

如您担心数据泄密请关注：窃取文件的途径和对策



1、网络工具传输

问题：通过 QQ、MSN、E-MAIL、网络 U 盘、BT、FTP 等各种网络工具向外发送文件，只要有网络，想用屏蔽软件或禁止端口根本无法解决文件通过网络传送的问题，除非在完全没有网络的环境里工作，但是没有网络的工作环境又给工作带来不便

解决方案：安装加密软件后：文件违规发送出去后，文件打开是乱码或者打不开，但不影响网络使用

2、图纸打印带走

问题：在企业里，图纸打印有时候是很随意的，员工可以趁老板或员工不在，有意打印一些关键资料，日积月累地带走

解决方案：安装加密软件后：可以禁止特定电脑对加密文件打印，对关键文件实行集中打印管理，同时可以监控打印的详细内容

3、偷走电脑主机

问题：对于直接盗取电脑主机，根据中国法律，电脑主机价值构成职务侵占罪立案条件，企业无法通过法律途径制裁员工，资料被盗损失却无法衡量

解决方案：安装加密软件后：被盗电脑开机后无法连接服务器验证，客户端自动关闭，所有文件无法打开

4、系统截图发送

问题：员工可以利用截图的方式把文件内容通过网络发送出去，例如 QQ 截图

解决方案：安装加密软件后：当打开加密过的文件，截图功能被屏蔽，无法从加密文件截图

5、移动存储复制

问题：U 盘，移动硬盘，手机存储卡等通过 USB 及串口接入的移动存储设备都很常见，也是最容易将重要文件整批复制走的工具、就算 usb 端口屏蔽也极易破解，采取限制 USN 端

口的方式既不方便，也不能解决员工用其他端口接入的问题

解决方案：安装加密软件后：文件复制出去后，打开是乱码或无法打开，但不影响硬件设备及端口使用

6、直接拆走硬盘

问题：在端口屏蔽，互联网切断的情况下，某些员工采取极端方式拆走硬盘，不辞而别的离职，这样能一次性带走所有资料

解决方案：安装加密软件后：软硬件联合加密，拆走的硬盘安装到其他电脑上，文件自动锁定无法打开

7、笔记本介入复制

问题：员工带私人笔记本电脑到公司，并接入公司内部网络，趁机复制走大量文件。此外公司笔记本外出办公时，员工可趁机批量复制走笔记本上文件

解决方案：安装加密软件后：私人笔记本电脑，就算复制走文件，也无法使用文件。公司笔记本，可设置脱离公司网络后，不能使用电脑上的加密文档，或脱离公司网络达到一定时间后无法使用电脑上的加密文档



国骏，为您创造一个无感知的防泄密环境！