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：2018-09-04 15:06:20

云镜是什么？

云镜是一款针对于云上主机安全防护的防御产品，为云主机提供多层次全方位的系统防护技术，其融合了腾讯多年积累的海量威胁情报数据、漏洞信息。通过利用机器学习，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、异地登录提醒、木马文件查杀、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，防止数据泄露。

为何需要云镜？

服务器一旦被黑客入侵，企业面临哪些安全风险？

- **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、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。

使用云镜可以有效预防以及防御以上问题，保障企业网站的系统以及业务安全。

云镜主要功能

木马查杀

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。

木马文件检测依托腾讯云安全平台的全网恶意文件样本收集能力和基于机器学习的网站后门检测技术，可以实时准确的查杀各类木马恶意文件，同时提供恶意文件检测和一键清理等功能，第一时间清除木马后门文件，确保用户服务器的安全。

密码破解提醒

用户的主机可从互联网上进行登录，给了不法之徒进行暴力破解尝试入侵用户主机的机会，腾讯云安全通过多纬度多种手段，检测云服务器是否被尝试暴力破解其密码。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：2018-09-04 15:06:52

云镜的优势以及与其他主机安全产品的比较如下表格所示：

优势	云镜的优势	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；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；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。