**铱迅产品技术参数**

1. **堡垒主机技术参数**

1．字符协议不低于600个并发会话数，图形协议不低于100个并发会话数。可管理台数不低于150台，硬盘容量不低于500GB，至少配置6个10/100/1000M电口，2U设备，具备交流电源模块。

2．支持部门级别独立管理，针对用户的不同部门，让每一个部门能够独立管理自身资源，如部门管理员只能对该部门用户及主机设定访问规则，且只能查看该部门运维用户的审计录像和内容，但无法管理其他部门资源。默认管理员、审计员和运维人员权限分离。

3．支持本地密码认证、AD域认证等认证方式。

4．支持高级主动监控，每当产生会话时，均能在管理界面上打开可监控界面，且产生危险操作后，能够进行警报等内容的响应。

5．支持图形运维录像能够倍速播放及拖拉滚动条播放。

6．字符型远程操作协议：SSH、TELNET；图形化远程操作协议：RDP、VNC、X11；文件传输协议：FTP、SFTP。

7．数据库远程操作协议：支持ORACLE、MSSQL、Mysql等数据库远程访问协议审计。

8．支持通过应用发布中心系统扩展支持其他访问协议，如Ramin、PcAnywhere、HTTP/HTTPS等 ；允许用户快速自定第三方应用类型，如行业软件等；

9．支持对windows、Unix、Linux、Cisco网络设备的系统账号进行自动改密；管理员可自动以自动改密计划，设定计划名、开始时间、执行周期（多长时间更改一次）：支持对自动改密的密码强度进行设定，包括：长度、复杂度等内容；支持邮件自动发送改密结果。

10．WEB访问方式：支持WEB调用本地客户端方式访问远程服务器，并可以定制SecureCRT、PUTTY、Winscp的程序路径；WEB方式至少支持RDP、SSH、TELNET、FTP、Oracle、Mysql、MSSQL等访问方式；客户端菜单模式访问：支持通过常用客户端软件，如SecureCRT、PUTTY等，用户可通过字符菜单选择方式选择目标服务器并进行访问。

11．支持限制用户的允许登录时间、登录时间有效期；支持限制用户的登录IP，IP限制可添加多个IP或网段。

12．支持按用户限制RDP会话CONSOLE登录；支持按用户开启/关闭RDP会话中的剪贴板功能；支持按用户开启/关闭RDP会话中的磁盘映射功能；支持按用户开启/关闭SSH会话中的SCP功能。

13．支持对违规操作的指令进行忽略处理；针对SSH、Telnet访问操作，可以查看阻断命令日志。

14．支持记录数据库访问操作发生时间、客户端IP、服务器IP、运维审计系统用户、数据库账号、数据库操作命令等内容。

15．支持以WEB在线视频回放方式重现维护人员对服务器的所有操作过程。

16．支持审计文件离线播放。

17．系统状态监控；实时监控审计系统CPU、内存、磁盘的使用情况。

1. **安全审计系统技术参数**

1. 支持千兆网络环境监听，支持千兆电口、千兆多模光纤、千兆单模光纤接口，至少提供4个100/1000BASE-TX网口，可扩展到8个口，1个console；交流电源模块，2U设备。审计事件每秒入库速度至少在3000条/秒。

2．采用旁路部署方式，对原有网络不造成影响，网络审计产品的故障不影响现有网络的正常运行

3．支持数据库oracle各版本的审计，支持sql各版本的审计，支持db2各版本的审计 ，支持informix各版本的审计，支持sybase各版本的审计。

4．支持telnet协议的审计，能够审计用户名、操作命令等

5．支持对ftp协议的审计，能够审计用户名、命令、文件等

6．支持对http协议的审计，能够审计url、网页等

7．支持对smtp协议的审计，能够审计发件人、收件人、主题、正文等

8．支持对pop3协议的审计，能够审计发件人、收件人、主题、正文等

9．系统支持模糊匹配关键字设定规则

10．系统支持通过正则表达式匹配关键字设定规则

11．系统支持对不同的审计事件赋予不同的安全级别

12．实时监控对实时告警信息，当前会话进行详细察看；能够提供实时流量监视。

13．提供审计事件的检索功能，支持源ip、源端口、目的ip、目的端口、用户名、帐户、规则名、时间进行查询，支持组合条件查询方式

14．支持自定义查询条件模板，按模板进行查询

15．审计统计功能，支持按ip、部门、时间、协议、帐户等条件进行会话统计和审计事件的统计，提供top n统计方式，支持组合条件统计方式

16．支持自定义统计报告模板，按模板自动生成报告并自动发送到指定邮箱

17．报告导出文件功能，支持html、word、pdf等格式的导出

18．具有权限管理功能，可以对用户分级，提供不同的操作权限和不同的网络数据操作范围限制，用户只能在其权限内对网络数据进行审计和相关操作

19．系统可以对每一种权限的使用人员的操作进行审计记录，可以由用户管理员进行查询，具有自身安全审计功能

20．提供系统升级功能，能够通过升级包的方式实现升级

21．系统支持通过标准的syslog协议向将审计结果信息发送给第三方系统，以便第三方系统分析处理

1. **集中管理平台技术参数**

1．支持展现网络中安全设备的分布部署情况。用户能以列表方式，预览方式分别查看当前网络中的安全设备的工作状态，直观的反映设备的实际运行状态，并且能进行配置管理；

2．通过监控界面，用户就能够监控整个计算环境中所有安全设备的运行状态和性能分析，能够查看设备的CPU利用率，内存利用率，接口流量，接口利用率，并实时获得告警，便于采取应急响应行动。

3．通过集中管理平台对网络中部署的安全产品进行策略配置管理。策略管理的内容包括设备对象定义、、安全规则管理、安全策略配置等等。

4．支持安全设备的日志查询、日志分析、安全审计报表。

5．支持将所有的告警记录按发生时间、告警状态、事件类型、事件等级、源设备IP、源设备类型等信息列表显示，对告警信息进行分析和统计。

6．提供丰富的报表管理功能；根据时间、数据类型等生成报表，报表可以保存为Excel、Word等多种格式。

1. **网站安全监测系统**

1． 可支持不少于200个域名监控。至少配置6个10/100/1000M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B/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50万页面/每天，高端可达到100万页面/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赌博、邪教、广告、反政治、反政府、化学、社会、黑客等敏感内容，能够实时告警，并提供场景文件用于取证。

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．支持用户发现未知网站，可以通过ip＋端口方式进行查询，快速定位网络中的站点列表