kingston.com/encryptedsecurity

金士顿 / Ironkey 加密 USB 相比 BitLocker 的优势

MICROSOFT 的 BITLOCKER	金士顿 / IRONKEY 加密 USB 设备
产品特色	金士顿优势
1. 操作系统之间的有限兼容性： - 仅支持企业版和旗舰版 Windows 7 | 专业版和企业版 Windows 8.1 | Windows 10 - 不支持 Mac 操作系统 **2. 操作系统补丁/系统更新的问题** - 有错误的更新 - 修复的延迟 **3. 易受“ROCA”攻击** - BitLocker 中的加密缺陷 - “比 KRACK 更糟”- Google 和 Microsoft 遭受 存在 5 年的巨大旧加密漏洞的打击	**1. 操作系统之间的更佳兼容性：** - Windows® 10 | Windows 8.1 | Windows 8 | Windows 7 (SP1) | Mac OS X v. 10.10.x - 10.13.x | Linux Kernel v. 2.6 **2. 未受“ROCA”攻击影响**
1. 软件加密 - 在主机电脑上运行 **2. 易受漏洞攻击** - 可能受到键盘记录、探查、内存/哈希攻击	**1. 硬件加密** - 完全独立的保护 **2. 不受软件漏洞攻击** - 消除探查和内存哈希攻击 **3. 数字签名的固件** - 无法被修改 **4. 物理保护层** - 环氧树脂浸渍/填充的外壳可防止访问物理内存
1. 易受暴力攻击	**1. 10 次暴力攻击尝试防护** - 清理闪存盘或停用它 **2. 在 USB 闪存盘丢失或失窃时，防止任何人获取您的敏感数据**
1. 需要大量 MIS / IT 管理员	**1. 极少的 MIS 工作量 - 易于部署**
1. 使用较旧的 USB 技术标准 - 256 位 AES、CBC（以往标准） - 符合 FIPS 标准（未认证） ***注意：在较旧的 Windows 上无法访问利用 XTS-AES 加密的驱动器。可移动驱动器应继续使用 AES-CBC 128 位或 AES-CBC 256 位算法。***	**1. 金士顿采用最新的技术标准** - 256 位 AES、XTS（最高标准） - FIPS 197 和 140-2 Level 3 “认证” - 符合欧盟 GDPR 法规 - 符合 NYDFS - 23 NYCRR 500 法规 - 符合 TAA 标准

总的来说，金士顿 / IronKey 加密 USB 闪存盘被证明是为便携数据保护解决方案提供可靠性、兼容性和安全性的最佳解决方案。
它们100% 符合各种法规和标准 | 支持端点安全性，满足 DLP 需求 | 无需软件 / 驱动程序 | 专为快速、高效的部署设计。