天锐绿盾信息安全管理软件产品简介

厦门天锐科技有限公司

Xiamen Tipray Technology Co.,Ltd

目　录

一. 背景

随着计算机网络技术、数字通信技术飞速发展，大量的技术和业务机密存储在计算机和网络中，对网络安全性要求变得越来越高，需要有效地制定安全策略以保护机密数据信息。


您是否有这样的困扰：

- 员工通过 QQ、MSN、电子邮件、移动存储设备等方式随意将公司内部重要数据外发？
- 存储着公司重要数据的 U 盘、光盘、笔记本等设备，不慎丢失造成数据泄密？
- 公司机密文件，被员工获取并泄漏给竞争对手？
- 员工离职带走公司的重要数据文件，并格式化他们的电脑，造成重要数据文件泄漏、丢失？
- 发给客户的文档就像“放飞的风筝”，无法控制？
- 员工打印权限不受控制，给数据安全带来重大隐患？
- 外来计算机可以随意接入公司内网，造成数据泄密无法有效追踪其源头？
- ……

企业中不当的资源利用及员工上网行为往往是“罪魁”，在国内，诸如设计方案被窃取、关键客户名单和销售数据丢失等事件屡见不鲜，给企业造成了非常大的经济损失。

针对内部泄密的问题，天锐绿盾信息安全管理软件整合文件透明加密、内外网行为管理、硬件设备限制这几个方面来减少内部泄密的可能。

二. 功能简介

天锐绿盾信息安全管理软件（以下简称绿盾）是一套集文件透明加解密、上网行为管理和内网管理为一体的企业数据防泄密软件。文件在创建、编辑时自动加密，从泄密的源头控制，彻底控制信息的泄漏。打开时自动解密，不影响用户

的操作习惯，文件非法复制离开网络后，将无法打开。并对机密文件的使用过程进行全程监控管理，有效防止了被动和主动泄密，消除内部安全隐患于无形之中。

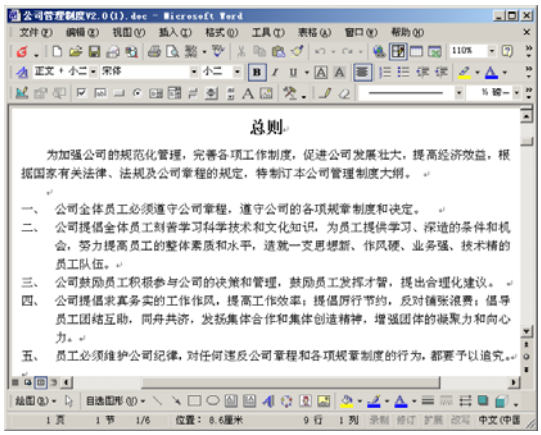
2.1 文件加密

2.1.1 文件透明加解密

绿盾采用 Windows 内核的文件过滤驱动实现透明加解密，对用户完全透明，用户打开文件、编辑文件和平常一样，甚至毫无感觉，不影响用户操作习惯。同时由于在文件读写的时候动态加解密，不产生临时文件，因此基本不影响速度。

如果加密文件通过 MSN、QQ、电子邮件、移动存储设备等手段传输到企业授权范围以外（企业外部），那么它将无法被正常打开和应用，打开将显示乱码，文件始终保持加密状态。

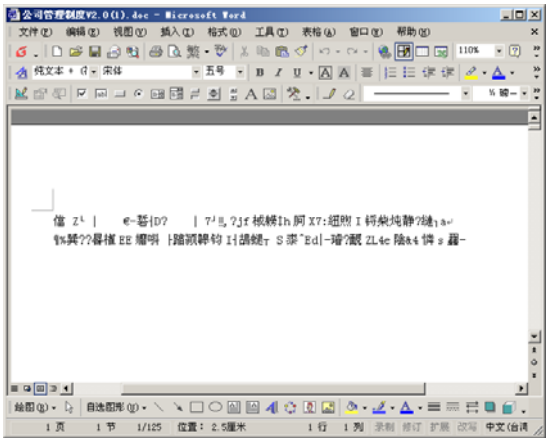
（在安装绿盾电脑上，正常使用）



在绿盾授权保护下，能正常阅读、编辑、复制文件，和平常使用没有区别

脱网后

（拷贝出去后，无法打开）



文件被非法带离，立即变成无法阅读的乱码

2.1.2 传播途径限制

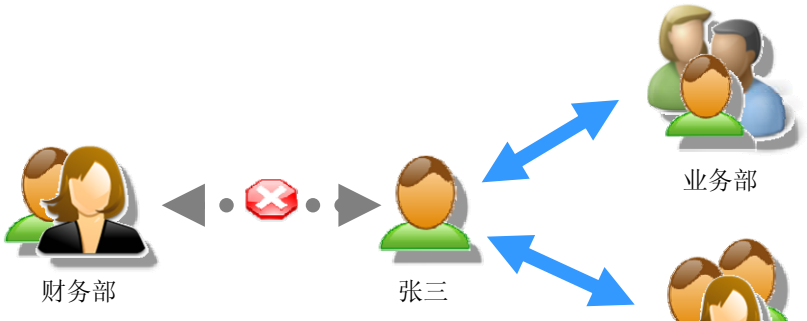
绿盾严格限制各种可能导致泄密的途径，如剪切板（内容复制黏贴）、截屏、打印、移动存储设备、网络传输等。

- 控制打印机、光驱、软驱、U 盘、打印支持水印
- 禁止屏幕截取（如 QQ 截屏、红蜻蜓截屏、屏幕录像工具等）
- 控制复制粘贴

- 禁止 OLE 插入
- 禁止 WPS 网盘
- 控制虚拟打印机

2.1.3 文件阅读权限

可以根据需要，设置不同部门、不同操作员的文档阅读权限，即授权指定部门或用户只能访问指定部门的文档，其他文档，即使获取到，也无法打开。

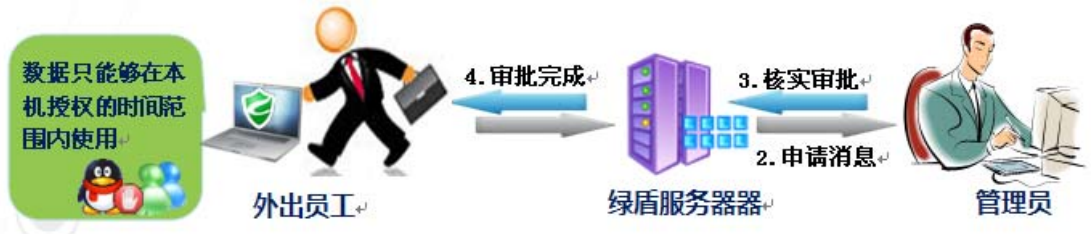


例如：张三可以阅读业务部和采购部的文档。不允许阅读财务部的文档。

2.1.4 离线管理

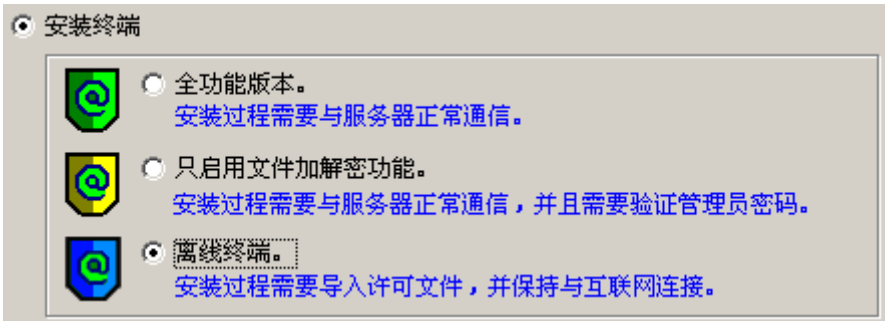
用于管理不能跟服务器通信的终端电脑，如出差、服务器故障等，在授权时间内，终端可以正常工作，超过离线时间，将无法打开加密文档。

- **短期离线：**主要用于当服务器电脑宕机、或者发生网络故障时，保证终端还可以正常工作的缓冲时间。也适用于需要晚上或周末回家办公的笔记本电脑，不用额外申请，方便快捷。
- **离线策略：**主要用于员工出差时间超过短期离线时间、或离线时间需要变更的情况。可以通过在线申请、导入离线策略文件等方式来实现终端离线工作。



- **离线终端：**主要运用于长期或永久脱离公司总部在外办公的电脑，一般是分

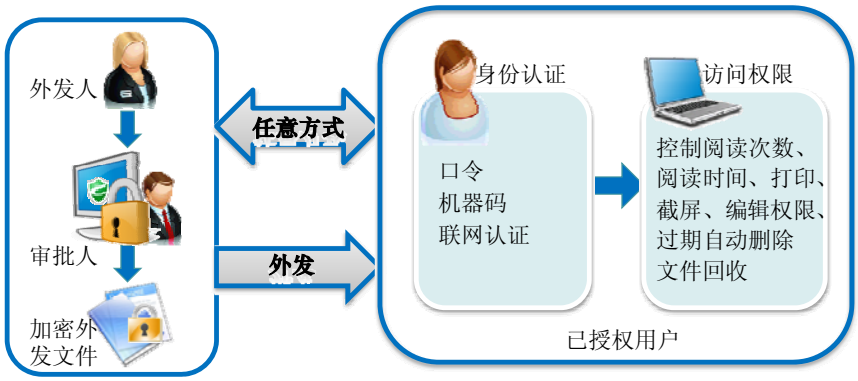
公司或办事处，保证他们能够正常访问总部的加密资料，同时防止他们电脑上的资料外泄。



2.1.5 文件外发管理

文件加密后，在本机上打开和在公司内流通都可以正常，但要外发出去，就要先解密或制作成绿盾外发文件。

- **批量解密**：具有批量解密权限的操作员可以自行解密，不需要申请；
- **申请解密**：普通终端可以向有审批权限的人员申请解密文件，审核通过后才可以解密成功；
- **邮件白名单**：可根据需要设置邮箱白名单地址，发送加密文件到白名单地址，加密的邮件附件自动解密，减少解密次数；
- **外发文件控制**：控制外发文件的操作权限，其中包括：打开次数、生存周期、密码验证、修改限制、截屏限制、打印限制、过期自毁等，超出限制将无法打开文件，防止外发文档二次扩散，确保信息安全；
- **外发新增功能**：支持认证机器码，减少机器码认证功能操作的复杂性。支持外发阅读器，大大提高外发文件打开速度，支持在域环境下使用外发文件。



2.1.6 审批流程

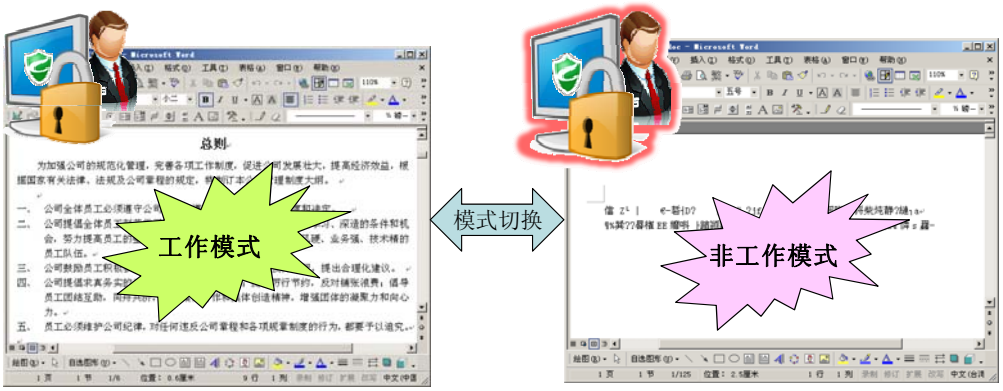
可以根据企业情况自定义审批流程，根据自定义的流程进行解密申请、离线申请、外发申请。流程支持多级审批、同级多人审批等模式，审批方式支持手动审批、离线自动审批、所有状态自动审批等。

（以文件解密申请为例）

同时支持 Web 审批，审批人员可以通过网页、手机、移动办公设备来处理申请。

2.1.7 工作模式管理

可根据需要，允许某些用户可以在规定的时间段内自由地切换工作模式：开启加密或关闭加密功能。在工作模式（开启加密）下，创建的文件自动加密；非工作模式（关闭加密）下，新创建的文件不加密，但不能打开加密文件。在非工作模式下，也可以同时关闭内外网监控功能。

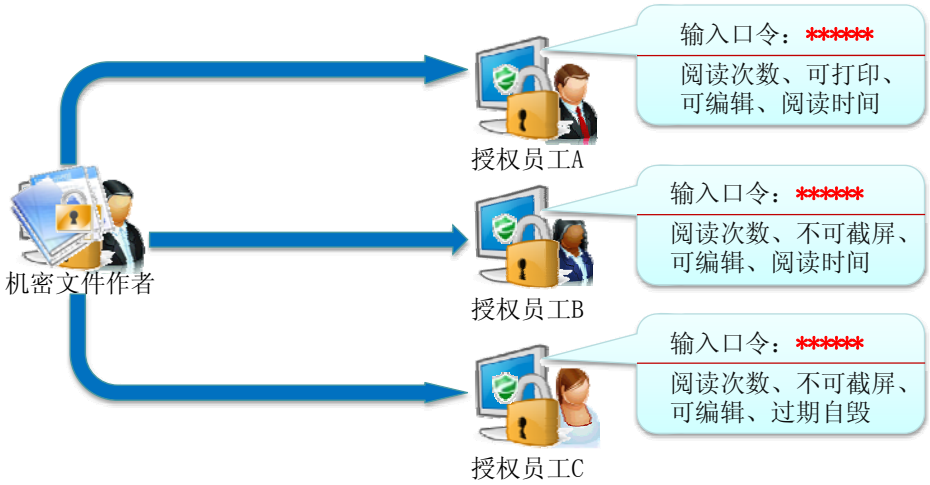


2.1.8 文件管理控制

文件管理控制分为文件集中管理和内部流转文件：

文件集中管理：类似 ftp 服务器，管理企业数据文件的访问权限：上传文件、下载文件、删除文件、增加子目录、修改目录、删除目录等。

内部文件流转：分级管理企业内文件，控制一些机密文档只能给指定的用户阅读，并限制访问权限，如打开次数、打开时间、修改、打印、截屏、过期自毁等操作权限，非授权人员即使获取到文件也无法打开。



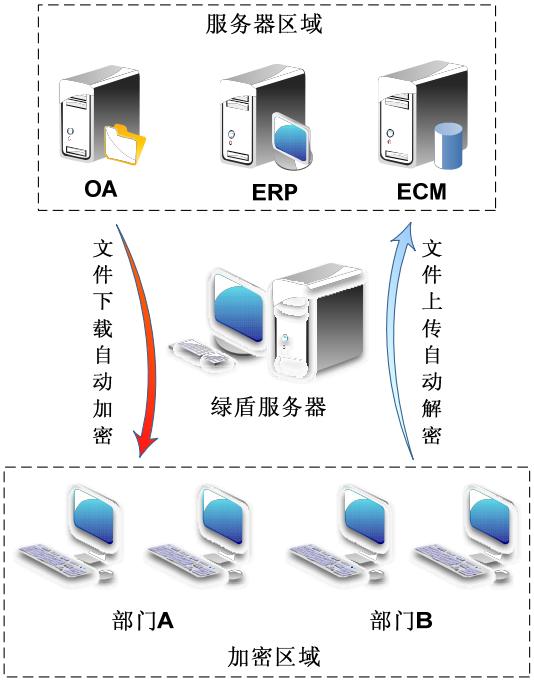
2.1.9 文件自动备份

可以根据需要，设置需要自动备份的文件类型。这些类型的文件在新建、或者编辑后会自动备份并上传到服务器进行保存，防止误操作或恶意删除带来的文件丢失，特别是员工离职格式化硬盘导致的文件永久丢失。

2.1.10 服务器白名单

企业一般会有很多服务器，如 OA 服务器、ERP 服务器、财务系统服务器，等等。绿盾可以在不改变应用服务器集群环境的情况下，做到：

- 加密文件上传到白名单服务器自动解密，没安装绿盾终端也可以在线阅读服务器上的文件；
- 白名单服务器上明文文件下载到终端后自动加密，防止文件下载泄密。



还可与绿盾数据安全网关相结合，做到只有安装绿盾终端的电脑才有权限访问指定的服务器。

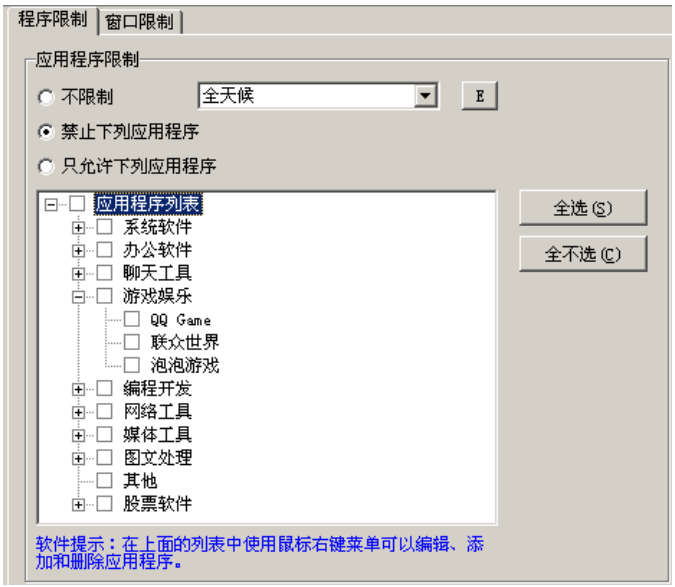
2.1.11 文件操作记录审计

全程记录文件的各种操作，包括新建文件、删除文件、打开文件、编辑文件、复制文件、重命名文件等，文件在移动磁盘、网上邻居等路径上的操作都可以监视到。还可以记录文件的打印操作，并能查看打印内容。

2.2 内网行为管理

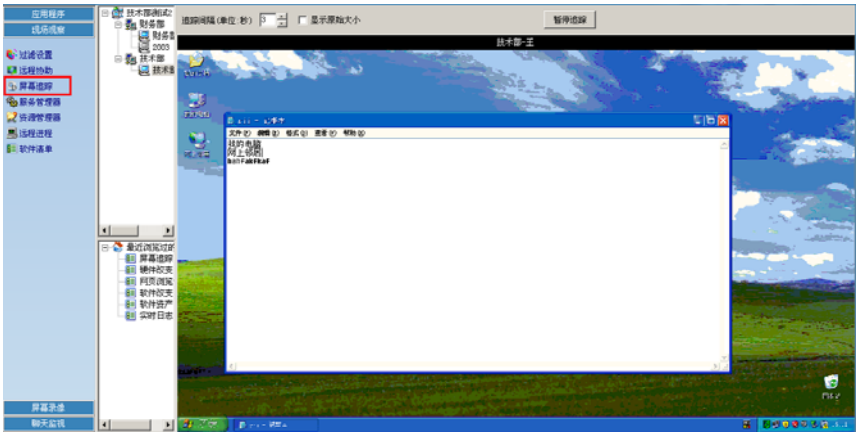
2.2.1 程序管理

设置程序白名单、黑名单，禁止指定应用程序的使用。记录、统计程序的使用情况，并形成报表，各种程序的运行时间、使用时间和使用频率占所有程序的百分比一目了然，可以大体了解员工花在哪个程序上的时间比较多，方便管理以提高工作效率。



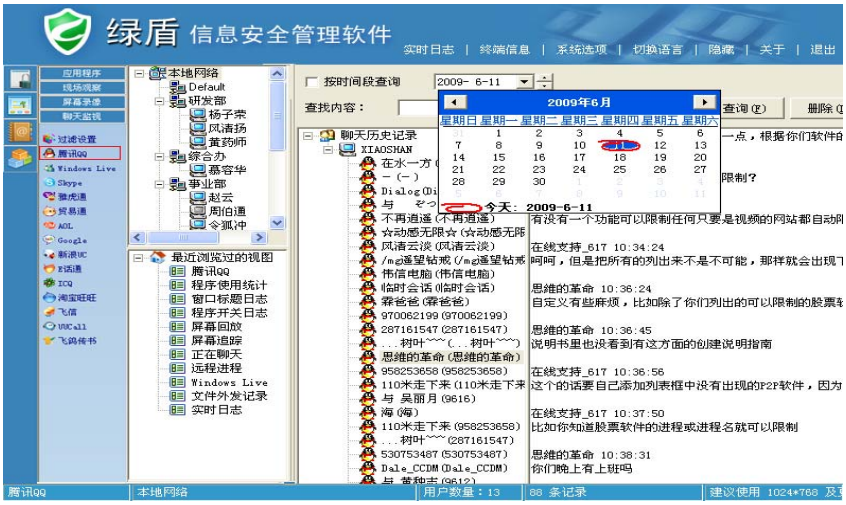
2.2.2 屏幕追踪

可以实时显示终端电脑的屏幕画面，追踪员工桌面操作情况，并可以定时进行屏幕录像，供事后查看。



2.2.3 聊天监控

可以监控主流聊天工具的文本聊天内容，如 QQ、MSN、阿里旺旺、飞信、skype 等，QQ 的文件发送情况也可以记录下来。记录可以导出为文本文件供事后审计查询。



2.2.4 远程维护

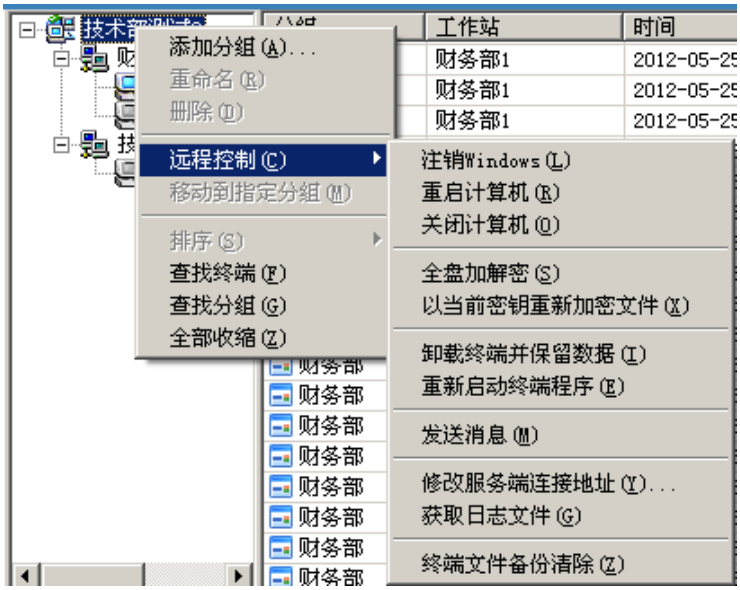
可以远程列出终端电脑当前正在运行的进程列表、系统服务情况，必要时可以结束某些进程或服务。

可以远程列出终端电脑的目录结构、文件列表，加密文件会显示加密锁，方便了解终端电脑上的文件加密情况。

可以远程列出终端电脑上的软件清单，了解终端电脑的软件安装情况。

可以远程注销、重启、关闭终端电脑，必要时也可以远程控制终端电脑桌面，方便管理员远程维护。

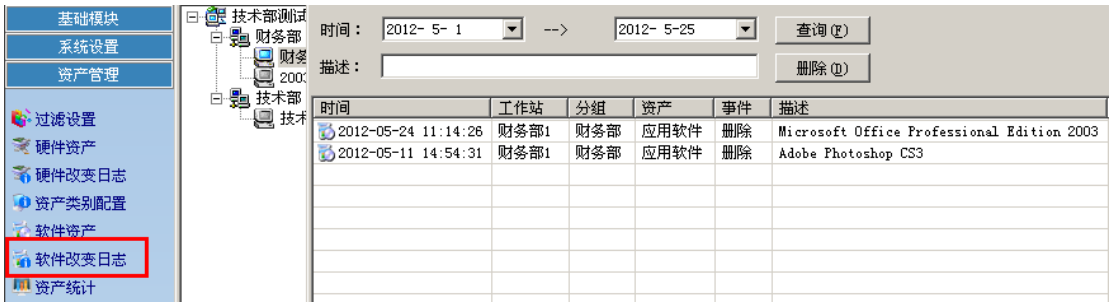
可以远程向终端电脑发送消息，如向违规用户发送警告通知等。



（以远程注销、重启、关闭、发送消息为例）

2.2.5 资产管理

可以远程列出终端电脑的软硬件详细配置，并可以精确记录软硬件变更情况。同时，在终端插入、拔出可移动磁盘、改变 IP 地址、MAC 地址、改变计算机名称时，也会以“报警日志”的形式记录下来。



（截图以软件改变日志为例）

2.3 上网行为管理

2.3.1 网页浏览记录

记录终端电脑的网页浏览信息：包括浏览时间、网站地址、网页标题、URL 等，双击 URL 可以追踪访问该网站。

工作站	时间	网站	标题	URL
财务部1	2012-05-24 16:32:43	www.126.com	126网易免费邮--你的专业电子邮局	http://www.126.com/
财务部1	2012-05-24 16:33:56	qzone.qq.com	QQ空间-分享生活，留住感动	http://qzone.qq.com/
财务部1	2012-05-24 16:34:50	www.sohu.com	搜狐-中国最大的门户网站	http://www.sohu.com/

2.3.2 上网限制

限制终端电脑的上网行为，可以做到禁止所有上网行为、禁止浏览所有网页、禁止或只允许浏览指定网站。也可以通过端口限制来禁止某些程序不能访问网络。上网限制可以更好规范员工的上网行为，提高工作效率。

（以网页限制为例）

2.3.3 浏览观察、统计

可以实时观察终端电脑各个程序的流量收发情况，也可以查询和统计某终端、某部门或整个公司在某时间点、某时间段的流量使用情况。统计情况可以导出为文本文件供事后审计查询。

日期	时间点	工作站	分组	收发数据量	发送数据量	接收数据量
2012-05-24	11	财务部1	财务部	1,858 K	231 K	1,627 K
2012-05-24	14	财务部1	财务部	360 K	72 K	288 K

2.3.4 邮件监控

可以监控终端电脑的邮件收发记录，内容包括发送时间、收发地址、邮件标题、正文内容、附件内容等。

2.4 硬件设备限制

管理 USB 存储设备、光盘、软盘的使用：允许使用、禁止使用或只读；可以设置打印机白名单，或打印程序白名单，只能指定的打印机或程序才能打印，并记录打印内容。对 U 盘还可以进行注册认证，终端只能使用通过认证的 U 盘，外来 U 盘不能使用。

2.5 功能优势

2.5.1 加密、内外网管理一体化

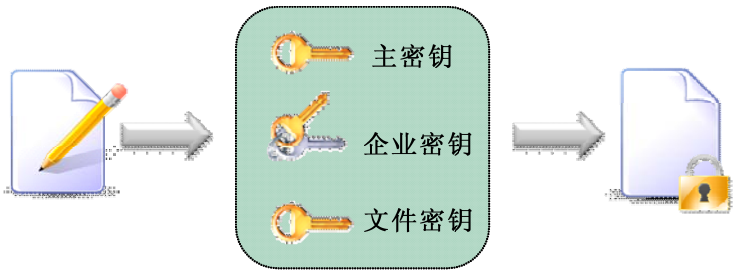
绿盾把文件加密、内网行为管理、外网行为管理一体化，在文件动态加解密

的同时，规范员工的操作行为，实时追踪终端电脑的操作行为，并可以把记录情况导出为日志报表供事后审计。

2.5.2 强大的三重密钥体系

绿盾采用独有的**三重密钥**管理，在安全上更有保障。

- **主密钥**：全球唯一，保证不能搭建出两套一样的加密环境，即保证任何两家使用绿盾的客户文件无法相互打开。
- **企业密钥**：企业自行设置，保证厂家获取到密文，也无法解密。目前其他加密软件都无法提供此功能。
- **文件密钥**：每个文件加密时会随机生成一个文件密钥，以提高加密的安全性。



2.5.3 灵活的用户认证

提供多种用户认证方式，满足不同应用需求：

- 用户名和密码登录
- 绑定电脑自动登录
- USBKEY 绑定登录
- 域结合登录

2.5.4 邮件白名单实现与 outlook、foxmail 结合

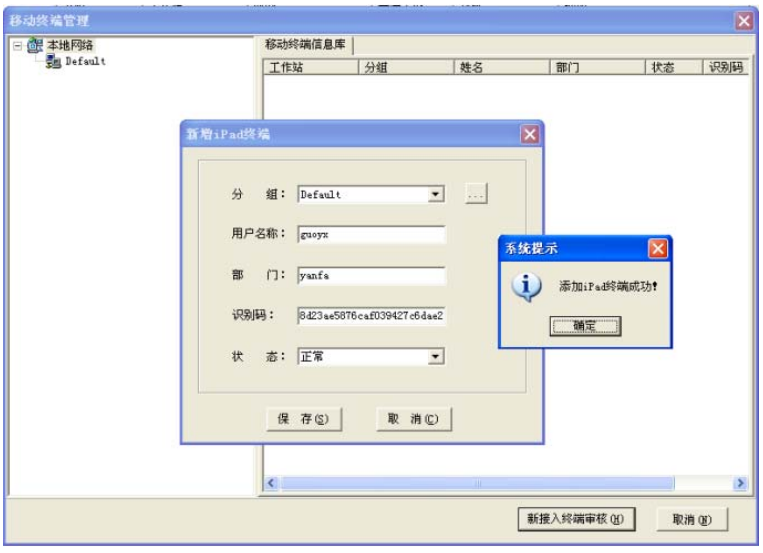
绿盾邮件白名单可以与 outlook、foxmail 结合，即通过 outlook、foxmail 发送邮件到邮件白名单地址，加密的邮件附件会自动解密，可极大地缓解审批压力，且不改变用户的操作习惯。

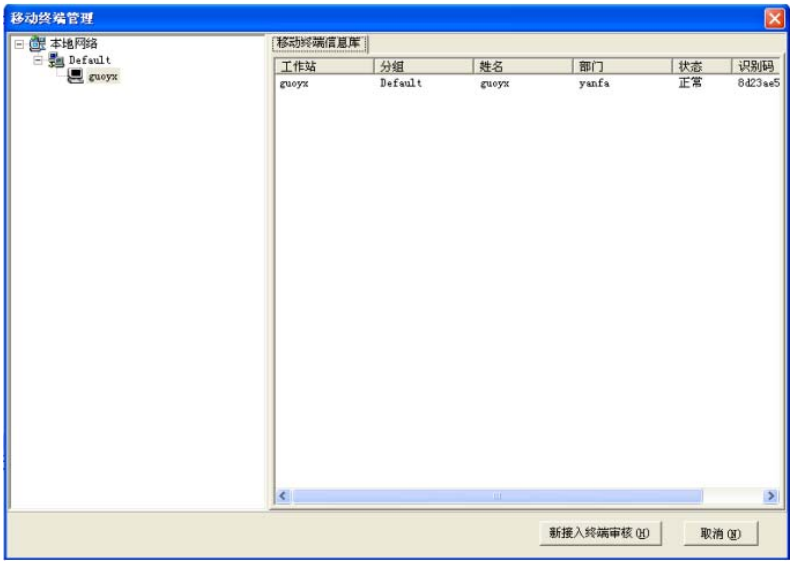
2.5.5 实用、灵活的审批流程

- 自定义多人多级审批（如：A/B 角色），可用性高；
- 流程审批即时消息提醒，提高了流程审批效率；
- 审批人员审批时需要输入合法口令，提高审批安全性；
- 审批可以在线查看或者下载文件内容；
- 支持 Web 审批方式，提高流程审批便捷性；
- 支持移动终端（如：iPad、iPhone、手机）流程审批；
- 支持审批人在线、离线、全部状态时自动审批；
- 可查询所有发起审批、待审批、已审批等信息。

2.5.6 支持 ipad、iphone

支持 iPad、iPhone 移动终端设备，实现在线阅读服务器上的加密文件，提高工作便捷。





2.6 技术优势

2.6.1 文件过滤驱动加密技术

绿盾采用 Windows 内核的文件过滤驱动实现透明加解密，对用户完全透明，用户打开文件、编辑文件和平常一样，甚至毫无感觉，不影响用户操作习惯。同时由于在文件读写的时候动态加解密，不产生临时文件，因此基本不影响速度。驱动层开发难度相对应用层要高。

2.6.2 自定义数据库

绿盾自主研发的数据库，存取速度快，兼容性好，安全稳定，同时降低企业投资成本。

- 为绿盾量身定做的数据库
- 存取速度极快
- 升级维护方便
- 数据库转移方便
- 数据库安全性高

2.6.3 严密的途径控制

严格控制各自可能导致泄密的途径：

- 控制打印机、光驱、软驱、U 盘
- 禁止屏幕截取（如 QQ 截屏、红蜻蜓截屏、屏幕录像工具等）
- 控制复制粘贴
- 禁止 OLE 插入
- 禁止 WPS 网盘
- 控制虚拟打印机

2.6.4 支持自定义可信进程

绿盾支持自定义添加受控程序，可以满足所有的应用程序加密，可以兼容 OA、ERP 等管理软件（C/S 架构、B/S 架构）。而其他大部分加密软件需要厂商二次开发完成。

2.6.5 安全容灾备份

可以根据需要，设置需要自动备份的文件类型，备份文件会自动上传到服务器进行保存，防止误操作或恶意删除带来的文件丢失。

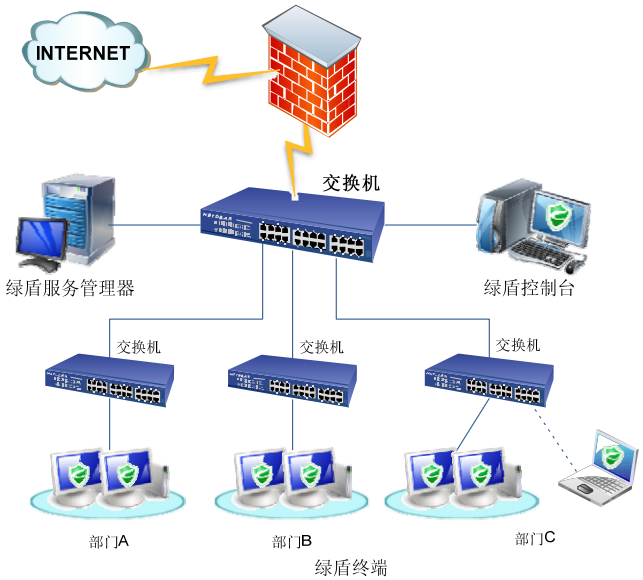
三．版本划分

根据不同客户的实际需求，绿盾按功能划分成以下三个版本：

绿盾版本	适用客户	用户上限	功能模块介绍
专业版	普通用户	2000	包含基础模块，像是文档加密、外发、打印、内外网、邮件白名单、U 盘认证等
行业增强版	行业用户	2000	在专业版的基础上，增加了服务器白名单、移动终端、工作模式、打印水印等
旗舰版	大型用户	无	在行业增强版的基础上，增加了服务器分布式部署、WEB 控制台和 WEB 审批等

四．系统组成

绿盾信息安全管理由绿盾服务管理器、绿盾控制台和绿盾终端三部分组成。



绿盾服务管理器：用于管理密钥、各种策略；用于存储系统的各项数据，如终端电脑的操作记录；处理来自于客户端的各项验证，等。

绿盾控制台：与绿盾服务管理器联接，对系统进行配置和管理。

绿盾终端：需要文件加密或需要监控的终端电脑。

五． 系统部署

5.1 服务器分布式部署

部署方式：公司总部与分公司部署一套绿盾；

管理效果：统一管理公司总部与分公司的所有人员，管理人员登录绿盾管理控制台能看到公司总部与分公司所有的终端用户。终端用户的权限管理，包括解密审批、外发审批和离线审批等各种审批流程都能在同一个控制台进行设置。同时，分公司的人员也可以交由公司总部的审批人员进行审批；

总结：统一管理公司总部与分公司的所有人员，支持同时查看公司总部与分公司的绿盾数据，分公司人员可以交由公司总部审批人员统一进行审批管理，分公司绿盾数据保存在分公司服务器上，无需实时上传到公司总部服务器上，数据交互受网络传输速度影响较大。

5.2 服务器单独式部署

部署方式：公司总部与分公司各自部署一套绿盾（各自的加密文件对方都能正常打开）；

管理效果：公司总部与分公司各自管理自己的绿盾，管理人员登录绿盾管理控制台只能看到各自的终端用户。终端用户的权限管理，包括解密审批、外发审批和离线审批等各种审批流程都只能设置自己公司相应的终端用户；

总结：不受网络传输速度影响，公司总部与分公司各自的加密文件依然可以互相打开使用，无法统一管理公司总部与分公司的所有人员，无法同时查看公司总部与分公司的绿盾数据，分公司需要自行设置审批人员进行审批管理。

六．关于天锐

6.1 企业简介

厦门天锐科技有限公司总部位于厦门珍珠湾软件园，是国家高新技术企业、双软认证企业。公司始终专注于研发具有自主核心技术和知识产权的软件产品，专业从事数据防泄密软件产品的研制、开发和销售。

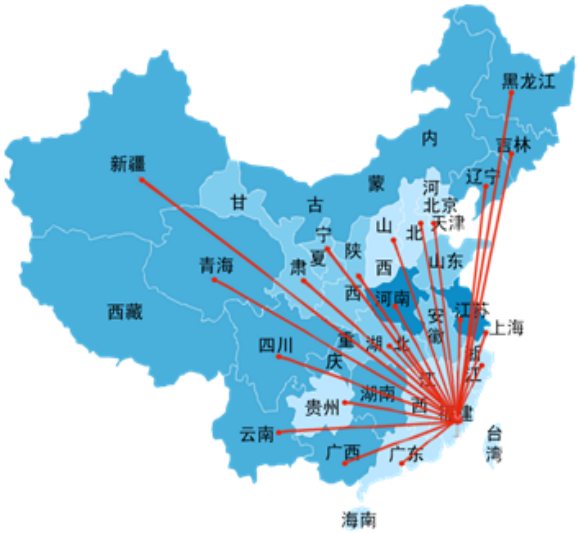
自公司成立伊始至今，公司始终倾力为企事业单位的信息安全、数据防泄密提供一体化顾问式解决方案，为客户提供优质的内网安全管理产品和适合多种行业的应用解决方案；提供专业的安全顾问咨询、教育培训和技术服务。通过为客户提供专业的安全产品和服务，多年来，用户遍及电力、电信、金融、烟草、政府、教育、企业等十几个行业，累计客户数量达数十万计。

公司秉持着“天道酬勤　锐利进取　研发创新　客户自上”的企业核心价值观，先后全国 50 多个城市成立办事处或技术服务点。多年来，通过为各类客户提供专业的安全产品和贴心的安全服务，公司实现“客户零投诉、实施零风险、服务快好稳”，市场占有率牢牢位居前列，领跑国内加密市场。

6.2 产品体系

6.3 分支机构

公司先后在全国50多个城市成立分公司、办事处和技术服务点，以安全可靠的产品及服务，领跑国内加密市场。



- 北京分公司
- 上海分公司
- 福州分公司
- 泉州分公司
- 宁波分公司
- 天津办事处
- 广州办事处
- 南京办事处
- 南宁办事处
- 郑州办事处
- 武汉办事处
- 沈阳办事处
- 温州办事处

……

……

6.4 产品资质

目前我司已有多个产品取得了著作权登记证书、软件产品登记证书、信息安全产品销售许可证，涉密产品认证证书、军工产品认证证书，并有多项专利。

6.5 部分典型用户