终端安全防护服务

1、面向≥1700 台终端（1500 台 windows、200 台信创）提供 3 年的终端安全防护服务。需配合现有 2 台深信服全网行为管理设备，配置准入模块，各自基础支持≥3000 终端准入功能，及不限数量的 portal 准入认证功能。

2、客户端集成服务：全网行为管理与终端安全管理客户端整合为单一客户端，支持多种准入认证方式（密码/IP/MAC/二维码/短信及 802.1x 认证），提供统一运维管理与安全防护服务。

3、配置与现有深信服防火墙、全网行为管理等设备联动，状态可查。

4、提供防病毒、勒索防护、账号风险分析、攻击溯源（支持 ATT&CK 可视化）、威胁响应处置服务，准入及安全事件日志记录与查询等服务。

5、内容详见附件，需严格满足带*****条款。

附件：

序号	服务名称	服务内容
1	全网行为管理-准入模块升级（仙霞岭路所区）	***1、该准入模块升级服务需部署于单位现有深信服全网行为管理硬件平台，型号 AC-1000-B2250，基础准入终端数不少于 3000；** **2、与统一端点安全管理系统客户端集成，整合为单一客户端，以简化用户操作（需提供配置截图）；** 3、配置同时支持用户密码认证、不需要认证以 IP 做用户名上线、不要需要认证以 MAC 做用户名上线、二维码认证、短信认证等认证方式； 4、配置 802.1x 认证，可对接本地和 AD 域用户源进行用户名密码认证（需提供配置截图）； 5、配置 Windows 桌面水印，支持设置水印的内容、透明度、密度，水印效果预览，离线时继续生效； 6、配置存储设备、网络设备、蓝牙设备、摄像头、打印机的使

		用管控；支持外设白名单，提供批量获取硬件 ID 的工具进行白名单配置； 7、配置对 U 盘、移动硬盘设置可读写、拒绝、可读、告警；可对拷贝的文件内容以及插入和拔出行为的审计； 8、配置放通或封堵 TCP\UDP 端口、ICMP 协议，可设置对所有 IP 或者指定 IP 执行，离线时继续生效（需提供配置截图）。 ***9、具备完善的准入日志查询、溯源功能。**
2	全网行为管理-准入模块升级（鳌山所区）	***1、该准入模块升级服务需部署于单位现有深信服全网行为管理硬件平台，型号 AC-1000-B2100，基础准入终端数不少于 3000；** 2、与统一端点安全管理系统客户端集成，整合为单一客户端，以简化用户操作（需提供配置截图）； 3、配置用户密码认证、不需要认证以 IP 做用户名上线、不要需要认证以 MAC 做用户名上线、二维码认证、短信认证等认证方式； 4、配置 802.1x 认证，可对接本地和 AD 域用户源进行用户名密码认证（需提供配置截图）； 5、配置 Windows 桌面水印，支持设置水印的内容、透明度、密度，水印效果预览，离线时继续生效； 6、配置存储设备、网络设备、蓝牙设备、摄像头、打印机的使用管控；支持外设白名单，提供批量获取硬件 ID 的工具进行白名单配置； 7、配置对 U 盘、移动硬盘设置可读写、拒绝、可读、告警；可对拷贝的文件内容以及插入和拔出行为的审计； 8、配置放通或封堵 TCP\UDP 端口、ICMP 协议，可设置对所有 IP 或者指定 IP 执行，离线时继续生效（需提供配置截图）。 ***9、具备完善的准入日志查询、溯源功能。**

3	终端安全防护服务（windows终端）	***1、本次服务终端数量不少于 1500 台，包含管理控制中心及终端客户端软件配置；** ***2、支持 windows 操作系统，如 windows7、windows10、windows11 等；** ***3、配置与全网行为管理集成，整合为单一客户端；配置实现终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能；** 4、配置勒索病毒整体防护体系入口，直观展示最近七天勒索病毒防护效果，包括已处置的恶意文件数量、已拦截可疑行为次数、已阻止的未知进程操作次数、已阻止的暴力破解攻击次数（需提供配置截图）； 5、对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、弱密码账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户； 6、对客户端的进行错峰升级，可根据实际情况控制客户端同时升级的最大数量，避免大量终端程序同时更新造成网络拥堵或 I/O 风暴； 7、配置与单位现有深信服下一代防火墙(AF-1000-FA40-AK)、深信服全网行为管理等的联动状态； 8、配置以可视化形式展现攻击故事，提供可视化的进程树溯源，可直观看出攻击入口、相关操作行为、高危实体文件等信息，协助客户进行事件攻击溯源和研判分析(需提供配置截图）； 9、配置显示攻击事件命中的 ATT&CK 相关技术，并对此技术做简要说明。便于用户了解攻击者的操作行为和目的，评估整体影响面(需提供配置截图）。

4	终端安全防护服务（信创终端）	***1、本次服务终端数量不少于 200 台，包含管理控制中心及终端客户端软件配置；** ***2、支持主流国产化操作系统（含服务器版），如银河麒麟、统信、中标麒麟等；** ***3、配置与全网行为管理集成，整合为单一客户端；配置实现终端统一管理，统一威胁处置，统一漏洞修复，威胁响应处置，日志记录与查询等功能；** 4、配置全网视角的终端资产统一清点，便于帮助用户快速发现风险面。清点信息包括操作系统、应用软件和终端账户，其中操作系统和监听端口支持从资产和终端两个视角进行统计和展示（需提供配置截图）； 5、配置与单位现有深信服下一代防火墙(AF-1000-FA40-AK)、深信服全网行为管理等的联动状态（需提供配置截图）； 6、支持展示各勒索病毒事件的病毒名称、影响终端、威胁进程、发生时间和处理状态； 7、支持对系统账号信息进行梳理，了解账号权限分布概况以及风险账号分布情况，可按照隐藏账号、可疑 root 权限账号、长期未使用账号、夜间登录、多 IP 登录进行账号分类查看，支持统计最近一年未修改密码的账户（需提供配置截图）。
5	终端准入服务	***1、实现根据 IP、终端类型设定，部分使用客户端进行准入认证、部分无法安装客户端的设备使用 portal 认证。使用 portal 认证的设备不占用 1700 台终端安全防护服务名额。** ***2、提供统一账号认证服务，同一账号可以同时使用 portal 和客户端方式认证多台设备。** ***3、具备完善的准入及安全事件的日志查询、溯源功能。**

6	其它	1、需要增加终端安全防护服务数量时，windows 终端每 100 个不高于 15000.00 元/3 年，信创终端每 100 个不高于 24000.00 元/3 年。 2、提供 7×24 小时在线技术支持。对于紧急安全事件，1 小时内响应并派遣技术人员到达现场处理。