

## 笔记本安全--硬盘加密解决方案

移动办公具有很强的灵活性和方便性，被越来越多的企业所应用。笔记本电脑作为移动办公中最主要的工具，同时也是企业重要资料的载体，经常受到安全威胁。展会上、回家的路上、交通工具中，甚至是洗手间里，都有可能成为笔记本电脑丢失的场所。“电脑赔得起，但资料遗失赔不起！后果无法挽回！”，这是很多人的想法。如果笔记本中存储着技术资料、财务数据或和企业发展策略密切相关的信息，丢失的后果，轻则让你的工作从头再来，重则被竞争者利用，从而影响到企业的发展。

当然，对于存储着机密数据的笔记本电脑来说，即使没有丢失，也有可能面临着被人恶意窃取数据的危机，而数据窃取是可以通过各种工具去实现的，包括拆卸电脑上的硬盘并连接到其他系统作为辅助硬盘的手段。

如何确保笔记本硬盘资料的安全性，防止信息泄露，成为企业日益关注的问题。因为只有数据安全的基础上，移动办公才能发挥更高的效率。

利用硬盘加密解决方案可保护笔记本电脑、工作站和服务器等设备的硬盘上的所有文件(包括操作系统的文件)的安全。即使硬盘被盗，您依然可放心数据不会被非授权人浏览或获取。

### 硬盘加密技术简介

硬盘加密产品主要提供用户硬盘加密、启动前认证两项功能。

#### 硬盘加密

对笔记本硬盘进行加密保护，可以降低信息被非授权者所利用的风险。硬盘加密采用业界公认的加密算法（例如 AES 256 位长度密钥），对硬盘进行高强度保护。目前的这种保护强度，不会被攻破。在没有经过授权的情况下，硬盘会处于加密保护状态，即使将其连接到其他系统也无法读取或存储硬盘数据，唯一处理的方式就是将硬盘格式化。采用硬盘加密技术的笔记本电脑，其硬盘上的所有数据被保护起来，大大降低机密数据泄露的风险。

#### 启动前认证

启动前认证功能是为了防止非授权者入侵操作系统存取机密数据。比如：用户可以使用软驱启动盘来进入Windows DOS命令提示字符窗口来复制硬盘中的系统文件。在用户启动电脑后，使用LC3 (LOphtCrack)等工具可以快速地获得Windows® NT和2000的密码。移除笔记本电脑的电池则可以轻易地破解BIOS等级的授权。

只有采用双因素身份认证的方式，才能达到高强度的安全保护。身份认证可以通过智能卡，一次性口令，或者是USB令牌的方式进行，具有更高的可靠性。当然，启动前的授权方式必须是可定制的。用户可以选择使用密码或令牌做为授权的方式。真正好的硬盘加密技术，并不是要通过多繁琐的加密步骤来困扰用户，而是为硬盘本身提供应有的保护。

用户每天都要登录系统，因此以不影响用户使用的前提下，简单的操作，高强度的保护，才能为用户提供一个安全、便利的环境。

## 硬盘加密和效能

安全固然重要，但必须要实用且不会对企业造成负面的影响，能够达到信息的稳私性。

硬盘加密的效果经常被提出来讨论，因为大多数人一致认为硬盘加密会大量降低系统执行的速度。这种说法的确值得检视一番，因为硬盘加密对于硬盘 I/O 和 CPU 的使用量会产生潜在性的影响。解决方法为，在硬盘加密时，通过分段硬盘加密技术，将硬盘加密对公司营运的影响降到最低，达到高安全且快速的加密效能。可靠的硬盘加密，须具备业界广泛认可硬盘加密的算法，支持 AES 256 位长度的密钥，也需支持其它算法(例如 TDES 和 IDEA)。

一般来说，硬盘加密产品需必备以下功能：

### 用户密钥文件

硬盘加密产品都需要一个密钥来加密硬盘中的数据，密钥的管理是一个重要的方面。SafeNet 的 ProtectDrive 产品中，提供了一个方便密钥管理的“syskey.bin”文件。在 ProtectDrive 安装时需要此文件。在对硬盘进行加密时，此文件将被用做加密硬盘的密钥文件的种子。若没有此文件，将无法移除 ProtectDrive、无法针对被加密的硬盘做解密，也不能处理密码复原的动作。这样把 Syskey.bin 交给管理员管理，解决了密钥管理的问题。

### 常用操作

SafeNet 的 ProtectDrive 有多种用户常用操作，可用来部署 ProtectDrive，其中大部分的操作方式根据用户的自身需要而设计。

常用操作：

- 将所有数据文件存放在「同一」个硬盘(例如：<D:>)并对此硬盘进行加密。系统硬盘则不进行加密。
- 将 syskey.bin 文件备份到外部磁盘装置(例如软盘)并妥善保存。不要将 syskey.bin 存放在 C:\(默认值)。如果未将硬盘中的 syskey.bin 备份，当硬盘毁损时，即使用户拥有 PD 备份文件也无法回复硬盘信息。
- 定期执行备份并妥善保存备份档。

### Windows 单点登录

硬盘加密产品需要为用户提供方便的系统登录方式，可以降低因为用户的网上冲浪，社会交际和写下密码而将密码泄露给未经授权使用者的风险。

使用串口、打印口及磁盘驱动器阻挡其它辅助装置拷贝未经授权的数据。专业用户可以通过辅助端口(例如串口和并口)及计算机系统的软盘驱动器拷贝信息。大多数的公司通常采用活动目录(Active directory)的功能强制禁止使用辅助装置。您可以在硬件加密方案提供的活动目录管理接口中，设定全域策略来限制所有用户使用二级存储设备。本地用户将无法修改域安全设定，这样就达到通过禁止使用二级存储设备来保护本机的机密信息的目的。

当有他人尝试存取时，就会显示登录警。显示登录警告可以提高用户的警觉性。如果发现可疑的登录，用户可以将旧密码更改为较安全的新密码或将此情况通告管理人员。当然，用户也必须随时提高警觉。通过定期对用户进行培训，可以增加用户对信息安全领域的知识。

### 备份和恢复

硬盘加密产品通常都提供数据备份和恢复的工具。当硬盘加密信息变更时，此产品将立即进行系统备份。当系统不稳时，可以使用由数据表文件组成的备份文件来恢复硬盘。

### 密码遗失

密码管理通常为 IT 的头号敌人。研究指出大部份密码管理的时间都花在如忘记密码等密码复原的问题上。以 SafeNet ProtectDrive 来看，它提供挑战一响应(Challenge-response)的机制进行密码恢复。用户必须按下功能键来产生一个 13 个字符的挑战码。和拥有用户 syskey.bin 档的管理人员联络并告知此挑战码，管理人员就可以为用户产生一个响应。在“响应”字段中输入此响应，用户就可以通过屏幕中的启动前登录。当用户登录系统后便可更改密码。

### 服务器端部署

硬盘加密方案需提供网络和客户端部署的服务器工具，此功能适用于大规模的硬盘加密安装部署。

### 总结

随着移动办公工作者数量与日俱增，笔记本电脑内的数据安全防护成为 IT 的重要任务。既要追求办公速率，又要保证信息在传递中的安全性，所以必须有适当的安全防护工具来保护信息本身。