2025年信息安全特征库更新调研

## 一、 项目概述

本次项目将主要为全院在用安防设备特工升级服务、质保服务、病毒库升级服务、漏洞规则库升级服务、感知系统探针特征库升级、维保服务、杀毒引擎更新服务、规则库升级服务等。

## 二、技术服务要求

## 安全设备产品特征库需求清单及要求

| **设备类型** | **区域** | **需求** |
| --- | --- | --- |
| 深信服EDR  （统一端点安全管理系统） | 对全院服务器、办公终端进行安全防护，防止病毒入侵。 | 1. 提供一年软件升级服务 2. 提供一年产品质保服务 3. 提供一年病毒库升级服务 4. 提供一年漏洞规则库升级服务 |
| 深信服态势感知平台  SIP-1000-E600 | 对全院全网网络安全日志进行收集并分析，辅助用户与运维人员进行处置决策，联动各安全设备实现威胁闭环联动处置。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年病毒库升级服务  4.提供一年感知系统探针特征库 |
| 深信服威胁潜伏探针  STA-100-B420 | 收集并分析内网流量上传至态势感知平台 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年感知系统探针特征库 |
| 深信服威胁潜伏探针  STA-100-B420 | 收集并分析业务外网流量上传至态势感知平台 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年感知系统探针特征库 |
| 深信服威胁潜伏探针  STA-100-B2100 | 收集并分析办公互联网流量上传至态势感知平台 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年感知系统探针特征库 |
| 深信服安全基线扫描  BVT-1000-A620 | 对全院服务器进行基线扫描。 | 1.提供一年软件升级服务  2.提供一年产品质保服务 |
| 深信服下一代防火墙  AF-1000-B1800 | 物理前置服务器防护点，实现物理前置机服务器访问流量过滤、拦截。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年杀毒引擎更新服务  4.提供一年云智订阅软件服务  5.提供一年维保服务 |
| 深信服下一代防火墙  AF-1000-FA40 | 前置虚拟化服务器防护点，实现物理前置机服务器访问流量过滤、拦截。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年杀毒引擎更新服务  4.提供一年云智订阅软件服务  5.提供一年维保服务 |
| 深信服下一代防火墙  AF-1750-TD | 蜜罐 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年蜜罐服务  4.提供一年维保服务 |
| 深信服下一代防火墙  AF2000-B2150 | 服务器服务器网关，承载内网服务器跨网段流量转发需求，同时启用流量过滤、业务防护的功能。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年杀毒引擎更新服务  4.提供一年云智订阅软件服务  5.提供一年维保服务 |
| 深信服下一代防火墙  AF2000-B2150 | 服务器服务器网关，承载内网服务器跨网段流量转发需求，同时启用流量过滤、业务防护的功能。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年杀毒引擎更新服务  4.提供一年云智订阅软件服务  5.提供一年维保服务 |
| 深信服下一代防火墙  AF-1750 | 医社保专线出口防火墙。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年杀毒引擎更新服务  4.提供一年云智订阅软件服务  5.提供一年维保服务 |
| 深信服下一代防火墙  AF-1000-B1800 | 院内职工办公互联网出口防火墙。 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年杀毒引擎更新服务  4.提供一年云智订阅软件服务  5.提供一年维保服务 |
| 深信服Web应用防火墙  WAF-2000-B2100 | 业务外网服务器网关、承载端口映射、WEBURL深度检测。 | 1.提供一年网关杀毒功能 |
| 深信服Web应用防火墙  WAF-2000-B2100 | 业务外网服务器网关、承载端口映射、WEBURL深度检测。 | 1.提供一年网关杀毒功能 |
| 深信服上网行为管理  AC-1500 | 天府院区免费WIFI行为管理 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年软件升级服务  4.提供一年规则库升级服务 |
| 深信服上网行为管理  AC-1200 | 天府院区办公互联网行为管理 | 1.提供一年软件升级服务  2.提供一年产品质保服务  3.提供一年软件升级服务  4.提供一年规则库升级服务 |

备注：若有少量缺项未统计在列表中，相关设备需包含在维保范围以内。

## 升级服务

服务描述：提供相关产品维护性版本自动升级服务以及最新系统版本的升级授权，并结合业务需求、使用情况及新版本特性，给出医院建议是否需要升级到最新版本。

服务内容：服务包含的现场软件升级需在符合商业惯例的合理范围内提供。包括提供软件升级的远程指导与协助。

维护性版本升级：提供维护性软件版本的自动升级，对于软件系统存在的隐患进行修复，一般情况下不增加新功能和新特性。

系统版本升级：通过在线平台推送最新系统版本资讯，新版本正式发布后根据用户业务需求、使用情况及新版本特性，建议是否需要升级到最新版本。

## 订阅式服务

主要包含：

（1）URL 库与应用识别规则库升级服务

（2）网关杀毒功能及更新服务

（3）未知威胁与杀毒订阅服务

（4）最新威胁防御规则库订阅服务