
Kingston
TECHNOLOGY
Why are
USB drives still
relevant today?
#KingstonIsWithYou

# Why are USB drives still relevant today?

## Foreword and contents

In today's digital era where 60% of all global corporate data is stored in the cloud[1], discussing the relevance of a storage technology approaching thirty years of age may seem a little odd. However, since its introduction, this storage staple has evolved and continues to do so.

Long gone are the days where USB drives were simply a standard means of connecting files, drives, and applications. Today's solutions not only boast vastly improved transfer speed, but they also provide reliable and secure portable media that are mandatory in many situations. But how are USB drives still relevant, when cloud storage solutions can seemingly offer many of the same benefits?

Within this eBook we'll discuss where USB flash drives belong amidst a cloud-dominated landscape. Supported by key insights from some of the leading industry experts, we'll explore how today's organisations are using USB drives and debate their place amongst software-based encryption, independent storage environments, and endpoint data security.

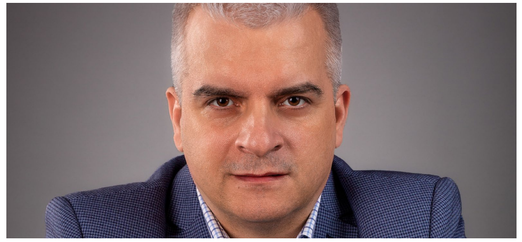


## Contributors

This eBook has been created with three industry experts in IT and emerging technologies.

### Rafael Bloom

Rafael has spent his career within senior Technology Product, Marketing Communications and Business Development roles. His advisory practice focuses on the new organisational, product and communications challenges of technological and regulatory changes. This highly diverse work involves subject matter expertise on information governance and compliance by design, data privacy and emerging technologies such as AdTech, Mobile & 5G, AI and Machine Learning.



### Tomasz Surdyk

With over 24 years of experience in IT security within governments, Tomasz is a leading figure when it comes to information security, personal data and cybersecurity. In his past, he has inspected ICT systems and networks that process classified information and personal data in government administration and has security clearance for NATO and the EU. For several years, he has been the owner of a company specialising in the implementation of secure solutions increasing the security of business information and personal data.

### David Clarke

David is recognised as one of the top 10 influencers by Thompson Reuter's "Top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and reg-tech in the UK" and is in the top 50 list of Global Experts by Kingston Technology. In the past, David held multiple security management positions such as Global Head of Security Service Delivery and Head of Security Infrastructure for Global FTSE 100 companies.

# The rise of the USB flash drive

When the first Universal Serial Bus (USB) drive appeared on the market over twenty years ago, its collective compatibility was a game-changer in the field of computer technology. With the ability to make multiple device operations widely accessible to the masses, the USB soon evolved, offering significantly faster data transfer, a USB 3.0 port and even greater capabilities accompanying the release of the first USB flash drive in 2000.

Since then, technology has come a long way in terms of mobile data storage and security needs. The focus is on today's generation of USB drives that are designed with very specific use cases in mind. From an enterprise perspective, increased remote and hybrid work, the use of cloud services, and cybersecurity concerns are driving a need for more effective solutions. Alongside this, regulatory requirements demand that data needs to be stored in a compliant manner. These pressures are often compounded by distributed and complex systems that may run "on-premise" and in the cloud.

Then there is the matter of rising volumes of structured and unstructured data, such as documents, emails, photos, videos, and metadata – all adding to the complexity of evolving enterprise storage needs.

But if cloud storage can answer many of these challenges, what relevance do USB drives have in today's business landscape?

> **Many people think of USB drives as being old-fashioned or trivial because of their use in the past as more or less disposable, low-performance, low-security devices.**
> - Rafael Bloom

# Portable storage that meets evolving demand

While the older patterns of USB drive use as a means for portable storage have faded out, the use of high-performance USB drives has emerged for personal, secure local backup with an extra layer of data protection and confidentiality. This can be highly important for compliance-sensitive data such as HR records, financial data, healthcare records, securing intellectual property (IP), and all personally identifiable information (PII). In addition, this generation of devices come with fast data transfer, storage, backup and security capabilities that can be used for:

- Regulatory information that needs to be hand delivered
- Legal and Financial papers that need to be delivered and printed out on site or offsite
- Any potentially hostile environment where Ransomware may be a threat
- Transferring to printing systems where network access is not allowed

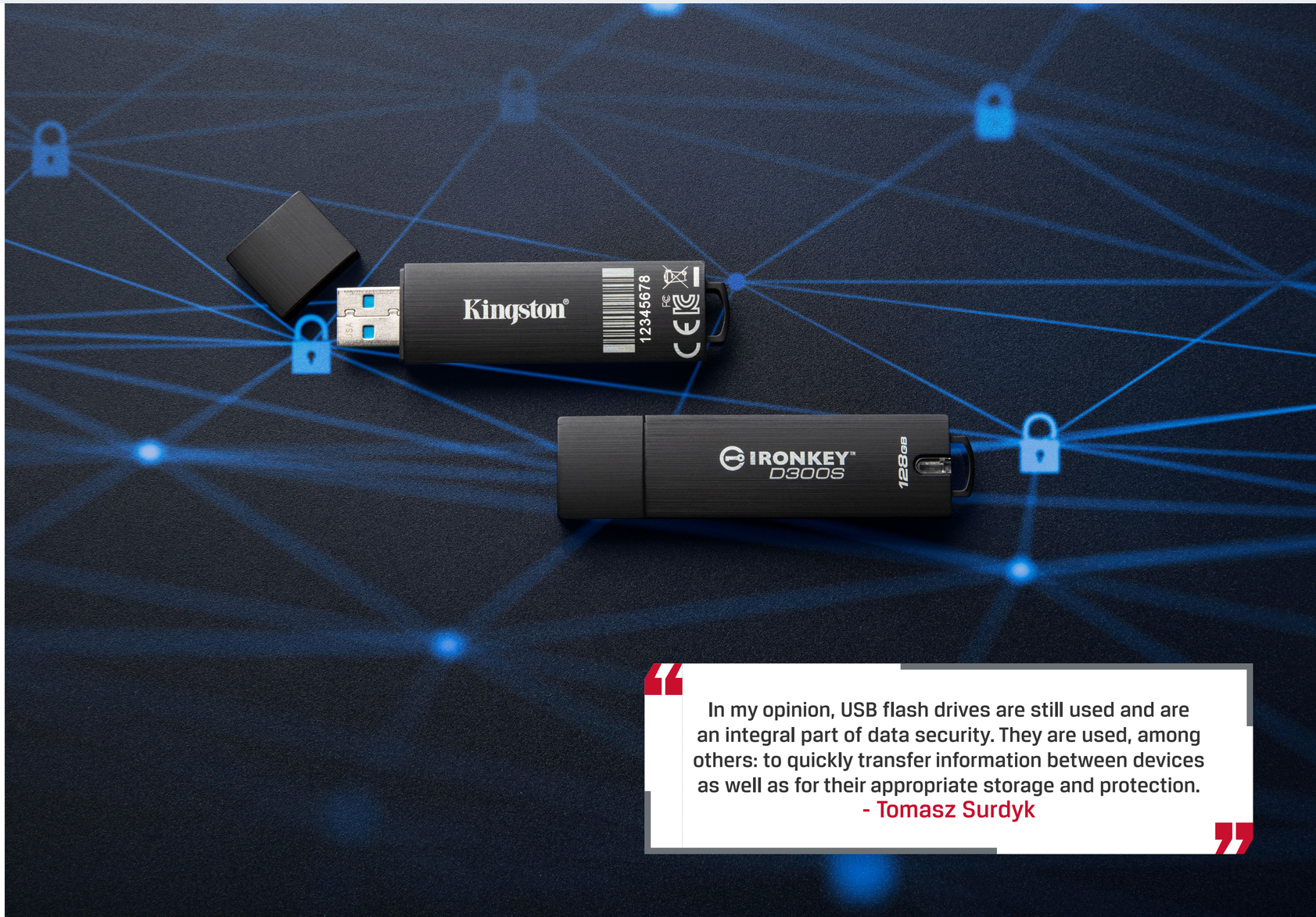
Leading encrypted USB providers Kingston Technology have kept pace with evolving demand with the release of solutions such as the Kingston IronKey™ S1000. This best-in-class encrypted USB drive meets the strictest standards with the ability to safeguard confidential data by providing XTS-AES 256-bit encryption along with a separate cryptochip that has strong anti-tampering protections. In addition, it is FIPS 140-2 Level 3 Certified. This means it's been formally validated by the US government for effectiveness as a piece of cryptographic hardware, making it ideal for organisations needing added peace of mind when it comes to data protection.

Such hardware-encrypted USB drives offer centralised secure device management solutions, whether their data is cloud-based or on-premise. Compliant encrypted data storage that's easy to use with no software needed also frees up valuable IT time, offering solutions designed for quick and efficient deployment.

# Portable storage that meets evolving demand

Back-up and archiving is another example where USB drives can be used to protect digital assets for the long term, and independently of 3rd party Cloud services. While it is true that large data transfers are easily handled in the Cloud, proprietary IP can still be sensitive enough for it to be worth storing on an encrypted, secured USB drive, which can be stored away from the internet and secured.

Then there will always be circumstances where an organisation needs data to be logically and physically under their control, especially when using encrypted drives. And there are cases where storage on a HDD/SSD cannot be encrypted. Using external encrypted USB drives solves this problem, such as the Kingston IronKey D300S. This USB flash drive features XTS 256-bit Advanced Encryption Standard (AES) hardware encryption, which is a type of block cipher that can encrypt 128-bit blocks of data. And when the need comes to encrypt data beyond this, AES will use the XTS block cipher mode that's capable of providing better and stronger data protection than previous modes.




> In my opinion, USB flash drives are still used and are an integral part of data security. They are used, among others: to quickly transfer information between devices as well as for their appropriate storage and protection.
> - Tomasz Surdyk

# Encryption: Hardware-based vs software-based

Looking at how data is encrypted, it can be argued that hardware encryption is easier to manage, and safer than software encryption. This is because the encryption process is kept separate from the rest of the host system, making it much harder to intercept or break. Centralised device-level management allows for drive control over intranet LAN and Internet connections, and can be an excellent tool for:

- Establishing and enforcing encrypted individual and / or group USB usage policies
- Auditing file activity to better track data as it moves in and out of your organisation
- Providing remote content backup for critical data transportation
- Remotely disabling devices when a USB is lost or compromised
- Performing remote password resets when forgotten

When authorised drives are correctly managed in this way, it minimises the risk of sensitive data being copied and shared. In addition, modern day hardware-encrypted USB drives offer a plethora of extra security features that help prevent files and messages being accessed or read by anyone other than the intended recipient.

> **I believe that hardware encryption is better than software encryption. The differences between the methods of hardware and software encryption are significant in terms of vulnerability to brute force attacks. In the case of hardware-encrypted devices, it is not easy to succumb to such attacks.**
>
> **- Tomasz Surdyk**

# Encryption: Hardware-based vs software-based

While businesses may consider software-based encryption because of cost, this may be a little short-sighted. Software-based solutions share the host device's encryption resources with other programs, so it is only as safe as the computer is and often require software updates that - if not maintained - will leave you vulnerable. Software-encrypted USB drives can be subject to unlimited brute force attacks to guess the password, and they have no means to resist software-based dictionary attacks - that can test millions of character combinations in short periods of time.

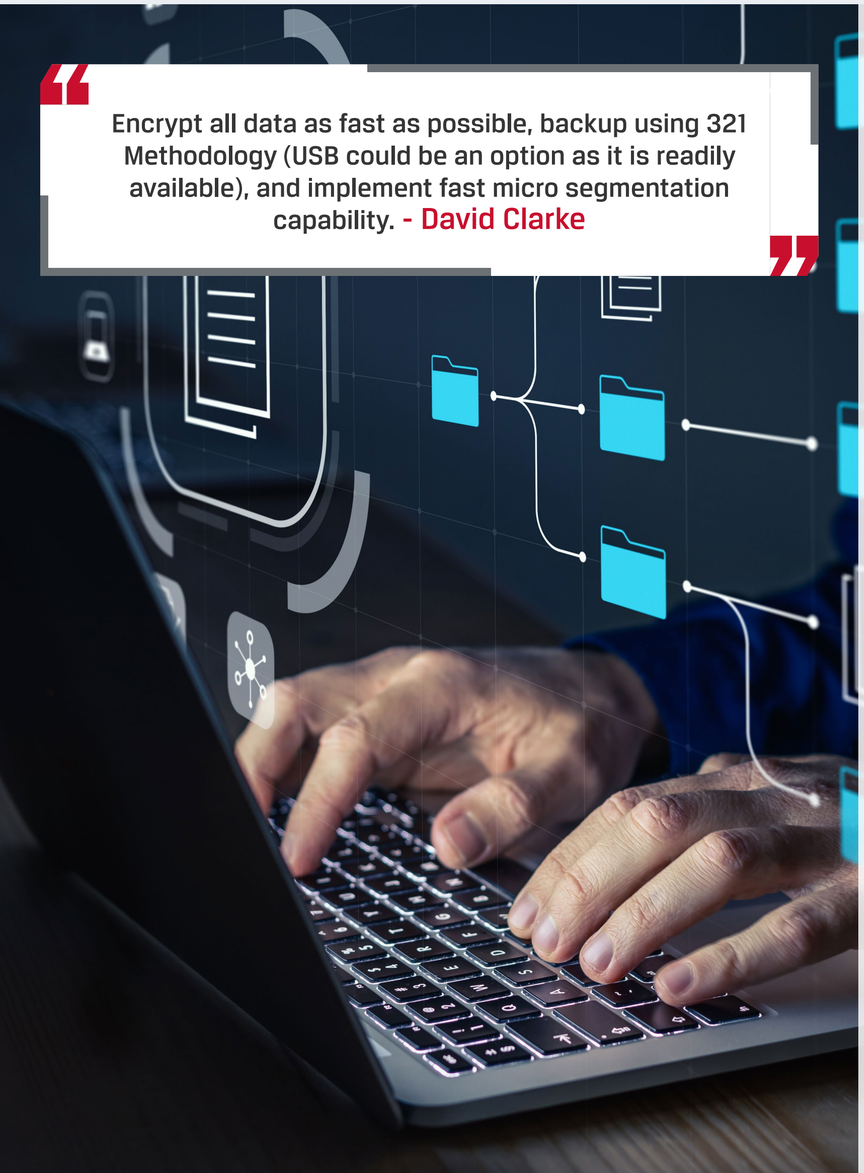
In addition, software encryption is also removable encryption. Any employee with a software encrypted drive can copy off the data, format the USB drive, and the encryption is removed. They can then copy back the data files and use the drive without the hassles of authenticating on different platforms and OS's.

As we mentioned previously, with hardware-based encryption, the physical "encryption" - and subsequent storage of data - occurs independently from the host system. This ensures an extra layer of defence, if systems were ever compromised.

This cannot be overlooked, particularly for those in industries such as financial, healthcare, and government. This is because regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS) often have strict requirements regarding encryption of sensitive information.

Complying with these regulations by using strong hardware-encrypted devices will ultimately help organisations avoid expensive fines, lawsuits, and potentially crippling reputational damage. While hardware-encrypted drives can be more costly than cheaper commodity USB drives, the legal costs of a breach can easily pay for hundreds of drives in just a few hours of legal consultation fees.

# The growing need to protect sensitive data



> Encrypt all data as fast as possible, backup using 321 Methodology (USB could be an option as it is readily available), and implement fast micro segmentation capability. - David Clarke

When it comes to protecting sensitive data against loss and theft, every organisation has an obligation to ensure their devices have adequate security features. It's also important to consider that while there is a myriad of ever-evolving cyber threats, the level of digital maturity and users own endpoint data management skills remain a prominent risk factor if not addressed. Insider threat that includes loss of data control or USB storage devices, the transmission of data outside a safe environment, the use of unencrypted USB drives, and the sharing of passwords can all be the result of a lack of end-user due diligence. All of which can be avoided with adequate training, education and the right USB drive solutions.

> Organisation should have a clear map of their data, including the level of importance and / or sensitivity of all its data sets, with the plan addressing the most important data first, either by physically removing connection to the data or making that data source go dark. Being able to isolate affected systems rapidly is key – and again, having a documented plan that you have practised is absolutely vital. - Rafael Bloom

Pre-planning and a well-practised communications structure also plays a key factor in dealing with a potentially existential threat. Today's cyber threats are intended to target organisations' weak points.

The best time to develop an encrypted USB plan is before it's actually needed, by incorporating encrypted USB drives and policies into your organisation's overall security strategy. Having no plan in place for encrypted USBs and no guidelines leaves you with nothing to build on, and your organisation open to risk at every level - including failure to comply with regulations, such as the General Data Protection Regulation (GDPR), with Article 32 specifically stating that sensitive data needs to be encrypted.

> Users process sensitive data. Losing this increases responsibility and significantly affects the image and safety of the company. In order to protect sensitive data, various security solutions should be used, including data encryption. - Tomasz Surdyk

# Securing sensitive financial data

Along with the security implications, there are also compliance standards that data storage and backup solutions must adhere to. Some of these practices, such as the need to manage and enforce data retention schedules, are common across verticals while others, such as migration of enterprise data to the cloud, are treated very differently.

In many verticals, such as financial services, regulations have come into effect that have made proper data management obligatory. Banks especially were initially highly reticent to use 3rd parties for storage and backup, and many still insist on owning all of their data infrastructure.

Financial institutions are also bound to comply with a growing list of data security regulations and standards, such as Sarbanes-Oxley Act (SOX) and the General Data Protection Regulation (GDPR). However, as the number of mobile employees and contractors grows, so does the risk of data leakage and failure to comply with the mandates imposed by such laws and standards.

The truth is, compliance efforts can be compromised with startling ease if mobile employees fail to safeguard their digital identities, portable workspaces, customer records and financial data they carry. That's why more organisations are moving towards mobile security solutions like Kingston IronKey encrypted USB drives, to protect digital identities and applications no matter where their employees take them.

> **When you consider the overall trend shift to a more distributed IT footprint and the sheer scalability of Cloud infrastructure, it is easy to see how most industries, and the bulk of SMEs, are no longer concerning themselves with managing refrigerated server rooms.**
>
> **- Rafael Bloom**

# Secure access to patient health data

Healthcare is another industry where data security is more important than ever. Patient information is at even greater risk of being stolen, with breaches exposing 45.67 million patient records in 2021, the largest annual total since 2015[2]. When it comes to data storage and backup, patient data is the critical and comprehensive medical information that allows healthcare providers to safely treat their patients.

This could include everything from patient Electronic Health Record (EHR) files containing health histories, tests, photographs and radiographic images, to administrative files including payroll records, patient insurance, and accounts payable. Faced with a growing mobile workforce and a global healthcare market that's undergoing major upheaval and transformation, it's no wonder today's healthcare providers are concerned with data security.

> With ransomware in particular being something of a growth industry, every organisation that handles sensitive data must consider how to operate under extreme duress. - Rafael Bloom

Further, failure to anticipate risks and meet strict mandates such as Health Insurance Portability and Accountability Act (HIPAA) or the Health Information Technology for Economic and Clinical Health Act (HITECH) could result in a costly healthcare data breach, which can further shake patient, partner, or regulator confidence.

With solutions such as the Kingston IronKey range of encrypted USB drives, healthcare organisations can set policies for passwords, application use, recovery, and more – across a handful of drives or thousands of them, from a single console. Mobile and front-line workers can be empowered to support more patients, with user-friendly solutions that remove the need for employees to install drivers or other software, in order to securely access their stored data. While users and administrators can easily and quickly lock down data, no matter where it goes.

# The USB drive in a future of cloud storage

> Cloud data storage is the present and the future. I still argue that physically securing data, e.g. by using encrypted USB drives, is the safest. Users do not have full control over what happens in the cloud. However, we have control over the data in encrypted USB drives, which we secure and store ourselves. Apart from us, no one has access to these media. - Tomasz Surdyk

**Now that the benefits of USB drives are clear, what exactly is their role in a future of cloud storage?**

A decade ago, USB drives were in huge demand as the primary tool to conveniently store and transfer data. However, with the impact of new hybrid work models and increasingly distributed teams, the cloud now provides fast, simple access from many devices to stored information. While flash drives were once immensely popular due to the unique comfort they offered for transporting files. Today, cloud storage services offer greater ease of file portability.

That said, there are still many limitations when it comes to cloud storage. Network connectivity is required, which not only dictates how and when files can be backed up or transferred – it adds an extra security concern. When a company mandates cloud usage, it's not necessarily able to control where data is accessed from. Therefore, the simple act of accessing a VPN using a personal or public Wi-Fi connection opens up the risk of being hacked. In addition, Cloud services are very compelling for threat actors, with majority of all malware (61%) now delivered via cloud applications[3].

> It is perhaps wise to consider what happens when cloud is unavailable, the scenarios where data must be 100% available, and where long-term storage could create a vulnerability. - David Clarke

# The USB drive in a future of cloud storage


USB encryption on the other hand can be done either through the device's hardware or via software. Hardware-centric, software-free encryption is the most effective means to provide protection from cyberattacks. It's an excellent, non-complicated solution to protect against data breaches, and can meet tough compliance standards with the ultimate security in data protection to help organisations confidently manage threats and reduce risks.

Since they are self-contained, hardware-encrypted USB drives do not require a software element on the host computer. No software vulnerability also eliminates the possibility of brute-force, sniffing and memory hash attacks. Software encrypted USB drives also face the risk that any user can disable the encryption by formatting the drive on any computer and using the drive to store sensitive data in an unprotected manner.

Hardware-encrypted USB drives also offer an exceptional physical means in keeping data secure. They permit information access criteria to be established by a user or admin, and can integrate with existing local endpoint solutions. This makes them a convenient and cost-effective solution for many scenarios where cloud storage would not work, or would not be as effective a solution. This might be when data needs to be stored from devices that are not networked, that needs to be private, or requires access to when offline.

> **If we think about data as being either 'hot' or 'cold' depending on its level of utility on a daily basis to an organisation, then it might be more efficient to put 'cold' data in the cloud and lean more on localised USB storage for 'hot' data, if operational continuity and high performance is a more important thing to the organisation, or to a particular business-critical function or process. - Rafael Bloom**

# Summary

While we can't predict the arrival of future innovation, what we can offer is an award-winning portfolio of USB drives offering a dynamic range of encrypted solutions for all levels of mobile data protection requirements. From USB drives that feature an alphanumeric keypad for easy-to-use PIN protection; to FIPS 140-2-Level 3 certification for the highest level of encryption along with anti-tampering protections; to SuperSpeed USB 3.1 technology that doesn't compromise on security, Kingston IronKey products are designed to meet your data challenges, with USB drives that promise powerful and effective data transport and mobile data storage solutions.

Our specialised team of experts are ready to support you at every step of your data storage journey, offering a trusted pair of hands when it comes to helping you find the right storage solution to meet your needs.

We have the skills and technical capability to help you keep confidential information safe and comply with new regulations, whether you're looking to build an encrypted USB plan, identify the best USB drives for your business, or establish and enforce security policies. Offering a highly personalised service, we are committed to delivering products that support your data storage priorities, enabling you to keep pace with the unprecedented speed at which the business world is moving.

## About Kingston

With 35 years experience, Kingston has the knowledge to identify and resolve your mobile data challenges – making it easy for your workforce to work securely without compromising your organisation.


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**