**服务器安全卫士**

产品定义

通过在服务器端安装轻量级的Agent进行安全监测和防护，监测数据由天翼云专业安全团队以报告的形式定期发送给客户，并对入侵等高危情况进行实时邮件通知，从而客户可以及时全面的了解服务器的安全状态，将安全从传统的安全事件防护变成一项持续安全响应和处理过程。功能涵盖弱口令检测、软件漏洞检测、防暴力破解、web后门、shell检测等多个维度，实现服务器安全的持续纵深保护。

术语解释

**Agent：**指服务器安全监测与防护代理软件，运行在客户服务器操作系统，该安全代理具备严格的权限和运行负载控制，保护服务器的同时对业务运行不产生影响。

**弱口令：**容易被别人猜测（包括信息泄露导致）或被破解工具破解的口令均为弱口令。软件漏洞：应用软件、中间件软件或操作系统软件在设计、实现上的缺陷或错误，被不法者利用，通过网络植入木马、病毒等方式来攻击或控制整个服务器，窃取服务器中的重要资料和信息，甚至破坏系统服务。

**Web后门：**Web后门是一段网页代码，主要以ASP、PHP、JAVA代码为主。由于这些代码都运行在Web服务器端，攻击者通过插入这段精心设计的代码，在Web服务器端进行某些危险的操作，获得某些敏感的技术信息或者通过渗透、提权获得服务器的控制权。

**反弹shell：**指黑客的恶意控制端监听在某TCP/UDP端口，被控制的服务器发起请求到该端口，并将其命令行的输入输出转到控制端。由于是内部主动外联请求，以防火墙为代表的产品无法检测与拦截此类攻击。

**POC：**Proof of Concept，中文意思是“观点证明”。漏洞报告中的POC是指一段说明或者一个攻击的样例，使得读者能够确认这个漏洞是真实存在的。

**CVSS：**Common Vulnerability Scoring System，即“通用漏洞评分系统”，是一个行业公开标准，其被设计用来评测漏洞的严重程度，并帮助确定所需反应的紧急度和重要度。

**Rootkit：**Rootkit是一种特殊的恶意软件，它的功能是在目标服务器上隐藏自身及指定的文件、进程和网络链接等信息，比较多见到的是Rootkit一般都和木马、后门等其他恶意程序结合使用。Rootkit通过加载特殊的驱动，修改系统内核，进而达到隐藏信息的目的。

产品规格

支持主流Linux（64位）和windows server（64位）服务器  
可提供以下产品规格：

|  |  |  |  |
| --- | --- | --- | --- |
| **产品功能** | **功能介绍** | **企业版** | **旗舰版** |
| 资产清点 | 自动清点主机内部资产如进程、端口、账号、应用等，实时掌握主机内部资产变化，为安全分析提供数据基础。 | **√** | **√** |
| 软件漏洞检查 | 精准本地分析漏洞，包含精准POC探测和版本漏洞探测；支持CVSS等漏洞信息详细描述，支持漏洞修复影响检查；提供命令级漏洞修复建议。 | **√** | **√** |
| 基线检查 | 高效基线模版、自动快速检测使基线管理行之有效；命令级修复建议，优化繁琐修复工作。 | **√** | **√** |
| 弱口令检查 | 弱口令自动检测，自动匹配账号名相关易猜解密码，支持弱口令字典自定义。 | **√** | **√** |
| 暴力破解监测与拦截 | 实时暴力破解多层次监控，支持暴力破解拦截功能，支持自动黑名单记录。 | **√** | **√** |
| 异常登录检查 | 实时异常登录监控，发现异常IP、区域、时间等的异常登录，支持恶意库匹配，支持自动更新黑名单功能。 | **√** | **√** |
| 操作审计（\*） | 实时操作命令记录，实时发现危险操作，支持审计规则自定义。提供应急响应回溯分析数据支持。 | **×** | **√** |
| Web后门监控 | 多维度Web后门识别，支持规则匹配、相似度匹配、沙箱检测、模式分析引擎检测等多种机制检测，具备实时监测能力。 | **×** | **√** |
| 后门诊断 | 精准发现系统内后门程序，如rootkit，提供详细后门程序分析报告与修复建议。 | **×** | **√** |
| 反弹shell监控（\*） | 支持实时监控黑客反弹shell攻击，支持攻击情况详细记录。 | **×** | **√** |
| 本地提权监控（\*） | 支持实时进程提权监测，支持进程提权过程详细记录。 | **×** | **√** |

注：（\*）功能暂不支持windows操作系统

产品功能

* 全面细致的风险分析报告：自动化细粒度风险分析,包括如弱密码；
* 软件漏洞、web网站风险等等,天翼云安全专家将可视化报告定期报送给客户；
* 所有安全风险、安全加固、漏洞修复等都具有详细的视图与可落地的操作指令；
* 无需安全专家配合即可轻松进行安全运维工作；
* 自内而外的监测防护：从服务器内部进行安全的监控与分析；
* 最高程度发现问题并第一时间对入侵进行响应与告警；
* 强大的风险检测能力：扫描超过20000个漏洞，并且给出明确的漏洞验证处理方法；
* 实时分析发现反弹Shell；实时监控暴力破解行为，迅速通知并阻断恶意IP；
* 多维度Webshell检测，最大程度发现Webshell威胁。

应用场景

* **云安全建设**

云环境下业务快速变化，传统边界式防御无法有效跟进业务变化。服务器安全卫士自动清点业务资产，实时掌握动态资产变化，确保不发生“马奇诺防线”的情况。

* **安全体系搭建**

服务器安全卫士基于角色的安全管理，自学习快速搭建完善的安全体系，完善安全防护中的防御、检测、回溯分析和预测能力，形成完整、联动的高级威胁防护体系。

* **统一管理**

防护的一大挑战是不知道有什么安全问题。服务器安全卫士自动检测风险、快速跟进新漏洞、多维度报表导出加强安全可视化、可管理性，持续控制低水平风险值。

* **漏洞应急响应**

现今漏洞爆发愈发频繁，如何定速定位高危漏洞是关键。服务器安全卫士依据资产清点为基础数据，在0day漏洞爆发的第一时间即可提供相关漏洞排查分析，快速定位漏洞分布。同时对0day漏洞利用攻击也具备实时入侵检测。

常见问题

**Q：服务器安全产品能解决什么问题？**  
A：服务器安全卫士产品是一个完整的服务器安全防护系统，帮助客户建立防御-检测-响应-预测全面安全体系。服务器安全卫士产品能够解决防御的问题，缩小系统攻击面，提升安全等级。也能够解决如何发现黑客的问题，包括:实时黑客行为特征锚点监控，检测黑客常见入侵手段；与业务正常行为结合分析，发现系统内部异常潜伏攻击。  
**Q：安装agent会不会对自身的业务稳定性产生影响？**  
A：不会。agent是纯应用层的，不会给系统装任何的驱动，不会影响系统的稳定性；agent对系统是只读的，不会改写任何数据；agent的带宽和资源占用很小；agent已经通过各种业务场景长时间运行测试。  
**Q：是否可以对内网主机进行监测防护？**  
A：可以。需要配置一台公网转发服务器。  
**Q：订购后如何部署？**  
A：订购成功后填写开通单，可以授权让天翼云安全专家部署，也可以在天翼云安全专家的指导下客户自己部署，部署过程非常简单。  
**Q：如何接收监测报告？**  
A：天翼云安全专家每周将监测报告发送至客户指定的邮箱。  
**Q：如何接收实时告警邮件？**  
A：天翼云安全中心将实时告警邮件发送至客户指定邮箱。