
Kingston
TECHNOLOGY
为什么 USB
闪存盘在今天
仍有存在意义?
#KingstonIsWithYou

为什么 USB 闪存盘在今天仍有存在意义?

前言与目录

在当今的数字时代，全球 60% 的企业数据存储在云中[1]，探讨已经存在近三十年的一项存储技术的存在意义，可能看起来有点奇怪。不过，自问世以来，这种主要存储产品在不断发展，直到今天仍未止步。

USB 闪存盘仅用作连接文件、闪存盘和应用的标准途径的日子一去不复返。今天的解决方案不仅具备大幅提升的传输速度，还提供许多情境必备的可靠、安全的便携式介质。但是，云存储解决方案似乎可以提供众多相同优势，USB 如何仍有存在意义呢?

在本电子书中，我们将探讨 USB 闪存盘在云主导的世界里所处的地位。我们将分享一些行业一流专家的真知灼见，并探索今天的组织如何使用 USB 闪存盘，并探讨它们在软件定义加密、独立存储环境和端点数据安全性领域的地位。

为什么 USB 闪存盘在今天仍有存在意义?

撰稿人

本电子书是与三位 IT 和新兴技术领域的行业专家一同撰写的。

Rafael Bloom

Rafael 在他的职业生涯中担任技术产品、营销沟通和业务发展相关高级职位。他的顾问工作重点关注技术和法规变更在组织、产品和沟通方面带来的新挑战。这项高度多样化的工作涉及多个领域的学科专业知识，包括通过设计实现信息治理与合规、数据隐私，以及广告技术、移动与 5G、人工智能和机器学习等新兴技术。

Tomasz Surdyk

Tomasz 拥有超过 24 年的政府部门 IT 安全经验，是信息安全、个人数据和网络安全领域的领军人物。过去，他曾负责检验用于处理政府部门机密信息和个人数据的 ICT 系统和网络。他还通过了北约和欧盟的安全调查。多年来，他还拥有一家公司，专注于实施安全解决方案来提高商业信息和个人数据的安全性。

David Clarke

在汤森路透“英国风险管理、合规和监管科技领域最具影响力的 30 位社交媒体思想领袖和思想家”中，David 获评为排名前 10 的影响家，并被金士顿科技评选为全球专家 50 强。David 之前曾在多家全球富时 100 指数公司担任各种安全管理职务，例如全球安全服务交付主管和安全基础设施主管。

USB 闪存盘的兴起

二十多年前，第一款通用串行总线 (USB) 闪存盘问世，它的整体兼容性成为计算机技术领域的游戏规则改变者。得益于能够向大众广泛普及多设备操作特性，USB 闪存盘获得了迅速发展，实现了大幅提升的数据传输速度、USB 3.0 接口和更强大的功能，远远超越了 2000 年推出的首款 USB 闪存盘。

自此之后，技术在移动数据存储和安全性需求方面取得了长足发展。重点在于最新一代的 USB 闪存盘，它在设计时考虑了非常具体的用途。从企业角度看，日益增加的远程办公和混合型办公、云服务的应用以及网络安全问题推动着市场对更有效解决方案的需求。与此同时，法规要求规定数据需要以合规方式进行存储。可能在“组织内部”和云中运行的分布式系统和复杂系统常常令这种局面雪上加霜。

此外，结构化数据以及文档、电子邮件、照片、视频和元数据等非结构化数据规模不断扩大，这都导致不断演变的企业存储需求越来越复杂。

但是，如果云存储可以应对许多此类挑战，那么 USB 闪存盘在今天的商业环境中有什么存在意义呢？

> 许多人认为 USB 闪存盘已经过时或无足轻重，因为它们在过去基本上被视为一次性、低性能、低安全性设备。- Rafael Bloom

满足不断变化的需求的便携式存储

USB 闪存盘用作便携式存储器的旧模式已经淡出舞台，而为个人安全本地备份使用高性能 USB 闪存盘开始兴起，可提供一层额外的数据保护和机密性。这可能对于与合规密切相关的数据非常重要，例如人力资源记录、金融数据、医疗保健记录、保护知识产权 (IP) 和所有个人可识别信息 (PII)。此外，这一代设备还具备更快的数据传输速度、存储、备份和安全性功能，可用于：

- 需要亲手交付的法规信息
- 需要在现场和异地交付并打印的法律文件和金融文件
- 可能有勒索软件威胁的任何存在潜在恶意的环境
- 转移到被禁止访问网络的打印系统

领先的加密 USB 设备提供商金士顿科技紧跟不断演变的需求，发布了金士顿 IronKey™ S1000 等解决方案。这款一流的加密 USB 闪存盘可满足最严格的标准要求，提供 XTS-AES 256 位加密以及具备强大防篡改功能的独立加密芯片，能够保护机密数据。此外，它通过 FIPS 140-2 Level 3 认证。这意味着美国政府正式验证了它作为加密硬件的有效性，因而它非常适合那些在数据保护方面需要额外安全性的组织。

无论数据在云中，还是在组织内部，这类硬件加密 USB 闪存盘都能提供集中式安全设备管理解决方案。无需软件即可轻松使用的合规加密数据存储还可释放宝贵的 IT 时间，带来可快速、高效部署的解决方案。

满足不断变化的需求的便携式存储

USB 闪存盘还可应用于备份和归档，用于长期保护数字资产，无需第三方云服务。不可否认，大量数据传输可在云中得到轻松处理，但专有 IP 可能仍然非常敏感，值得存储在安全的加密 USB 闪存盘中，这可以避开互联网并保证安全性。

在一些情况下，总是有组织需要在逻辑上和物理上控制数据，尤其是在使用加密闪存盘时。有时候机械硬盘/固态硬盘存储无法加密。利用金士顿 IronKey D300S 等外置加密 USB 闪存盘，就可以解决这个问题。这款 USB 闪存盘采用 XTS 256 位高级加密标准 (AES) 硬件加密，这种类型的块加密可以加密 128 位的数据块。当需要更高级的加密时，AES 会使用 XTS 块加密模式，提供比之前模式更好、更强的数据保护。

> 在我看来，USB 闪存盘仍在使用中，是数据安全不可或缺的组成部分。它们被用于各种用途，包括：在设备之间快速转移信息，以及提供合适的存储和保护。
>
> - Tomasz Surdyk

加密：基于硬件与基于软件

了解数据的加密方式后，可以说，相比软件加密，硬件加密更易于管理，也更加安全。这是因为加密流程与主机系统其余部分隔离开，使得截获或破解的难度大增。集中式设备级管理支持通过内部网 LAN 和互联网连接控制闪存盘，非常适合：

- 制定和强制执行个人和/或群组加密 USB 使用政策
- 审计文件活动以在数据进出组织时更好地追踪数据
- 为关键的数据传输提供远程内容备份
- 在 USB 丢失或被入侵时远程停用设备
- 在忘记密码时执行远程密码重置

当以这种方式正确管理授权的闪存盘时，就可以最大限度降低敏感数据被复制和分享的风险。此外，现代的硬件加密 USB 闪存盘提供大量额外的安全特性，有助于阻止目标接收方以外的任何人访问或读取文件和消息。

> 我认为硬件加密优于软件加密。硬件加密和软件加密两种方法在防范暴力破解攻击方面的能力差异巨大。硬件加密设备不容易被此类攻击攻破。
>
> - Tomasz Surdyk

加密：基于硬件与基于软件

企业可能会出于成本考虑而选择软件定义加密，但这可能有点短视。基于软件的解决方案与其他程序共享主机设备的资源，因此，安全性最多与计算机相当，并且常常要求进行软件更新，否则容易遭受攻击。软件加密 USB 闪存盘容易被无限制的暴力破解攻击猜出密码，并且没有任何方法阻止基于软件的词典攻击，这种攻击能在短时间内测试数百万个字符组合。

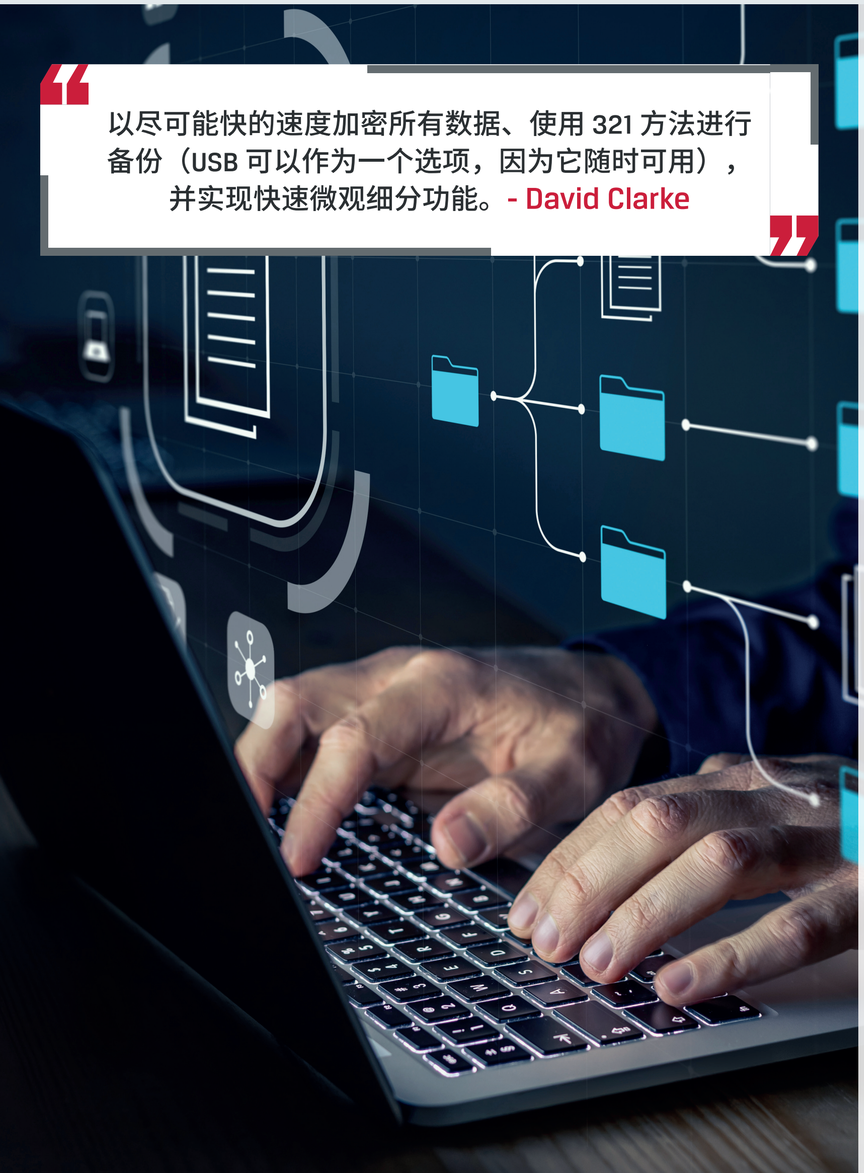
此外，软件加密还是可移除加密。任何拥有软件加密闪存盘的员工都可以复制走数据、格式化 USB 闪存盘，从而移除加密。他们然后可以复制回数据文件并使用闪存盘，而不必在不同平台和操作系统上进行麻烦的身份验证。

如前文所述，利用硬件加密，物理加密和后续数据存储的操作独立于主机系统。如果系统遭到入侵，这可以提供一层额外的防御。

这点无法被忽视，尤其是对于金融、医疗保健和政府等行业的人士而言。这是因为美国《健康保险携带和责任法案》(HIPAA) 和《支付卡行业数据安全性标准》(PCI DSS) 等法规常常对敏感信息加密制定了严格要求。

通过使用强大的硬件加密设备遵从这些法规，将最终有助于组织避免代价高昂的罚款、诉讼和潜在的声誉损害。硬件加密闪存盘可能比更廉价的大宗商品 USB 闪存盘价格高，不过，泄露产生的诉讼成本高昂，几小时的法律咨询费用就可以轻松购买数以百计的闪存盘。

保护敏感数据的需求日益扩大



> 以尽可能快的速度加密所有数据、使用 321 方法进行备份（USB 可以作为一个选项，因为它随时可用），并实现快速微观细分功能。- David Clarke

在保护敏感数据以避免丢失或失窃问题上，各个组织都有义务确保他们的设备拥有充足的安全性特性。此外还应考虑，面对众多不断演变的网络威胁，数字成熟度和用户个人端点数据管理技能若未得到应对，仍会是突出的风险因素。无论是数据控制或 USB 存储设备丢失等内部威胁，还是在安全环境之外进行数据传输、使用非加密 USB 闪存盘以及共享密码，都可能是用户尽责调查缺失的结果。合适的训练、培训和正确的 USB 闪存盘解决方案可以避免所有这些问题。

> 组织应清楚地了解自己的数据，包括所有数据集的重要性和/或敏感度水平，并制定计划优先处理最重要的数据，包括从物理上移除连接或让数据源下线。关键在于能够迅速隔离受感染的系统，并且制定您已执行的记录在案的计划绝对至关重要。- Rafael Bloom

预先规划和熟悉的沟通结构也是应对潜在威胁的关键因素。当今的网络威胁旨在针对组织的弱点。

最好在需求实际出现之前制定加密 USB 闪存盘计划，将加密 USB 闪存盘和政策融入组织的整体安全性战略。如果未制定加密 USB 闪存盘计划和相应指南，那么您将缺少构建基础，您的组织会在各个层级面临风险，包括未能遵从法规，例如欧盟《一般数据保护条例》(GDPR)，其中第 32 条明确规定敏感数据需要加密。

> 用户处理敏感数据。丢失敏感数据会让公司担负更多责任，并大幅影响公司的形象与安全性。为了保护敏感数据，应运用各种安全性解决方案，包括数据加密。- Tomasz Surdyk

保护敏感的金融数据

除了安全影响，还存在数据存储和备份解决方案必须遵从的合规标准。一些实践在垂直市场司空见惯，例如管理并执行数据保留计划的需求，而另一些实践被对待的方式截然不同，例如企业数据迁移到云中的操作。

在金融服务等许多垂直市场，各种法规已经生效，使合适的数据管理成为强制性规定。一开始银行尤其对使用第三方存储和备份高度谨慎，许多银行仍然坚持保留自己的全部数据基础架构。

金融机构还必须遵从日益增长的数据安全性法规和标准，例如美国《萨班斯・奥克斯利法案》(SOX) 和欧盟《一般数据保护条例》(GDPR)。不过，随着移动办公员工和承包商数量的增长，数据泄露和未遵从此类法律和标准要求的风险增加。

事实上，如果移动办公员工未能保护他们的数字身份、便携工作空间、他们携带的客户记录和金融数据，合规工作很容易遭受挫折。这就是为什么更多组织转向使用金士顿 IronKey 加密 USB 闪存盘来保护数字身份和应用，而无论员工将它们带到何处。

> 考虑到向更加分散的 IT 环境转变的整体趋势和云基础架构的强大可扩展性，很容易看到多数行业和大部分中小型企业不再操心如何管理冰冷的机房。
> - Rafael Bloom

安全访问患者健康数据

在医疗保健业，数据安全也比以往任何时候都重要。患者信息失窃的风险越来越大，2021 年就有 4567 万条患者记录遭到泄露，为 2015 年以来最多的一年[2]。在数据存储和备份方面，患者数据是关键、全面的医疗信息，可让医疗保健提供商安全地治疗患者。

这可能包括从患者电子健康记录 (EHR)（包括健康历史记录、测试、照片和射线影像文件）到行政文件（包括工资记录、患者保险和应付款项）在内的各种文件。面对日益增长的移动办公员工和经历重大动荡和转型的全球医疗保健市场，今天的医疗保健供应商对数据安全性感到担忧就不足为奇了。

> “特别是勒索软件在某种意义上形成一个日益壮大的行业，各个处理敏感数据的组织都必须考虑如何在极端胁迫下运营业务。- Rafael Bloom”

此外，如果未能预测风险并满足严格的法规要求，例如美国《健康保险携带和责任法案》(HIPAA) 或《卫生信息技术促进经济和临床健康法案》(HITECH)，都可能导致代价高昂的医疗保健数据泄露，这可能会进一步动摇患者、合作伙伴或监管机构的信心。

利用金士顿 IronKey 系列加密 USB 闪存盘等解决方案，医疗保健组织可以利用单个控制台，对少数或数以千计的闪存盘制定密码、应用程序使用、恢复等方面的政策用户友好的解决方案让员工无需安装驱动程序或其他软件即可安全地存取他们存储的数据，从而可以帮助移动办公员工和一线员工服务更多患者。用户和管理员可以轻松快速锁定数据，而无论数据在哪里。

未来云存储世界中的 USB 闪存盘

> 云数据存储代表了现在和未来。我仍然认为，使用加密 USB 闪存盘等产品在物理上保护数据仍是最安全的方案。用户无法完全控制云中的操作。不过，我们可以控制我们在加密 USB 闪存盘中保护和存储的数据。除了我们，没有人可以存取这些介质。
> - Tomasz Surdyk

现在，我们清楚了 USB 闪存盘的优势，那么它们在未来的云存储世界中究竟扮演什么角色？

十年前，USB 闪存盘是便捷存储和转移数据的主要工具，需求巨大。不过，在全新混合型工作模式和日益分散的团队的影响下，云现在支持从众多设备快速、简单地存取已存储的信息。得益于在文件传输方面的独特便利性，闪存盘曾经非常受欢迎。今天，云存储服务提供更高的文件便携性。

尽管如此，云存储仍然存在许多局限性。网络连接必不可少，这不仅决定了文件备份或转移的方式和时间，还带来了额外的安全顾虑。公司可以强制使用云，但不一定能够控制从哪里访问数据。因此，使用个人或公共 Wi-Fi 连接访问 VPN 的简单行为就会带来黑客攻击风险。此外，云服务对于不法分子极具吸引力，现在多数恶意软件 (61%) 是通过云应用传播的[3]。

> 我们可能最好要考虑云不可用时会发生什么、数据必须 100% 可用的情形，以及长期存储可能形成漏洞的情形。- David Clarke

未来云存储世界中的 USB 闪存盘

另一方面，USB 闪存盘加密可以通过设备的硬件或通过软件完成。以硬件为中心、无需软件的加密是防范网络攻击最有效的方法。这是一款不复杂的优秀数据泄露防范解决方案，可凭借极高的数据保护安全性满足严格的合规标准要求，帮助组织充满信心地应对威胁并降低风险。

硬件加密 USB 闪存盘属于自足式设备，无需主机计算机上的软件。由于不存在软件漏洞，这消除了暴力破解、嗅探和内存哈希攻击的可能性。软件加密 USB 闪存盘还面临的另一个风险是，任何用户都可以通过在任何计算机上格式化闪存盘来停用加密，并使用闪存盘以不受保护的方式存储敏感数据。

硬件加密 USB 闪存盘还提供卓越的物理方式来确保数据安全。它们允许由用户或管理员建立信息存取标准，并可与现有的本地端点解决方案相集成。在云存储无法工作或云存储不是有效解决方案的众多情形中，这使它们成为具有成本效益的便捷解决方案。这可能是数据需要存储在未联网的设备中、数据需要保持私有，或数据需要在离线时进行存取。

> 如果我们根据每天数据对组织的效用水平将数据分为“热”数据或“冷”数据，那么，如果业务连续性和高性能对于组织或对于特定的业务关键型职能或流程更为重要，更高效的做法可能是将“冷”数据放在云中，并为“热”数据更多使用本地 USB 存储设备，
>
> - Rafael Bloom

总结

我们无法预测未来出现的创新，但我们可以提供屡获殊荣的 USB 闪存盘产品组合，针对各个层级的移动数据保护要求提供一系列充满活力的加密解决方案。从通过自带数字键盘提供易用 PIN 保护的 USB 闪存盘，到可实现最高级加密的 FIPS 140-2-Level 3 认证以及防篡改保护，再到不影响安全性的 SuperSpeed USB 3.1 技术，金士顿 IronKey 产品可应对您的数据挑战，带来强大、有效的数据转移和移动数据存储解决方案。

我们设立专门的专家团队，在您的数据存储历程的每一步为您提供支持，帮助您找到可满足需求的合适存储解决方案。

我们具备相应的技能和技术能力，可帮助您确保机密信息的安全并遵从新法规，而无论您是寻求制定加密 USB 闪存盘计划、为您的企业寻找最合适的 USB 闪存盘，还是制定并实施安全性策略。通过提供高度个性化的服务，我们致力于提供合适的产品，支持您的数据存储优先级，并让您可以紧跟前所未有的商业世界变革步伐。

关于金士顿

凭借 35 年的丰富经验，金士顿积累了发现和应对移动数据挑战的知识，让您的员工可以安全、轻松地办公，同时不会让您的组织陷入危险之中。

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou