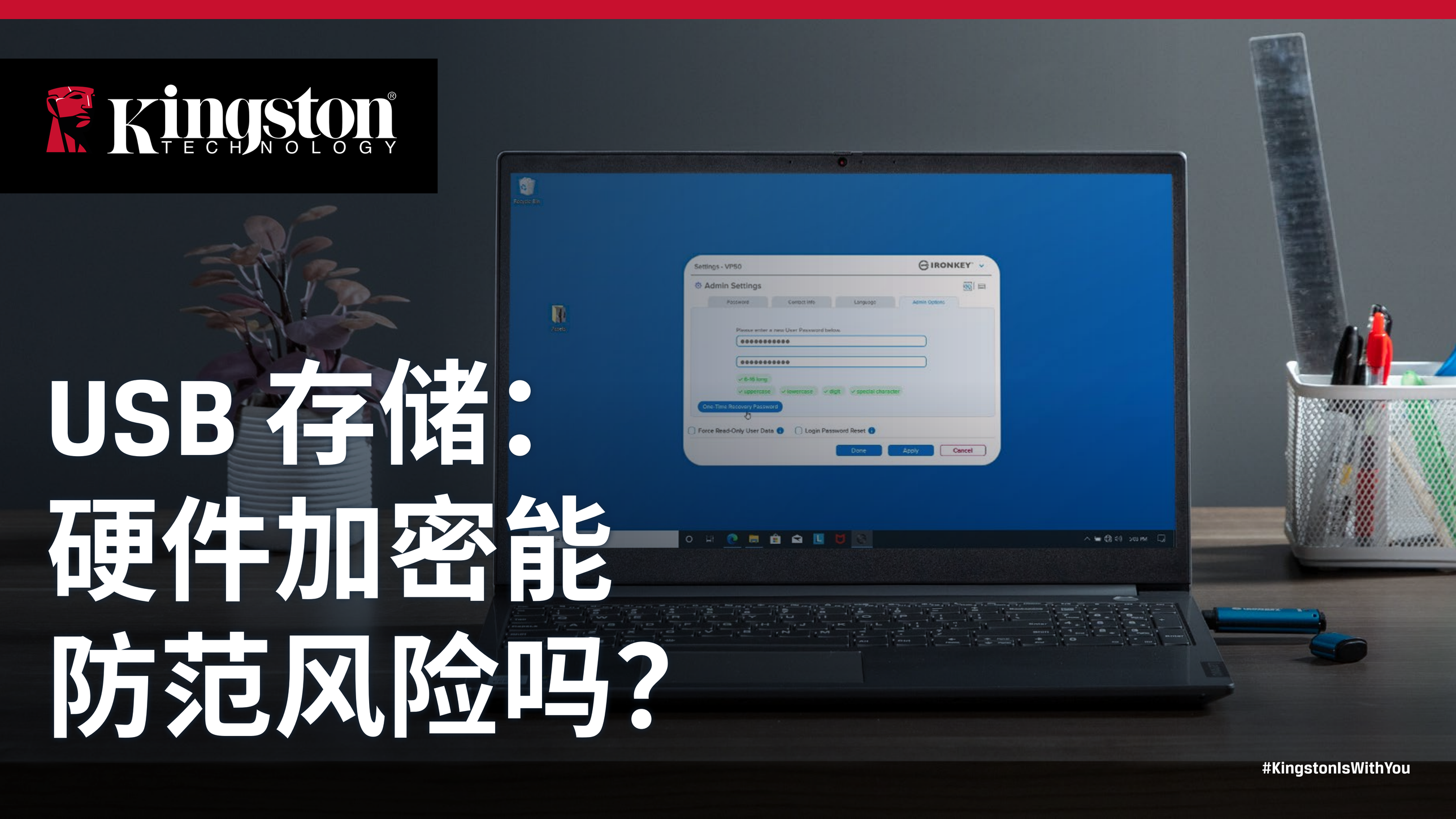
Kingston
TECHNOLOGY
USB 存储：
硬件加密能
防范风险吗？
Settings - VP50
IRONKEY
Admin Settings
Password
Contact Info
Language
Admin Options
Please enter a new User Password below.
6-16 long
uppercase
lowercase
digit
special character
One-Time Recovery Password
Force Read-Only User Data
Login Password Reset
Done
Apply
Cancel
#KingstonIsWithYou

USB 存储：硬件加密能防范风险吗?

前言与目录

网络安全比以往更受关注，但太多的企业对网络安全威胁不甚了解并且准备不足。据 UpCity 调查，在美国，只有 50% 的企业制定了网络安全计划；其中又有 32% 在新冠疫情开始后未再更新其网络安全计划，这表明许多组织正在迁移到远程或混合工作模式。而网络攻击频率却在不断攀升 - 在全球，遭受勒索软件攻击的企业数量从 2020 年的 37% 增长到 2021 年的 66%[1]。

网络安全威胁可能给企业带来灾难性的影响 - 除了金钱损失、数据丢失、安全之外，企业声誉在短期和长期也会受到不利影响。

网络安全威胁的一个共同传播因子是 USB 闪存盘。由于使用方便 - 插入电脑就可以用，USB 闪存盘在很多企业普遍存在。但很准确地说，这种简便性也让 USB 闪存盘很容易遭受攻击：只要放错位置或被盗，就可能被恶意攻击者获取敏感数据。这正是加密起重要作用的地方，它可以确保 USB 闪存盘的安全使用，减少个人和企业的任何相关风险。本电子书解答了以下重要问题：

- 为什么加密的 USB 闪存盘对于防范网络攻击至关重要?
- 企业哪些地方容易遭受攻击?
- 他们可以如何保护自己?

目录	页码

USB 存储：硬件加密能防范风险吗？

撰稿人

本电子书由 IT 和新兴技术的行业领军人物与我们的技术专家联合制作。

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。

Pasi Siukonen

Pasi 负责领导一支专家团队，在金士顿产品方面为人力资源、营销、现场销售、技术支持和客户服务等金士顿部门提供支持。他关注的主要产品是闪存和固态硬盘产品线。

商品与加密 USB 闪存盘之间的差异

商品（未加密）USB 闪存盘的访问和使用极为简便，硬件加密可以增加几层安全性 - 物理和数字 - 大大提升 USB 存储的安全性。商品未加密 USB 闪存盘容易获取、成本低且携带方便，对用户而言非常方便，但对旨在窃取敏感数据、在公司网络中引入恶意软件或勒索软件等的恶意攻击者同样非常方便。由于 USB 的使用非常频繁，因此遭受网络攻击的机率很高。与商品 USB 闪存盘相关的风险主要有两种：

- **勒索软件攻击：**这些基于 USB 的攻击包括在公司网络中引入恶意软件，掌握公司信息和/或通过加密系统进行勒索。用以攻击的工具通常是 BadUSB，现已成为最主要的恶意软件。
- **窃取数据：**恶意攻击者只要获得未采取适当安全保护措施的丢失、被盗或无人监管的 USB 闪存盘，就很容易获取 USB 闪存盘上存储的数据 - 无论是客户信息、源代码还是敏感的财务和业绩数据。

BadUSB 是一种攻击，可以利用固件无保护的 USB 闪存盘的弱点，然后使用恶意软件进行编程。这些恶意工具随处常见，网络罪犯很容易获取，但大众对这些工具的认识仍然不足，因此攻击很容易得逞，只需要将商品 USB 闪存盘的固件更换为破解的固件，然后 USB 闪存盘就可以伪装成键盘，主要运行脚本来攻击防火墙。因为很多网络攻击是由怀有或没有恶意的无戒备心内部人员执行的，所以企业使用加密的 USB 闪存盘极为重要，它会利用有保护的数字签名固件来防范这些攻击，从而降低网络罪犯成功的机率。

> **与管理 USB 的成本相比，重建基础架构或支付勒索及其他敲诈的成本高得多。 - David Clarke**

为什么使用加密的 USB?

加密的 USB 闪存盘特别设计为保护其中包含的数据，以及 USB 闪存盘可能连接的任何设备中的数据，让它们变成任何企业 IT 资源中的重要工具。网络安全威胁变得越来越高级，因此加密的 USB 闪存盘的功能也要升级，保持领先于利用这些设备的网络罪犯。在 Kingston IronKey™ 硬件加密产品系列中，多年来开发并不断添加了很多强大的功能，比如最强 XTS 模式下的 AES 256 位加密、耐用的防篡改外壳、数字签名的固件、虚拟键盘、复杂密码或密码短语模式等，可确保用户有力地防范所有方式的攻击。

由于对网络风险知之甚少，尽管商品 USB 闪存盘有着各种各样的漏洞，很多企业还是会选择使用。闪存盘也一样，容易获取，成本低，缺乏公司审批流程，因此，软件加密的使用在其中扮演着重要角色。关于遵守各种 IT 和网络安全标准，例如 ISO27001、GDPR、SOC2 和 WISP 政府最佳实践，通常没有企业级的最佳实践政策或流程。这意味着风险的评估依据往往是人们的看法，而非证据，这导致很多企业留下容易被攻击的漏洞。

虽然有些企业可能结合使用商品 USB 闪存盘与现有的软件加密工具，但经常得不偿失，因为任何人从互联网上免费或付费获取相关工具就能破解很多软件加密的 USB 闪存盘。用户使用简单的格式化也可以方便地删除 USB 闪存盘的软件加密，或者在不支持的操作系统平台上使用 USB 闪存盘。虽然硬件加密的 USB 具有无法关闭的始终加密功能，但它们是专用的；构建为防篡改、防破坏并使用数字签名的固件，以确保 USB 闪存盘的真实性和完整性。限制密码尝试次数（暴力攻击保护）和虚拟键盘（防范按键记录和屏幕记录）是加密 USB 闪存盘（如 IronKey VP50）的另外两项功能，它们遵守行业最佳实践，防止恶意攻击者从毫无戒心的用户提取密码。

> 如果 IronKey USB 闪存盘检测到固件已被篡改，将会加固 USB 闪存盘，并且不会启动，从而增强网络安全性。- Pasi Siukonen

谁面临风险?

实际上，任何无法控制其 USB 的公司都存在风险 - 他们往往不知道准确的风险是什么。但有些因素让某些公司对网络罪犯更具吸引力，也更容易成为网络攻击的目标。

对于医疗保健和金融行业的公司，它们的数据不仅对网络罪犯更具吸引力，而且一旦泄露，对公司及其客户的影响更严重。在英国，2017 年针对英国国家医疗服务系统 (NHS) 的网络攻击导致 19,000 多个预约被取消，NHS 因输出丢失而造成的成本达 9200 万英镑，此外还有恢复数据和系统的费用。这不仅让受感染的病人无法获得医疗保健，而且 NHS 因未能迅速响应之前的网络威胁警告或采取相应的行动而受到严厉批评。所有企业都应及时了解网络安全的最新动态，处理敏感信息 ，涉及特殊类别数据的企业则更应加倍警惕网络风险。

公司的价值（按营业额衡量）越高，恶意攻击者可能获得的回报就越大，因此这些公司面临的网络威胁也越大。但这并不意味着小公司不需要关注网络安全；大企业虽然是更有吸引力的攻击目标，但它们通常也有解决网络威胁的资源和专门人员。另一方面，许多中小企业没有专门的网络安全团队，而且高管在 USB 管理之外，因此一旦受到攻击，特别容易出现灾难性的后果。有些研究表明，中小企业实际上更容易成为网络攻击的目标。

身处高级管理职位的员工面临的风险更大；这些人容易被跟踪，而且通常在企业中有管理权限，网络管控 - 如 USB 管理程序 - 不适用他们，因此会成为网络罪犯容易获得战果的攻击目标。使用始终有硬件加密的 USB 闪存盘，深入了解网络安全，并遵循最佳实践和程序，对减少风险和防范攻击大有帮助。

> 在最近的网络安全事件中，很多恶意攻击者专门利用了内部人员有意或无意的帮助。
> - David Clarke

谁面临风险?

> 企业在对抗网络安全威胁时做得不够。
> - David Clarke

供应链是企业的另一个潜在弱点，供应链攻击也司空见惯。2013 年，美国零售企业 Target 遭遇了零售史上最大的一次数据泄露事件，泄露了逾 4 千万客户的借记卡和信用卡信息。虽然 Target 本身非常关注网络安全，在遇到攻击之前刚刚安装了一套全面的网络安全系统，但攻击者渗透了 Target 的一家第三方供应商，通过他们进入了 Target 的主要数据网络。最终，Target 接到了 90 宗法律诉讼，公司因此次数据泄露损失了 6100 万美元；虽然他们对攻击没有直接责任，但其供应链网络安全的这一弱点足以造成经济和声誉上的损害。

员工权变措施也可能成为弱点之源。这些权变措施可帮助员工提高其日常工作的效率，但他们往往会忽略基本的安全流程和最佳实践，例如密码管理。虽然 NCSC 和 CISA 的指导非常直接明了，但在实践中通常难以实施，特别是不熟悉 IT 和网络安全的团队成员。部署一支专门的网络安全团队肯定有用，但为员工提供合适的工具 - 例如硬件加密 USB 闪存盘 - 也对减少员工权变措施造成的风险大有帮助。

> 今天的硬件加密 USB 闪存盘容易采用和集成现有的网络安全策略：从各种接口（图形化、键盘、触摸屏）到广泛的操作系统支持，还具备满足所有企业需求的容量。- Pasi Siukonen

企业如何减少网络攻击的风险?

从企业的立场来看，保护端点和数据安全有大有可为。如果没有 GRC（治理、风险、合规），网络安全的失败不可避免，因此熟悉并遵循流程对企业保护自己特别重要。安装强大的端点安全软件也可抵御很多网络威胁，任何安全漏洞的修补都要尽快。

> 对于风险管理，是否采用强制加密策略与是否选择备份数据同样重要，甚至更重要。
> - Pasi Siukonen

但在个人层面，加密的硬件可以大幅减少面对网络安全威胁的漏洞。随着远程和混合工作方式的兴起和持续，特别是结合过去一年网络攻击更多的现实情况，确保企业每个层级的员工安全地处理、传输和读取公司数据变得比以往更加重要。硬件加密的 USB 可让用户享受闪存盘的便携性和简便性，同时也可极大地减少其相关风险；而放错位置或被盗的商品 USB 闪存盘可能意味着数据、金钱、声誉等的损失，硬件加密的 USB 闪存盘设计为保护敏感数据，防范广泛的各种攻击。随着网络罪犯开发出新的攻击方法，加密的 USB 闪存盘也在不断发展，应对新的挑战。

最终，处理网络攻击的成本可能是巨大的。确实，在企业层级采用加密的 USB 闪存盘可能涉及更多的审批和设置，但长期看来，也可为公司节省大量成本 - 包括勒索费用以及因声誉受损而失去的收入。仅仅数据泄露带来的法律成本这一项，就能轻松抵消硬件加密 USB 闪存盘所增加的成本。

> Kingston 长期致力于提供出色的加密 USB 解决方案，其产品组合可让任何企业满足其网络安全配置，即提供行业标准强制的硬件加密、符合端点策略的设计、设备管理能力。
> - Pasi Siukonen

总结

Kingston 一直致力于网络安全领域的发展，确保我们的 IronKey 加密 USB 闪存盘跟上最新的要求，满足大型和小型企业的网络安全需求。随着网络安全越来越成为全球关注的焦点，我们相信，如果有合适的工具和知识供他们使用，企业可以全副武装地应对面前的这些挑战，保护他们自己、他们的员工和客户。

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。

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021