环境加密与文档加密产品对比

数据保密产品发展至今只有短短几个年头，尚未形成统一的行业标准，也未出现在行业内具有垄断地位的企业。大致上来说，数据防泄密产品分为两类：文档加密类产品和整体防护类（或者称为环境加密）产品。两类产品设计理念和功能迥异，都处在不断的发展和互相借鉴中。需要特别指出的是，大多数客户对于数据防泄密产品的选择往往不够重视，将其和普通的软件产品等同对待。而事实上，数据防泄密项目和现有的企业信息系统密切相关，并非简单的加密一些文件或者硬盘了事。从这几年的应用情况看，数据防泄密项目想要实施成功，除了选择合适自身的产品外，更加需要客户的重视和配合，其难度不亚于ＥＲＰ项目。在不甚了解的情况下，仓促的选择产品并实施，项目失败率几乎就是１００％。这样的反面案例数不胜数。

这里主要结合使用的实际情况，从项目风险的角度分析两类产品在大中型企业中部署时的优缺点，以供参考。

项目风险分为以下几种：

1.数据加密后被破解的风险

文档加密是对应用软件进行控制，生成的文档在保存时被写入密钥，但该密文在装有加密产品客户端的电脑上被打开时，加密软件会先对密文自动解密，然后才能正常打开，也就是说，该加密文件，在内存中依然是明文存在的，可以通过“读内存”直接提取明文，绕过加密，安全级别较低；环境加密采用整体防护，非法外出的文件才会被加密，如果要破解，唯一的方式就是暴力破解，其难度相当大，安全级别高。

2.对人员使用习惯的改变

使用习惯改变越小，意味着项目推进的阻力越少。不管哪类产品，一旦上线，必然会导致员工以往的行为受到约束。比如，以往可以随便用ｑｑ外发文件，现在无法发送或者发送出去的都是密文。在这一点上，文档加密产品对人员使用习惯的改变较小，员工可以自由的发送非加密性质的文件，优于整体防护类产品，但同时带来的风险也较大，有可能员工会将敏感数据伪造成非加密性质文件。但无论哪类产品，员工都必须按照设定的方式重新规范自身行为，这点需要企业自上而下的推动。

3.数据的损毁几率

加密就要解密，也必然存在加密和解密失败的风险，由此产生的结果就是数据损毁，极大影响员工的日常工作，导致系统无法上线。在这点上，整体防护类产品要远优于文档加密类，因为文档加密对数据有直接和频繁的加解密处理，数据损毁率很高，整体防护类产品的加密在数据传输边界

处进行，对数据本身不做处理，损毁率很小。从以往的项目经验看，损坏数据几乎已经成为文档加密产品的代名词和无法逾越的瓶颈（尤其是终端环境复杂的研发制造型企业里），而整体防护类产品不会出现此类情况。

4.应用系统升级风险

前面提到过文档加密是通过控制软件来加密，必然会涉及到软件版本的问题，例如：某一文档加密软件现在可以支持到 WORD2010，将来微软新推出了 WORD2012，这时候必须要开发商将 WORD2012 添加为受控软件才可以实现加密，用户可能还要为此不断升级而增加一系列的费用；而环境加密不存在此类风险。

5.管理制度变更风险

管理制度变更风险指数据保密系统上线后，企业的管理制度和流程出现一定的变化，此时，数据保密系统必然要随之进行一定的调整。如果不能快速和有条理的完成调整工作，将会对企业正常的管理和生产秩序造成极大干扰。文档加密产品只能以“文档“为主要管理维度，和管理制度之间并无直接对应关系。当制度改变时，需要同时熟悉文档加密系统和管理流程的人员进行调整，该调整并无标准步骤和过程，存在很大的操作风险。整体防护类产品基于“数据风险管理体系“的设计理念与企业的管理流程密切相关，任何一条数据保密策略必然对应着一条显性或隐形的管理制度。比如外发邮件时的黑白名单管理、是否加密控制就和企业的外发管理制度完全匹配。当企业管理制度和流程发生改变时，只需要找到对应的策略并进行修改，就可以完整相应的调整工作，简单快速。

6.产品下线风险

下线风险指企业在某些因素的推动下，需要卸载数据保密系统并恢复到系统上线前状态时面临的风险。

对于**文档加密产品**来说，加密数据以单个加密文件的形式散落在内网的各个终端上，取消数据加密对业务系统造成的干扰并恢复数据将是一个及其复杂和漫长的过程。企业需要付出的下线成本不亚于上线成本。这使得企业的应用信息完系统完全被加密系统“挟持“，成为一个潜在的巨大风险，可能会在不远的将来让企业付出沉重代价。

对于整体防护类产品，所有数据在没有任何受控策略下，都会以明文形式传输和应用，管理员可以随时通过删除”数据出口“处的加密策略，迅速消除加密体系对原有信息体系的影响，下线风险极低。

通过以上 6 点对比，基本可以得出结论，对于大中型研发制造型企业来说，整体防护类产品的理念更为适用。归根结底，整体防护类产品更看重与现有信息系统和管理制度的匹配与融合，文档加密类产品更看重对操作者使用习惯的影响和改变，因此，前者需要企业做出一定的投入和让步来

确保防泄密系统的顺利上线，但是一旦上线以后，运行将更为顺畅，后期管理和维护更为容易；后者更符合目前客户对于加密产品的普遍看法”不泄露数据，不影响工作“，但潜在的风险很大；前者更像是个系统，后者更像个软件，前者更适合于大中型企业的整体管理需求，后者更适合于小规模企业的快速应用。

以上分析主要基于两类产品的设计理念，但好的理念未必会真正附诸实现，所以，考察厂家的实力和案例非常的重要，具体案例是否属实，应用环境如何，需要更多的实地考察和交流。