附件4

大数据发展中心运维服务内容及需求

一、机房运维服务

**（一）服务内容**

1.延续dongyang.gov.cn域名的证书，延续时间2年。

2.延续cn域名以及证书，域名及证书延续时间均为2年。

3.延续dongyang.gov.cn的域名使用期限，延续时间5年。

**（二）设备清单**

| 序号 | 交换机、安全设备 | 型号 |
| --- | --- | --- |
| 1 | 明御数据库审计与风险控制系统 | DAS-DBAUDITOR |
| 2 | 深信服 | VPN-3050 |
| 3 | 深信服 | VPN-3050 |
| 4 | 华为核心交换机 | S9306 |
| 5 | 正元OA测试机 | x3650 |
| 6 | 润和移动OA | x3650 |
| 7 | 协同办公数据库 | x3650m3 |
| 8 | 协同办公WEB备用 | x3650m4 |
| 9 | 协同办公WEB | x3650m4 |
| 10 | 老OA数据库 | x3650m2 |
| 11 | 老OA-LDAP | x346 |
| 12 | 市委机要 | x3650m3 |
| 13 | 润和移动OA测试 | x3650 |
| 14 | 服务器虚拟化 | x3850x6 |
| 15 | 服务器虚拟化 | x3850x6 |
| 16 | 服务器虚拟化 | x3850x6 |
| 17 | 服务器虚拟化 | x3850x6 |
| 18 | 服务器虚拟化 | x3850x6 |
| 19 | 服务器虚拟化存储 | VNX5400 |
| 20 | 服务器虚拟化 | 联想7X99 |
| 21 | 服务器虚拟化 | 联想7X99 |
| 22 | 服务器虚拟化 | 联想7X99 |
| 23 | 服务器虚拟化 | 联想7X99 |
| 24 | 服务器虚拟化 | 联想7X99 |
| 25 | 服务器虚拟化 | 联想7X99 |
| 26 | 交换机 | S5720 |
| 27 | 交换机 | S5720 |
| 28 | 交换机 | S6720s |
| 29 | 交换机 | S6720s |
| 30 | UPS | 华为 |

**（三）服务要求**

落实机房运维的整体性工作要求。

二、终端安全杀毒服务

（一）服务内容

服务终端数量：授权5000点以上。

终端类型：PC、服务器（Windows、linux、信创操作系统等）

服务内容：终端安全防护

（二）终端安全防护性能要求

|  |  |  |
| --- | --- | --- |
| 序号 | 服务  要求 | 具体描述 |
| 1 | 全网风险可视 | 1.支持当前待处理高危风险展示，包括弱口令、待处理病毒、待处理漏洞数据，并支持一键跳转到对应处理页面。  2.支持控制台动态更新显示全网终端安全状态分布，包括：终端总数、在线终端数、防护中终端数、异常设备数。  3.支持查看当前安全防护信息数据，包括渗透追踪防护、勒索防护数据、病毒防护数据、系统登录防护数据、web请求防护数据。  4.支持查看当前top 5风险资产、top 5威胁ip、top 5威胁区域。  5.支持实时查看当前安全动态。 |
| 2 | 一体化安全策略 | 1.支持自定义安全策略、安全策略可继承，内置多个初始策略模板，包括防护模板、审计模板。  2.支持通过对终端制定模板的方式做到一键策略下发。  3.支持设置策略修改规则，包括是否允许用户修改策略以及不允许修改的时间。 |
| 3 | 联动能力 | 支持与用户的大数据智能安全平台联动进行病毒扫描并查杀，漏洞利用处置等能力。 |
| 4 | 系统性能监控 | 1.支持对CPU使用率监控、内存占用率监控、磁盘读写监控、上下行流量监控。  2.支持对CPU、内存、磁盘读写、网络上下行流量达到配置阈值时告警。  3.支持对CPU、内存达到一定阈值时客户端进行熔断。  4.支持网络通信全时监控。 |
| 5 | 资产指纹 | 1.支持自动收集终端资产信息，包括计算机名称、内核版本、操作系统、处理器、主板、内存、硬盘、显卡、终端版本、病毒库版本、最近更新时间等。  2.支持自动收集终端资产：监听端口、运行程序、账号、软件、启动项等信息，并支持从资产的维度和信息的维度去查看数据，支持数据的导出。 |
| 6 | 高级威胁防护模块 | 1.支持对本机的扩展行为（信息收集、权限提升）进行监测，防止侵权行为和信息泄露。  2.识别渗透过程中的隧道代理（端口映射、端口转发、内网代理），可阻断隧道代理搭建行为。  3.对失陷后主机远控持久化行为进行检测（反弹shell、远程控制），可阻断远控。  4.对内网的恶意攻击行为进行识别（漏洞利用、横向移动），可阻断恶意探测行为。  5.可对渗透的收尾阶段的数据清除行为进行识别和阻断。 |
| 7 | 系统安全性模块 | 1.支持防端口扫描，锁定恶意的端口扫描，并记录告警。  2.支持系统/域控环境下的弱口令检测。  3.支持扫描后对高危漏洞进行自动修复。  4.支持设置对修复完成后的补丁文件进行删除。  5.支持对系统登录行为进行一定的限制，可设置单个IP请求时间、登录失败次数、IP临时锁定时间。  6.支持网络分域访问，在服务端设置不同网络访问域，资产在同一时间只能访问任意一个网络域，支持资产自主切换不同网络访问域。  7.支持基于IP及域名设置探测地址，实时感知违规外联行为，针对违规外联行为支持多种处置方式，包括不做处理、弹窗提醒用户，并关机、弹窗提醒用户并断网。  8.支持反渗透监控，包括横向渗透的危险操作等。  9.支持网站漏洞防护，防护内容包括SQL注入、XSS、应用程序漏洞及自定义规则。  10.支持智能检测防御CC攻击，并可进行高、中、低三档设置。  11.内核级防火墙（业务间流量东西向隔离）功能，包括IP、端口、协议、流向等细粒度权限控制。  12.支持流量画像，支持全网流量可视化。  13.支持登录防护，包括以系统账号为粒度的异常登录防护、支持4个任意维度（任意IP）任意域名，任意计算机名，任意时间）的系统登录访问策略设置。  14.支持显示隐藏的系统账户。  15.具有系统漏洞扫描和修复功能，提供真实漏洞补丁。在补丁依赖关系上支持重启验证机制（保证补丁安装的稳定性）。管理中心可作为补丁服务器，支持管理中心可上网和不可上网两种情况。提供离线补丁下载器，按需智能获取内网所需补丁。  16.支持扫描的漏洞类型包括但不限于操作系统漏洞（Windows、Linux等）、数据库漏洞（MySQL等）、Web容器漏洞（Tomcat、Apache、Ngnix等）及其他组件漏洞。  17.支持对文件变化的审计。  18.移动存储介质管理：  （1）支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括授权、启用、停用、删除、导出注册列表、行为监控及审计等。  （2）支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批。  （3）支持管理员设置自动审批客户端注册请求。  （4）支持从资产维度、设备维度对存储介质的权限进行精细化设置，同一设备可针对不同的资产设置不同的读写权限，有效控制不明来历的移动存储可能带来的病毒传播等隐患。  （5）支持设置U盘的使用时间。  19.支持对无线网卡、光驱、软驱、打印机、调制解调器、红外设备、蓝牙设备、摄像头、鼠标、键盘、手机/数码设备的权限管理。  20.支持对USB接口、串口/并口、1394控制器、PCMCIA等接口的控制。  21.支持开启进程黑名单，阻止不受信任的程序启动和生成，同时支持路径和MD5两种形式。  22.支持开启白名单，对白名单内的文件的操作进行放行。  23.支持对资产的远程端口进行修改，并支持自动添加本机系统防火墙策略。 |
| 8 | 云端威胁鉴定 | 1.对文件HASH、IP、域名、邮箱等IOC指标进行动静态鉴定，通过和云端威胁情报进行碰撞，实时返回威胁结果。  2.联动威胁情报，支持对外联IP、DNS解析、可疑文件进行实时情报鉴定，实现风险一站式实时监测。  3.基线检查：  支持自定义基线巡检任务包括资产范围、基线策略、巡检时间。  支持等保1级到等保4的系统基线检查，系统范围包括Debian、Linux、Oracle Linux、Suse、Windows。 |
| 9 | 防病毒模块 | 1.支持文件实时监控，在文件执行、文件修改、存储介质连接时自动触发。  2.支持多种扫描模式包括极速模式、低资源占用模式设置，且低资源占用模式可自定义CPU使用率。  3.支持对资产进行快速扫描、全盘扫描、自定义扫描，并对病毒扫描结果进行导出。  4.支持从资产视角和病毒视角展示病毒查杀概况，并对病毒进行处理。  5.支持多引擎设置，包括默认引擎、深度扫描引擎。  6.支持对压缩包扫描及深度进行设置，默认9层深度。  7.支持对文件扫描进行跳过，默认50M以上文件进行跳过。  8.支持自定义病毒处理方式，包括自动处理、记录、删除。优先对病毒文件进行修复，并将修复前的病毒文件进行备份。  9.支持对顽固流行病毒进行智能拦截。  10.针对Windows系统，提供内核级的数据防护能力，保护文件不被恶意修改、加密等，可自定义配置保护的文件及目录，支持设置例外进程。  11.升级系统：  支持病毒库、补丁库的离线升级及在线升级；支持管理平台、终端软件安装包、终端软件更新包、系统漏洞库、弱口令库的离线升级。  客户端程序支持在线热升级，升级之后旧版本驱动等程序无残留。 |
| 10 | 资源占用 | 客户端占用内存80M以下，CPU占用3%以下。 |

**（三）安全服务**

1.软件升级：提供病毒库、程序升级服务。

2.应急响应：对于新发现的病毒、零日漏洞，厂商能够于24小时内作出响应，及时通知用户，并提供专门应急预案、处置工具或专杀工具。

3.技术支持：支持7×24小时威胁溯源服务。