绍兴终端防泄密软件推荐

生成日期：2025-10-26

目前，国内电脑文件保护软件、电脑文件防泄密软件很多，大都也可以实现较为有效的电脑文件安全管理。例如，有一款“大势至USB端口管理软件它不只可以完全禁用U盘、移动硬盘、手机存储卡等所有带有USB存储功能的设备，防止通过U盘、移动硬盘复制电脑文件的行为，而且还可以完全禁止电脑发邮件、禁止网盘上传电脑文件、禁止FTP上传电脑文件、禁止QQ发送文件等，从而完全杜绝了员工通过各种途径泄露电脑文件的行为。同时，软件基于强度高的自我保护和加密举措，使得员工无法察觉、无法卸载，大限度地保护了电脑文件的安全。防泄密软件的目标就是对于内部机密数据做到“只能用，不能带走”。绍兴终端防泄密软件推荐

防泄密软件主动加密技术采用的是一对一的直观思维，因此其支持的目标是以应用程序为单位的，而且一般和应用程序的版本还有关系，因为同一个应用程序未必能够支持不同版本的插件。也不是所有的应用程序都支持插件技术。事实上，能够支持插件的应用程序只限于Office□CAD等大型通用化应用软件，专门用软件和一般的小型软件都不支持非法插件。因此，这种技术应用环境受到诸多限制，而且由于从原理上不能保证受支持应用软件之外的软件的适用性，因此这种技术基本面临淘汰。绍兴终端防泄密软件推荐由于管理手段和物理手段保护电脑文件安全、防止数据泄密方面存在着较大的负面影响。

市场上防泄密软件（防泄密系统）鱼龙混杂、良莠不齐，作为单位用户怎样衡量防泄密系统的优劣呢？其实只要从几个方面考察就可以确定防泄密软件的质量：1）稳定性。稳定性是压倒一切的指标。如果没有稳定性，这种防泄密系统就是失败的产品。防泄密系统为了达到访问控制目的，实现得不好就会影响操作系统的稳定，质量差的防泄密系统造成程序崩溃、死机甚至蓝屏屡见不鲜。2）透明度。防泄密系统的透明度是指安装部署防泄密系统前后对于用户正常工作操作计算机的差别。好的防泄密系统通过实时加揭秘技术不改变任何使用方式和操作习惯。

文档加密的相关知识：文档加密可以监控和处理可能导致应用程序泄露的另存为、打印、复制和粘贴、发送电子邮件等操作。只有通过数据安全系统管理机，系统管理员才能揭秘和合法分发文件。此外，对文件的签发进行了严格的记录和审查。在文档加密的服务器端，数据安全系统服务器管理员可以监控管理机作为部门服务器的工作状态，实时配置管理机的功能授权，汇总审计操作日志管理，及时发现系统安全隐患。数据安全系统管理机管理员可以实时监控客户端计算机安全服务的工作状态，并在管理机上配置客户端计算机的功能授权，及时发现隐藏的文件安全风险。文档加密采用内核级透明加揭秘技术，对电子文档采用自动、强制、实时的加密策略，实现图文文档的安全保护。文件加密的出发点不是防止文件被取出；是为了确保任何人以任何方式复制的文件都经过加密和保护，未经授权不得使用。主动加密技术从原理上来说只要能够准确监控机密数据的流向就可以实现。

选择防泄密软件需要看哪些方面？1.注意授权管理和其企业的操控权。在主要数据的保护和处理过程之中，不只需要保证数据不被他人盗了造成损失，更需要保证企业拥有自主管理控制数据渠道的权利。因此用户在挑选专业放心的防泄密软件时，需要针对其本身系统管理员的管理能力进行对比，保证相关的主管人员能够根据自己的权限进行各种数据的整合处理，拥有本身对数据的操控权利并且能够自主的进行数据的管理，才能够让这种品质高的防泄密软件真正的为企业的业务执行做出铺垫。2.注意加密技术防范稳定性。据悉系统化的加密技术能够有效的提高其数据的安全度和防范能力等表现力，而具备更加专业的访问控制和其加密防护的技术等科学的操作体系，才能够让其本身的数据和相应的文件拥有防入侵的功能，因此用户在挑选可靠放心的防泄密软

件时，更需要拥有加密数据的管理能力同时提供良好的防范技术作为保障条件，才能够达成更好的防泄密效果和准确的数据管理能力等成果。对于网络、串口、并口、调制解调器、蓝牙、1394等通信端口和设备，在涉密系统中都有使用控制方式。绍兴终端防泄密软件推荐

在防泄密系统中，访问控制技术同样被大量使用。绍兴终端防泄密软件推荐

在防泄密技术中，定义成机密的数据是应该以加密形式存在的。这里不讨论完全基于访问控制形式保护数据的方案，基于访问控制的保护与真正的防泄密是完全不同的两个领域，防泄密必须解决安全环境失效的情况下的数据不泄密，访问控制是不考虑安全环境失效的情况的。在防泄密系统中，访问控制技术同样被大量使用，比如对涉密的对象的涉密访问控制、涉密计算机的同机虚拟隔离技术等。但防泄密技术的本质是数据加密，访问控制只是辅助的手段。良好的防泄密系统的安全架构不应该建立在访问控制的基础上。防泄密系统必须确保安全环境失效时的机密数据处于加密状态。绍兴终端防泄密软件推荐