KINGSTON IRONKEY™

软件加密 与 硬件加密

托管

通过与计算机上的其他程序共享计算机资源且对数据进行加密– 安全性与您的计算机完全一样。

使用安置在加密闪存盘上的**专用处理器。**

密码

将**用户密码**作为对数据进行干扰的加密密钥。

处理器包含一个**随机生成器**，可生成通过用户密码解锁的加密密钥。

更新

可能需要进行软件更新。

从主机系统进行**卸载加密**，从而可提高性能。

解密

由于使用易于获取的在线工具**对暴力攻击的保护不力**，软件加密很容易受到黑客攻击。

确保**加密硬件**中的密钥和关键参数的安全。

身份验证

身份验证使用**主机系统资源。**

身份验证在**硬件加密的硬盘上进行。**

保护

容易遭受攻击，安全性与主机系统一样。

预防最常见的攻击，如冷启动攻击、恶意代码、暴力破解攻击。

安装

操作系统**兼容性可能不同。**

不需要在主机 PC 上安装任何类型的软件。

灵活

可以在**所有类型的介质**上执行加密。

加密**与特定设备绑定**，因此始终处于加密状态。

成本

在**小型应用**环境中具有较高的成本效益。

在**大中型应用**环境中具有较高的成本效益，容易扩展。

咨询专家

规划合适的解决方案时需要了解项目的安全目标。
聆听 Kingston 专家的指导，以最有效的方式保护敏感数据。

www.kingston.com

#KingstonIsWithYou #KingstonIronKey