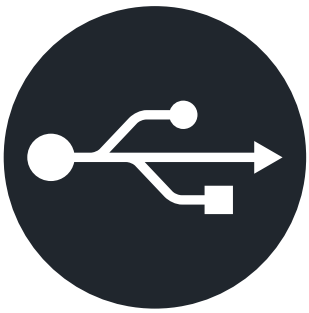
How to allow USB drive access
without compromising endpoint security

#KingstonIsWithYou #KingstonIronkey

Introduction

In January 1996, the official USB 1.0 specification upon release was heralding a new era of uniformity, convenience and versatility for peripheral device vendors and end users alike. 27 years later, it maintains backwards compatibility with each revision, and USB endures as a cornerstone of computer hardware interface from servers to smartphones.



USB's plug-and-play simplicity and ever-increasing speeds have made USB portable storage evolve as one of the big winners. Yet, such convenience has a trade-off when it comes to data security. In today's world, without the use of proper tools such as endpoint protection on host computers and proper data security practices, users with careless attitude towards using portable USB storage leave themselves and others exposed to possible data breaches that could be costly to the end user and can even compromise an entire organisation or government.

In addition to protecting the host environment, the USB drive should also be secured with password protection and on-device hardware encryption. This offers the most robust defence against intrusion. We'll be going over some best practices to use USB drives more securely along with a more in-depth look into USB drives in general.

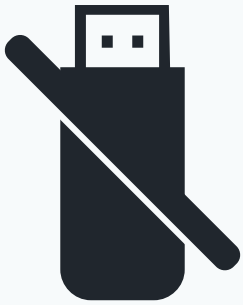
While a combined approach is ideal, it's the robustness of the encryption and the hardware components of the USB drive itself that are of paramount importance. These benefit sectors from finance to healthcare to manufacturing and the military. They also play a role in remote working where network access is either unavailable, vulnerable or impractical.

USB hardware encrypted drives are available with different certification ratings while providing a range of security features. By examining their attributes and opportunities for customisation, their suitability as stand-alone solutions are also illustrated by securing their place in all manners of sensitive environments.

Port authority: USB storage meets Endpoint management data loss prevention software

For decades, anti-virus and anti-malware applications have offered protection at the most fundamental level – automatically scanning downloads and attached devices and reporting or acting on suspicious content. Protection from Next Generation Anti-Virus (NGAV) software takes this a step further. Instead of relying solely on a continually updated database of virus signatures, NGAV adds machine learning and behavioural detection features that can identify and mitigate against unknown threats.

It's not the only weapon in the armoury though, and for those wanting bulletproof protection from user peripherals and more, Endpoint Management Data Loss Prevention (DLP) software provides the means to deny any kind of access to USB ports and other access points.



The 'Block All Ports' attitude to security can certainly eliminate risk, and, in some circumstances, may be desirable, but such a policy can often prove to be a very blunt instrument with undesirable consequences.

Yet, some IT administrators prefer to decline requests to open USB ports on user machines since doing so on these endpoints will allow direct access through the enterprise firewall. Such caution is understandable but when it comes to enabling access for USB storage, provisioning this privilege doesn't have to be a massive security headache if certain prerequisites are observed.

An essential requirement is an endpoint management application suite that features threat detection scanning on anti-virus/anti-malware solutions as well as centralised monitoring and management of all the user endpoints.

Generally, this straightforward approach appears in various guises in unified solutions from popular vendors such as McAfee MVision, Sophos Intercept X, Symantec Endpoint Security, Trend Micro Smart Protection and WinMagic SecureDoc to name a few.

Refinements in whitelisting

When it comes to securing USB storage devices, the method deployed is dependent on the level of protection required. A simple yet effective approach is to whitelist USB storage devices by utilising their respective Vendor Identifier (VID) and Product Identifier (PID) values. One thing about all USB peripherals is that manufacturers each have a unique VID, but the PID changes for every new product that is released.

For whitelisting, using a manufacturer's VID alone would be too broad to be secure since every USB device it has ever produced would be permitted. The PID offers more refinement and demands that only a specific model be granted access to the host system.

While this is an improvement, it's still not ideal. USB storage devices are hugely popular as it enables users to acquire their own devices matching the authorised models. Keeping these things in mind, Kingston Technology offers a bespoke solution to tighten up USB storage device security.

Available through its customisation programme, custom PID profiles specific to an organisation can be created and applied to a range of Kingston encrypted USB flash drives. Companies deploying devices featuring a tailored product identifier not only benefit from simplified whitelisting but greatly enhanced security. With no matching custom PID, even seemingly identical devices independently purchased by employees will be denied access.

While the use of custom PIDs will enable IT administrators to bring new USB storage devices on stream quickly

and easily, a more granular alternative is to use individual device serial numbers that are featured on most Kingston encrypted USB drives. This arrangement requires that each unique device serial number is registered with the endpoint management suite. Initially, this will involve processing by IT staff, and Kingston can provide a list of serial numbers with each order – these are always alphanumeric and non-sequential. Choosing this method allows for far more flexible policies based on ownership of the individual drive with the bonus of precise provenance tracing of devices which can be invaluable in forensic IT scenarios. Some Kingston drives do include a serial number and a barcode on the casing for electronic scanning, and other drives can be customised to add a barcode and serial number on the casing for businesses; these items can be used for drive tracking.

By default, endpoint management systems provide access to VID/PID for port blocking and whitelisting. What Kingston offers is a more versatile way of leveraging these features to enable more accommodating and imaginative policies to facilitate USB storage device use. By establishing an appropriate identification method, a blanket 'Block All Ports' stance is not only over simplistic, but it becomes unnecessary.

Secure, compliant solutions for remote users

When it comes to security, whitelisting devices is only dealing with half of the problem, or to put it another way, half of the solution.

The convenience and simplicity of USB storage devices makes them indispensable in many businesses and institutions where portability is key to experiencing frictionless data transfers. In most environments, for reasons of compliance and good IT hygiene, it's necessary to equip staff with encrypted USB drives for such tasks. By utilising a combination of password protection and device encryption, portable storage is provided with safeguards to prevent access to sensitive data should a device be lost, stolen or left in a potentially vulnerable situation.

This is not a one-size-fits-all solution as encryption techniques vary, and the most significant differences come to light when comparing software and hardware encryption solutions. So, which is better? It depends on your needs, but a more diligent question would be to ask, "Which is more secure?"

Software encryption is essentially a budget choice that will satisfy some sectors with smaller operations. It would also suit businesses whose data transfers are not considered to be sensitive and whose concerns have more to do with policy compliance.

Yet, software encryption's modus operandi is also its Achilles' heel as it requires client facing applications that rely on a computer to perform the encryption tasks. Hence, by association, a software encrypted storage device is only as safe as the host computer.

Exposure to exploits is also heightened as hackers with access to the computer's memory can "sniff" the encryption/decryption keys. The data on the drive can also be subject to brute force attacks as the password access protection is not needed if the encrypted files can be accessed and copied.

Remember, software-based encryption is likely to need software updates from time to time which can complicate implementation by creating additional burden for IT staff. Worst of all, software encryption can be totally removed by frustrated employees who have problems with the drive's portability across platforms. Drive users can copy the encrypted drive's data to a computer, reformat the drive to a non-encrypted drive, and then recopy the data onto the drive. At this point, the data would be unsecured and totally vulnerable to a breach. For compliance purposes with data privacy laws and regulations, this is unacceptable as the USB drive's security can be effectively disabled.

On-chip encryption: the hard and fast solution

By contrast, a hardware encrypted USB drive functions independently of the computer as it features a dedicated processor embedded on the actual drive that manages the encryption. It has an always-on encryption process with protection against brute force password attacks; encrypted data is not accessible and cannot be copied.

Kingston's enterprise and military grade hardware encrypted USB drives utilise AES 256-bit encryption in XTS mode. A globally approved encryption technique, the AES 256-bit provides rigorous data safeguards. By utilising two separate keys at different stages of the encryption/decryption process, XTS mode has a similar effect to encrypting the data twice.

In use, the encryption key is derived from the drive controller's random number generator which the user's password unlocks. As authentication takes place within the device's crypto-hardware, encryption keys and other critical security functions are protected against common exploits such as BadUSB, cold boot attacks, malicious code and brute force attacks.

One of the most immediate benefits of hardware encryption is that the performance of the drive is significantly better than a software encrypted drive as there is no offloading of encryption tasks onto the host computer. Everything takes place within the drive.

Hardware encrypted USB drives such as the Kingston IronKey D500S are password protected devices that are encrypted out of the box. In use, only the write-protected launcher volume is visible to begin with as this contains the application used to authenticate the password and unlock the main encrypted storage volume. This procedure avoids installing any kind of driver or software on the host PC.

Furthermore, Kingston hardware encrypted USB drives feature digitally-signed firmware which prevents any firmware manipulation within the device. Having this additional layer of security provides protection against attacks such as BadUSB which exploits an inherent vulnerability in USB device firmware. This can lead to covertly executed commands or malicious code being run on the host computer.

Of course, a 'Block All Ports' approach would limit the risk of BadUSB exploits, but why sacrifice productivity with such outdated practices? As highlighted above, a secure environment can be maintained in tandem with portable storage device use if simple procurement and deployment procedures are in place to introduce hardware encrypted USB drives.

Secure and compliant remote working

For remote workers, being away from the safeguards of an organisation's secure working environment demands a revised strategy as well as a fresh look at priorities.

When it comes to a remote security plan, is there any benefit to block the USB ports on your employee's laptop only to have them connect via the internet to access a server to upload or retrieve documents? On the road, an open internet connection such as an insecure or untrusted Wi-Fi access point may be all that's available and this introduces a wide variety of danger that greatly increase the possibility of a breach. Threats such as data interception and surveillance

through spoofing, Man-in-the-Middle (MitM) attacks, and network eavesdropping are just a few of the increasingly sophisticated hacking methods available to cybercriminals. Even VPNs have been compromised.

An organisation's network connection to the internet is just another endpoint, and its inherent exposure makes it an extremely vulnerable and targeted entry point. Opening it up to remote access carries its own security risks especially when it comes to sensitive data.

Entrusting remote workers with password protected and hardware encrypted USB drives effectively eliminates potential networking vulnerabilities. Yet, making such provisions requires closer examination of the USB drives available and how they meet the demands of each remote working environment. This isn't a simple matter of making a choice about the drive's capacity or whether it should have its serial number logged. This concerns the physical construction of the device itself.

Tamper-proofing safeguards: The solid options

The main issue here is whether a hardware encrypted USB drive is tamper-proof or not. Just how secure a device is to such interference is reflected in standards such as FIPS 140-3, which has several levels that scrutinise the resilience of a drive's physical construction without using cryptographic methods.

The related FIPS-197 certification observes only the hardware encryption attributes and devices such as the IronKey Vault Privacy 50 series and Vault Privacy 80 External SSD which are enterprise-oriented models where data security requirements are not at the military grade level. These drives are less expensive but lack the protection against physical drive tampering.

With FIPS 140-3 Level 3 certification (pending), the methods deployed to expose device tampering are rated as military grade. Kingston supplies these FIPS 140-3 Level 3 drives to enterprises, governments and military worldwide.

Using epoxy internally to coat all the drive circuitry need for security and gluing the internal components to the casing creates another wall of defence. Any attempt to open the metal case would be extremely difficult and would cause the internal chips and other components to break eventually making the drive non-functional. With this hard and opaque epoxy in place, tampering with vital components becomes a near impossible task. Devices such as the Kingston IronKey D500S and S1000 contain this additional security measure.

These device protections are not confined to physical measures alone, and the Kingston IronKey S1000 takes tamper proofing to another level. The IronKey S1000's internal cryptochip can detect any physical tampering and will render the drive unusable as soon as the device is powered up. Relying on hardware encrypted USB storage devices to access and transfer sensitive files is a pragmatic move that facilitates frictionless remote operations and effectively guarantees security in the field.

Make sure you research the USB drives hardware and security features to see if it's up to the task for your specific needs and use case. Each USB drive should be reviewed on a case-by-case basis with trusted accreditations helping to guide these decisions. Whatever the priorities, Kingston offers a range of hardware encrypted USB drive solutions and customisation options at affordable price points that address all manner of environments: from general compliance all the way up to the toughest military specifications.

Safety first: No networks, no problems

Today, the office has no borders and as work-from-home continues to flourish, it has brought remote access vulnerability issues into the spotlight for many companies. Many are experiencing these challenges for the very first time and are looking for more secure ways of accommodating this growing trend.

To support these needs in a broad range of industries, hardware-encrypted USB storage devices are already well-established and provide a secure solution where the transfer of data via networks can be impractical or undesirable for several reasons.

In finance, regulators frequently request data to check on a firm's conduct and compliance. The risk of exposure is far too great to contemplate using a network to transfer sensitive documents containing precise details of investments, market trading and other confidential banking activities. The simple and effective solution is to deliver this information on a hardware encrypted USB drive.

The use of secure USB drives to transfer files in healthcare environments is a daily occurrence. This is also for the convenience of doctors or consultants who may wish to analyse files, refer to them for research, or present case examples to medical students. There are also more practical needs when it comes to proprietary systems such as medical imaging devices where network access is absent or insecure. By utilising compliant hardware-encrypted USB drives, files can be easily transferred for use elsewhere.

Dos and don'ts

✓ **Do use compliant, secure drives** and review specifications to procure drives that match the needs of each deployment.

✗ **Don't authorise a random or personal Bring Your Own Device (BYOD) policy** – for any company, losing unencrypted drives is too high a price in terms of financial and reputational damage.

✓ **Do deploy an endpoint management suite** and use hardware-encrypted USB drives that offer distinctive whitelisting features.

✗ **Don't leave anything to chance.** Properly assess requirements for on-premises and remote working environments.

✓ **Do educate staff** on security matters. It is in their own interests that the company remains protected from security breaches.

✗ **Don't make security so painful** that users seek workarounds that could lead to shadow IT solutions being utilised. Just because a blanket policy has always been applied does not mean it will suit all scenarios. The workplace is changing and by choosing the right solutions new policies can be developed and enforced.

In this scenario, the Kingston IronKey Keypad 200 (KP200) comes into its own. As an OS independent drive, there is no launcher volume to enter the password, but instead, features an alphanumeric keypad that unlocks the device for use on any platform. Like a Swiss Army knife of hardware encrypted USB drives, its usage extends to manufacturing; securely transferring applications authored in the IT research and development world to machinery controlled by operational technology (OT) platforms. For mixed platform operations that also feature Linux, the KP200 is one of the most straightforward secure solutions available.

Hardware-encrypted USB storage devices have a vital role to play in law enforcement too. They protect and securely transfer case files, images and other evidence to field operatives, investigative squads, and forensic teams. Kingston offers an additional benefit as it can provide drives with the internal serial number printed on the external casing alongside a barcode. Issuing and cataloguing drives become simple and easy to track. It's as easy as manually logging a serial number or as swift as scanning a barcode – auditing and inventory management couldn't be easier. It's a feature that appears as standard on the Kingston IronKey D500S, D500SM and S1000B/E drives but is also available for other hardware encrypted models as part of the Kingston Customisation programme.

Security and storage mobility: The state of the art

Password protection, hardware encryption, tamper-proof safeguards, granular endpoint whitelisting, military grade FIPS 140-3 level 3 certification (pending), and at-a-glance-logging are off-the-shelf features of Kingston USB drives that can be deployed without delay.

These robust security defences ensure that the USB drive and its data remain secure in its host environment. While the specifications are impressive on paper, picking a model randomly without any research won't necessarily provide an ideal match for some organisations with more exacting requirements.

As an independent manufacturer, Kingston offers a wide range of options to satisfy customer needs. Through the Kingston Customisation programme, advanced solutions are available and are designed to deliver a seamless user experience.

Secure customisation goes beyond supplying an organisation with its own USB PID for whitelisting. The launcher application's security profile can also be customised using fifteen different preferences from contact and company details to enabling password hints and determining the maximum number of password attempts. Externally, company branding (co-logo) is available as well as a range of colours for specific drives. With a minimum order of fifty drives, all these features provide an effortless integration path for device deployment.

If an endpoint management application suited to secure USB storage is not already in place, there is a management solution that is available for organisations that wish to manage their fleet of Kingston drives including options to remotely reset passwords.

USB's ubiquity and convenience have seen it outlive a variety of promising technologies and for many tasks the immediacy and convenience of USB storage endures. Readily available and always secure, protected USB drives offer a simple solution that can be readily appreciated.

Why worry about network data breaches in remote environments? With Kingston IronKey hardware encrypted USB storage devices, the answer is in the palm of your hand.

To learn more about how Kingston can help visit kingston.com/ironkey or for more specific questions, ask one of our Encrypted USB experts.

#KingstonIsWithYou #KingstonIronkey