7个步骤为你的USB存储设备保驾护航 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/142/2021_2022_7_E4_B8_AA_E6_AD_A5_E9_AA_A4_c101_142700.htm 现在像USB闪存这样的个人存储设备功能已经非常强大了，它们在各种各样的企业中开始普遍存在。这些设备本来是作为消费级应用的产品，因此普遍缺乏安全，控制以及辅助管理工具。很多雇员不假思索地用着他们从本地的办公用品中心买来的那些简陋的存储设备，把工作带回家或者带出工作场所。数以百万的人们带着个人存储设备，因此这些无辜的小工具就被用来扩大恶意攻击的影响力，以及其他非法企图比如从企业窃取信息等。 即使人们很谨慎地使用这些设备，存储在USB硬盘中的数据也没有被包含在公司的一些常规手续之内，比如备份，加密或者资产管理。那些公司如何能够追踪通过这些设备进出公司的数据呢？在这种情况下，保护公司数据的安全对任何公司的IT部门来说都是一个极大的挑战。 近期一些事件 近期业内的一些事件已经引起人们的关注，致使IT专家们认识到必须使用新的策略和技术来保护存储在个人存储设备中的信息了。 如下是发生在哪些把信息带回家的人身上的一些事情： 肯塔基大学的一位教授发现他的闪存被偷了，于是他以前的6500名学生的隐私信息就处在了危险之中。这些数据种包含学生的名字，年纪以及个人社会安全码，它们将导致数千人处在身份窃贼的威胁之中，更不用说他们那被侵犯的隐私了。 阿富汗Bagram城外的集市上，有人出售带有机密军事信息的闪存。美军这才意识到他们得保护USB硬盘的数据安全，找出能够跟踪这些设备的方法，并且确保重要信息不被

未经授权的员工访问。 安全提示 如果雇员将公司的信息存储在无保护的个人存储设备上，那么他们一出门就将公司置于风险之中。审计公司会面临账单信息泄漏的风险，而如果病人的信息落入坏人手里，医院就遭殃了，还有财务公司也需要确保机密数据不丢失。一旦公司数据落入坏人手中，毋容置疑公司将面临极大的风险与威胁。公司会失去信誉，卷入诉讼纠纷，以及致使雇员遭受身分信息被窃或者上当受骗等等一系列的麻烦。 个人存储设备的风险可以划分为如下几点：由于设备丢失或者被窃而导致的数据泄漏 未经许可的数据提取 引入恶意代码 企业关注USB设备的漏洞 市场上有数以百万种USB存储设备，机密的公司数据一直在此间流动同时面临丢失或被窃的风险。敏感的公司数据丢失所导致的潜在损失每天在呈几何级数倍的增长，这种情况使人们越来越强调采用针对移动存储设备的恰当安全措施的必要性。如下是跟移动存储设备相关的一些主要的安全问题： 数据泄漏为了使数据泄漏的风险最小化，企业应当限定员工只使用公司认可的USB设备。 规章制度所有组织都应当确保他们遵循了政府以及安全规章制度比如SOX, HIPAA, GLB, California SB 和FISMA以便降低数据丢失的可能性。首先，他们要做的是建立明确的安全策略，将该策略在员工中公布并且通过使用监听，追踪以及备份移动设备上的所有技术等手段来加强这些策略。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com