主机安全

产品简介

产品文档

腾讯云

文档目录

产品简介
产品介绍

最近更新时间：2020-06-29 16:05:03

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，利用机器学习为用户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。

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用户流失。
- **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。

主机安全主要功能

木马检测

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力，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，保护用户服务器的安全。

密码破解提醒

用户的主机可通过互联网登录，给了不法之徒进行暴力破解尝试入侵用户主机的机会。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用户进行告知。

登录行为审计

基于用户的常用登录地和恶意登录源两个维度，对服务器的登录日志进行分析，识别出服务器登录流水中的异地、异常登录行为，并且实时通知给用户。根据服务器的账户登录行为分析，对可疑的登录行为提供实时告警通知。
基于云服务器的流水查询功能，用户可以对比流水与自己登录行为的差异，得出是否有异常登录行为，并采取相应的安全措施。

漏洞管理

对主机上存在的高危漏洞风险进行实时预警和提供修复方案，包括系统漏洞、Web 类漏洞，帮助企业快速应对漏洞风险。

资产管理

支持对机器进行分组标签管理，基于组件识别技术，快速掌握服务器中软件、进程、端口的分布情况。

产品优势

最近更新时间：2020-06-29 16:03:34

腾讯主机安全与其他主机安全产品的优势比较如下表所示：

优势	腾讯主机安全	其他主机安全产品
黑客行为检测	**基于腾讯全网威胁情报数据源，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：2020-06-11 15:48:51

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、记录键盘和攻击 DDoS 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。

主机漏洞检测

主机漏洞检测（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。

登录审计

登录审计采集服务器上的 RDP 和 SSH 登录日志，上报来源 IP、时间、登录用户名、登录状态等信息到云端进行风险计算，对非法登录进行实时告警。

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。