天锐绿盾加密软件

产品名称	天锐绿盾加密软件
公司名称	深圳市天宇勤信息技术有限公司
价格	面议
规格参数	品牌:天锐绿盾
公司地址	深圳市宝安区西乡街道固戍社区石街工业区3号楼中宝大厦508（注册地址）
联系电话	0755-29668261 18929328150

产品详情

【文件透明加密模块】

文件透明加密模块是防止电子文件由于单位内部员工泄露而开发的内核驱动层加密系统。在不影响员工对电脑任何正常操作的前提下，文件在复制、新建、修改时被系统强制自动加密。加密的文件只能在单位内部电脑上正常使用，一旦脱离内部网络环境，在外部电脑上使用是乱码或无法打开。文件只有被管理员解密之后，带出单位后才能正常使用。

支持类型：

word、excel、powerpoint、金山wps、写字板、autocad、pro/e、ug、solidworks、caxa、pretel dxp、开目cad、solidedge、cimatron、power mill、mentor、esprit2004、3dmax、犀牛、coreldraw、photoshop、illustrator、中望cad、浩辰cad、visual c++、delphi等等。

支持系统：windows xp\2000\2003\vista\windows7 \windows8

技术级别：内核级驱动层加密

驱动层加密工作在windows内核，随着windows开机而运行，在运行过程中不会被恶意停止。驱动层加解密动作都是在文件打开的时候动态解密，文件保存的时候自动加密，不产生临时文件，安全性更好，效率更高。

功能特点：

1. 动态全程加密

终端操作员在打开文件时，绿盾根据权限，自动解密；终端操作员在新建文件、编辑文件时，绿盾自动加密存储。保证存放在硬盘为密文，无需用户干预。这些加密过的文件，无论通过何种方式（邮件、网上邻居、u盘拷贝、聊天工具传输），泄漏出去的文件均无法打开。

2. 严格密钥管理

每个单位都会分配到唯一的主密钥，加密过的文件拿到同样装有绿盾的单位，由于密钥不同也无法打开。同时，单位也可以自行设置密钥，提高系统安全级别。

3. 文件无缝使用

在装有绿盾的单位电脑上打开加密文件，不需要输入密码即可直接打开，且在同一单位内部装有绿盾的电脑之间文件可以相互打开，做到文件的无缝使用以及单位员工间的无缝使用。

4. 文件解密管理

采取流程解密、手工解密、邮件解密三种方式灵活组合运用，满足不同单位的业务需求。流程解密类似于oa线上审批流程，由申请人发起申请，在指定审批人的审批通过后，文件自动解密。手工解密则是直接授权给终端对自己文件解密，简单方便，一般用于高级管理员。邮件解密则全部通过电子邮件完成，将文件作为邮件附件提交申请，管理员审核通过后，邮件发送时文件自动解密。同时所有解密的内容，包括申请人、审批人、时间、文件标题及内容等，都在服务器上自动记录，以备单位查询。

5. 客户端离线管理

即使出差或工作需要外带笔记本暂时离开单位环境，可通过离线授权及设定资料正常使用时间及自动销毁时间，而使重要数据一直处于加密状态，避免外出时有意或无意的传播。

6. 组、角色管理

可将用户分成若干组，并可在组里建立多级子组，做到自定义分组，并在组的基础上加以管理范围定义。可以根据组设置相应的管理员。同时在用户上又可以自定义角色。角色和组管理相结合，使得管理更系统化。

7. 文件远程备份

客户端在图纸文件保存时会产生文件副本远程同步备份到服务器，有效的避免硬盘损坏带来的文件毁灭性损坏，也有效的预防内部员工恶意删除。

8. 文件操作日志

客户端对文件复制、删除、改名等操作都会自动形成系统日志，供系统管理员查阅分析。

9. 禁止截屏操作

可以控制系统截屏、qq截屏等各种类型的截屏，防止利用截屏将文件部分外泄。

10. 文件权限控制

支持某一部门的文档只能在指定部门或指定范围内流通，禁止其他部门员工读取、使用该文档。

11. 远程在线升级

服务器升级后，通过服务器可以远程对客户端进行更新升级，便于系统维护。

12. 兼容性好

绿盾兼容了国内外近20种杀毒软件，包括诺顿、卡巴斯基（kaspersky）、mcafee、瑞星、江民、金山毒霸、360安全卫士、nod32、趋势等。

13. 一体化解决方案

绿盾从产品模块上分，除加密模块外，还包括屏幕监控模块、聊天内容监控模块、应用程序管理模块、arp防火墙、资产管理、文件加解密、邮件管控、上网行为管理等，为企事业单位提供完整全面的一体化信息安全解决方案。【文件外发控制】

因业务需要，企事业单位经常会碰到需将一些重要的电子文档发给客户或者合作伙伴的情况，可要将文件外发，就必须对原有的图纸加密，一旦解密发出去，就意味着单位的这些重要图纸文件将不再受到控制，这些图纸文件如果被窃取或者无序传播，可能会对单位造成巨大的损失，核心资料面临着被外泄的可能。

文件外发控制针对文件解密后在外部泄露的可能而提供对应解决方案，当需要外发单位内部文档时，只需进行外发申请后经单位高管审核确认即可明文外发，同时对外发文件还能设置打开的次数、使用有效期、是否在指定电脑上打开等，有效防止外发文档的二次扩散。

一、文件外发打印控制（自带浏览器）

通过虚拟打印机的方式，将图片、文本、图纸文件转换成类似pdf格式的绿盾专用图档文件。文本本身自带浏览器，把这个文件发给客户，客户不需要启动任何外部浏览器和程序，点击文件时就会启动自带的浏览器就可以阅读，文件内容不能拷贝、不能打印，只能阅读。

1. 可设置时间、使用次数、密码、网络同步验证、指定计算机多种参数。

2. 无论复制成多少个副本，多个副本的操作次数总和为当时设定的次数。

3. 网络时间同步验证，解决修改系统时间来达到篡改有效时间的问题。

二、文件外发控制（非浏览器方式）

与浏览器形式最大的区别是，不改变文件类型，只是将图纸文件经过外发系统特殊算法加密发给合作单位，比如dwg文件外发系统加密后，还是用cad软件打开dwg文件。只是合作单位在打开外发加密文件，必须启动外发系统客户端。外发系统并不影响外合作单位其机器上的自有文件，只对外发系统加密的文件完成加解密操作。合作单位可以在外发系统控制下，阅读及编辑等进一步操作。特别适用一些结构复杂的委外设计、委外加工的三维文件，也适合一些execl及acc文件外发阅读控制。

1. 可设置时间、使用次数、密码、网络同步验证、指定计算机多种参数。

2. 可设置打印权限、剪切版加密、屏幕截图功能限制。

3. 可适用于三维图纸及复杂文件外发控制，文件在外部可以继续编辑修改。

4. 无论复制成多少个副本，多个副本的操作次数总和为当时设定的次数。

5. 网络时间同步验证，解决修改系统时间来达到篡改有效时间的问题。

【移动终端管理模块】

为了便于移动办公，系统支持添加

、修改或删除移动终端信息（支持ipad、iphone及android系统的移动终端），用户可通过移动终端在线阅读加密文档，如查看oa系统上的加密文件或加密的邮件附件，在方便移动办公的同时，保护企事业单位数据安全。

【密级管理模块】

对于单位内部的机密文件，做到统一管理，分级负责。可根据实际工作需要，设置指定负责人的密级级别，从而限制机密文件的阅读权限。即：

某一级别的操作员所制作的文件，只有高于或等于该级别的人员才能够阅读。有效保障机密文件的安全性。

【服务器白名单】

企事业单位无需在内部应用系统上安装任何插件，事前通过数据防泄密系统统一配置，要求终端加密文件上传到指定服务器是明文，或者密文；单位内部的加密终端根据下发配置要求，系统会自动判断，如果要求明文存储，自动解密后上传，无需人工干预。

【离线管理】　针对所有员工笔记本办公，公司统一设定默认时间（如：72小时），在默认时间内，携带笔记本回家办公和公司内部一样的安全管理效果；对于员工出差时，可在线向上级申请，授予一个合理时间，携带笔记本出差办公，和在公司内部一样的安全管理效果；有些电脑需要长期脱离公司网络，或者无法连接网络的情况下也需要保护电脑上的文件，同时查看公司其他电脑上的加密文件，这时，可以选择在这类电脑上安装离线终端。