

密文卫士™ — 全面防范又简单易用的电子文档防泄密软件

上海谷巨软件有限公司

2007-9-6

摘要：保护企业电子文档需要防范各种泄密渠道，由于 Windows 系统的复杂性和功能的强大，许多防泄密软件只能防范部分泄密途径。对于用户来说，如果防泄密软件哪怕存在一个不能防范的漏洞，整个系统就是行同虚设。而要防范如此多的泄密途径，防泄密软件的开发难度可想而知。上海谷巨软件有限公司研发的密文卫士™软件，能够全面防范各种泄密途径，而且由于采用了简单的安全模型，整个系统非常简单易用，不需要配置复杂而又易出错的所谓策略。

关键词：电子文档防泄密软件 泄密途径 密文卫士

1 全面的防泄密软件

密文卫士™软件根据简单的安全模型，使用了透明实时加解密、虚拟磁盘、进程监控、防火墙、文件安全传输等技术，实现了全面防范而又简单易用的防泄密系统。

密文卫士™软件安全模型的创新之处就是提出了电脑的涉密态概念，即一个电脑即可以工作在普通的状态，也可以工作在涉密态。安全模型的基本概念就是：系统没有进入涉密态，涉密文件不可见；系统进入涉密态，只有信任进程可以访问涉密文件；同时非涉密磁盘不可以执行写操作。

对于 Windows 系统，泄密途径很多，根据泄密的主观意识，可以分为主动和被动泄密；根据泄密的物理介质，可以分为硬盘泄密、移动磁盘泄密、U 盘泄密、CD/DVD-RW 泄密、智能手机泄密、网络泄密等；根据泄密的技术手段，可以分为黑客工具、木马、病毒、网络侦听、宏脚本二次开发等。

对于这些泄密途径，依靠单一的技术手段是难于实现全面防范的。必须采用多种方式的防范技术，通过将这些防范技术有机地整合在一起，实现全面地防范。

密文卫士™软件的技术之一就是透明实时加解密。透明实时加解密的作用就是在保存时自动加密保存的内容，在读取时自动解密读取的内容。透明实时加解密实现了文件在保存时的加密，可以防止电脑丢失、被盗，以及其它复制到移动盘、U 盘、CD/DVD-RW 等移动介质时的泄密。但是透明实时加解密不能够防范网络侦听（指读取网络共享加密文件时）、宏脚本等泄密。

特别要注意的是，单一的透明实时加解密防泄密软件产品不能防止一个具有二次开发能力的应用程序的宏脚本泄密。

比如 Office Word，如果规定所有 Word 文件自动加解密，那么，一个具有基本脚本编写能力的人，可以写出一个不超过 100 行的宏，将需要的任意加密文件解密发送出去。原因在于，宏运行在 Word 的进程之内，防泄密软件很难判断读请求来自 Word 本身，还是来自宏。宏读取到的文件是自动解密的，然后它可以把它通过网络发送出去，由于没有写操作，发送的内容不会自动加密的。

密文卫士™软件使用了虚拟磁盘来保存在涉密态的数据，所有虚拟磁盘的读

写通过透明实时加解密驱动程序完成。由于在涉密态系统禁止普通磁盘的写操作，这个虚拟磁盘除了保存用户自己的工作文件外，所有临时文件都自动保存在虚拟磁盘内。谷巨软件计划在新版本的密文卫士™软件中，将页面交换文件也放在虚拟磁盘中，进一步提高系统的安全等级。

由于使用了唯一可写的虚拟磁盘，为系统带来了许多便利之处。如不需要禁止用户截屏键，截屏键对于一些用户来说是用频率很高，没有它会非常不方便。许多防泄密软件都禁止使用截屏键，而密文卫士™软件不需要禁止它的使用。原因很简单，通过截屏键复制下来的屏幕内容保存到哪里去呢？只能保存到虚拟磁盘，即涉密盘。

密文卫士™软件的进程监控功能监控进程的启动和磁盘操作。只有信任的进程才能启动，不信任的进程不能启动。在进行磁盘操作时，只有信任的进程才能访问虚拟磁盘。这样，可以防止一些木马、病毒的运行，无论它们是否是隐藏的进程，都可以被拦截。

密文卫士™软件的防火墙功能强大，不仅可以拦截出站连接，还可以拦截进站连接。拦截出站连接，就是为了防止自动发送泄密，或者通过信任进程的二次开发宏脚本发送泄密；拦截进站连接，是为了防止通过外部将数据复制出去。

密文卫士™软件的防火墙只允许通过自己本身的网络通讯。为方便沟通和交流，配备了专门的文件交换和聊天会议功能。

密文卫士™软件的文件交换和聊天会议通过一个类似于 SSL 的安全通讯协议来完成，可以防止通过网络侦听泄密。

下面这个表格是密文卫士™软件功能和防范的泄密途径一览表。

密文卫士™功能和防范泄密途径一览表

功能 \ 防范	被动泄密				主动泄密			
	电脑失窃	黑客	木马、病毒	网络侦听	写盘	智能手机	宏脚本	网络发送泄密
透明实时加解密	★	★	★		★	★		
虚拟磁盘	★	★	★		★	★		
进程监控		★	★		★	★		
防火墙		★	★		★	★	★	★
安全文件交换				★				
安全聊天会议				★				
公钥认证加密				★				

2 方便易用的防泄密软件

密文卫士™软件提供了全方位、多角度的防泄密保护。同时它又具有方便易用的特性。

首先，对于普通用户而言，密文卫士™软件不禁止任何 Windows 键盘操作，如截屏、拖放、复制粘贴等。

密文卫士™软件还可以随时退出涉密态，比如为客户发送一份漂亮的 Word 文档，用户可以退出密文卫士™来编辑发送。如果全程强制加密，这个几乎就不可能了，除非请求解密或者发送一个丑陋的 TXT 文档（恐怕也不行），这无论对于

普通用户还是管理员都不胜其烦。

使用密文卫士™软件的企业可能担心员工总是在涉密态外面编辑文件工作，然后复制一份到涉密态的加密磁盘去，这样自己就可以私自保留一份自己的工作成果了。对于这种忧虑，谷亘软件认为，个人的成果，即使使用全程强制加密，他也可以回家再写一份，只要他记忆力不会太差。

对于企业，真正重要的是集体创作的结晶，即全体员工反复修改创作的电子文档。只要是经过密文卫士™软件文件交换系统共同编辑的文件，员工是无法复制出去的。

由于能够随时退出密文卫士™软件，员工和管理人员不会增加额外的工作，也不会产生抵触的情绪。

其次，密文卫士™软件不需要管理员配置大量的策略，基本上是零策略，除了维护一个有限长度的信任进程的基线列表。

有些访泄密软件需要配置大量的策略，虽然可能提供了缺省的配置，但是也需要仔细地审查，大量的策略配置对于日益增长的企业规模和应用数量，会逐渐成为一种负担和漏洞来源。

密文卫士™软件将需要的配置都内置在系统内部，用户基本上可以即装即用，初始化和日常管理都非常方便。

3 结论

密文卫士™软件采用了透明实时加解密的虚拟磁盘技术，结合防火墙技术和其它技术的综合应用，把普通电脑打造一个涉密电脑。该涉密电脑使用方便，和使用普通电脑基本一样，还可以在两种状态之间随意切换，管理员也不需要配置大量繁琐枯燥易出错的策略，真正实现了方便易用。