KINGSTON IRONKEY™

硬件与软件加密对比

了解主要差异以及更适合您需求的方案。

在数据安全的持久战中，硬件加密和软件加密的区别，归根结底在于安全存在于何处，以及在实际使用中暴露程度如何。在 U 盘和固态硬盘中，加密的内置位置决定了数据保护的安全程度，以及它对周围系统的依赖有多大。

硬件	与	软件
加密密钥管理 加密密钥由硬件内部生成，并安全存储在硬盘中。		**加密密钥管理** 用户密码直接用作加密密钥，密钥可能驻留在系统内存中。
暴力攻击防护 专为抵御暴力破解而设计：通过限制尝试次数，在达到上限后自动擦除硬盘数据，防止设备丢失或被盗时敏感信息泄露。		**暴力攻击防护** 容易遭受暴力破解攻击，计算机会尽力限制解密尝试的次数，但黑客可能会进入计算机内存并重置尝试计数器
软件或驱动程序要求 主机系统无需安装驱动程序或软件。		**软件或驱动程序要求** 需要安装软件和驱动程序，且操作系统兼容性可能各有不同。
加密资源 使用硬盘内置的专用加密处理器。		**加密资源** 依赖主机的 CPU 和系统资源来加密和解密数据。
主机系统依赖/暴露风险 安全性隔离在设备内部，即使连接到不可信或已感染的计算机，数据依然受到保护。		**主机系统依赖/暴露风险** 安全性依赖主机操作系统，若计算机感染恶意软件，则更容易遭到攻击。
加密状态 加密始终处于开启状态，无法移除或绕过。		**加密状态** 加密可能被启用、禁用或配置不当。
性能影响 性能影响极小，加密由硬件处理器承担。		**性能影响** 可能对性能产生负面影响，因为加密会占用CPU 资源。
灵活性 加密与特定 U 盘或固态硬盘绑定。		**灵活性** 几乎可在任何存储介质上实现

软件加密灵活多变，硬件加密则将安全隔离在设备内部，降低系统级风险的暴露。了解两者各自的数据保护和访问控制机制，有助于根据自身工作流程和风险承受能力，选择合适的安全方案。

www.kingston.com/ironkey