软件加密与法规遵从：
应对重大安全风险的更实惠解决方案

监管与合规要求

数据安全过去仅用来监管 IT 部门，但由于持续不断的消费者数据泄露，世界各地的政府对企业施加了越来越多的要求，以加密和保护所有个人身份数据。

从医疗保健领域的 HIPAA，到欧洲、中东和非洲地区的 GDPR 和美国加州的 CCPA，法规强制要求对受保护的数据类型进行加密。过去 3 年多以来，由于这些法规及其相关罚款和法律赔偿风险大幅提升，合规组织数量出现了指数级增长。

面对这些变化，IT 部门正在艰难应对安全与风险相关成本。在整个新冠疫情期间，预算往往被用于硬件和防火墙投资，而减少了对数据加密的关注。

事实上，使用 Microsoft BitLocker® 或来自 Symantec、McAfee 等公司的端点管理软件的软件加密正在不断增加。一些企业和消费者还利用部分供应商提供的带“保险库”软件的标准 USB 闪存盘。

加密与传输中的数据

员工与消费者存在随身携带数据的需求。他们可以选择多个方案，例如使用：

1. 云服务：出色的方案，可从任何接入互联网的设备上访问。不过，灵活性需要付出代价。云中数据存储方案令用户或公司失去了对数据的控制权，并且存在潜在风险。我们曾见过过云服务器未锁定或门户大开的情况。
2. 标准 USB 闪存盘：携带 USB 闪存盘看起来更加安全，不过，闪存盘丢失所造成的数据泄露风险可能非常大。例如，丢失包含机密信息的 USB 闪存盘或洗衣房抽屉装满遗失的 USB 闪存盘的新闻比比皆是。
3. 硬件加密 USB 闪存盘：这类 USB 闪存盘采用自定义架构，配备板载加密控制器和访问控制。通常采用最强大的 XTS 模式 AES-256 位加密对数据进行加密，还可能配备其他保护举措来防范物理攻击和固件攻击。这类闪存盘由专精安全设备的公司制造，虽然价格比标准 USB 闪存盘贵，但提供更高的数据安全性。FIPS 197 或 FIPS 140-2 Level 3 闪存盘提供更高防护级别，让用户高枕无忧。
4. 带有软件加密的标准 USB 闪存盘：为了实现法规要求的安全性，可以使用采用 BitLocker 或其他工具的软件加密方案。这属于相当不错的方案，成本相对较低，还能提供同样的 AES-256 XTS 加密。

不难看到，在多数情况下，企业和行业倾向于选择第四个方案，即配备软件加密的标准 USB 闪存盘，主要因为 BitLocker 或其他数据保险库等软件加密是“免费”的。

软件加密不符合法规要求

对于企业安全专业人士而言，软件加密提供的加密功能与更昂贵的硬件加密 USB 闪存盘完全一样。但确实如此吗？捉襟见肘的预算促使企业采用软件加密以满足合规要求，而未注意到软件加密的黑暗面。

软件加密 USB 闪存盘存在什么问题？静态数据和传输中的数据难道未经 AES-256 XTS 加密？通常情况下如此。问题在于：软件加密被视为“可移除加密”。

等一下，可移除？这是否意味着软件加密 USB 闪存盘的加密可被用户停用？

答案是肯定的。用户可移除 USB 闪存盘的软件加密功能。您可能会问，他们为什么这样做？这是不仅因为他们能这么做，还因为他们希望不输入密码就能访问文件，或者他们只是忘记了密码，但需要使用 USB 闪存盘。

如何移除加密 USB 闪存盘的软件加密

对于不希望输入复杂密码或其他密码即可访问数据的用户而言，流程其实非常简单：

1. 将软件加密闪存盘插入计算机
2. 格式化闪存盘
3. 闪存盘格式化后，所有加密都会移除。
4. 将包含机密信息的文件复制到闪存盘，即可轻松访问

用户可以在无限制的计算机上轻松完成此操作。IT 部门可能禁止在公司计算机上使用格式化命令，但这可以在不属于公司的任何其他计算机上完成。

从合规角度看，轻松移除数据加密意味着公司提供的闪存盘现在未经加密，尽管一旦通过上述方法移除加密，闪存盘中的加密数据就会被视为永久丢失（加密密钥与数据绑定）。一旦加密被移除，复制到设备中的任何数据会被视为不安全，并可能不合规，从而可能导致违反 HIPAA、GDPR、CCPA 等相关法规。

非加密闪存盘丢失的后果

如果公司分配的 USB 闪存盘丢失或无法找到，即便公司一开始没有发现，但之后也会通过社交媒体了解到，公司可能不得不遵守特别的合规要求，这可能要求他们：

1. 实施法庭调查以确定丢失了什么数据
2. 咨询法务人员，确定是否存在违法行为
3. 确定是否必须告知客户

这种情况下，丢失一个 USB 闪存盘可能造成代价高昂的损失。每小时的法律费用超过数百美元，整个合规流程可能产生成千上万美元的费用，此外还存在潜在罚款、客户诉讼和其他诉讼，以及数据泄露带来的尴尬处境。

如果是出于低成本实现了软件加密采购，则没有考虑到上述风险及其巨大的财务后果。

在公司网络中使用非加密 USB 闪存盘，还有一个危险。这通常被称作“BadUSB”。BadUSB 是一种恶意软件类型，不法分子会利用 BadUSB 通过 USB 存储设备突破公司的防火墙，并向公司的网络防御系统引入恶意软件。

BadUSB

当 USB 闪存盘插入计算机中时，计算机的芯片组控制器会开始通过固件与 USB 闪存盘握手。在 Microsoft/macOS/Linux 等操作系统注意到 USB 闪存盘已插入之前，这种交换就已发生。每个 USB 闪存盘都有一个固件会在闪存盘插入 USB 端口时运行。

不法分子发现，通过将 USB 闪存盘中运行的固件替换为存在恶意的其他固件，可以利用这种握手机制引入恶意软件，其中的恶意固件会在目标计算机系统与 USB 闪存盘通信时向系统注入恶意软件。标准 USB 闪存盘中由控制器执行的内部固件不具备安全性，因此，BadUSB 天生就是用来渗透防火墙和突破网络防御措施的 USB 闪存盘武器。

多数公司试图禁止在他们的系统中使用 USB 闪存盘，甚至向 USB 端口注入环氧树脂。不过，他们发现各级员工需要使用 USB 设备随身携带数据。例如，高管人员希望随身携带数据开展工作或提供给无法访问公司云的外部法律或财务顾问公司；承包商需要数据开展工作，但无法访问公司数据库；财务分析师急需完成月度报告，需要在家中处理电子表格。

上述分析表明，使用标准 USB 闪存盘和软件加密解决方案存在重大风险。一开始看起来成本较低的方案最终可能害处巨大、代价高昂。仅仅两三个小时向律师咨询潜在数据泄露的费用，就会抹除使用这种低成本解决方案带来的节省。

硬件加密 USB 闪存盘是实现法规遵从的最佳方案

什么使硬件加密 USB 闪存盘成为这些合规应用的最佳方案：

1. 硬件加密的 USB 闪存盘的加密功能始终处于启用状态：用户无法关闭加密、重置密码规则（最小长度、复杂性），也无法停用自动密码重试。软件加密不会阻止通过软件词典攻击实现的重复密码猜测行为，而硬件版本则会限制密码重试，并在密码输错 10 次或更少次数时锁定数据。这在超级计算机时代提供了非常高的安全性。
2. 硬件加密闪存盘使用高级加密控制器并融入了多种安全特性：我们不会始终披露全部安全应对举措，但可以谈谈其中一个防范 BadUSB 的应对举措。在工厂，当固件仅在硬件加密闪存盘上加载时，固件会经过数字签名并加载。这意味着，当这些加密 USB 闪存盘插入计算机时，加密控制器首先会通过数字签名检查固件的完整性，并且仅在通过验证后才会加载固件。任何替换固件的尝试都会导致闪存盘变砖，闪存盘将无法运行，因而不存在威胁。
3. 硬件加密 USB 闪存盘可以包含针对具体公司的定制产品 ID (PID)。这些高级闪存盘可以包含一个编入的数字标识符，因此，如果闪存盘插入公司的内部或外部防火墙，闪存盘会被识别为公司发放的闪存盘。例如，如果员工丢失了公司闪存盘并在零售店购买了相同型号，新购买的闪存盘将无法通过公司网络的验证。这种定制为 USB 闪存盘应用增添了一层安全防护。
4. 硬件加密闪存盘可以迅速实现成本节省：单单减少和消除风险一项就能让回报周期大幅缩短。

金士顿是世界最大的加密 USB 闪存盘制造商，提供具备不同功能和价位的闪存盘系列。直接联系金士顿，商谈我们可以如何帮助您让高管、员工、承包商等各方通过使用加密 USB 闪存盘解决方案保持合规。