腾讯云T-Sec主机安全-服务器安全 入侵检测 漏洞管理

产品名称	腾讯云T-Sec主机安全-服务器安全 入侵检测 漏洞管理
公司名称	昆山昱唯网络科技有限公司
价格	3.00/个
规格参数	品牌:腾讯云 产品:T-Sec主机安全
公司地址	花桥国际商务城曹新路70号
联系电话	17601404160

产品详情

什么是主机安全

主机安全是一款针对于云上主机安全防护的产品，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和漏洞风险预警等安全防护服务，主要包括密码破解拦截、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。

主机安全目前提供基础防护与专业防护两个版本，不同版本主机安全提供的主要功能区别。

为什么需要主机安全

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您流失。

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。

主机安全主要功能文件查杀

网站后门木马又叫 WebShell，一般是黑客通过漏洞入侵网站后放置的 ASP、PHP、JSP 等动态脚本。黑客可以通过后门木马持续控制服务器，进行文件上传下载、执行命令等各种破坏行为，对网站安全危害极大。基于机器学习的网站后门检测技术并依托腾讯云安全平台的全网恶意文件样本收集能，木马文件可以实时准确的检测各类木马恶意文件，同时提供恶意文件检测和一键隔离等功能，保护您服务的安全。

异常登录

基于您的常用登录地和恶意登录源两个维度，对服务的登录日志进分析，识别出服务器登

录流水中的异地、异常登录为，并且实时通知给您。根据服务器的账户登录为分析，对可疑的登录为提供实时告警通知。基于云服务器的流水查询功能，您可以对比流水与自己登录为的差异，得出是否有异常登录为，并采取相应的安全措施。

密码破解

您的云服务器可通过互联网登录，给了不法之徒进行暴力破解尝试入侵您云服务器的机会。腾讯云安全通过多维度多种手段检测云服务器是否被尝试暴力破解其密码。若检测有异常，会通过站内信或者短信等渠道对您进行告知。

恶意请求

主机安全通过对外界请求行为的实时监控及处理能力，实现对恶意请求行为的有效识别。若检测到恶意请求行为，主机安全系统会向您提供实时告警通知。

高危命令

基于腾讯云安全技术及多维度多种手段，对系统中命令实现实时监控，并且可通过配置规则对命令危险程度进行等级划分。若检测出高危命令，主机安全系统会向您提供实时告警通知。

本地提权

若出现以低权限进入系统，并通过某些手段提升权限，获取到高权限的事件，很有可能为黑客的攻击行为，该行为会危害到云服务器的安全。主机安全的本地提权功能可实时监控您服务器上的提权事件，并能对提权事件详情进行查看和处理，同时也支持白名单创建功能，用于设置被允许的提权行为。

反弹 Shell

反弹 Shell 功能是基于腾讯云安全技术及多维度多种手段，对服务器上的 Shell 反向连接行为进行识别记录，为您的云服务器提供反弹 Shell 行为的实时监控能力。

漏洞管理

主机安全对云服务器上存在的高危漏洞风险进行实时预警并提供修复方案，包括系统漏洞及 Web 类漏洞，帮助企业快速应对漏洞风险。

基线管理

腾讯云主机安全支持对基线检测项的定期检测和一键检测、支持对指定主机上的指定基线项进行检测、支持通过检测策略了解基线通过率及风险情况，同时可提供基线和检测项的风险等级和修复建议，同时提供腾讯云默认基线策略，有助于您更好的管理服务器中的基线安全。

网络防御

基于腾讯云安全技术，实时监控网络攻击行为，支持检测的威胁类型包括：Webshell 探测、Struts
漏洞利用、代码仓库拉取、代码注入攻击、命令注入攻击及机器批量控制利用等。

安全运营

根据《网络安全法》规定，日志存储时长不少于6个月，推荐每台服务器配置30GB存储容量以便采集和留存日志数据。日志分析提供木马、漏洞及网络安全事件等多维度的安全日志，支持语句检索和查询，并提供可视化报表、统计分析和导出功能，让您能够快速的排查和溯源主机上的安全事件，并提升运营效率。