**安华金和产品技术参数**

1. **安全审计设备参数**

1、2U可上架硬件平台，支持多核处理，系统标配4个10/100/1000Mbps网络接口。最大并发连接数>=100万，每秒新建连接数>=8000。

2、支持网络旁路部署方式模式，不需要更改原有网络结构、数据库服务器相关配置等即可进行产品的部署，产品运行不影响现有网络和业务的正常运行，通过https方式进行系统配置管理，

3、支持系统资源监控，包括：CPU占用率，内存占用率，当前流量监控

4、支持添加多个管理员，不同管理员可划分不同权限，管理员登录系统时只显示他所具有权限的页面，不具有权限的页面不显示。

5、支持外接数据库，审计数据可直接存储到外围数据库服务器上

6、支持在线、本地两种方式升级

7、支持多种数据库类型审计，包括Oracle，Microsoft SQL Server，DB2，Sybase, Informix、MySQL、人大金仓（Kingbase）、达梦(DM)等，

8、支持对数据库会话的完整审计，可以完整分析出每条数据库会话的会话源IP，源MAC，源Port，目标IP，目标MAC，目标Port，会话起止时间，数据库用户名、数据库表名、执行操作等会话内容

9、支持对网页浏览的记录，记录用户的IP，MAC，访问时间，类别,URL地址等

10、支持对下载文件名关键字进行审计

11、支持对网页提交内容关键字进行审计

12、可根据URL分类库进行分类审计

13、支持对搜索内容关键字进行审计

14、支持对POP3、SMTP、Webmail记录，记录邮件发件人、收件人、标题、正文、附件、大小等外发信息。

15、支持图形报表功能，能够根据用户、应用、流量生成图形报表

16、产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。

1. **堡垒机设备参数**

1、2U机架，接口数≥6个千兆电口，可扩展接口，硬盘不小于1T；图形操作并发数不少于350个，字符操作并发数不少于500个；提供管理设备License数量200个。

2、采用物理旁路、逻辑网关的方式接入，对现有主机和网络环境不做任何修改,不在服务器和客户端安装引擎。

3、图形终端协议：Windows RDP、VNC、X11等

字符终端协议：Telnet、SSH等

文件传输协议：FTP、SFTP等

数据库类型：Oracle、Sqlserver2000\2005\2008、DB2、Sybase、Informix、Mysql等

WEB应用：HTTP、HTTPS等

APP应用：AS400等

4、支持C/S与B/S运维方式，使用运维工具时，无需安装JAVA等特定工具，不改变用户使用习惯

5、可以指定系统用户查看该用户可管理的资产信息；可以指定资源名/资产IP/账号名查看资产属于哪些系统用户管理

6、系统角色需按权限要求进行划分，至少有系统管理员、设备管理员、审计管理员、普通用户等多种角色。

7、系统提供身份认证，登录系统时支持动态口令、radius认证、AD域和数字证书等认证。

8、支持以excel格式批量导入和导出用户帐号；

9、系统支持AIX、HP-Unix、Solaris、SCO-Unix、Linux、Windows等主机服务器操作系统、各类网络/安全设备、主流的数据库服务器、业务管理系统等。

10、支持对目标设备进行分组管理，并保证将分组的设备可以实现细化授权。

11、支持对目标设备进行批量管理，如批量导入目标设备信息、批量导出目标设备信息。便于对目标设备进行统一管理。

12、支持口令代填功能，系统提供用户访问真实资源时的自动登录，从而简便运维操作。

字符类协议代填，支持SSH、Telnet口令代理

图形类协议代填，支持RDP、VNC、X11口令代理，其中VNC能够支持账号密码格式的代填

文件传输类协议代填，支持FTP、SFTP口令代理

13、支持linux、unix、网络设备、windows2000/2003/2008等的自动改密功能；

无需通过插件、引擎或特殊端口对目标设备进行自动改密。密码策略包括：执行周期(按每月、每周、每天、定时)，密码生成(随机密码、指定密码)，密码复杂度(长度、数字、大小写字母、特殊字符)，

14、系统提供访问控制功能，支持对系统的用户登录进行可配置的策略设置，根据策略因子：用户或用户组、日期、每月、每周、时间、源地址、目标地址、目标端口、目标账号、动作(接受、拒绝)来定制访问策略对用户或用户组行为进行控制。

15、系统可以对字符操作的命令进行控制，通过制定命令黑白名单实现对命令的有效管理，可以对命令集合进行告警或者自动阻断。

16、支持命令记录：字符终端命令记录、图形终端键盘操作记录、数据库运维SQL命令

17、支持在线监控用户屏幕操作信息，可以切断任意恶意或危险操作会话

18、系统具备对登录人员进行审计，如登录时间、登录用户、登录IP、登录方式、登录是否成功登日志信息。

19、导出日志可以使用离线播放器进行日志查看，包括命令、录像等。

20、系统具备在对系统制定报表任务时，可以配置时间周期，实现按照每天、每周、每月、立即等时间生成报表。

21、产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。

1. **安全管理中心平台参数**

1、产品支持网络安全设备资产集中管理，能够把资产管理和组织结构或者网络拓扑结构紧密结合；支持IP地址、域名和资产树等多种资产管理方式；支持通过\*.CSV文件将地址导入到资产树功能；可以通过多种维度搜索并定位资产，包括并不限于：节点或设备名称、资产IP范围、资产管理员、资产操作系统类型、资产风险等级、漏洞名称、开放的端口、资产banner信息等。

2、产品支持安全设备日志集中告警平台，可以灵活配置告警内容、告警方式、告警资产范围等内容。

3、支持安全设备IP地址，端口，设备名称，登录帐号，密码，版本，类型，工程师管理接口等重要参数的设置

4、支持分析安全设备的网络故障日志，接口状态日志，高可用性日志，系统日志，bypass日志

5、支持安全设备的CPU使用率，内存使用率，磁盘剩余空间，接口流量等设备状态的展示

6、支持提供统计分析告警功能，针对告警事件能够按照攻击事件、危险程度等条件做进行绝对值统计分析和环比统计分析并产生告警，告警参数应支持用户自定义。

7、支持通过源IP地址、目的IP地址、事件类型，危险程度，攻击手段，服务类型和触发行为对安全设备攻击告警日志进行过滤

8、产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。

1. **网站安全监测系统**

1． 可支持200个域名监控。至少配置6个千兆电口，2U设备，具备交流电源模块。

2． 采用SSL加密通信方式，用户可以通过C/S架构远程方便的对产品进行管理，产品无需安装任何控制台和第三方数据库。

3． 网页挂马监测：可远程对监测的目标站点进行网页挂马监测，其监测频率可以自定义，引擎检测能力至少达到30万页面/每天，能够将挂马网页以及攻击者最终所使用的恶意代码进行保存。

4． 暗链监测；可以监测到相应的暗链，以便及时清查。

5． 网站敏感内容监测：可监测网页中出现的黄，赌，毒，反共等敏感内容，能够实时告警，提供取证依据。

6． 支持基于组织结构站点资源视图，允许用户从不同维度来关注资产的风险情况。总部可以根据资产树的根节点信息来查看整体风险情况，各单位可以根据自己的管理权限查看学校内各子部门的风险整体情况和各种风险的分布情况。产品提供风险趋势数据。

8． 支持基于关键页面远程对目标站点进行监测，允许用户自定义设置监测的关键页面，可增、删、变更关键页面，根据设置的关键页面进行网页监测。

9． 产品自备网络工具功能，支持相关的网络工具如ping、traceroute。

10．未知网站发现，可以通过端口扫描方式进行查询，快速定位网络中的站点列表

11. 产品提供三年原厂软件更新服务、产品保修服务、远程支持服务。