重要的财务数据、文档方案、设计图纸等科研数据是企业重要的资产，信息保密工作非常重要，需要严防外泄。传统电脑办公模式下很难有效的应对信息泄密的风险。那么，在不影响正常办公的情况下，有没有行之有效的方案可以保障数据安全？答案是肯定的，可以通过对相关部门的电脑进行桌面虚拟化改造并配合凤凰卫士数据安全系统的解决方案防止信息外泄。

## 方案简要介绍如下：

**1、桌面虚拟化改造**

利用原有的办公电脑（前提是满足应用需求）安装桌面虚拟化负责日常终端运算工作，然后再用服务器部署桌面虚拟化平台及管理系统，负责对所有终端的集中管控及数据存储。所有软件及数据全部存储于服务器，终端使用账号登陆之后才可以使用服务器的资源进行办公。服务器可以对每个终端的使用权限进行限制，并对终端接口进行管理。通过虚拟化改造，实现了数据的集中储存和管控，大大提高了数据安全性，而且也提升了管理效率。

**2、配套凤凰卫士数据安全系统，防止数据在未授权情况下使用**

进行桌面虚拟化改造之后，由于数据集中存储及管控，USB 接口也受监管，在不连接外网的情况下，原本是可以保障数据安全的，但阻断外网连接在实际工作中是不现实的，会给办公造成极大的不便，也会引起员工的抵触。既要满足办公需求又要保障数据安全那么就需要对敏感文件进行加密，这样即使文件通过网络外发，若没有获得授权，接收方打开文件就会是一窜窜乱码，不会造成涉密。

**3、桌面虚拟化改造不会影响原有的办公习惯**

虚拟化改造后的办公桌面与原来仍然一样，实际使用体验感与原来的模式没有区别，不会给员工造成任何工作不适。

**4、设计部电脑桌面虚拟化改造的成本**

利用原有的电脑进行虚拟化改造，防止数据外泄所需要的投入包括：

**服务器：**用于集中管控各个终端和统一存储；

**虚拟化终端授权：**按终端许可用户收取授权费用；

**凤凰卫士数据加密系统虚拟化终端授权：**按终端许可用户数收取使用费。

利用原有电脑改造的桌面虚拟化属于重终端轻服务器的模式，运算主要分布于各个终端，因此对服务器的性能要求不高，投入的成本很低。虚拟化终端授权及凤凰卫士数据加密系统是依据终端使用数量来确定费用的，每个点的投入成本也在极大多数企业可以接受的合理范围之内。

从实际的项目实施经验来看，目前这种方案是针对设计部门涉及 3D 应用，数据需要高度保密的最可行桌面虚拟化方案，具有实施简单、效果可靠、费用较低突出优势。