主机安全

产品简介

产品文档

腾讯云

文档目录

产品简介
产品概述

最近更新时间：2023-12-26 15:19:16

本文将为您介绍主机安全的基本情况。

产品概述

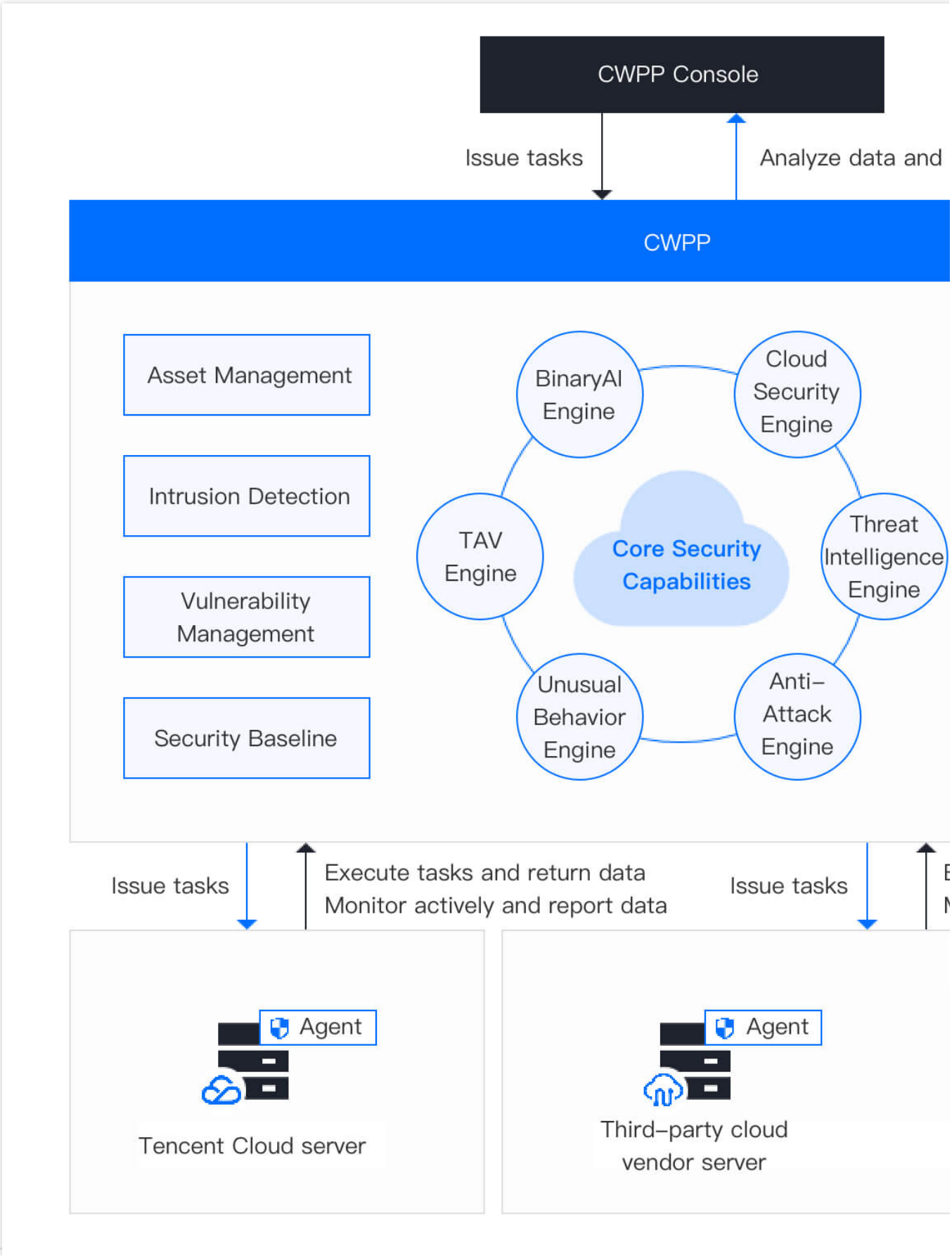
主机安全（Cloud Workload Protection，CWP）是一款针对多云主机的安全防护产品，基于腾讯安全积累的海量威胁数据，利用机器学习为您提供黑客入侵检测、漏洞风险告警等安全防护服务，主要包括密码破解阻断、异常登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系。

所获资质

主机安全已通过云计算产品信息安全、CSA、CSTR等多项国际权威认证。
VB100——连续通过42次，检测100%
AV-C——获得29个A+评级，连续三年Top Rate产品
Gartner——荣获主机安全市场指南推荐
AMTSO——全球AMTSO成员
AVAR——亚洲反病毒联盟成员
EICAR——欧洲反病毒协会会员

工作原理

安装主机安全客户端的服务器，可获得主机安全的六大安全能力。
用户通过主机安全控制台下发检测任务时，客户端将执行检测任务并回传数据，在主机安全控制台上可统一查看并处理安全事件。


CWPP Console
Issue tasks
Analyze data and
CWPP
Asset Management
Intrusion Detection
Vulnerability Management
Security Baseline
BinaryAI Engine
Cloud Security Engine
TAV Engine
Core Security Capabilities
Threat Intelligence Engine
Unusual Behavior Engine
Anti-Attack Engine
Issue tasks
Execute tasks and return data
Monitor actively and report data
Issue tasks
Agent
Tencent Cloud server
Agent
Third-party cloud vendor server

名词	描述

主机安全控制台	腾讯云自主研发的云原生安全系统。 提供一站式主机安全解决方案，从预防-防御-检测-响应形成安全闭环。
客户端	主机安全官方安全插件，支持混合云主机。 可向主机安全云平台实时同步风险信息，也可执行主机安全控制台下发的检测或处理任务。
腾讯云服务器	云服务器（CVM）、轻量应用服务器（Lighthouse）、边缘计算机器（ECM）。
非腾讯服务器	第三方云厂商服务器、IDC服务器。
主机安全云平台	主机安全云平台是安全信息处理的中枢，可持续检测分析各服务器客户端回传的信息，拥有六大核心安全能力，可从各个维度上判断主机安全情况。 1. TAV引擎：高效查杀二进制木马病毒。 2. BinaryAI引擎：基于深度学习算法的二进制识别引擎，高效查杀恶意样本。 3. 云查杀引擎：基于深度自学习算法，云查多引擎鉴定，高效查杀国内外流行木马、病毒文件。 4. 威胁情报：积累百亿威胁情报资源库，实时动态更新和鉴定恶意文件、IP、域名等信息。 5. 攻击防御：实时监控网络攻击行为，包括：Webshell 探测、Struts 漏洞利用、代码仓库拉取、代码注入攻击、暴力破解等攻击行为，提供自动防御能力。 6. 异常行为：基于异常特征实时匹配，多行为组合威胁检测，实时检测并告警恶意入侵事件。

支持版本

主机安全目前提供基础版、专业版、旗舰版三个防护版本，不同版本功能区别，请参见 功能介绍与版本比较。

产品使用

注册腾讯云账号后，您可以通过主机安全控制台进行安全防护设置，关于控制台操作，请参见 操作指南。

产品优势

最近更新时间：2023-12-26 15:19:26

本文将为您介绍主机安全的产品优势。

产品优势

腾讯云主机安全与其他主机安全产品相比，优势如下：

优势	腾讯云主机安全	其他主机安全产品
黑客行为检测	基于腾讯全网威胁数据源，实时检测黑客攻击行为。	基于单机行为数据进行判断，检测能力弱，无法快速响应。
木马文件检测	后端集成腾讯电脑管家新一代 TAV 反病毒引擎及哈勃分析系统，极速响应未知风险。基于机器学习的 WebShell 检测引擎，有效对抗加密变形类恶意脚本。	可执行恶意文件的检测能力缺失，基于正则、字符逻辑匹配方式对 WebShell 进行检测，误报、漏报风险高。
免安装、维护	自动关联云平台服务器运维信息,购买云服务器、轻量应用服务器或边缘计算机器即可使用相关信息。安全策略云端自动更新，无需人工维护各种安全检测脚本文件。	需要用户登录服务器手动安装，且需要一定安全技术能力的人进行安全策略配置。
集中运维	安全事件可在控制台统一管理，省去登录多台服务器的麻烦。主机资产集中管理，快速构建安全可视化运维平台。	需要登录到服务器上，对单个安全事件进行处理。
低资源占用	自研轻量级 Agent，绝大部分计算和防护在云端进行，对服务器的资源消耗占用低。	软件客户端内存占用高，普遍消耗在100M以上，业务峰期会影响服务器性能。

基本概念

最近更新时间：2023-12-26 15:19:33

本文将为您介绍主机安全的基本概念。

基本概念

主机安全涉及的常见概念如下。

安全基线

安全基线（Security Base Line）指为了满足安全要求，相关系统和服务安全配置必须达到的一定标准和基本要求。通过对不同配置和策略的具体项目来评估产品是否达到安全基线，包括账号配置安全、口令配置安全、授权配置、日志配置、网络配置等。安全基线评估结果在一定程度上，反映了服务器的安全性。

木马病毒

木马病毒是指隐藏在正常程序中的一段具有特殊功能的恶意代码，是具备破坏和删除文件、发送密码、记录键盘和 DDoS 攻击等特殊功能的后门程序。

WebShell

WebShell 就是以 ASP、PHP、JSP 或 CGI 等网页文件形式存在的一种命令执行环境，也称为一种网页后门。黑客在入侵了一个网站后，通常会将 ASP 或 PHP 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，然后使用浏览器来访问 ASP 或者 PHP 后门，得到一个命令执行环境，以达到控制网站服务器的目的。

漏洞检测

漏洞检测（Host Vulnerability Detection）指基于主机 Agent 在主机内部发现漏洞的一种方式。将漏洞检测模块运行于主机内部，直接进行验证或者采集信息，来判断主机是否存在漏洞。

系统组件

组件（Component）或者通用组件，在主机安全层面主要泛指服务、应用对应的 Web 容器、软件等，例如 Nginx、Wordpress 等，而系统组件主要指非 Web 类的系统软件。

通用组件漏洞

通用组件漏洞又称为通用漏洞（Common Vulnerability），主要指通用组件而非业务自开发代码产生的漏洞，例如 WordPress 某个 SQL 注入、组件 Bash 的破壳漏洞等。

未授权访问

未授权访问（Unauthorized Access）是不满足安全基线导致的一类问题，主要指相关服务没有对服务的访问条件进行限制，例如设置密码、限制访问来源等，导致任何人都可以直接连接服务进行操作，从而产生安全问题。

异常登录

通过采集服务器上 RDP、SSH 登录日志，上报登录源 IP、登录用户名、登录时间、登录地等信息到云端进行风险评定，对非法登录进行实时告警通知。

隔离文件

隔离技术把存在恶意行为的木马、病毒文件进行隔离存储，避免恶意文件持续扩散。

应用场景

最近更新时间：2023-12-26 15:19:41

本文将为您介绍主机安全的常见应用场景。

应用场景

服务器一旦被黑客入侵，企业面临以下安全风险：
业务被中断：数据库、文件被篡改或删除，导致服务无法访问，系统瘫痪。
数据被窃取：黑客窃取企业数据后公开售卖，客户隐私数据被泄漏，造成企业品牌受损和客户流失。
被加密勒索：黑客入侵服务器后通过植入不可逆的加密勒索软件对数据进行加密，对企业进行金钱勒索。
服务不稳定：黑客在服务器中运行挖矿程序，并通过 DDoS 木马程序获取经济利益，消耗大量的系统资源，导致服务器不能提供正常服务。
使用主机安全可以有效预防以上问题，保障企业主机安全。

关联产品

最近更新时间：2023-12-26 15:19:48

本文将为您介绍与主机安全产生关联的其他腾讯云产品。

关联产品

以下腾讯云产品与主机安全存在关联：

腾讯云产品	涉及主机安全功能	关联描述
云服务器（CVM） 轻量应用服务器（Lighthouse） 边缘计算机器（ECM）	全部功能	云服务器、轻量应用服务器、边缘计算机器均为腾讯云提供的计算服务，是主机安全的防护对象。
云硬盘（CBS）	漏洞修复	主机安全漏洞自动修复需要先进行快照备份，此处运用了云硬盘快照服务作为支持。

功能介绍与版本比较

最近更新时间：2023-12-26 15:21:38

本文将为您介绍主机安全的各版本功能特性。

产品优势

不同版本的主机安全提供的主要功能对比如下表所示：

类别	内容	详细描述	基础版 免费	专业版 包年包月：12美元/个/月	旗舰版 包年包月：27美元/个/月
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。	✓	✓	✓
资产管理	资产概览	可查看全部主机及各项资产指纹的统计情况。也可查看账号、端口、进程、软件应用、数据库、Web 应用、Web 服务、Web 框架、Web 站点 TOP5。	✓	✓	✓
	主机列表	可查看目前已接入主机安全的所有服务器的信息，帮助您全面了解资产的安全状态。	✓	✓	✓
	资产指纹	可为您提供主机资源监控、账号、端口、进程等详细的资产盘点数据，同时，您也可以基于资产指纹功能，对已发生的安全事件风险影响面进行快速调查。	×	✓ 支持10种指纹	✓ 支持15种指纹
入侵检测	文件查杀	Webshell 检测：提供常用的 Web 网站类脚本木马后门检测，包含 ASP/PHP/JSP/Python 等脚本语言。 二进制检测：提供对二进制可执行类的病毒木马检测，例如 DDoS 木马、远控、挖矿类软件等，文件类型包括 exe、dll、bin 等，并告警用户。	✓ 累计免费5条，超过则停止检测	✓ 支持检测，无自动隔离	✓ 支持检测+自动隔离
	密码破解	支持对 SSH、RDP 等暴力破解行为进行实时检测、告警、阻断功能，支持登录白名单配置。 支持用户自定义暴破阻断规则设定，例如，判断条件规则（1分钟5次等），阻断时长	✓ 只检测，无阻断	✓ 支持检测+自动阻断	✓ 支持检测+自动阻断

		（阻断15分钟等）。 事件记录包含：破解状态、服务器、来源IP、来源地、登录用户名、攻击时间、尝试次数、阻断状态等信息。			
	异常登录	支持实时检测登录行为，自动识别非白名单IP 登录，识别出恶意登录行为。 支持白名单配置，条件包括：登录来源地、来源 IP、服务器、登录用户名及登录时间。	✓	✓	✓
	恶意请求	支持实时检测主机内外联恶意域名请求，提供威胁源信息和事件记录，并自动告警用户。	×	✓	✓
	本地提权	针对本地提权行为实时告警，并支持白名单配置。 事件记录包含：服务器/名称、提权用户、提权进程、父进程、父进程所属用户、发现时间、文件路径及进程树等。	×	✓	✓
	反弹shell	针对反弹 shell 行为实时告警，并支持白名单配置。 事件记录包含：服务器/名称、连接进程、父进程、目标主机、目标端口、发现时间、文件路径、进程树及执行命令等。	×	✓	✓
	高危命令	记录云服务器上执行的 bash 命令，实时监控被审计规则判断为危险的操作。 提供默认规则配置，以及支持用户自定义规则配置。 事件记录包含：服务器/名称、命中规则名、危险等级、命令内容、登录用户及操作时间等。	×	✓	✓
漏洞管理	应急漏洞	支持检测近期紧急漏洞检测（例如 0day 等）。 漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。	✓ 累计免费5条，超过则停止检测	✓ 支持检测，无修复	✓ 支持检测+部分修复
	Linux 软件漏洞	支持常用 Linux 软件漏洞检测，提供修复方案，例如：gnutls 资源管理错误等 Linux 软件漏洞。 漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。			

	Windows 系统漏洞	通过实时同步微软官网补丁源，对 Windows 系统漏洞进行检测并提供修复方案，避免黑客通过 Windows 系统漏洞攻击或威胁您的服务器安全。 漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。			
	Web - CMS 漏洞	支持常用 Web 类型的漏洞检测，提供修复方案，例如 phpMyAdmin 及 WordPress 等 Web 类组件。 漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。			
	应用漏洞	提供系统服务弱口令、系统服务和应用服务的漏洞检测服务。 漏洞详情包含：漏洞描述、漏洞类型、威胁等级、修复方案、参考链接、披露事件、CVE 编号、CVSS 评分及雷达图等。			
安全基线	CIS 基线标准	支持CIS、弱口令等基线检测，并提供修复方案。 展示不同基线策略下的检测服务器、检测项、基线通过率、基线检测项 TOP5 和服务器风险 TOP5 检测结果信息，支持一键检测和定期检测。	✓ 累计免费5条，超过则停止检测	✓ 支持检测，无自定义	✓ 支持检测+自定义
	腾讯云基线标准				
	弱口令基线				
高级防御	核心文件监控	可以配置核心文件的监控规则并查看及处理监控事件，同时也支持白名单设置，用于放行被允许的文件访问行为。(目前暂只支持 Linux 内核，版本为3.10以上的操作系统)	×	×	✓
设置中心	告警通知	支持短信、邮件等告警通知发送方式，支持输出告警事件列表。	✓	✓	✓
	授权管理	成功购买主机安全专业版或旗舰版可在授权管理页面绑定要升级防护的主机。已成功升级防护的主机也可进行解绑操作。	✓	✓	✓
性能	资源占用	agent 资源消耗低，不影响系统正常运行，CPU 小于5%，内存小于30M。	✓	✓	✓
	稳定性要求	系统具有高可靠性及稳定性设计，在云服务器出现异常情况时，可进行降级或自杀等机	✓	✓	✓

		制，确保业务的正常运行。			
	多操作系统支持	兼容 Windows 、CentOS、Debian、RedHat 等主流操作系统。	✓	✓	✓