一、采购内容及要求

升级服务期限为三年，云中心部署在内网，包括内网管理中心1个，服务器授权24个，升级内容包括软件版本、应用漏洞防护特征库、威胁行为防护特征库、虚拟补丁特征库、主机系统防范策略库等，当前软件版本3.1.23.20。软件功能如下：

（1）web应用防护：支持nginx、apache等主流web服务器，支持weblogic、tomcat等主流java中间件；具有SQL注入、跨站脚本攻击等网络漏洞攻击防护；能识别CC攻击，并自动屏蔽IP地址；具有webshell自动隔离、webshell实时防护、未知sql注入漏洞防护、struts2漏洞防护、反序列化漏洞防护、命令执行漏洞防护等高级安全防护；针对公开的0day漏洞能及时发布虚拟补丁进行防护。

（2）系统防护：支持windows、centos、麒麟、统信等主流操作系统，包括操作系统加固、防暴力扫描、防暴力破解等功能。可实现应用网络访问过滤、IP层流量过滤、文件读写防护、进程创建监控、应用白名单控制、高危操作拦截等主机防护功能。

（3）日志管理：对应用漏洞防护、系统防护、系统登录等非法行为均记录日志，可分类查询，可根据起止时间查询，日志明确显示攻击时间、攻击类型、攻击IP、攻击详情等信息。

（4）资源监控：可对服务器的CPU、内存、磁盘、网络等资源进行监控，达到设定阈值后报警。

（5）管理中心：具备攻击行为统计分析和可视化展示，对安全事件能进行详细分析，展示事件概要描述、攻击摘要、攻击记录，方便管理员进行安全防护策略调整；提供详细的操作审计日志。