技术参数：

1. 标准1U或2U机架式服务器，带安装套件
2. ≥2个千兆电口，1个console口，冗余电源，≥16G内存，数据盘可用空间≥4T，包含至少50个日志源授权， 3年原厂质保服务(包含硬件设备维修、软件更新、漏洞修复等)。
3. 支持各类安全设备、网络设备、中间件、服务器、数据库、业务系统等日志对象的日志数据采集，支持常见操作系统如Windows，CentOS，Debian等系统的日志采集，支持Syslog等常见类型日志
4. 设备要求具备开箱即用能力，内置常见日志模型，自动解析主流网络设备、安全设备和中间件的日志数据
5. 支持自定义日志模式，支持通过正则、分隔符、json、xml的可视方式进行自定义规则解析，支持对解析结果字段的新增、合并、映射，以满足除内置解析规则之外未被覆盖的日志类型的解析。
6. 支持通过正则、通配符、范围搜索等多种方式模糊搜索，支持根据时间、严重等级等进行组合查询；可根据具体设备、来源、IP地址、URL进行具体条件搜索；支持可设置定时刷新频率，根据刷新时间显示实时接入日志事件
7. 支持根据时间轴查询日志
8. 支持常见类型编码的解析能力或提供内置工具，如Base64、Unicode、Urlencode等
9. 支持生成统计报表，报表内容正确，能够以PDF等文件格式导出报表。
10. 系统具有防恶意暴力破解账号与口令功能，支持可设置口令错误次数、超过错误次数锁定、锁定时间可设置等功能。支持后台管理页面黑白名单功能。
11. 支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备IP、源IP、目的IP等方式快速检索安全事件告警，支持自定义告警规则，告警支持邮件、短信等方式
12. 支持大屏幕展示模式
13. 支持数据盘磁盘空间管理功能，支持低可用空间告警、过期日志自动清理、重要日志自动备份等功能
14. 产品具有《计算机信息系统安全专用产品销售许可证》或《网络关键设备和网络安全专用产品安全认证证书》等必须的安全类产品销售许可，软硬件品牌统一，非OEM产品