企业主机安全

产品介绍

文档版本 19

发布日期 2025-02-11

华为云计算技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为云计算技术有限公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为云计算技术有限公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是企业主机安全

企业主机安全（Host Security Service，HSS）是以工作负载为中心的安全产品，集成了主机安全、容器安全和网页防篡改，旨在解决混合云、多云数据中心基础架构中服务器工作负载的独特保护要求。

HSS不受地理位置影响，为主机、容器等提供统一的可视化和控制能力。

HSS通过对主机、容器进行系统完整性的保护、应用程序控制、行为监控和基于主机的入侵防御等，保护工作负载免受攻击。

主机安全

主机安全是提升主机整体安全性的服务，通过主机管理、风险预防、检测与响应、高级防御、安全运营、网页防篡改功能，全面识别并管理主机中的信息资产，实时监测主机中的风险并阻止非法入侵行为，帮助企业构建服务器安全体系，降低当前服务器面临的主要安全风险。

在主机中安装Agent后，您的主机将受到HSS云端防护中心全方位的安全保障，在管理控制台可视化界面上，您可以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。

主机安全的工作原理如图1-1所示。

图 1-1 工作原理

主机安全的组件功能及工作流程说明如下：

表 1-1 组件功能及工作流程说明

组件	说明
管理控制台	可视化的管理平台，便于您集中下发配置信息，查看在同一区域内主机的防护状态和检测结果。
HSS云端防护中心	● 使用AI、机器学习和深度算法等技术分析主机中的各项安全风险。 ● 集成多种杀毒引擎，深度查杀主机中的恶意程序。 ● 接收您在控制台下发的配置信息和检测任务，并转发给安装在服务器上的Agent。 ● 接收Agent上报的主机信息，分析主机中存在的安全风险和异常信息，将分析后的信息以检测报告的形式呈现在控制台界面。
Agent	● Agent通过HTTPS和WSS协议与HSS云端防护中心进行连接通信，默认端口：10180。 ● 每日凌晨定时执行检测任务，全量扫描主机；实时监测主机的安全状态；并将收集的主机信息（包含不合规配置、不安全配置、入侵痕迹、软件列表、端口列表、进程列表等信息）上报给云端防护中心。 ● 根据您配置的安全策略，阻止攻击者对主机的攻击行为。 **说明** ● 如果未安装Agent或Agent状态异常，您将无法使用企业主机安全。 ● Agent可安装在华为云弹性云服务器（Elastic Cloud Server，ECS）/裸金属服务器（Bare Metal Server，BMS）、线下IDC以及第三方云主机中。 ● 根据操作系统版本选择对应的安装命令/安装包进行安装。 ● 网页防篡改、容器安全与主机安全共用同一个Agent，您只需在同一主机安装一次。

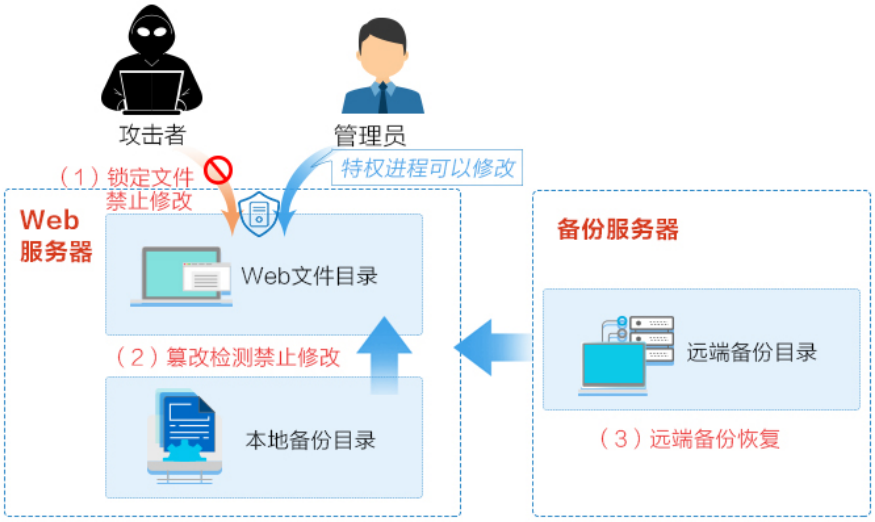
容器安全

容器安全是HSS为容器提供的一种防护能力，通过部署在容器宿主机中的Agent，能够扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题；同时容器安全提供容器进程白名单、文件只读保护和容器逃逸检测功能，可以有效防止容器运行时安全风险事件的发生。

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，从而保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。

图 1-2 网页防篡改原理



2 产品优势

企业主机安全是一个用于全面保障主机整体安全的服务，能帮助您高效管理主机的安全状态，并构建服务器安全体系，降低当前服务器面临的主要安全风险。

集中管理

实现检测和防护的一体化管控，降低管理的难度和复杂度。

- 将Agent安装在华为云ECS服务器/BMS服务器、线下IDC以及第三方主机中，您可以集中管理同一区域内多样化部署的主机。
- 您可以在安全控制台上统一查看同一区域内主机中各项风险的来源，根据各项风险的处理建议处理主机中的各项风险；利用多样化检索、批量处理等功能，快速分析同一区域内所有主机的风险。

全面防护

提供事前预防、事中防御、事后检测的全面防护，全面降低入侵风险。

轻量 Agent

Agent占用资源极少，不影响主机系统的正常运行。

网页防篡改

- 使用第三代网页防篡改技术，内核级事件触发技术，锁定用户目录下的文件后，有效阻止非法篡改行为。
- 篡改监测自动恢复技术，在主机本地和远端服务器上实时备份已授权的用户所修改的文件，保证备份资源的时效性。当企业主机安全检测到非法篡改行为时，将使用备份文件主动恢复被篡改的网页。

3 应用场景

主机安全

- 统一安全管理

  企业主机安全提供统一的主机安全管理能力，帮助用户更方便地管理云服务器的安全配置和安全事件，降低安全风险和管理成本。

- 安全风险评估

  对主机系统进行安全评估，将系统存在的各种风险（账户、端口、软件漏洞、弱口令等）进行展示，提示用户及时加固，消除安全隐患。

- 账户安全保护

  提供覆盖事前、事中和事后的账户安全保护功能。支持双因子认证登录，防止用户云服务器上的账户遭受暴力破解攻击，提高云服务器的安全性。

- 主动安全防御

  通过清点主机安全资产，管理主机漏洞与不安全配置，预防安全风险；通过网络、应用、文件主动防护引擎主动防御安全风险。

- 黑客入侵检测

  提供主机全攻击路径检测能力，能够实时、准确地感知黑客入侵事件，并提供入侵事件的响应手段，对业务系统“零”影响，有效应对APT攻击等高级威胁。

容器安全

- 容器镜像安全

  即使在Docker Hub下载的官方镜像中也常常包含了漏洞，而研发人员在使用大量开源框架时更加剧了镜像漏洞问题的出现。

  容器镜像安全对镜像进行安全扫描，将镜像中存在的各种风险（镜像漏洞、账号、恶意文件等）进行展示，提示用户及时修改，消除安全隐患。

- 容器运行时安全

  通常容器的行为是固定不变的，容器安全服务帮助企业制定容器行为的白名单，确保容器以最小权限运行，有效阻止容器安全风险事件的发生。

4 产品功能

企业主机安全有基础版、专业版、企业版、旗舰版、网页防篡改版和容器版供您选择，主要功能包括：**总览**、**资产概览**、**主机管理**、**容器管理**、**主机指纹**、**容器指纹**、**漏洞管理**、**基线检查**、**容器镜像安全**、**应用防护**、**网页防篡改**、**勒索病毒防护**、**文件完整性管理**、**病毒查杀**、**动态端口蜜罐**、**容器防火墙**、**应用进程控制**、**容器集群防护**、**主机安全告警**、**容器安全告警**、**白名单管理**、**策略管理**、**历史处置记录**、**安全报告**、**容器审计**、**安装与配置**等。每个版本支持的功能存在差异，您可以根据自身的业务需求选择合适的版本。

- 如需用于测试或个人用户防护主机账户安全，可使用**基础版（无数量限制，只支持部分功能的检测能力，不支持防护能力）**。
- 如有高阶防护的需求，推荐使用旗舰版。
- 如有网站或关键系统防篡改需求，推荐使用**网页防篡改版**。
- 如有镜像安全、容器运行时安全需求，以及容器化部署业务，推荐使用**容器版**。
- 如果主机涉及重要资产或存在高风险情况（例如：对外暴露EIP、保存有关键资产、存在数据库等），以及主机有应用安全防护需求，建议使用**旗舰版或者网页防篡改版**。

须知

- **企业版**已经停止出售，建议您购买**旗舰版**防护您的主机！
- 为防止未防护主机感染勒索、挖矿等病毒后传染给其他主机，导致企业内网整体沦陷，**建议您的云上主机全部署企业主机安全**。
- 购买企业主机安全防护配额版本后，支持升级版本和切换版本，详细操作请参见**升级防护配额版本**和**切换防护版本**。
- 本文表格中使用的标识含义如下：
  - √表示支持
  - ×表示不支持

总览

总览呈现云上资产整体安全评分和防护配置情况等，方便您掌握资产安全动态。

表 4-1 总览功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
总览	实时展示所有资产的安全评分、安全风险和防护地图，帮助您了解主机和容器的安全状态以及存在的安全风险。	√	√	√	√	√	√

资产概览

资产概览呈现资产状态和清点情况。

表 4-2 资产概览功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
资产概览	所有主机的资产状态、清点情况统计，包括Agent状态、防护状态、配额状态、资产指纹等。	√	√	√	√	√	√

主机管理

主机管理功能支持按照主机维度查看和管理目标服务器。

表 4-3 主机管理功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
主机管理	所有主机资产管理，包含主机的防护状态、配额绑定、策略分配等，提供Linux主机的批量安装agent功能。	√	√	√	√	√	√

容器管理

容器管理功能支持按照容器维度查看和管理目标服务器、以及管理容器镜像和容器实例的安全风险。

表 4-4 容器管理功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
容器节点管理	所有容器节点管理，用户可为容器节点启停防护，以及部署防护策略。	×	×	×	×	×	√
容器镜像	提供本地镜像、三方镜像仓/SWR镜像、CI/CD镜像安全扫描，并展示镜像扫描结果和漏洞、异常配置修复建议，帮助用户发现和解决镜像安全风险，避免不安全的镜像部署到生产环境。	×	×	×	×	×	√
容器	展示容器实例信息，如果存在不安全的容器实例，用户可执行隔离、停止操作。	×	×	×	×	×	√

主机指纹

主机指纹功能支持采集主机中的端口、进程、Web应用、Web服务、Web框架和自启动项等资产信息，用户通过主机指纹功能集中清点主机中的各类资产信息，及时发现风险资产。

表 4-5 主机指纹功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
账号	检测当前系统的账号信息，帮助用户进行账户安全性管理。 **支持的操作系统**：Linux、Windows。 **检测周期**：每小时自动检测。	×	×	√	√	√	√
开放端口	检测当前系统开放的端口，帮助用户识别出其中的危险端口和未知端口。 **支持的操作系统**：Linux、Windows。 **检测周期**：每30秒自动检测。	×	×	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
进程	监测运行中的进程并进行收集及呈现，便于用户自主清点合法进程，发现异常进程。 **支持的操作系统：**Linux、Windows。 **检测周期：**每小时自动检测。	×	×	√	√	√	√
软件	监测并记录当前系统安装的软件信息，帮助用户清点软件资产，识别不安全的软件版本。 **支持的操作系统：**Linux、Windows。 **检测周期：**每日自动检测。	×	×	√	√	√	√
自启动项	对系统中的自启动项进行检测，及时统计自启动项的变更情况。 **支持的操作系统：**Linux、Windows。 **检测周期：**每小时自动检测。	×	×	√	√	√	√
Web应用	Web应用主要统计、展示推送发布web内容的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息。 **支持的操作系统：**Linux、Windows（仅支持Tomcat）。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√
Web服务	统计、展示对外提供web内容访问的软件详细信息，您可查看所有软件的版本、路径、配置文件、关联进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Web框架	统计、展示Web内容对外呈现时所使用框架的详细信息，您可查看所有框架的版本、路径、关联进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√
Web站点	统计、展示存放Web内容的目录及对外提供访问的站点信息，您可以查看所有目录及权限、以及和站点所关联访问路径、对外端口、关键进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√
中间件	统计、展示所使用到的所有软件信息，您可查看所有中间件所关联的服务器、版本号、路径、关联进程等信息。 **支持的操作系统：**Linux、Windows。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√
数据库	统计、展示提供数据存储的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息； **支持的操作系统：**Linux、Windows（仅支持MySQL）。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
内核模块	统计、展示运行在内核层的全量程序模块文件，您可查看所有模块所关联的服务器、版本号、模块描述、驱动文件路径、文件权限、文件哈希等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	√	√	√	√

容器指纹

容器指纹功能支持采集容器中的账号、端口、进程、集群、服务和工作负载等资产信息等，用户通过容器指纹功能集中清点容器中的各类资产信息，及时发现风险资产。

表 4-6 资产指纹功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
账号	检测的容器系统中的账号信息，帮助用户进行账户安全性管理。 **支持的操作系统：**Linux。 **检测周期：**每小时自动检测。	×	×	×	×	×	√
开放端口	检测容器系统中的开放的端口，帮助用户识别出其中的危险端口和未知端口。 **支持的操作系统：**Linux。 **检测周期：**每30秒自动检测。	×	×	×	×	×	√
进程	监测运行中的进程并进行收集及呈现，便于用户自主清点合法进程，发现异常进程。 **支持的操作系统：**Linux。 **检测周期：**每小时自动检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
软件	监测并记录当前容器系统安装的软件信息，帮助用户清点软件资产，识别不安全的软件版本。 **支持的操作系统：**Linux。 **检测周期：**每日自动检测。	×	×	×	×	×	√
自启动项	对容器系统中的自启动项进行检测，及时统计自启动项的变更情况。 **支持的操作系统：**Linux。 **检测周期：**每小时自动检测。	×	×	×	×	×	√
Web应用	Web应用主要统计、展示推送发布web内容的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	×	√
Web服务	统计、展示对外提供web内容访问的软件详细信息，您可查看所有软件的版本、路径、配置文件、关联进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	×	√
Web框架	统计、展示Web内容对外呈现时所使用框架的详细信息，您可查看所有框架的版本、路径、关联进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Web站点	统计、展示存放Web内容的目录及对外提供访问的站点信息，您可以查看所有目录及权限、以及和站点所关联访问路径、对外端口、关键进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	×	√
中间件	统计、展示所使用到的所有软件信息，您可查看所有中间件所关联的服务器、版本号、路径、关联进程等信息。 **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	×	√
数据库	统计、展示提供数据存储的软件详细信息，您可以查看所有软件的版本、路径、配置文件、关键进程等信息； **支持的操作系统：**Linux。 **检测周期：**1次/周（每周一凌晨04：10）。	×	×	×	×	×	√
集群列表	统计、展示集群的详细信息，您可以查看所有集群的类型、节点、版本、状态等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	×	√
服务	统计、展示服务和断点的详细信息，您可以查看所有服务的命名空间、所属集群等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
工作负载	统计、展示工作负载（有状态负载、无状态负载、守护进程集、普通任务、定时任务、容器组）的详细信息，您可以查看所有工作负载的状态、实例个数、命名空间等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	×	√
容器实例	统计、展示容器实例的详细信息，您可以查看所有容器实例的状态、所属POD、所属集群等信息。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	×	√

漏洞管理

漏洞管理支持检测主机中的Linux软件漏洞、Windows系统漏洞、Web-CMS漏洞、应用漏洞和应急漏洞，帮助用户识别潜在风险。

表 4-7 漏洞管理功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Linux漏洞检测	通过与漏洞库进行比对，检测主机的Linux操作系统官方维护的软件（非绿色版、非自行编译安装版；例如：kernel、openssl、vim、glibc等）存在的漏洞。 **支持的操作系统：**Linux。 **检测周期：**自动扫描（默认每日自动扫描）、定时扫描（默认每周一次，基础版不支持）、手动扫描（基础版不支持）。	√	√	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Windows漏洞检测	通过同步微软官方的补丁公告，检测主机的Windows操作系统存在的漏洞。 **支持的操作系统：**Windows。 **检测周期：**自动扫描（默认每日自动扫描）、定时扫描（默认每周一次，基础版不支持）、手动扫描（基础版不支持）。	√	√	√	√	√	×
Web-CMS漏洞检测	通过对主机中的Web目录和文件进行检测，识别Web-CMS漏洞，提升Web服务安全性。 **支持的操作系统：**Linux、Windows。 **检测周期：**自动扫描（默认每日自动扫描）、定时扫描（默认每周一次）、手动扫描。	×	√	√	√	√	√
应用漏洞检测	检测主机中开源的jar包、elf文件等的漏洞，比如log4j、spring-core的漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**自动扫描（默认每周一自动扫描）、定时扫描（默认每周一次）、手动扫描。	×	×	√	√	√	√
应急漏洞检测	通过软件版本比对和POC验证的方式，检测主机上运行的软件和依赖包是否存在漏洞，将存在风险的漏洞上报至控制台，并给您提供漏洞告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**定时扫描（需要手动配置开启）、手动扫描。	×	√	√	√	√	√

基线检查

基线检查支持扫描主机系统和关键软件含有风险的配置、弱口令、口令复杂度策略，支持的检测基线包含安全实践，且可自定义选择检测的子基线项、修复漏洞风险。

表 4-8 基线检查功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
口令复杂度策略检测	检测系统中的口令复杂度策略，给出修改建议，帮助用户提升口令安全性。 **支持检测的操作系统：** Linux。 **检测周期**：每日凌晨自动检测、手动检测。	√	√	√	√	√	√
经典弱口令检测	检测系统账户口令是否属于常用的弱口令，针对弱口令提示用户修改。 **支持检测的操作系统：** Linux、Windows。 **检测周期：**每日凌晨自动检测、手动检测。	√	√	√	√	√	√
配置检查	对常见的Tomcat配置、Nginx配置、SSH登录配置进行检查，帮助用户识别不安全的配置项。 **支持检测的操作系统：** Linux、Windows。 **检测周期：**每日凌晨自动检测、手动检测。	×	×	√	√	√	√

容器镜像安全

容器镜像安全支持扫描镜像仓库与正在运行的容器镜像，发现镜像中的漏洞、恶意文件等并给出修复建议，帮助用户得到一个安全的镜像。

表 4-9 容器镜像安全功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
SWR镜像仓库漏洞	通过与漏洞库进行比对，检测SWR镜像仓库存在的系统漏洞、应用漏洞，对当前镜像中存在的漏洞进行提醒。 **支持的操作系统：**Linux。 **检测周期：**手动检测。	×	×	×	×	×	√
镜像恶意文件	检测镜像是否携带恶意文件（Trojan、Worm、Virus病毒和Adware垃圾软件等），帮助用户识别出存在的风险。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

应用防护

应用防护为运行时的应用提供安全防御。您无需修改应用程序文件，只需将探针注入到应用程序，即可为应用提供强大的安全防护能力。

表 4-10 应用防护功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
SQL注入	检测防御SQL注入（SQL Injection）攻击，检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
OS命令注入	检测防御远程OS命令注入（OS Command Injection）攻击，同时检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
XSS	检测防御存储型跨站脚本(Cross-Site Scripting，XSS)注入攻击。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
Log4j RCE漏洞检测	检测防御远程代码执行的控制攻击，并支持对攻击行为进行阻和拦截。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
上传Webshell	检测防御上传危险文件的攻击或将已有文件改名为危险文件扩展名的攻击，同时检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
内存马注入	检测防御内存马注入攻击。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
XXE	检测防御XXE注入（XML External Entity Injection）攻击，检测web应用是否存在对应漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
反序列化输入	检测使用了危险类的反序列化攻击。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
文件目录遍历	获取访问文件的路径或目录，匹配是否在敏感目录或敏感文件下。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
Struts2 OGNL	OGNL代码执行检测。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
JSP执行操作系统命令	检测可疑行为—通过JSP请求执行操作系统命令。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
JSP删除文件	检测可疑行为—通过JSP请求删除文件失败。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
数据库连接异常	检测可疑异常—数据库连接抛出的认证和通讯异常。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
0 day漏洞	检测执行命令的堆栈哈希是否在Web应用的白名单堆栈哈希表里。 **支持的操作系统：**Linux、Windows。 检测周期：实时检测。	×	×	×	√	√	√
SecurityManager权限检测异常	检测可疑异常，即SecurityManager抛出的异常。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
JNDI注入	检测防御JNDI注入攻击，检测Web应用是否存在对应漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
表达式(Expression)注入	检测防御表达式注入攻击，检测Web应用是否存在对应漏洞。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

网页防篡改

网页防篡改实时检测并拦截篡改指定目录下文件的行为，并可快速获取备份的合法文件恢复被篡改的文件，从而保护网站的网页、电子文档、图片等文件不被黑客篡改和破坏。

表 4-11 网页防篡改功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
静态网页防篡改	防止网站服务器中的静态网页文件被篡改。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	×	√	×
动态网页防篡改	为Tomcat提供动态网页防篡改能力，防止网站数据库中动态网页内容被篡改。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	√	×

勒索病毒防护

勒索病毒防护支持自定义勒索防护策略，帮助您识别检测已知勒索病毒攻击，支持通过静态、动态诱饵识别部分未知的勒索攻击。

表 4-12 勒索病毒防护功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
勒索病毒防护	帮助您识别检测已知勒索病毒攻击，支持通过静态、动态诱饵识别部分未知的勒索攻击。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

应用进程控制

应用进程控制功能支持检测并告警恶意进程运行，帮助用户构建安全的应用进程运行环境。

表 4-13 应用进程控制功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
应用进程控制	支持管控服务器中应用进程的运行，通过学习服务器运行的应用进程特征，将应用进程划分为可信进程、恶意进程和可疑进程，允许可疑、可信进程正常运行，对恶意进程运行进行告警，帮助用户构建安全的应用进程运行环境，避免服务器遭受不受信或恶意应用进程的破坏。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

文件完整性管理

文件完整性管理支持检查并记录关键文件的更改。

表 4-14 文件完整性管理功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
文件完整性管理	检查Linux系统的关键文件，帮助用户及时发现发生了可能遭受攻击的更改。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√

病毒查杀

病毒查杀功能支持检测服务器中的病毒文件，可帮助用户清理潜在的恶意威胁。

表 4-15 病毒查杀功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
病毒查杀	病毒查杀功能使用特征病毒检测引擎，支持扫描服务器中的病毒文件，扫描文件类型覆盖可执行文件、压缩文件、脚本文件、文档、图片、音视频文件，用户可根据自身需要，自主对服务器执行“快速查杀”、“全盘查杀”、“自定义查杀”扫描任务，并及时处置检测到的病毒文件，增强业务系统的病毒防御能力。 **支持的操作系统：**Linux、Windows。 **检测周期：**手动检测。	×	√（仅支持快速查杀）	√	√	√	√

动态端口蜜罐

动态端口蜜罐功能利用真实端口作为诱饵端口诱导攻击者访问，在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机。

表 4-16 动态端口蜜罐功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
动态端口蜜罐	动态端口蜜罐功能是一个攻击诱捕陷阱，利用真实端口作为诱饵端口诱导攻击者访问；在内网横向渗透场景下，可有效地检测到攻击者的扫描行为，识别失陷主机，延缓攻击者攻击真正目标，从而保护用户的真实资源。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

容器防火墙

容器防火墙为容器环境提供的防火墙服务。

表 4-17 容器防火墙功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
容器防火墙	对容器集群内部和外部的网络流量进行控制和拦截，防止恶意访问和攻击。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

容器集群防护

容器集群防护功能支持检测镜像中存在的不合规基线、漏洞恶意文件，防止不安全的容器镜像部署到集群。

表 4-18 容器集群防护功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
容器集群防护	支持在容器镜像启动时检测其中存在的不合规基线、漏洞和恶意文件，并可根据检测结果告警和阻断未授权或含高危安全风险的容器镜像运行。 **支持的操作系统：** Linux。 **检测周期：** 实时检测。	×	×	×	×	×	√

主机安全告警

主机安全告警支持识别并阻止入侵主机的行为，实时检测主机的风险异变，检测并查杀主机中的恶意程序，识别主机中的网站后门等。

表 4-19 主机安全告警功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
未分类恶意软件	对运行中的程序进行检测，识别出其中的后门、木马、挖矿软件、蠕虫和病毒等恶意程序。 **支持的操作系统：** Linux、Windows。 **检测周期：** 实时检测。	×	√	√	√	√	√
病毒	对服务器进行实时检测，对在服务器资产发现的各种病毒进行告警上报。 **支持的操作系统：** Linux、Windows。 **检测周期：** 实时检测。	×	√	√	√	√	√
蠕虫	对服务器中入侵的蠕虫或已存在的蠕虫进行检测、查杀，并进行告警上报。 **支持的操作系统：** Linux、Windows。 **检测周期：** 实时检测。	×	√	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
木马	对隐藏在正常程序中具备破坏和删除文件、发送密码、记录键盘等特殊功能的程序进行检测，发现时立即进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
僵尸网络	检测主机资产中是否存在已被传播的僵尸程序，一旦发现立即进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
后门	实时检测服务器系统是否存在后门漏洞，对发现的后门病毒进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
Rootkits	检测服务器资产，对可疑的内核模块和可疑的文件或文件夹进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
勒索软件	检测来自网页、软件、邮件、存储介质等介质捆绑、植入的勒索软件。 勒索软件用于锁定、控制您的文档、邮件、数据库、源代码、图片、压缩文件等多种数据资产，并以此作为向您勒索钱财的筹码。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
黑客工具	检测服务器是否存在用来控制服务器的非标工具，一旦发现立即上报告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
Webshell	检测云服务器上Web目录中的文件，判断是否为Webshell木马文件，支持检测常见的PHP、JSP等后门文件类型。 ● 网站后门检测信息包括“木马文件路径”、“状态”、“首次发现时间”、“最后发现时间”。您可以根据网站后门信息忽略可信文件。 ● 您可以使用手动检测功能检测主机中的网站后门。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
挖矿软件	实时检测服务器中是否存在挖矿软件，并对发现的软件进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
远程代码执行	实时检测服务器是否存在被远程调用的情况，一旦发现立即进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
Redis漏洞利用	实时检测Redis进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Hadoop漏洞利用	实时检测Hadoop进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
MySQL漏洞利用	实时检测MySQL进程对服务器关键目录的修改行为，并对发现的修改行为进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
反弹Shell	实时监控用户的进程行为，支持告警和阻断进程的非法Shell连接操作产生的反弹Shell行为。 支持对TCP、UDP、ICMP等协议的检测。 目前支持阻断的反弹shell类别：exec反弹Shell、Perl反弹Shell、AWK反弹Shell、Python反弹Shell.b、Python反弹Shell.a、Lua反弹Shell、mkfifo/openssl反弹Shell、PHP反弹Shell、Ruby反弹Shell、使用rssocks进行反向代理、Bash反弹Shell、Ncat反弹Shell、exec重定向反弹Shell、Node反弹Shell、Telnet双端口反弹Shell、nc反弹Shell、Socat反弹Shell、rm/mkfifo/sh/nc反弹Shell、socket/tchsh反弹Shell。 **支持的操作系统：**Linux。 **检测周期：**实时检测。 **说明** 启用反弹Shell自动阻断需确保满足以下条件： 1. 在“HIPS检测”策略中，开启“自动化阻断”。该功能默认关闭，需要手动开启。具体操作请参见**配置策略**。 2. 确保已开启恶意程序隔离查杀。该功能默认关闭，需要手动开启。具体操作请参见**开启恶意程序隔离查杀**。	×	√	√	√	√	√
文件提权	检测当前系统对文件的提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
进程提权	检测以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
关键文件变更	对于系统关键文件进行监控，文件被修改时告警，提醒用户关键文件存在被篡改的可能。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
文件/目录变更	实时监控系统文件/目录，对创建、删除、移动、修改属性或修改内容的操作进行告警，提醒用户文件/目录可能被篡改。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
进程异常行为	检测各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。 对于进程的非法行为、黑客入侵过程进行告警。 进程异常行为可以监控以下异常行为： ● 监控进程CPU使用异常。 ● 检测进程对恶意IP的访问。 ● 检测进程并发连接数异常等。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
高危命令执行	实时检测当前系统中执行的高危命令，当发生高危命令执行时，及时触发告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
异常Shell	检测系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、复制、硬链接、访问权限变化。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
敏感文件访问	检测未经授权访问或修改敏感文件的行为。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
Crontab可疑任务	检测并列出当前所有主机系统中自启动服务、定时任务、预加载动态库、Run注册表键或者开机启动文件夹的汇总信息。 帮助用户通过自启动变更情况，及时发现异常自启动项，快速定位木马程序的问题。 **支持的操作系统**：Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
系统安全防护被禁用	检测勒索软件加密前准备动作：通过注册表关闭Windows Defender实时保护功能，一旦发现立即上报告警。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	×	√	√	√	×

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
备份删除	检测勒索软件加密前准备动作：删除备份格式文件或Backup文件夹下的文件，一旦发现立即上报告警。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
异常注册表操作	检测通过注册表关闭系统防火墙、勒索病毒Stop修改注册表并写入特定字符串等操作，一旦发现立即上报告警。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
系统日志删除	检测到通过命令或工具清除系统日志的操作时进行告警。 **支持的操作系统：**Windows。 检测周期：实时检测。	×	×	√	√	√	×
可疑命令执行	● 检测通过命令或工具创建、删除计划任务或自启动任务。 ● 检测远程执行命令的可疑行为。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
可疑进程运行	检测未经过认证或授权的应用进程运行，一旦发现进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
可疑进程文件访问	检测未经过认证或授权的进程访问指定的目录，一旦发现进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
暴力破解	检测“尝试暴力破解”和“暴力破解成功”等暴力破解。 ● 检测账户遭受的口令破解攻击，封锁攻击源，防止云主机因账户破解被入侵。 ● 如果账户暴力破解成功，登录到云主机，则触发安全事件告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√	√
异常登录	检测主机异地登录行为并进行告警，用户可根据实际情况采取相应措施（例如：忽略、修改密码等）。 如果在非常用登录地登录，则触发安全事件告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√	√
非法系统账号	检测主机系统中的账号，列出当前系统中的可疑账号信息，帮助用户及时发现非法账号。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√
用户账号添加	检测使用命令创建隐藏账户，一旦创建成功后用户交互界面和命令查询均不可见。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	×	√	√	√	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
用户密码窃取	检测主机中的系统账号和密码Hash值被异常获取的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	√	√	√	√
未知网络访问	检测对服务器未监听的端口进行访问的行为。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	×	×	√	√	√
云蜜罐	检测到连接主机蜜罐端口的行为，进行告警上报。	×	×	×	√	√	×
异常外联行为	检测到服务器存在异常外联可疑ip的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux（仅支持5.10及以上内核版本）。 **检测周期：**实时检测。	×	√	√	√	√	√
端口转发检测	检测到利用可疑工具进行端口转发行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
可疑的下载请求	检测到利用系统工具下载程序的可疑HTTP请求时进行告警。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	×	√	√	√	×
可疑的HTTP请求	检测到利用系统工具或进程执行远程托管脚本的可疑HTTP请求时进行告警。 **支持的操作系统：**Windows。 **检测周期：**实时检测。	×	×	√	√	√	×

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
端口扫描	检测用户指定的端口存在被扫描或者嗅探的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	√	√	√
主机扫描	检测网络对主机规则覆盖（包含对ICMP、ARP、nbtscan是覆盖）的扫描活动，一旦发现立即上报告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	√	√	√
进程注入	检测将恶意代码注入到正在运行的进程的行为，一旦发现立即告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
动态库注入进程	检测通过劫持动态链接库中的函数，从而实现白加黑注入代码的行为，一旦发现立即告警上报 。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√
内存文件进程	检测通过memfd_create的系统调用，创建一个只存在于RAM中的匿名恶意文件，从而执行恶意文件的行为，一旦发现立即告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	√	√	√	√	√

容器安全告警

容器安全告警支持对Docker、Containerd容器引擎进行入侵行为检测，实时监控容器节点运行状态，发现挖矿、勒索等恶意程序，发现违反容器安全策略的进程运行和文件修改，以及容器逃逸等行为并给出解决方案。

表 4-20 容器安全告警功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
未分类恶意软件	对容器中运行的程序进行检测，识别出其中的后门、木马、挖矿软件、蠕虫和病毒等恶意程序。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
病毒	对容器进行实时检测，对在容器环境中发现的各种病毒进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
蠕虫	对容器环境中入侵的蠕虫或已存在的蠕虫进行检测，并进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
木马	对隐藏在正常程序中具备破坏和删除文件、发送密码、记录键盘等特殊功能的程序进行检测，发现时立即进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
僵尸网络	检测容器环境中是否存在已被传播的僵尸程序，一旦发现立即进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
后门	实时检测容器环境是否存在后门漏洞，对发现的后门病毒进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
Rootkits	检测容器环境，对可疑的内核模块和可疑的文件或文件夹进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
勒索软件	检测容器场景下勒索软件，并进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
黑客工具	检测容器环境是否存在用来控制容器的非标工具，一旦发现立即上报告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	√	√	√	√
Webshell	检测容器中Web目录中的文件，判断是否为Webshell木马文件，支持检测常见的PHP、JSP等后门文件类型。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
挖矿软件	实时检测容器环境中是否存在挖矿软件，并对发现的软件进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
漏洞逃逸攻击	监控到容器内进程行为符合已知漏洞的行为特征时，触发逃逸漏洞攻击告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
文件逃逸攻击	监控发现容器进程访问了宿主机系统的关键文件目录（例如：“/etc/shadow”、“/etc/crontab”），则认为容器内发生了逃逸文件访问，触发告警。即使该目录符合容器配置的目录映射规则，仍然会触发告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
反弹Shell	实时监控容器环境用户的进程行为，及时发现进程的非法Shell连接操作产生的反弹Shell行为。支持对TCP、UDP、ICMP等协议的检测。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
文件提权	检测当前容器系统对文件的提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
进程提权	检测容器环境以下进程提权操作： ● 利用SUID程序漏洞进行root提权。 ● 利用内核漏洞进行root提权。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
关键文件变更	对于容器场景系统关键文件进行监控，文件被修改时告警，提醒用户关键文件存在被篡改的可能。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
文件/目录变更	实时监控系统文件/目录，对创建、删除、移动、修改属性或修改内容的操作进行告警，提醒用户文件/目录可能被篡改。 支持的操作系统：Linux。 检测周期：实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
进程异常行为	检测容器场景下各个主机的进程信息，包括进程ID、命令行、进程路径、行为等。 对于进程的非法行为、黑客入侵过程进行告警。 进程异常行为可以监控以下异常行为： ● 监控进程CPU使用异常。 ● 检测进程对恶意IP的访问。 ● 检测进程并发连接数异常等。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
容器进程异常	● 容器恶意程序 监控容器内启动的容器进程的行为特征和进程文件指纹，如果特征与已定义的恶意程序吻合则触发容器恶意程序告警。 ● 容器异常进程 对于已关联的容器镜像启动的容器，只允许白名单进程启动，如果容器内存在非白名单进程，触发容器异常程序告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
容器异常启动	监控新启动的容器，对容器启动配置选项进行检测，当发现容器权限过高存在风险时触发告警。 支持以下容器环境检测： ● 禁止启动特权容器(privileged:true) ● 需要限制容器能力集（capabilities:[xxx]） ● 建议启用seccomp（seccomp=unconfined） ● 限制容器获取新的权限(no-new-privileges:false) ● 危险目录映射(mounts:[...]) **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
高危命令执行	实时检测容器场景系统中执行的高危命令，当发生高危命令执行时触发告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
高危系统调用	Linux系统调用是用户进程进入内核执行任务的请求通道，容器安全监控容器进程，如果发现进程使用了危险系统调用，触发高危系统调用告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
异常Shell	检测容器系统中异常Shell的获取行为，包括对Shell文件的修改、删除、移动、复制、硬链接、访问权限变化。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
敏感文件访问	监控容器内已配置文件保护策略的容器镜像文件状态。如果发生文件修改事件则触发文件异常告警。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
容器镜像阻断	在Docker环境中容器启动前，告警并阻断**镜像异常行为策略**中指定的不安全容器镜像运行。 **支持的操作系统：**Linux。 **检测周期：**实时检测。 **说明** 需**安装Docker插件**。	×	×	×	×	×	√
可疑命令执行	• 检测通过命令或工具创建、删除计划任务或自启动任务。 • 检测远程执行命令的可疑行为。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
运行时异常行为	提供网络、主机、Pod、容器、进程、系统调用多层次防护，可监控容器中出现的进程、文件、网络活动、进程capabilities、系统调用共5种运行时异常行为，支持对异常行为进行告警和阻断，阻止容器逃逸，保护容器运行时的安全。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
暴力破解	检测容器场景下“尝试暴力破解”和“暴力破解成功”等暴破异常行为，发现暴破行为时触发告警。 支持检测容器场景下SSH、Web和Enumdb暴破行为。 **支持的操作系统：**Linux。 **检测周期：**实时检测。 **说明** 目前暂仅支持Docker容器运行时的暴力破解检测告警。	×	×	×	×	×	√
非法系统账号	检测容器场景系统中的账号，列出当前系统中的可疑账号信息并告警上报，帮助用户及时发现非法账号。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
用户密码窃取	检测容器环境中系统账号和密码Hash值被异常获取的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
异常外联行为	检测到容器环境中存在异常外联可疑ip的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux（仅支持5.10及以上内核版本）。 **检测周期：**实时检测。	×	×	×	×	×	√
端口转发检测	检测到容器环境中利用可疑工具进行端口转发行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
Kubernetes事件删除	检测集群中删除Kubernetes事件的行为，一旦发现进行警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Pod异常行为	检测集群中存在创建特权pod、静态pod及敏感配置pod的异常行为，以及对现存pod执行的异常操作，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
枚举用户信息	检测存在枚举集群用户的权限以及可执行操作列表的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
绑定集群用户角色	检测绑定、创建高权限集群角色或Service Account的行为，一旦发现进行告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
进程注入	检测将恶意代码注入到正在运行的进程的行为，一旦发现立即告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
动态库注入进程	检测通过劫持动态链接库中的函数，从而实现白加黑注入代码的行为，一旦发现立即告警上报 。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√
内存文件进程	检测通过memfd_create的系统调用，创建一个只存在于RAM中的匿名恶意文件，从而执行恶意文件的行为，一旦发现立即告警上报。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

白名单管理

白名单功能包含**告警白名单**、**登录告警白名单**和**系统用户白名单**，如需避免某些告警误报发生，可以将告警事件加入对应的白名单。

表 4-21 白名单管理功能介绍

功能名称	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
告警白名单	处理告警事件时，将告警事件加入到告警白名单。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√	√
登录告警白名单	将目标登录端IP和登录端用户名加入登录告警白名单，HSS将对白名单内的IP和用户的访问行为进行忽略，不再告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√	√
系统用户白名单	对于主机中新添加的root用户组权限用户（非root用户）可添加到系统用户白名单，避免HSS进行风险账号告警。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	√	√	√	√	√	√

策略管理

用户可以根据需要进行**策略管理**配置，自定义安全检测规则，并可为不同的主机组或主机/容器应用不同的策略，以满足不同应用场景的主机/容器安全需求。

表 4-22 策略管理功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
策略管理	支持自定义检测策略配置与下发，能够为每组或每台主机灵活配置检测规则，便于精细化安全运营。 ● 查看策略组列表 ● 依据默认策略组和已创建的策略组添加策略组 ● 自定义策略 ● 修改和删除策略组 ● 针对策略组包含的策略，进行修改和关闭策略 ● 在“主机管理”页面可以对主机进行批量部署策略 **支持的操作系统：** Linux、Windows。 **检测周期：**实时检测。	×	√（仅支持默认专业版策略组）	√（仅支持默认企业版策略组）	√	√	√

历史处置记录

历史处置记录呈现漏洞、安全告警事件、病毒查杀等的处置历史。

表 4-23 历史处置记录功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
历史处置记录	提供漏洞、安全告警事件、病毒查杀等的历史处置记录，方便您查看相关处理时间和处理人等信息。	×	√	√	√	√	√

安全报告

HSS支持以天、周、月的形式输出用户资产的安全报告。

表 4-24 安全报告功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
安全报告	呈现每周或每月的主机安全趋势以及关键安全事件与风险。	×	√	√	√	√	√

容器审计

容器审计支持监控和记录集群容器、非集群容器以及SWR镜像仓的各类操作和活动，以日志记录呈现在HSS控制台供用户查看和分析。

表 4-25 容器审计功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
容器审计	容器审计功能支持对容器集群中的各种操作和活动进行监控和记录，可帮助用户洞察容器生命周期的各个阶段，包括创建、启动、停止和销毁等，以及容器之间的网络通信和数据传输情况。用户通过审计和分析，可以及时发现并处理安全问题，从而确保容器集群的安全性、稳定性。 **支持的操作系统：**Linux。 **检测周期：**实时检测。	×	×	×	×	×	√

安装与配置

安装与配置提供Agent管理、常用登录地、常用登录IP、SSH登录IP白名单、恶意程序自动隔离查杀、双因子认证、告警配置、容器安装与配置等功能，可满足不同应用场景的主机/容器安全需求。

表 4-26 安装与配置功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
Agent管理	可查看所有服务器的Agent状态，可进行升级、卸载、安装等操作。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√	√
常用登录地	配置常用登录地后，服务将对非常用地登录主机的行为进行告警。每个主机可被添加在多个登录地中。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√	√
常用登录IP	配置常用登录IP，服务将对非常用IP登录主机的行为进行告警。 **支持的操作系统：**Linux、Windows。	√	√	√	√	√	√
配置SSH登录IP白名单	SSH登录IP白名单功能是防护账户爆破的一个重要方式，主要是限制需要通过SSH登录的服务器。 配置了白名单的服务器，只允许白名单内的IP通过SSH登录到服务器，拒绝白名单以外的IP。 **支持的操作系统：**Linux。	√	√	√	√	√	√
恶意程序隔离查杀	开启恶意程序隔离查杀后，HSS对识别出的后门、木马、蠕虫等恶意程序，提供自动隔离查杀功能，帮助用户自动识别处理系统存在的安全风险。 **支持的操作系统：**Linux、Windows。 **检测周期：**实时检测。	×	√	√	√	√	√

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版
双因子认证	通过密码+短信/邮件认证的方式，彻底防范账号暴力破解行为。 **支持的操作系统：**Linux、Windows。	按需：× 包年/包月：√	√	√	√	√	√
插件管理	对插件进行安装、卸载、升级及统一管理。 **支持的操作系统：**Linux。	×	×	×	×	×	√
容器安装与配置	提供集群接入HSS入口，同时支持集群、非集群容器的Agent升级、卸载操作。 **支持的操作系统：**Linux。	√	√	√	√	√	√

主机安全自保护

主机安全自保护是企业主机安全的自我保护功能。

表 4-27 主机安全自保护功能介绍

服务功能	功能概述	基础版	专业版	企业版	旗舰版	网页防篡改版	容器版

Windows自保护	防止恶意程序卸载Agent、篡改企业主机安全文件或停止企业主机安全进程。
	支持的操作系统：
	Windows。
	说明
	• 自保护功能依赖AV检测、HIPS检测或者勒索病毒防护功能使能驱动才能生效，只有这三个功能开启一个以上时，开启自保护才会生效。
	• 开启自保护策略后的影响如下：
	  • Agent不支持通过主机的控制面板卸载，支持通过企业主机安全控制台卸载。
	  • 企业主机安全的进程无法被终止。
	  • Agent安装路径C:\Program Files\HostGuard下除了log目录、data目录（如果Agent升级过，再加上upgrade目录）外的其他目录无法访问。
		×	×	×	√	√	×

Linux自保护	防止恶意程序停止企业主机安全进程、卸载Agent。
	支持的操作系统：Linux。
	说明
	• 开启自保护策略后的影响如下：
	  • Agent不支持通过命令卸载，支持通过企业主机安全控制台卸载。
	  • 企业主机安全的进程无法被终止。
		×	×	×	√	√	√

5 免费服务

企业主机安全HSS提供以下两种免费服务：

- 免费试用HSS基础版30天

  购买华为云弹性云服务器（Elastic Cloud Server，ECS）时，可以勾选免费试用一个月主机安全基础版，免费体验HSS基础版30天。HSS基础版提供操作系统漏洞检测、弱口令检测、暴力破解检测等功能，具体功能支持详情请参见**产品功能**。免费试用更多内容，请参见**免费试用HSS基础版30天**。

- 免费体检

  HSS为未开启防护的华为云弹性云服务器（Elastic Cloud Server，ECS）和开启了免费体检的华为云云容器引擎（Cloud Container Engine，CCE）提供每月一次的免费体检服务，支持检测服务器的软件资产、操作系统漏洞以及弱口令风险并生成安全报告供用户查看。免费体检更多内容，请参见**免费体检**。

6 个人数据保护机制

为了确保您的个人数据（例如用户名、密码、手机号码等）不被未经过认证、授权的实体或者个人获取，HSS通过加密存储个人数据、控制个人数据访问权限等方法防止个人数据泄露，保证您的个人数据安全。

收集范围

HSS收集及产生的个人数据如表6-1所示。

表 6-1 个人数据范围列表

类型	收集方式	是否可以修改	是否必须
邮箱	服务器开启双因子认证后，HSS定时获取对应消息通知服务主题订阅的邮箱	否	是
手机号	服务器开启双因子认证后，HSS定时获取对应消息通知服务主题订阅的手机号	否	是
登录位置信息	服务器开启防护后，登录云服务器时，HSS记录的用户登录位置信息。	否	是

存储方式

HSS通过加密算法对用户个人敏感数据加密后进行存储。

- 邮箱、手机号：加密存储
- 登录位置信息：不属于敏感数据，明文存储

访问权限控制

用户个人数据通过加密后存储在HSS数据库中，数据库的访问需要通过白名单的认证与授权。

7 安全

7.1 责任共担

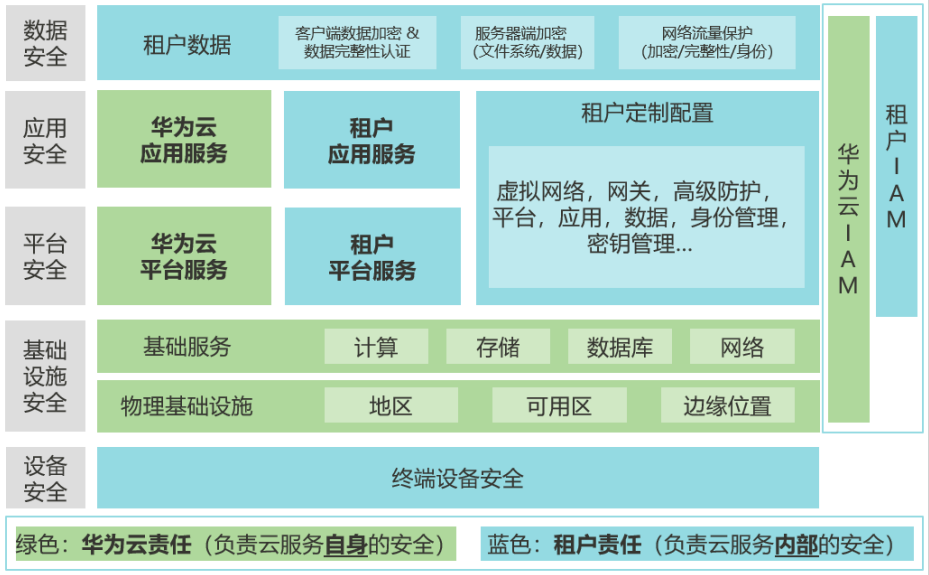
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如**图7-1**所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的IaaS、PaaS和SaaS类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的IaaS、PaaS和SaaS类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 7-1 华为云安全责任共担模型



7.2 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 7-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 7-3 资源中心

7.3 资产识别与管理

HSS会收集账号、进程、开放端口、自启动项、软件、Web框架、Web站点等16类主机和容器资产信息，并展示资产清点情况，帮助用户及时发现主机和容器中存在风险的资产。

表 7-1 HSS 的资产管理相关功能

功能	说明	详细介绍
资产概览	资产概览展示用户全量主机和容器资产的清点情况，包括Agent状态、配额状态、账号、端口、进程、软件、自启动项等。方便用户在一个页面了解全量资产数据。	资产概览
主机指纹	主机指纹采集主机的账号、开放端口、进程、软件、自启动项、Web站点、Web框架、中间件、内核模块、Web服务、Web应用、数据库资产，并展示资产的详细信息，帮助用户排查发现异常主机资产。	主机指纹
容器指纹	容器指纹采集容器的账号、开放端口、进程、软件、自启动项、Web站点、Web框架、中间件、Web服务、Web应用、数据库、集群、服务、工作负载和实例资产，并展示资产的详细信息，帮助用户排查发现异常容器资产。	容器指纹

7.4 身份认证与访问控制

使用统一身份认证服务（Identity and Access Management，简称IAM）对租户纳管的HSS资源进行精细的权限管理，您可以：

- 根据企业的业务组织，在您的华为云账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用HSS资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将HSS资源委托给更专业、高效的其他华为云账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

  有关创建HSS权限策略的详细介绍，请参见创建用户并授权使用HSS。

7.5 数据保护技术

HSS通过如下数据保护手段和特性，保障HSS中的数据安全可靠。

数据保护手段	说明
传输加密（HTTPS）	微服务间管理数据传输进行加密，防止数据在传输过程中泄露或被篡改。用户的配置数据传输采用安全协议HTTPS，防止数据被窃取。
数据冗余存储	资产信息、告警事件等数据存储均具备副本备份恢复能力。

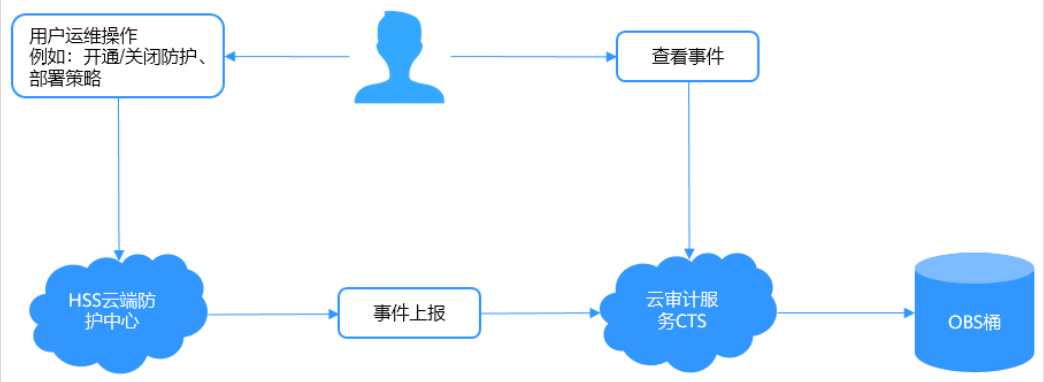
数据保护手段	说明
数据加密存储	HSS通过敏感数据加密保证用户数据的安全性。

除此之外，服务节点可开通HSS服务网页防篡改功能，实现对业务数据的防护。

网页防篡改功能开通详情请参见**开启网页防篡改**。

7.6 审计与日志

云审计服务（Cloud Trace Service，以下简称CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景



CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。

支持云审计的HSS操作列表详情请参见**支持云审计的HSS操作列表**。

7.7 服务韧性

HSS提供四层可靠性架构，通过检测、承受、恢复三个方面保障系统在收到攻击后可以手动、自动恢复服务能力，保障服务和数据的持久性和可靠性。

表 7-2 可靠性架构保证数据稳定

能力分类	能力项	目标	分类
检测	态势感知	对接态势感知服务，利用企业主机安全上报的告警/漏洞/基线检查结果评估资产风险	系统
	云监控服务	对接云监控服务，监控HSS的资源使用情况、业务的运行状况，并及时收到异常报警做出反应，保证业务顺畅运行	系统
承受	防攻击	Agent提供自防护能力，防KILL、防篡改能力	安全

能力分类	能力项	目标	分类
	数据备份	支持关键数据100%备份，即使数据库遭到完全损坏，也可以根据以前备份数据恢复业务。	系统
	业务自保护	HSS采用微服务化部署，微服务独立部署和启停。 Agent严格控制资源占用，资源超限进行隔离或逃生，不影响租户业务功能，系统可用资源不足降级。	系统
恢复	系统恢复	虚拟机故障/业务系统故障，支持自动重建和手工重建	系统
	进程保护	进程退出时，自动拉起微服务进程，保证业务快速恢复。	系统

7.8 监控安全风险

云监控服务（Cloud Eye，CES）为用户的云上资源提供了立体化监控平台。通过云监控您可以全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

HSS提供基于云监控服务的资源监控能力，帮助用户监控账号下的服务器防护情况，执行自动实时监控、告警和通知操作。用户可以实时监控未开启防护服务器数量、有风险服务器数量和未安装/已离线Agent数量等信息。

关于HSS支持的监控指标，以及如何创建监控告警规则等内容，请参见**监控**。

8 HSS 权限管理

如果您需要对华为云上购买的HSS资源为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全地控制云资源的访问。

通过IAM，您可以在华为云账号中给员工创建IAM用户，并授权控制员工对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有HSS的使用权限，但是不希望他们拥有删除HSS等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用HSS服务，但是不允许删除HSS的权限，控制他们对HSS资源的使用范围。

如果华为云账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用HSS的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您号中的资源进行付费。关于IAM的详细介绍，请参见**《IAM产品介绍》**。

HSS 权限

默认情况下，管理员创建的IAM用户没有任何权限，您需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

HSS部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效，如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问HSS时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对HSS服务，管理员能够控制IAM用户仅能对某一类云服务器资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分。

如表8-1所示，包括了HSS的所有系统权限。

表 8-1 HSS 系统权限

系统角色/策略名称	描述	类别	依赖关系
HSS Administrator	企业主机安全（HSS）管理员，拥有该服务下的所有权限。	系统角色	• 依赖Tenant Guest角色。 Tenant Guest：全局级角色，在全局项目中勾选。 • 购买HSS防护配额需要同时具有ECS ReadOnlyAccess、BSS Administrator和TMS ReadOnlyAccess角色。 – ECS ReadOnlyAccess：系统策略，弹性云服务器的只读访问权限。 – BSS Administrator：系统角色，费用中心（BSS）管理员，拥有该服务下的所有权限。 – TMS ReadOnlyAccess：系统策略，标签管理服务的只读访问权限。
HSSFullAccess	企业主机安全所有权限。	系统策略	购买HSS防护配额需要具有BSS Administrator角色。 BSS Administrator：系统角色，费用中心（BSS）管理员，拥有该服务下的所有权限。 SMN ReadOnlyAccess：系统策略，消息通知服务的只读访问权限。
HSSReadOnlyAccess	企业主机安全的只读访问权限。	系统策略	SMN ReadOnlyAccess：系统策略，消息通知服务的只读访问权限。

相关链接

- IAM产品介绍
- 创建用户并授予HSS

9 约束与限制

主机防护限制

HSS支持对**华为云主机、第三方云主机和线下数据中心（IDC）**进行防护，具体支持防护的主机类型包括：

- 华为云
  - 华为云弹性云服务器（Elastic Cloud Server，ECS）
  - 华为云裸金属服务器（Bare Metal Server，BMS）
  - 华为云云桌面（Workspace）
- 第三方
  - 第三方云主机
  - 线下IDC

容器防护限制

HSS支持对**华为云集群容器、第三方云集群容器以及线下IDC自建集群容器**进行防护。具体支持防护的容器类型如**表 容器防护限制**所示。

表 9-1 容器防护限制

类别	支持防护的容器类型	约束与限制
华为云	• CCE集群容器 • 非集群纳管的容器	• **容器运行时**限制：Docker、Containerd。 • 集群类型限制：CCE标准版、CCE Turbo版。 • 节点资源剩余要求：内存必须50MiB及以上，CPU必须200毫核(m)及以上。 • 资源占用限制：在集群上安装Agent时，HSS会在集群上创建HSS的命名空间。

类别	支持防护的容器类型	约束与限制
第三方	• 阿里云集群容器 • 腾讯云集群容器 • 微软云集群容器 • 自建集群容器 • IDC自建集群容器 • 非集群纳管的容器	• 集群编排平台限制：1.19及以上Kubernetes。 • 节点操作系统限制：Linux系统。 • 节点规格要求：CPU必须2核及以上，内存必须4GiB及以上，系统盘必须40GiB及以上，数据盘必须100GiB及以上。 • 不支持防护Galera 3.34和MySQL 5.6.51或更早版本的集群。

防护配额限制

在企业主机安全中，防护配额是分配给主机或容器节点的防护资源，每台主机或容器节点开启防护都需要绑定一个防护配额。

以下是防护配额的一些使用限制：

- 防护配额不能跨区域使用。

  购买防护配额时，请正确选择区域信息。不同类型主机，选择区域请参考**表 防护配额区域限制**。

  表 9-2 防护配额区域限制

类别	主机类型	防护配额区域说明
华为云	• 华为云弹性云服务器ECS • 华为云裸金属服务器BMS • 华为云云桌面Workspace	请选择ECS/BMS/Workspace所在区域购买主机防护配额。 HSS不支持跨区域使用，如果主机与防护配额不在同一区域，请**退订配额**后，重新购买主机所在区域的配额。
第三方	• 第三方云主机 • 线下IDC	第三方主机购买配额时选择的区域因接入HSS的方式而不同： • 公网接入：即主机能够访问公网，通过公网将主机接入HSS。目前仅部分区域支持主机通过公网接入HSS，具体区域请参见**哪些区域支持接入非华为云主机?**，请结合主机所在区域综合考虑就近选择购买配额的区域。 • 专线代理接入：即主机不能访问公网，需要通过“专线+代理”的方式接入HSS，该方式对区域没有限制。您想将主机接入哪个区域，即选择哪个区域。

- 一个防护配额只能绑定一个主机或一个容器节点。
- 一个区域最多支持购买50000个防护配额。

- 防护配额购买完成后，您的主机或容器还未被防护，请前往HSS控制台参考界面提示为主机或容器安装Agent并开启防护。

操作系统限制

企业主机安全的Agent、系统漏洞扫描功能对操作系统有一定限制，部分操作系统暂不支持。

HSS对操作系统的限制请参见：

- **表 HSS对Windows操作系统的限制（x86架构）**
- **表 HSS对Linux操作系统的限制（x86架构）**
- **表 HSS对Linux操作系统的限制（Arm架构）**

说明

- CentOS 6.x版本由于Linux官网已停止更新维护，企业主机安全也不再支持CentOS 6.x及以下的系统版本，谢谢您的理解！
- 本文表格中使用的标识含义如下：
  - √表示支持
  - ×表示不支持

表 9-3 HSS 对 Windows 操作系统的限制（x86 架构）

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
Windows 10（64位）	√ **说明** 仅支持华为云云桌面使用该操作系统。	×
Windows 11（64位）	√ **说明** 仅支持华为云云桌面使用该操作系统。	×
Windows Server 2012 R2 标准版 64位英文(40GB)	√	√
Windows Server 2012 R2 标准版 64位简体中文(40GB)	√	√
Windows Server 2012 R2 数据中心版 64位英文(40GB)	√	√
Windows Server 2012 R2 数据中心版 64位简体中文(40GB)	√	√
Windows Server 2016 标准版 64位英文(40GB)	√	√
Windows Server 2016 标准版 64位简体中文(40GB)	√	√

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
Windows Server 2016 数据中心版 64位英文(40GB)	√	√
Windows Server 2016 数据中心版 64位简体中文(40GB)	√	√
Windows Server 2019 数据中心版 64位英文(40GB)	√	√
Windows Server 2019 数据中心版 64位简体中文(40GB)	√	√
Windows Server 2022 数据中心版 64位英文(40GB)	√	×
Windows Server 2022 数据中心版 64位简体中文(40GB)	√	×

表 9-4 HSS 对 Linux 操作系统的限制（x86 架构）

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
CentOS 7.4（64位）	√	√
CentOS 7.5（64位）	√	√
CentOS 7.6（64位）	√	√
CentOS 7.7（64位）	√	√
CentOS 7.8（64位）	√	√
CentOS 7.9（64位）	√	√
CentOS 8.1（64位）	√	×
CentOS 8.2（64位）	√	×
CentOS 8（64位）	√	×
CentOS 9（64位）	√	×
Debian 9（64位）	√	√
Debian 10（64位）	√	√
Debian 11.0.0（64位）	√	√
Debian 11.1.0（64位）	√	√
Debian 12.0.0（64位）	√	×
EulerOS 2.2（64位）	√	√

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
EulerOS 2.3（64位）	√	√
EulerOS 2.5（64位）	√	√
EulerOS 2.7（64位）	√	×
EulerOS 2.9（64位）	√	√
EulerOS 2.10（64位）	√	√
EulerOS 2.11（64位）	√	√
EulerOS 2.12（64位）	√	√
Fedora 28（64位）	√	×
Fedora 31（64位）	√	×
Fedora 32（64位）	√	×
Fedora 33（64位）	√	×
Fedora 34（64位）	√	×
Ubuntu 16.04（64位）	√	√
Ubuntu 18.04（64位）	√	√
Ubuntu 20.04（64位）	√	√
Ubuntu 22.04（64位）	√	√
Ubuntu 24.04（64位）	√ **说明** 暂不支持暴力破解检测。	×
Red Hat 7.4（64位）	√	×
Red Hat 7.6（64位）	√	×
Red Hat 8.0（64位）	√	×
Red Hat 8.7（64位）	√	×
OpenEuler 20.03 LTS（64位）	√	√
OpenEuler 20.03 LTS SP4（64位）	√	×
OpenEuler 22.03 LTS SP3（64位）	√	×
OpenEuler 22.03 LTS（64位）	√	×
OpenEuler 22.03 LTS SP4（64位）	√	×

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
AlmaLinux 8.4（64位）	√	√
AlmaLinux 9.0（64位）	√	×
RockyLinux 8.4（64位）	√	×
RockyLinux 8.5（64位）	√	×
RockyLinux 9.0（64位）	√	×
HCE 1.1（64位）	√	√
HCE 2.0（64位）	√	√
SUSE 12 SP5（64位）	√	√
SUSE 15（64位）	√	×
SUSE 15 SP1（64位）	√	√
SUSE 15 SP2（64位）	√	√
SUSE 15 SP3（64位）	√	×
SUSE 15.5（64位）	√	×
SUSE 15 SP6（64位）	√ **说明** 暂不支持暴力破解检测。	×
Kylin V10（64位）	√	√
Kylin V10 SP3（64位）	√	×
统信UOS 1050u2e	√ **说明** 暂不支持文件逃逸检测。	√

表 9-5 HSS 对 Linux 操作系统的限制（Arm 架构）

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
CentOS 7.4（64位）	√	√
CentOS 7.5（64位）	√	√
CentOS 7.6（64位）	√	√
CentOS 7.7（64位）	√	√
CentOS 7.8（64位）	√	√
CentOS 7.9（64位）	√	√
CentOS 8.0（64位）	√	×

操作系统版本	Agent支持情况	系统漏洞扫描支持情况
CentOS 8.1（64位）	√	×
CentOS 8.2（64位）	√	×
CentOS 9（64位）	√	×
EulerOS 2.8（64位）	√	√
EulerOS 2.9（64位）	√	√
EulerOS 2.10（64位）	√	√
EulerOS 2.11（64位）	√	√
EulerOS 2.12（64位）	√	√
Fedora 29（64位）	√	×
Ubuntu 18.04（64位）	√	×
Ubuntu 20.04（64位）	√	√
Ubuntu 22.04（64位）	√	√
Ubuntu 24.04（64位）	√ **说明** 暂不支持暴力破解检测。	×
Kylin V7（64位）	√	×
Kylin V10（64位）	√	√
Kylin V10 SP3（64位）	√	×
HCE 2.0（64位）	√	√
统信UOS V20（64位）	√	√ **说明** 仅统信UOS V20服务器E版、D版支持系统漏洞扫描。
统信UOS V20 1050e（64位）	√	√
统信UOS V20 1060e（64位）	√	√
OpenEuler 22.03 LTS（64位）	√	×

Agent 限制

- 如果服务器安装了360安全卫士、腾讯管家、McAfee软件等第三方安全防护软件，请先卸载再安装主机安全Agent；第三方安全软件与主机安全Agent存在不兼容的情况，会影响主机安全的防护功能。
- 主机或容器节点安装Agent后，Agent可能修改如下系统文件或配置：

- Linux系统文件：
  - /etc/hosts.deny
  - /etc/hosts.allow
  - /etc/rc.local
  - /etc/ssh/sshd_config
  - /etc/pam.d/sshd
  - /etc/docker/daemon.json
  - /etc/sysctl.conf
  - /sys/fs/cgroup/cpu/（在该目录下新建HSS进程的子目录）
  - /sys/kernel/debug/tracing/instances（在该目录下新建CSA实例）
- Linux系统配置：iptables规则
- Windows系统配置：
  - 防火墙规则
  - 系统登录事件审核策略及登录安全层和认证方式配置
  - Windows Remote Management信任主机列表

暴力破解防护限制

为Windows主机开启防护时，需要授权开启Windows防火墙，且使用企业主机安全期间请勿关闭Windows防火墙。

如果关闭Windows防火墙，HSS无法拦截账户暴力破解的攻击源IP；即使手动关闭后开启Windows防火墙，也可能导致HSS不能拦截账户暴力破解的攻击源IP。

10 HSS 与其他云服务的关系

使用企业主机安全，您将可以同时使用消息通知服务接收告警通知信息，使用统一身份认证服务管理用户权限，利用云审计服务审计用户行为。

弹性云服务器/裸金属服务器

企业主机安全的Agent软件可安装在华为云ECS服务器/BMS服务器上，同时，客户端软件也可安装在第三方主机中。为保障您获得优质可靠的服务，建议您使用华为云主机。

- 关于弹性云服务器的详细内容，请参见**弹性云服务器用户指南**。
- 关于裸金属服务器的详细内容，请参见**裸金属服务器用户指南**。

云容器引擎

云容器引擎（Cloud Container Engine，CCE）基于云服务器快速构建高可靠的容器集群，将节点纳管到集群，企业主机安全通过在集群所在节点上部署Hostguard-agent，为集群中所有可用节点上的容器应用提供防护。

说明

云容器引擎提供高可靠、高性能的企业级容器应用管理服务，支持Kubernetes社区原生应用和工具，简化云上自动化容器运行环境搭建。更多信息请参见《云容器引擎用户指南》。

容器镜像服务

容器镜像服务（Software Repository for Container，SWR）是一种支持容器镜像全生命周期管理的服务，提供简单易用、安全可靠的镜像管理功能，帮助用户快速部署容器化服务，更多信息请参见《容器镜像服务用户指南》。企业主机安全通过扫描镜像中的漏洞与配置信息，帮助企业解决传统安全软件无法感知容器环境的问题。

消息通知服务

消息通知服务（Simple Message Notification，简称SMN），是一个可拓展的高性能消息处理服务。

- 开启告警通知前，您需先配置“消息通知服务”。
- 开启消息通知服务后，当您的主机遭受攻击或被检测出有高危风险时，您将接收到企业主机安全发送的各项风险告警通知。

- 在“告警通知”界面，您可以根据运维计划选择“每日告警通知”和“实时告警通知”。

关于SMN的详细内容，请参见《 消息通知服务用户指南 》。

统一身份认证服务

统一身份认证服务（ Identity and Access Management，简称IAM ），是一个免费的身份管理服务。通过IAM服务，您可以根据HSS用户的身份，对HSS用户的权限进行精细化隔离和控制。IAM是权限管理的基础服务，无需付费即可使用。

关于IAM的详细内容，请参见《 统一身份认证服务用户指南 》。

云审计服务

云审计服务（ Cloud Trace Service，CTS ），是一个专业的日志审计服务。云审计服务能够记录主机中用户对企业主机安全的操作，方便您对主机执行安全分析、合规审计、资源跟踪和问题定位等审计工作。云审计服务是管理日志的基础服务，无需付费即可使用。

关于CTS的详细内容，请参见《 云审计服务用户指南 》。

11 基本概念

账户破解

账户破解指入侵者对系统密码进行猜解或暴力破解的行为。

基线

基线是指操作系统和数据库配置需要满足的最低安全配置要求，基线范围包括账号管理，口令策略配置，授权管理，服务管理，配置管理，网络配置，权限管理等。HSS提供等保合规基线、云安全实践基线、通用安全标准基线检测，可满足用户多种安全合规检测需求。

弱口令

弱口令指密码强度低，容易被攻击者破解的口令。

恶意程序

恶意程序指带有攻击或非法远程控制意图的程序，例如：后门、特洛伊木马、蠕虫、病毒等。

恶意程序通过把代码在不被察觉的情况下嵌到另一段程序中，从而达到破坏被感染服务器数据、运行具有入侵性或破坏性的程序、破坏被感染服务器数据的安全性和完整性的目的。按传播方式，恶意程序可以分为：病毒、木马、蠕虫等。

恶意程序包括已被识别的恶意程序和可疑的恶意程序。

勒索病毒

勒索病毒，是伴随数字货币兴起的一种新型病毒木马，通常以垃圾邮件、服务器入侵、网页挂马、捆绑软件等多种形式进行传播。

一旦遭受勒索病毒攻击，将会使绝大多数的关键文件被加密。被加密的关键文件均无法通过技术手段解密，用户将无法读取原来正常的文件，仅能通过向黑客缴纳高昂的赎金，换取对应的解密私钥才能将被加密的文件无损的还原。黑客通常要求通过数字货币支付赎金，一般无法溯源。

如果关键文件被加密，企业业务将受到严重影响；黑客索要高额赎金，也会带来直接的经济损失，因此，勒索病毒的入侵危害巨大。

双因子认证

双因子认证是指结合密码以及验证码两种条件对用户登录行为进行认证的方法。

网页防篡改

网页防篡改为用户的文件提供保护功能，避免指定目录中的网页、电子文档、图片等类型的文件被黑客、病毒等非法篡改和破坏。

集群

集群是同一个子网中一个或多个弹性云服务器（又称：节点）通过相关技术组合而成的计算机群体，为容器运行提供计算资源池。

节点

在容器中，每一个节点对应一台弹性云服务器（Elastic Cloud Server，ECS），容器运行在节点上。

镜像

镜像（Image）是一个特殊的文件系统，除了提供容器运行时所需的程序、库、资源、配置等文件外，还包含了一些为运行时准备的配置参数。镜像不包含任何动态数据，其内容在构建之后也不会被改变。

容器

容器（Container）是镜像的实例，容器可以被创建、启动、停止、删除、暂停等。

容器运行时

容器运行时（Container Runtime）是Kubernetes最重要的组件之一，负责真正管理镜像和容器的生命周期。Kubelet通过Container Runtime Interface (CRI)与容器运行时交互，以管理镜像和容器。

安全策略

安全策略是指容器运行时需要遵循的安全规则，如果容器违反了安全策略，容器安全服务控制台的“运行时安全”页面会显示容器异常。

项目

项目用于将OpenStack的资源（计算资源、存储资源和网络资源）进行分组和隔离。项目可以是一个部门或者一个项目组。

一个账户中可以创建多个项目。

防护配额

目标主机开启检测防护需要绑定的对象，即防护配额。

在企业主机安全购买的不同版本的数量在控制台中是以防护配额的描述呈现。

示例：

- 购买了1个企业版，即企业版可用防护配额数量为1个，只能绑定任意1台主机。
- 购买了10个旗舰版，即旗舰版可用防护配额数量为10个，可分配至10台不同主机进行分别绑定。

