据路径、进程二进制路径、启动参数 | × | √ |
| | 软件应用 | 展示主机上的软件应用信息，包含软件应用的软件应用名、当前版本、安装信息、状态、发现时间 | × | √ |
| | 第三方组件 | 展示主机的第三方组件信息，包含第三方组件的版本、安装路径、相关网站 | × | √ |
| | 系统安装包 | 展示主机的系统安装包信息，包含系统安装包的包名、总述、版本、安装时间、类型、安装路径 | × | √ |
| | Jar包 | 展示主机Jar包信息，包含包名、类型、是否可执行、版本号、绝对路径 | × | √ |
| | 计划任务 | 展示主机上的计划任务信息，包含计划任务的计划任务名、执行周期、执行命令或脚本、执行用户、运行目录 | × | √ |
| | 环境变量 | 展示主机环境变量信息，包含变量名、变量类型、用户名、变量值 | × | √ |
| | 内核模块 | 展示主机上内核模块信息，包含模块名、模块大小、模块描述、模块版本、模块路径、引用计数、依赖项 | × | √ |
| 漏洞风险 | 风险概览 | 展示漏洞检测结果信息、漏洞发现趋势、漏洞处理趋势和各类风险统计 | √ | √ |
| | 应急漏洞 | 展示近期爆发出的高危漏洞，支持应急漏洞检测，实时检测资产安全情况 | × | √ |
| | 系统漏洞 | 检测并管理系统中存在的漏洞，支持主机粒度的漏洞扫描并导出扫描结果。漏洞详情包含：漏洞描述、风险等级、修复建议、参考链接、安全建议CVE 编号、雷达图等。 | √ | √ |
| | 网站漏洞 | 通过本地扫描发现网站的漏洞，可以提供对网站漏洞的修复 | × | √ |
| | 弱口令 | 展示安全体检的弱口令信息，包含弱口令的说明、风险危害以及修复建议 | √ | √ |
| | 风险账号 | 展示安全体检的可疑高权限账号和空密码账号，提供查看高危账号的详细信息、危害以及修复建议，可以提供禁用、信任和忽略操作 | × | √ |
| | 配置缺陷 | 展示安全体检的配置缺陷信息，包含配置缺陷的相关说明信息，风险危害以及修复建议 | × | √ |
| 入侵检测 | 入侵概览 | 展示整体的入侵威胁情况，图表分析入侵威胁分布情况，30天入侵威胁发现趋势 | √ | √ |
| | 威胁分析 | 展示不同类型威胁的攻击趋势和不同类型攻击威胁的详细攻击特征信息，并可以对攻击IP加入黑名单 | √ | √ |
| | 病毒木马 | 展示安全体检和实时防护的二进制病毒木马信息，包含病毒的类型、hash、路径，并且提供对病毒的隔离、信任和下载 | × | √ |
| | 网站后门 | 展示安全体检和实时防护的webshell文件信息，包含webshell的类型、hash、路径，并且提供对webshell文件隔离、信任、下载和查看操作 | × | √ |
| | 反弹Shell | 展示安全体检和实时防护的反弹shell进程、进程运行参数、父进程和父进程运行参数、本地地址和反弹的目的地址 | × | √ |
| | 异常账号 | 展示影子账号的信息和威胁特征、修复建议 | × | √ |
| | 日志异常删除 | 展示安全体检检测到的日志删除事件，以及操作用户和日志路径 | × | √ |
| | 异常登录 | 展示异常登录信息，包括异常地点、异常IP、异常时间和暴力破解登录信息 | √ | √ |
| | 异常进程 | 展示安全体检的子进程高于父进程权限进程、隐藏进程和隐藏端口进程信息，进程hash等 | × | √ |
| | 系统命令篡改 | 展示安全体检检测到的系统命令被篡改的信息，包括篡改后的hash, 路径、篡改系统命令的危害和建议，并提供隔离和信任操作 | × | √ |
| 合规基线 | 基线检查 | 对服务器操作系统（Windows和Linux）配置和web容器配置的基线内容进行检查 | √ | √ |
| | 基线模板 | 支持设置合规基线检测的基线模板，设置模板基础信息、规则信息 | × | √ |
| | 检查策略 | 支持设置合规基线检测的策略模板，选择检查项和被检查服务器 | × | √ |
| 安全防护 | 暴力破解防护 | 包括FTP暴力破解防护，MySQL暴力破解防护，远程登录暴力破解防护，MSSQL暴力破解防护。支持设置暴力破解防护模式记录和拦截模式，设置触发暴力破解防护的规则和冻结时间以及受保护的端口 | √ | √ |
| | 扫描防护 | 防恶意端口扫描攻击，支持设置防护的模式记录和拦截模式，触发扫描防护的规则和IP冻结时间 | × | √ |
| | 病毒防护 | 病毒和WebShell实时防护，支持设置实时防护的等级、病毒和webshell检出后处理方式，支持设置实时防护引擎 | × | √ |
| | IP黑白名单 | 支持设置防护的IP黑白名单 | × | √ |
| | 端口安全 | 设置端口的安全策略，包含端口号、协议、策略以及例外的IP | × | √ |
| | 访问控制 | 设置系统文件和注册表保护的防护规则和自定义文件的防护规则 | × | √ |
| | 远程登录保护 | 支持修改远程登录的端口，并指定可远程登录的IP地址或IP段 | × | √ |
| | 进程行为控制 | 支持进程行为控制 | × | √ |
| 安全监控 | 登录监控 | 监控主机登录情况，可以设置常用地点、常用IP、常用时间段，监控类型有异常地点、异常时间、异常IP和暴力破解登录情况 | √ | √ |
| | 完整性监控 | 包括文件完整性监控和账号完整性监控，文件完整性监控包括文件被修改、删除和新增，支持设置文件夹和特定文件监控，支持白名单路径和文件类型。账号完整性包括账号是否存在修改账号用户名、修改账号密码、修改账号权限、删除账号和新增账号的操作 | × | √ |
| | 操作审计 | 监控主机上的shell命令并记录命令内容、进程和操作用户和登录IP，可以通过定义的规则进行筛选威胁的命令 | × | √ |
| | 会话监控 | 监控主机上网络连接情况，采集会话连接的协议、本地地址、本地端口、外部地址、外部端口、进程等会话信息，并生成主机会话连接图表 | × | √ |

# 术语说明

| 基本概念 | 解释 |
| --- | --- |
| 基线 | 基线一般指配置和管理系统的详细描述，或者说是最低的安全要求，包括服务和应用程序设置、操作系统组件的配置、权限和权利分配、管理规则等。 |
| 漏洞 | 漏洞是指在操作系统实现或安全策略上存在的缺陷，例如操作系统软件或应用软件在逻辑设计上存在的缺陷或在编写时产生的错误。攻击者可以对这类缺陷或错误进行利用，从而能够在未获得授权的情况下访问和窃取您的系统数据或破坏系统。系统漏洞需要系统管理员及时处理并修复，否则将带来严重的安全隐患。 |
| 本地提权 | 本地提权漏洞是指攻击者在实施网络攻击时获得了系统最高权限，从而取得对网站服务器的控制权。 黑客利用该漏洞可突破安全防御系统，直接威胁用户的系统和数据安全。 |
| 弱口令 | 指密码强度低，容易被攻击者破解的口令 |
| WebShell | 以asp、php、jsp或者cgi等网页文件形式存在的一种命令执行环境，也可以将其称做为一种网页后门。黑客入侵网站后，通常会将后门文件与网站服务器WEB目录下正常的网页文件混在一起，使用浏览器来访问后门后得到一个命令执行环境，即可控制网站服务器 |
| 暴力破解 | 使用自动化工具，通过穷举法获取用户账户的个人密码 |
| XSS攻击 | 跨站脚本攻击，攻击者在Web页面中插入恶意Script代码，当用户浏览该页之时，嵌入其中Web里面的Script代码会被执行，从而达到恶意攻击用户的目的 |
| SQL注入 | 通过把SQL命令插入到Web表单提交或输入域名或页面请求的查询字符串，最终达到欺骗服务器执行恶意的SQL命令 |
| CC攻击 | 攻击者借助代理服务器生成指向Web服务器的合法请求，导致服务器无法处理正常访问请求 |