安腾计算机信息反泄密解决方案

© 2019安腾（ITEN）软件有限公司

All rights reserved

安腾计算机信息反泄密解决方案

©Copyright 2003～2019 By Itensoft co.,Ltd

注意

本方案中的内容基于**安腾软件**的反商业泄密解决方案。本材料的相关权利归安腾（ITEN）软件有限公司所有。书中的任何部分或全部内容未经本公司许可，不得转印、影印或复印。

© 2019安腾（ITEN）软件有限公司

All rights reserved

目 录

一、 需求分析.....4
1. 需要保护什么数据.....4
2. 需要保密的数据信息存储与流动的几种形式.....5
3. 需求总结.....7
4. 部署预期.....7
二、 安腾计算信息反泄密整体解决方案.....10
1. 安腾加密的技术体系及场景应用.....11
1.1. 文档的实时透明加密.....11
1.2. 多种加密方式.....12
1.3. 文档密级和权限管理.....12
1.4. 外发文控制.....14
1.5. 移动介质与打印管理.....15
1.6. 涉密审批.....16
1.7. 移动端安全.....17
1.8. 邮件白名单.....18
1.9. 日志审计.....19
1.10. 笔记本离线外带管理.....19
1.11. 内容保护.....20
1.12. 水印控制.....20
1.13. 系统兼容性方案介绍.....21

1.14. 备份系统介绍 21
1.15. 应用安全 22
1.16. 多种认证方式 22
1.17. 灵活的客户端在线策略 22
2. 实施流程与效果预测 23
2.1 实施流程 23
2.2 效果预测 26
三、 技术支持与售后服务 29
1. 培训安排 29
2. 技术支持与服务方案 29
四、 关于我们 30

一、需求分析

随着工信融合的不断深入，制造企业环境在不断发生变化，越来越多的工作依赖 IT 支撑， 信息数据已经成为企业重要的基础资源。企业在日常办公生产大量图纸文档数据，同时增加了 ERP、PDM、CRM 和 SCM 等专业系统，企业内部的数据类型越来越丰富，企业数据尤其是非结构化数据文档信息成爆炸式增长，如何全面保护企业数据资产安全，成为企业发展中必须重视的问题。

为切实提高公司信息安全的管理水平，有效的对企业数据进行安全管理，特别是针对具有自主知识产权以及业务运营所需关键信息的防泄漏保护工作，防止信息通过移动介质、网络传输等渠道被泄露，企业在自我风险评估及需求调研后决定部署数据反泄密系统。

利用专业的加密技术、计算机安全技术和用户行为监控技术，ITEN 安腾正致力于为各种规模的制造企业提供安全集成和简便化安全管理。

经过调研分析，通常情况下，企业对文档加密和信息反泄密会有以下功能需求，具体如下：

1. 需要保护什么数据

企业需要保密的数据类型大概可以分以下几个方面：

- 研发数据：这类数据主要包括研发数据、设计图纸、实验数据等；
- 经营数据：这类数据主要包括企业在运营时候产生的各种文件，如规章制度、人员信息、策划文案等；

- 销售财务数据：这类数据主要包括企业、销售数据、账务数据、员工的工资信息等；
- 其他数据：这类数据主要是产生在在外销售人员自己电脑的销售类数据。

2. 需要保密的数据信息存储与流动的几种形式

1） 企数据存储和流通往往有着自己的特殊性：

① 本地终端数据

当今企业中存在最多的数据就是这种非结构化、分散保存在终端的、无序存储的数据信息，此类数据信息特点是：存储位置乱，电脑使用人员有完全使用的权限，并且无法进行管理。

② 应用系统数据

企业采用了大量例如 ERP、CRM、OA、KM 等一系列的企业协同办公平台系统，甚至有很多企业也都采取了无盘工作站、虚拟机或者云系统，这些系统在应用中会存储大量的企业内部数据信息，虽然它们有一定的文档分类管理作用，但是对数据的权限使用者来说，他们可以任意支配这些数据，从而导致这些数据信息完全没有保障可言。

③ 研发设计系统数据

研发企业特殊的研发用的专业系统用来存放各种研发设计和分析数据，由于这些系统都是市面上不常见的系统，而且系统涉及到很多特殊格式文件。

④ 各地区销售电脑与笔记本上的数据

企业销售体系中各地销售代表身上有着企业最重要的终端销售数据，而且这些数据完全没有规范的管理办法，所以这些数据一旦遗失就会给整个公司带来各种不可预估的损害。

⑤ 总部与分支机构间的数据沟通

一般现在公司都会有很多的分支机构，有的分支机构在外地。这就需要我们要有整体的部署方案，不然各地区单独部署，总部没有监管权限会造成各地数据混乱，责任不明确。

⑥ 各部门之间的数据隔离

由于制造类企业也会有很多敏感部门，比如研发部、财务部、实验室等，所以必然有各部门间数据交互需要权限识别的功能，不然一个普通员工就可以查看各种敏感信息，肯定会导致泄密的发生。

2) 针对于以上的数据类型我们可以预估出以下几个可能产生泄密的方式：

① 外部入侵

国内生产企业同行之间的竞争也非常激烈，这就不排除有黑客或者商业间谍因为种种原因通过各种技术手段进入公司内网窃取数据。

② 内部泄密

内部因素是最难控制的因素，它往往由对企业不忠或不满的员工、离职或辞退的员工以及新晋或试用期的员工主动地去盗窃或者恶意破坏一些企业的内部数据。

③ 无意泄密

这类泄密主要是由于员工管理不善导致在出差过程中电脑、U 盘或者手机遗失从而造成的泄密 。

3. 需求总结

3.1 防止信息泄密的主要需求

- 公司内部的文档需要进行强制加密，且文档只能在公司内部使用，未经允许拿到外部的文件无法打开；
- 满足文件密级的需求，同时公司内部要针对各个部门，甚至精确到各个员工进行权限细分；
- 针对员工出差的笔记本以及移动办公设备要有保护解决方案；
- 可以对各个不同地区的分部进行统一的部署与管理。

3.2 集团企业的特殊需求

- 无缝整合 OA/ERP/CRM 核心业务系统；
- 兼容 PDM/PLM 数据管理系统；
- 无缝对接各种实验、分析系统；
- 支持 AD 域、终端虚拟化；
- 满足灵活、复杂的保密管理要求。

4. 部署预期

主要通过部署安腾反泄密软件实现上述功能需求，具体实现的效果如下：

4.1 加密用户创建的文档，提高安全性

由于需要保护公司多个部门，不同部门间对保护的应用程序及安全策略要求都有区别；特别是技术研发部门有数量庞大技术图纸，要保证这些技术图纸文件在使用时自动转化为密文，但是当密文不经授权外发到其它部门或外网时，加密文档将不能使用；文件在创建、存储、应用、传输等环节中均以加密形式存在，软件客户端在文件加密和解密操作都在系统后台自动进行，不改变员工原有的工作习惯和工作方式。

4.2 控制集团内部文档的权限，实现加密与权限无缝衔接

因为后期公司组织架构可能会比较复杂，因此针对不同的分子公司部门，不同的人员，特别是设计部门的大量图纸文档，生成的加密文档可以根据预先的设置加入相应的权限信息，同时也可以手动指定文档的权限，实现如哪些人可以看，哪些人可以修改，哪些人可以打印等控制。

4.3 支持员工在外地出差时，进行密文文档的使用

企业的员工在外地出差或者与供应商、客户进行商务及技术交流时，需要从内部网络携带大量的技术资料在外进行工作或把相关加密文件外发出去；因此，要保证企业的技术资料在离开内网后还能处于受保护的状态，保证数据的安全性。考虑到员工外出时候的时间不确定性，当外出电脑的使用时间可以实现控制，超出时间范围无法打开涉密文件。

4.4 保护重要外发文档安全，防止二次泄密

企业在日常办公中，需要和供应商或外部客户的人员进行工作上的交流。一些重要涉密图纸文档在对外交流时，能够控制外发文档的权限，如只读、另存、打印、有限使用时间，并可以实现对外发文档绑定电脑、绑定介质（如 U 盘)、打开次数、打开密码，设置水印等功能。 采用灵活的方式控制文件的使用权限，防止外部人员滥用随意传播造成文档泄密。

4.5 保证便利的对外交流

企业在日常办公中，需要和供应商或驻外单位的人员进行工作上的交流。那么，就需要在保证文件安全性的基础上，不妨碍在办公过程中的对外信息交流，尽量不影响用户的正常办公，安腾软件提供了一个完善的审批平台，可以灵活高效的进行文档解密或者外发的审批操作。

4.6 杜绝通过网络或者移动存储设备泄密

在日常办公过程中，会经常使用到网络或者移动存储设备交换办公文档。而这种使用模式容易造成用户有意或者无意地将文件带离办公环境。因此，需要控制用户使用移动存储设备的使用；并对计算机终端各种可能存在泄密的端口进行监控及审计。

二、安腾计算信息反泄密整体解决方案

安腾电子文档安全管理系统（安腾文档加密软件）是安腾根据多年来积累的众多的市场反馈的经验，包括功能性、安全性、可靠性等，特别是针对政府单位和大型企业的需求而研发，其内部架构有着相当大的弹性。“安腾文档加密软件”以加密与鉴别技术为核心，不仅具有自动加密、U 盘管控、打印控制、程序控制、日志监控、自动备份、外发文件控制等功能，还将身份认证与权限管理嵌入系统中，具有身份识别与权限控制等功能，可适用任何管理需求大型规模的企业和机构，是国内最先进、最稳定、最安全的计算机信息反泄密解决方案。

事前主动防御:安腾文档加密软件对已有的或正在生成的 Office、CAD、PDF、txt 等各种格式的电子文档及设计图纸进行加密保护，被加密的文档只能被授权用户在授权环境（如,企业内部网络）中应用，文档在创建、存储、应用、传输等环节中均为加密状态,未经授权或脱离授权环境，加密信息均无法打开使用。

事中有效控制：安腾文档加密软件的加密过程不会因修改程序或进程名，更改保存文件后缀等作弊手段而失效，同时加密文档的复制/剪切/拖放/粘贴等操作也受到限制,向非加密文件中拖放/拷贝/粘贴的操作将被自动禁止。除此以外，安腾文档安全软件对打印机,U 盘等存储工具,笔记本电脑均有控制措施，并借助分组策略和身份权限的认证管理等技术进行更细化的设置和保护。

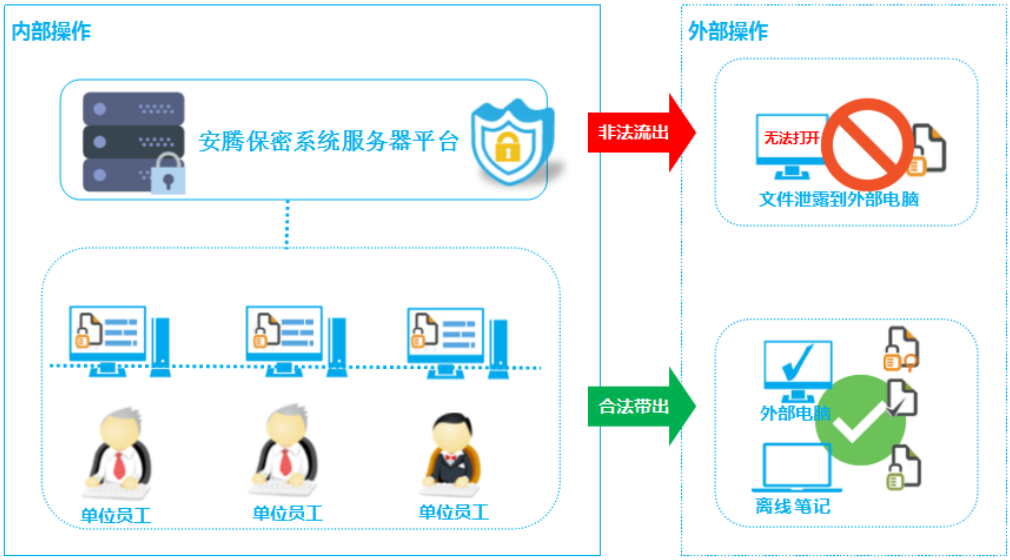
事后溯源补缺：安腾文档加密软件提供日志记录和自动备份功能，前者可以将指定的操作过程详细、完整地记录下来，方便监督检查和问题溯源;后者可以在文件被有意或无意删除或损坏时，通过备份资料及时恢复。文件在备份的传输、存储和恢复过程中均以加密形式存在。

安腾（ITEN）认为：“稳定性和安全性是第一位的”，反泄密方案不仅要考虑现在的需求，也要考虑未来企业的需求和应用。

1. 安腾加密的技术体系及场景应用

1.1. 文档的实时透明加密

在用户的涉密电脑上安装客户端，自动强制地对需要保护的图纸文档进行自动加密。这些文档只能在内部使用，无论采取什么方式被带离内部环境以后，该文档将无法打开。这样一种加密过程无需也无法干涉，基本不影响员工使用习惯，是一种完全透明的加密过程。



如图：文件在内部使用时和平时的工作状态没有任何区别，但是一旦文件非法带出公司则无法读取，而通过审批就可以合法带出。

1.2. 多种加密方式

可以根据公司具体需要，针对不同的员工的不同程序可以设定不同的加密模型，安腾加密软件提供多种加密模型：打开加密、修改加密、智能加密、不加密和手动加密：

打开加密：未加密文件一经打开便被软件自动加密。

修改加密：只有对未加密的文件进行修改保存后，软件才会对其进行加密。

智能加密：选用此加密方式打开加密的文件修改保存后文件为加密文件，打开未加密文件，修改保存后文件则为未加密文件，新建的文件不自动加密。该功能适用于 office、pdf 类软件。

不加密：软件不对电脑上的文件进行任何加密操作，但仍然可以打开加密的文件。

手动加密：针对智能加密和不加密模型的终端如果想要加密文件，可以手动对文件加密。

1.3. 文档密级和权限管理

同常见的透明加密产品相比，安腾加密软件采用 PKI 体系。其加密不再依赖于一般透明加密产品所采用的密钥而是依赖数字证书。既能实现对文件进行密级管理，也能适应企业日常的灵活权限控制。

这种 PKI 体系指纹内置方案的内核加密技术，是目前为止，在常见的五种内核加密实现方式中最完善的加密技术。该方案将加密标识内置于文件内，成为文件的一部分。当要打开文件时，会首先检查此文件是否含有加密标识。如果有，则对此文件进行透明解密。当要保存文件时，对内存中的文件流进行透明的加密，

然后写上加密标识。指纹内置方案，使得身份认证技术成为可能。通过不对称算法和对称算法的结合，然后在指纹中加入相应的证书，使得可以真正实现一份文档某些人（身份）可以打开，而其他人（身份）则不可以。

实现文件密级

安腾文档加密软件可以兼容文件密级管理需求，比如：默认情况下文件定为绝密、机密和秘密三个密级，可以设置三张数字证书为：绝密、机密、秘密，人员的身份按照实际情况可以设置为也设置为绝密、机密和秘密；身份为绝密的人员可以查看所有密级的文件，身份为机密的人员查看机密和秘密的文件；身份为秘密的人员只能查看秘密级别的文件。

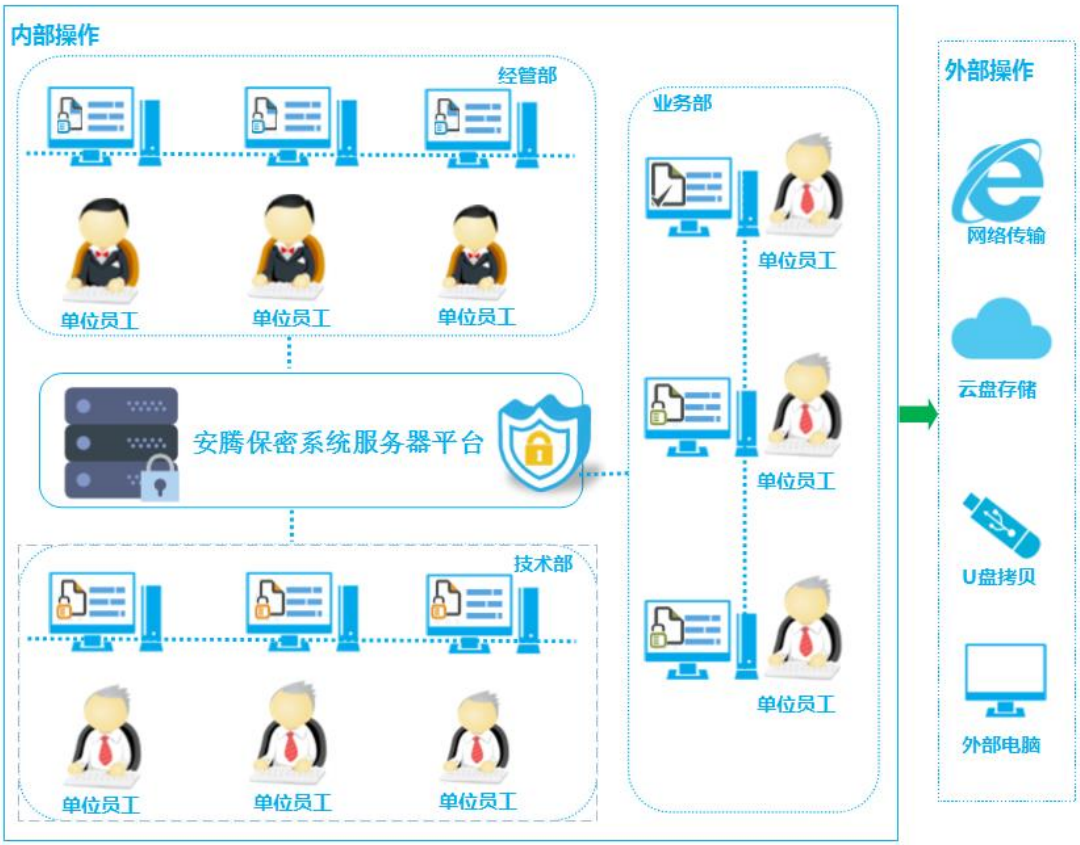
文件在部门间流转无需解密

比如：默认情况下，技术部的文件只能由技术部打开。当销售部需要某份技术文件时，由技术部负责人将该文件的权限属性设定为允许销售部或者销售部某个人可以打开即可。整个内部过程无需解密，文件始终处于加密状态。

灵活方便的设置可满足多种工作模式

既可以设置某一个人同时拥有多种身份以便打开不同权限的文件，也可以设置允许一个文件可以被其它身份的人打开。这种身份和权限还可以根据需要随时调整。

安腾文档权限管控支持自动权限控制和手动权限控制。



注：蓝色为经管部文档，黄色为技术部文档，绿色为业务部文档。

1.4. 外发文控制

通过外发文件控制软件，可以对需要向外发送的投标书、财务资料、图纸等重要文件的打开、修改、打印及使用时间等权限进行设置，超过该设置期限，将成为无效文件，从而有效防范所授权外发的重要文件在离开公司管控范围后而产生的泄密情况的发生。

借助安腾文档加密软件的外发文档控制功能，用户可以实现以下功能：

只　　读：指定文档是否可以修改；

禁止复制：指定文档打开后是否可以进行“另存为”操作；

禁止打印：指定文档可否打印；

禁止截屏：指定文档是否允许执行截屏操作；

使用时限：指定文档只能在指定时间内使用；

使用次数：指定文档打开的次数；

绑定电脑：设置只能在双方约定的电脑上打开文档；

密码校验：验证文档打开密码，用于防止文档意外丢失泄密；

绑定 U 盘：智能将文档拷在指定的 U 盘上才能打开；

自动销毁：超过使用次数和使用时间后，自动将文档删除。



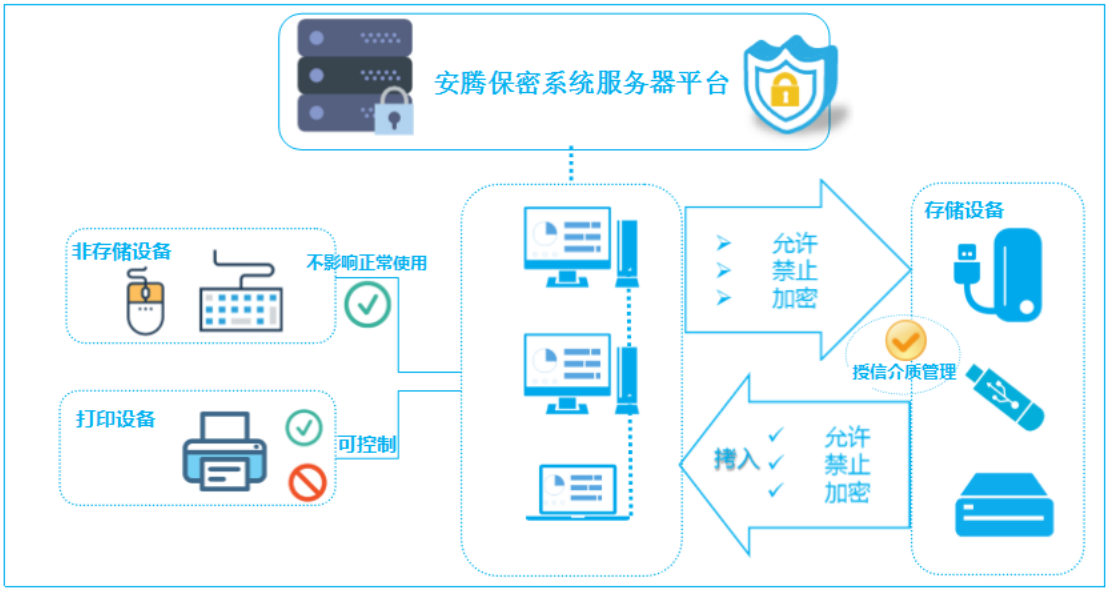
1.5. 移动介质与打印管理

安腾文档加密软件采取的是存储特性识别，所以在管理的时候不用担心会对一些使用这些端口的其他设备造成干扰。

对一些可能产生泄密端口进行控制，如打印机端口和移动存储设备（U 盘、MP3、手机等）端口。对打印机端口进行管控，可以设定某人或者某组是否可以打印涉密文档。对于移动存储设备端口管控，则可以根据实际要求，设置出强大的使用规则。对于入和出（相对电脑而言）可以分别进行控制，组合后可以实现 9 种使用规则。实现如只读、禁用、拷入加密、拷出加密、只出不入等诸多功能。

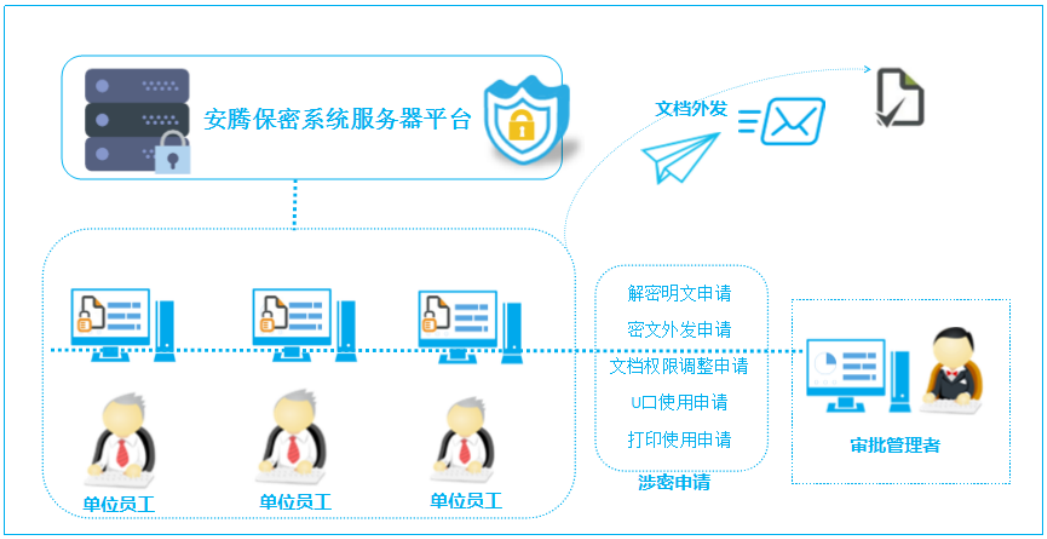
同时提供了可信介质管理功能，经过公司认证许可的介质，可以在公司指定范围内的终端电脑上正常使用，而不受禁止拷贝功能限制。

可控制指定客户端能否使用打印功能，也可以控制指定客户端电脑只可以打印某类文件不能打印其他文件，比如只能打印 office 文档，不能打印图纸。



1.6. 涉密审批

安腾文档加密软件提供灵活便捷的审批方式，大大方便了企业内部的审批效率。



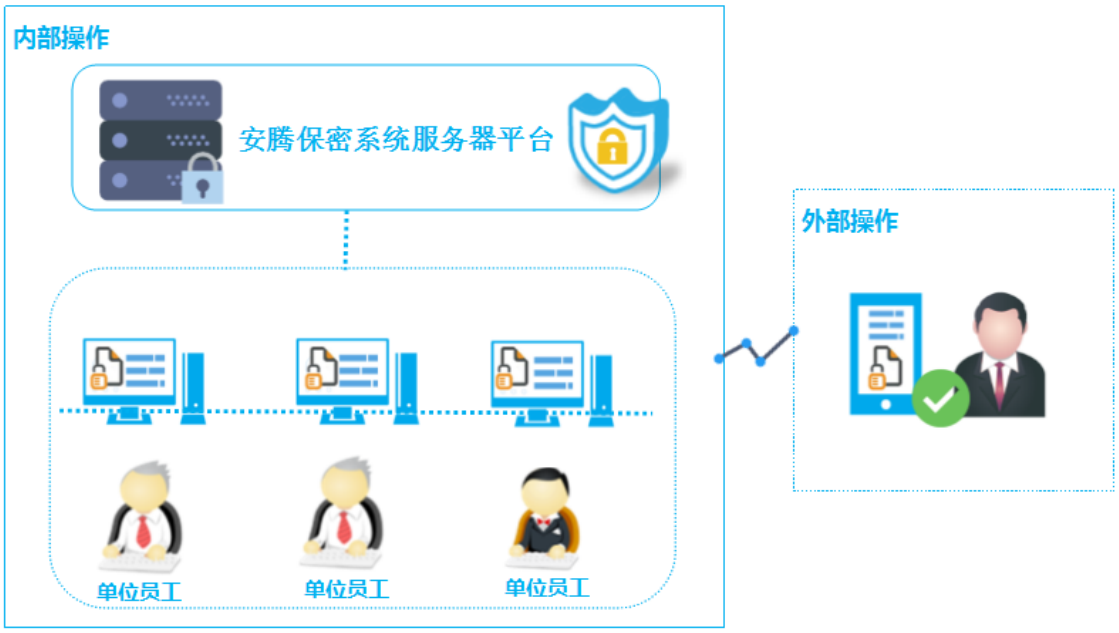
在客户端默认安装安腾解密助手审批端，当有解密、跨部门借阅文件、外发文、打印、使用 U 盘、恢复复制粘贴功能等时，可以通过解密助手向审批端发出相关申请，审批端的负责人可以根据申请的情况做出相应的授权。同时将在服务器上形成相关日志。

安腾文档加密软件支持单级审批和多级审批，同时还可以自定义审批流程；单机审批主要实现对保密文档的解密、外发、权限调整等操作的流程审批，也可以自定义审批人的管理权限；多级审批可以实现多人对加密文档的解密、外发、权限调整等复杂的特殊流程；同时支持异地审批。

1.7. 移动端安全

企业在正常办公中多多少少都会遇到审批者不在公司或者不在位置上的情况，这时候就必须要有相应的解决方法。所以安腾文档加密软件推出了移动审批端，方便用户不在电脑旁边的时候进行加解密的审批操作。

同时针对领导和经常外出员工移动办公而推出的移动文档安全，保证员工可以直接使用移动终端进内部文件的阅读与使用，保证了员工的手机安全与办公的便利性。



1.8. 邮件白名单

邮件白名单主要附件自动解密的功能；主要分为邮件发送者白名单和邮件接收者白名单：

邮件发送者白名单：将文件通过附件的形式发送给其他用户，这些加密的附件将会自动解密掉。

邮件接收者白名单：用户将加密的文件通过邮件附件的形式发送给指定的用户（邮件接收者白名单），该用户收到的附件会自动解密（注意：用户进行多个邮件同时发送附件的时候，如果含有非白名单用户，那么这封邮件的附件将不会执行解密操作，白名单用户收到的附件将依旧处于加密状态。）

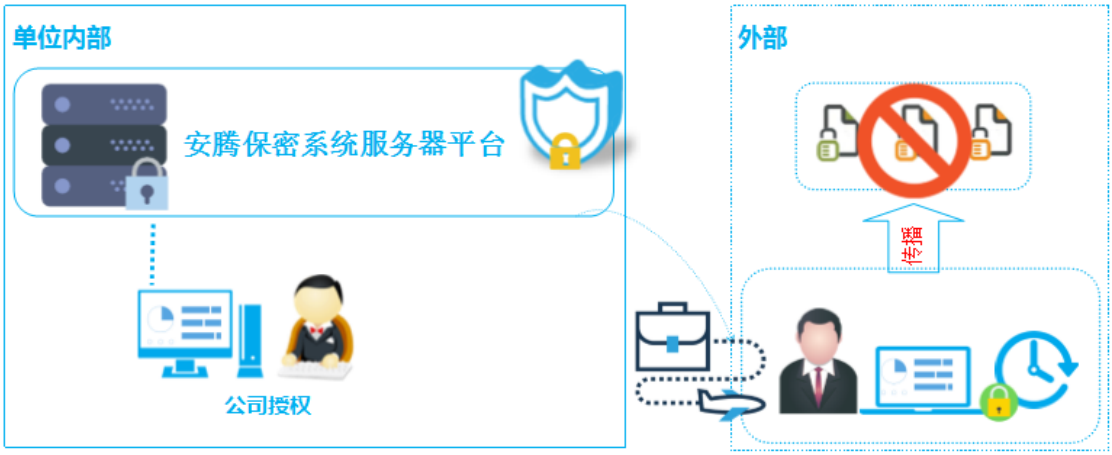
比如：对于长期合作信任的供应商，可以将对方邮箱添加到邮件接收者白名单，这样给该供应商发送的邮件附件可以自动解密；将公司领导邮箱添加到邮件接收者白名单，这样领导邮箱发送给其他人的邮件附件可以自动解密。

1.9. 日志审计

安腾文档加密软件提供涵盖了一系列涉密的日志信息的审计功能。

详细记录受控终端操作日志、管理平台操作日志、申请与审批操作日志、涉密数据操作日志、外发数据操作日志，对于可能导致泄密的操作进行监控，如打印、拷 U 盘、解密文件，终端打开文件，修改文件，删除文件等操作日志传送至服务器，以备后期追查；同时详细记录管理端、解密端和服务器端的管理操作日志，方便追溯审计。

1.10. 笔记本离线外带管理



笔记本外带方案：

第一种是完全授权的方式，在这种方案下笔记本电脑在公司授权后，可以永久在外部使用公司赋予的策略来进行文档的使用。

第二种是半授权方式，在这种方案下笔记本电脑被授权只能在规定时间内插上时钟加密狗以后才可以正常的使用赋予的策略来进行文档的使用，一旦授权时间已过或者加密狗没有插在电脑上，外带笔记本将无法在使用涉密文档。如果需要延长出海

以上两种方案，用户在使用涉密文档的时候都不可以私自的将文件交由第三方来使用且使用的都是公司内既定好的策略。如果

1.11. 内容保护

针对涉密文档实现虚拟打印保护、复制粘贴保护、OLE 插入保护、拖放保护和抓屏保护，防止涉密内容泄露。

虚拟打印保护是实现文档在使用虚拟打印机转换文件格式后，转换成的新格式的文件也是加密文件，未经授权带出，还是不能使用。

复制粘贴保护是防止加密文档内容向不加密文件内复制粘贴，但是不影响从未加密文档内向加密文档内复制内容。

拖放保护是防止从加密文档内直接向未加密文档内拖拽文档内容，不影响从未加密文档向加密文档内拖拽内容。

OLE 插入保护是防止 cad 类的文件通过 OLE 插入泄密。

抓屏保护能够防止员工通过 QQ 等软件提供的截屏功能将涉密文档通过图片的方式泄露出去。

1.12. 水印控制

为了震慑拍照，安腾文档加密软件还为常用的文档图纸提供了可自定义的水印功能；可根据实际情况设置是否显示水印，水印分为屏幕水印和打印水印：

屏幕水印：打开密文文件时显示水印；

打印水印：打印密文文件时显示水印。

1.13. 系统兼容性方案介绍



安腾文档加密软件可以兼容现在市面上 Windows xp 及以上的全部微软系统（包括 64 位）、macOS 系统，移动端支持安卓和 IOS 系统，可以进行各种分布式或者集中部署，并且针对各种企业常见的应用系统都有良好的兼容措施，甚至可以提供各种接口方便用户进行二次开发与自定义。

1.14. 备份系统介绍

安腾文档加密软件提供了一整套的基于 FTP 的文件备份系统，它会根据文件的后缀名进行全本的版本备份，可以根据用户的设定在规定的时间备份最近几次文档修改的内容。

这种备份功能可以避免员工离职或者对公司不满时，恶意删除各种重要文档是对公司造成不可预估的损失，也可以当做一个简易的文档的版本管理系统。

注：这种备份是强制性的。

1.15. 应用安全

企业内部所有数据都是加密的，为了不影响企业应用系统(比如：CRM、REP、PDM/PLM)的正常试用，安腾文档加密软件可以通过服务器控制功能实现在企业内部向应用服务器上传文件时自动解密，如果员工从指定应用服务器下载文件时则自动解密。

对于企业自己研发的应用系统，安腾可以提供加密接口，应用系统服务器可以调用加密接口，实现文件上传解密，下载加密。

安腾文档加密软件可以和加密网关配合，只允许安装有安腾客户端的终端访问指定的应用系统，如果终端没有安装安腾加密软件的客户端，即便知道用户名密码也无法登录指定的应用系统。

1.16. 多种认证方式

安腾文档加密软件提供多种认证方式，可根据用户实际情况选择：

硬件认证：通过终端硬件信息认证，硬件信息包含终端主板、硬盘、网卡等

用户名认证：通过终端登录的用户名认证

AD 域认证：和 Windows AD 域控同步组织结构，通过域用户认证

EXCEL 导入：如果没有 AD 域，但是向采用用户名认证，可以试用 EXCEL 导入用户信息；

LDAP 兼容：系统可以与 LDAP 等第三方认证系统兼容

1.17. 灵活的客户端在线策略

根据实际应用和网络情况，客户端可以设置不同的在线策略：

极进模式：这种模式下，客户端需要和服务器保持通信，在这种模式下，客户端与服务器的通信一旦断开，则无法打开已加密的文档。

温和模式：这种模式下，客户端只要和服务器进行一次通信握手后就可以正常使用加密文档，使用过程中服务器即使断开依旧可以打开加密文档，直到客户端电脑重新启动。

离线模式：这种模式下客户端可以离线使用，如果想控制客户端的离线时间，可以设置允许离线的时间，并且可以选择是否使用加密狗来进行时间控制。使用加密狗的情况下，如果狗与电脑分离，那么文件便会无法打开。

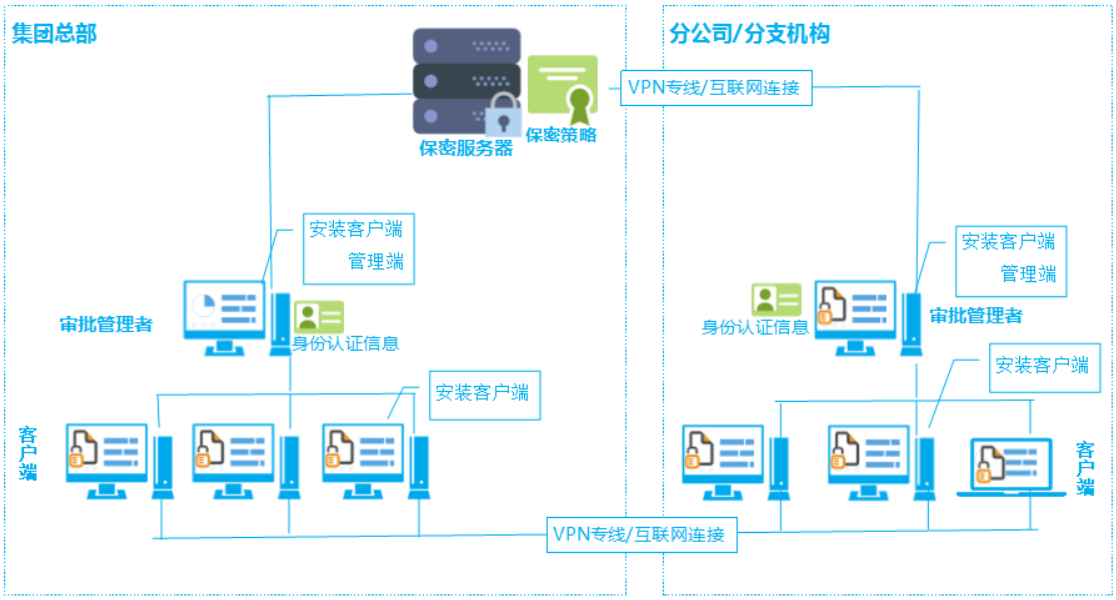
2. 实施流程与效果预测

2.1 实施流程

a) 系统的架构部署

公司的总部与下属公司之间一般存在投资管理、战略管理和操作型管理等管理模式，无论哪种模式，都是以集团公司的职能部门对下属公司的对口部门的条线管理为主。所以这就涉及到了集团数据与软件的集中管理问题，由于安腾加密提供是一种 B/S 模式的管理平台，所以我们可以选择只需要在集团总部架设一台服务器来进行软件的集中管理。采用这种方式进行部署时，需要有 VPN 专线通讯或 Internet 网络以保证下属企业或分支机构电脑能够访问到安腾加密的加密服务器上，其效果类似总部部门之间的文档加密模式。

具体部署情况如下图：



如果没有外部网络的公司可以考虑采用在分公司设置分服务器方式，这样也可以有两种模式：

（1）分公司服务器与总部服务器基本密钥设置一致，其效果类似于集团公司部门之间的关系；

（2）分公司服务器与总部服务器基本密钥不一致，可以将分公司的密钥信息放入总部服务器中，其效果是分公司类似总部的一个部门。

b） 用户的权限分配

- **集团管理总部各部门间的权限分配**

集团公司总部一般由各个相对独立的职能部门组成，其中部分职能部门承担着对下属公司相关部门的条线管理工作。在管理流程上可能存在以下全部或部分要求：

- 集团公司总裁享受最高权限，可以打开公司内部所有密文，并可以配置解密功能。
- 集团公司副总裁可以打开其下属部门的所有密文，并可以配置解密功能。

- 不同部门之间的密文可以设置为互通互读，也可以设置为不能互通互读。如果需要将 A 部门的密文发给不互通的 B 部门阅读，可由 A 部门的管理者对此份文件的权限进行调整，设定 B 部门或者 B 部门的某人可以打开此份文件。其他未授权人员即使获取文件也无法打开。
- 某些部门在有特殊需求的时候可以设定成该部门的文件在某些部门只能只读，无法编辑和无法打印。

- **集团与下属公司之间的权限分配**

集团公司与下属公司密文之间的联络主要存在以下几种情况：

- 当集团某部门往其它部门、下属分公司等发送某份已加密的文档时，其负责人可以通过管理端程序设置该文档的打开权限，这种权限甚至可以设置到个人。当其它部门或下属机构等需要类似传送时，具有同样的功能。
- 具有条线管理职能的部门，可以设置成上级管理部门无障碍浏览下属企业被管理部门的加密文档，而下属企业在未经授权的情况下不能打开上一级管理部门的加密文档。也可以设置成互相限制或者互相不限制状态。

c) 受控软件的设定

安腾提供了市面常见的超过一百种的各类办公、设计类软件的集成，甚至还提供了自定义接口来让客户自己添加一些特有的需要加密的软件。在用户自行添加如果有障碍的时候安腾软件还提供协助服务。

d) 备份功能的设定

在企业内部配置好备份服务器后，在备份界面中将需要备份的文件格式以及备份的时间与份数后，将备份的策略赋予给指定的几台电脑。

2.2 效果预测

- **内部文档数据的保密效果预测**

对于存在于各个终端计算机的涉密文档图纸等，通过安装客户端进行强制性加密保护。实施以后，在同一公司或同一部门内部，文档可以自由的流通，就如同没有安装安腾加密一样。但当文件未经授权流出公司，文件则变成乱码。如果文件需要交给客户或公司外面的人，则需要经过管理人员的批准解密。安腾加密并能与 OA、ERP 等多种内部管理系统完美对接，不会影响原有的工作环境。

- **内部数据使用时的效果预测**

1、由于采取了加密技术，各种网络传输、邮件传输如果未经解密操作，发出去的密文是无法打开的；而对于像销售部等与外界交流很频繁的部门，则可以使用邮件服务器，设置信任邮箱地址，安腾加密将自动对发往信任邮箱的邮件进行解密操作，同时自动记录邮件的收发操作日志。

2、安腾加密对于密文将自动限制其复制、粘贴、抓屏等行为，也可以对于打印设备进行禁止使用、限时使用、记录打印日志等加以控制；

3、安腾加密可以针对各种存储设备进行信任例外与管理，有禁止使用、只读、自动加密和开放使用等模式；

- **不同岗位之间信息浏览和管理限制预测**

1. 对于不同部门或小组之间的信息壁垒，安腾加密通过分组策略加以解决；
2. 对于不同层级管理人员的文档管理权限，安腾加密通过分级策略实现上级对下级文档管理的授权与审批。

- **与客户之间的交流效果预测**

由于外部交往频繁，对于部分重要文件公司有时需要对外发文件进行控制。

根据控制的紧密程度，可以有多种选择：

1、解密助手：通过客户端解密助手的申请解密功能，审核负责人在确认文件安全性以后同意将文件解密，客户端便会将这个文件变为明文，这样只要在规定的时间内将这个明文发出去就可以了。与此同时，相关解密操作会在服务器形成记录日志，并且解密的文件原件会在服务器或者指定的 FTP 下保存下来。

2、通过外发文件管理控制软件

可以对一个需要外发的文件设置其读写权限、打开次数、打印权限、存活时间、修改等权限，然后发送给客户，客户通过网络认证或硬件认证的方式接受相关权限。对于已经设置好的权限，还可通过远程修改。

3、在客户的专用计算机上安装一个客户端，该计算机专门用于接收公司发送的加密文档并可以正常使用。

- **重要文档的备份预测**

设定好备份的部分重要电脑会在指定的时间，将指定类型的文件备份至 FTP 中，管理者可以在服务器端进行这些文件的查阅以及管理。

- **外带笔记本与移动终端设备的管控预测**

一些普通员工的出差电脑设定为允许离线的模式，方便其在各种没有网络或者环境恶劣的情况下进行办公，这些电脑如果在外地重装系统的话只需要将客户端安装好后接入 VPN 或者 Internet 网络中就可以直接在服务器上自动获取到之前给其分配的权限信息。

而一些重要或者敏感的电脑外出的时候需要设定离线的时间以及绑定时钟加密狗，这些电脑在外地使用的时候一旦超出其所获得的离线时间后，只需要接入

VPN 或者 Internet 网络就可以在服务器上进行离线时间的再次刷新，而在携带笔记本的时候，时钟加密狗与笔记本需要分开存放，这样一旦电脑丢失，电脑中的所有敏感数据都将无法打开。

外出员工的移动终端平台安装手机版 APP，从而保证员工可以直接使用移动终端进内部文件的阅读与使用，保证了员工的手机安全与办公的便利性。

三、技术支持与售后服务

1. 培训安排

安腾软件在项目实施中，可以根据项目组的要求和安排，就系统的实现原理、功能介绍、安装测试、系统初始化、备份与恢复等的培训。安腾软件将长期提供免费的远程技术咨询、远程技术协助等服务。

需要为此做好配合工作，包括确定并组织参加培训的人员，确定培训场所，配备白板、投影设备等工具，建议安排专人负责考勤和现场监督。

2. 技术支持与服务方案

质量保证期：安腾软件提供一年期的质量保证期，从系统安装完成之月度起计算 12 个月（包括完成当月）。质量保证期内，免费提供技术支持、软件维护与升级等服务。

重大问题及时响应：如遇系统导致的重大问题，安腾软件承诺技术人员 24 小时内现场响应，48 小时内解决问题 (非本地客户方需负担交通、住宿等基本费用)。

质量保证期内回访：安腾软件项目组成员每季度至少远程回访 1 次。

软件升级：在质量保证期内，客户有权利无条件使用新版本的软件。在过了质量保证期后，如遇软件 Bug、漏洞等自身原因，安腾软件将主动或根据客户的要求进行修补、升级。

四、关于我们

安腾（ITEN）是中国计算机信息反泄密软件和文档加密软件的始创者和领导品牌，长期专注政府和企业计算机信息反泄密研究，为企事业单位提供领先的计算机信息反泄密解决方案。旗下拥有“文档守望者”、“安腾”、“安腾”等多个品牌产品线，能够满足不同行业和规模客户的信息安全保密需求。

安腾始终专注于透明加密软件的研发，是国内最早从事文档、图纸、代码等透明加密的研发厂商，对于加密软件有着深刻的理解。安腾力求产品的使用简单、功能实用、运行可靠。多年来得到了客户的广泛认可和信赖，安腾也为计算机反泄密领域“安全”的代名词。

安腾加密软件采用了国际领先的 PHOENIX 内核的专有加密技术，可以满足广大用户单位对文档、图纸等关键电子信息的保护需求，具有安全性、便利性和可靠性的特点。该软件在不改变原文件格式的前提下实现文档的安全流通，有效防止恶意用户通过电子邮件、移动硬盘、U 盘、打印等途径泄密重要数据文件，做到"事前主动防御、事中灵活控制、事后有效追踪"。安腾软件深刻理解企事业单位对信息安全与知识产权保护的需求，以专业的手段、先进的技术为企业提供系统化的解决方案。

安腾软件已在机械、电子、化工、设计院、服装设计与制作、广告、印刷包装、制造和政府等行业中得到广泛应用，得到用户的赞许和好评。安腾软件凭借先进的技术和在信息安全领域的丰富经验，每 3 个月到 6 个月更新一次版本，以保持产品不断完善、保持技术的不断领先，使用户得到更新、更安全的服务。

安腾软件坚持走专业化发展的道路，坚持"技术领先、服务先导"的经营理念，致力于信息安全领域的技术进步和市场推广，安腾软件正努力实现从技术型公司向技术与服务型公司转变，致力成为中国信息安全领域标志型企业。

"技术领先，服务先导"、"满足客户需求，为客户创造价值"是我们一直坚持的经营理念。我们从深刻理解企业信息安全与知识产权保护需求出发，以先进的技术、专业的服务、认真而细致的工作，为客户提供一体化的解决方案；我们高度关注客户的满意度和忠诚度，以满足客户需求，为客户创造价值为己任；我们高度重视企业品牌的树立和维护，努力成为客户信任的信息安全技术专家和长期合作伙伴。