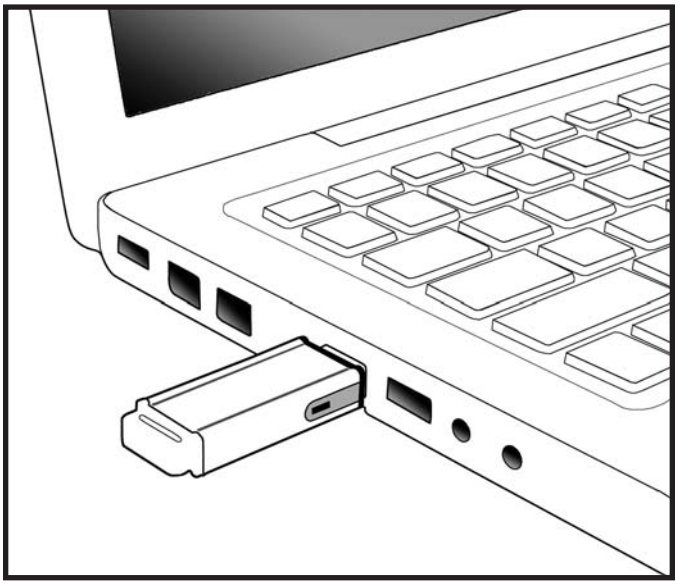
11 Questions to Ask When Buying a Secure Flash Drive. (And why they are important)

By: Emmett Jorgensen, Kanguru Solutions

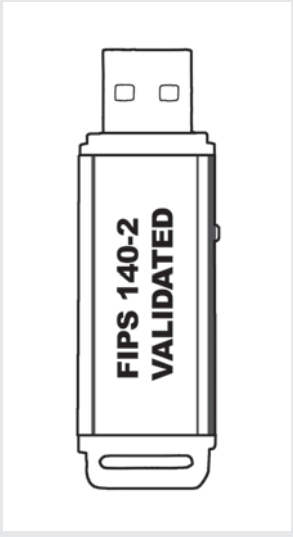


Flash drives: Petite, portable storage devices capable of storing gigabytes of data. These incredible devices have revolutionized the business world with their convenience and portability; however, there is a darker side to the revered little flash drive. Their tiny size often makes them easy to lose and their storage capacity allows massive amounts of potentially sensitive data to be stored on them. If lost or stolen, a tiny unsecure flash drive has the potential to cause a huge data breach.

As state, federal and business regulations tighten on information security and impose fines and sanctions for data breaches, the question arises: Should flash drives be banned from work environments, as the Department of Defense did in the fall of 2008[i]? Or can they be used in a safe manner without limiting the very attributes that make them so popular?

The answer to this will vary greatly depending on your organizational policies and security standards; however, there are options for using flash drives securely.

Enter encrypted flash drives. While encryption is important, there are many more factors to take into consideration in the overall security of flash drives. Here we will help you decipher the technical jargon and figure out the best solutions for your needs with 11 questions to ask when buying a secure flash drive.



Question #1: What is the overall level of security and has it been certified by an independent, accredited entity?

Why it is important: Generally, the higher the encryption level (128-bit, 256-bit), the more difficult it is for a hacker to break. However, it is also very important that the device be tested for other relevant factors such as encryption tunnels, a true random number generator, physical security features, hashing, and the security of the device's firmware.

"A weakness in any one of these areas may compromise the overall security of the device (and may be prevalent in untested, consumer level devices)." Said Nate Cote, VP of Product Management at Kanguru Solutions.

A good rule of thumb is to purchase devices that are "FIPS 140-2 Validated"[ii] or have passed "Common Criteria" to ensure their security has been thoroughly tested. FIPS, or Federal Information Processing Standards, are standards and guidelines outlined by the National Institute of Standards in Technology for the security of computer systems.

Question #2: Is it hardware or software encrypted?

Why it is important: Hardware and software based encryption each have their own benefits and weaknesses. Hardware encrypted flash drives tend to be preferred since they perform faster than software encrypted flash drives, have less vulnerabilities, and require no special software to be installed on host computers. Software encryption benefits include less upfront cost.

Questions #3: Does it work on multiple operating systems? (Windows, Mac, Linux, etc.)

Why it is important: Many encrypted flash drives are OS specific, meaning they only work on Windows or Mac, but not both. This can be a severely limiting factor for companies or users that work with multiple platforms. If your organization uses multiple OS, then make sure the secure flash drive you choose also works across multiple platforms.

Question #4: Does using its encryption require admin rights on host computers?

Why it is important: Another question pertaining to usability. Some secure flash drives require administrator rights before their security features can be used on a computer. No admin rights, no ability to use the security features on your drive. (Or worse yet, no use of the drive at all.) Look for a secure drive that doesn't require admin rights to utilize its encryption.

Question #5: Does the flash drive have on-board anti-virus?

Why it is important: Flash drives without on-board anti-virus can unknowingly play host to malware like Stuxnet[iii] and Conficker, spreading to any host computer they are plugged into. Flash drives with on-board anti-virus can protect your drive and whatever host computer it is being used on against virus and malware threats. Additionally, drives with on-board anti-virus can be used to scan any host computer for malware or viruses, essentially making them a portable anti-virus solution.

Question #6: Can it be configured to require a complex password? (Letters, numbers, symbols, upper/lower case, etc.)

Why it is important: Regardless of how strong the drive's security architecture, this security can be seriously undermined by a weak password. Look for the ability to configure your password and make sure it uses a combination of letters, numbers and even symbols. Also, the longer the password, the more secure. For instance, a hacker using the processing power of multiple workstations could crack an 8 character password (using only upper or lower case letters) in approximately 35 minutes. It would take the same hacker 30 years to crack a 12 character complex password using a combination of letters, numbers and symbols.

Question #7: Does the device lock out or erase data after a set number of invalid login attempts?

Why it is important: This feature prevents brute force attacks. Try the wrong password too many times and the device can be either disabled or even deleted, preventing access.

Questions #8: Can a master password be used?

Why it is important: This feature allows for a system administrator to recover your data in the event you forget your password. It's also great for companies that need to access the files of former employees.

Question #9: Can it be remotely managed?

Why it is important: If your flash drive containing sensitive info (Social Security #, bank accounts, customer credit card info, etc.) has been lost or stolen, remote management features allow the device to be disabled or deleted, ensuring that its data never falls into the wrong hands! This feature also helps companies meet industry security regulations such as HIPAA and Sarbanes Oxley. Remote management also allows the device to be updated with the latest patches and security policies of the governing organization.

Questions #10: Does the drive offer a virtual keyboard for entering the password?

Why it is important: A virtual keyboard can prevent key logging programs from capturing your keyboard keystrokes when you enter your password. A virtual keyboard is another layer of protection against malicious intent.

Question #11: Can the flash drive be restricted to only certain IP ranges and domains?

Why it is important: This feature can allow organizations to prevent their flash drives from being used on computers outside their boundaries if desired. This is a great feature for organizations that want to make sure the drives aren't used on outside, unauthorized computers or networks.

In conclusion, flash drives are far too beneficial to be banned outright and avoided. Used with the correct combination of security features, they are a major asset to most organizations, providing a portable platform for storage and applications needed in today's corporate IT environments.

While this list is by no means all encompassing, it should provide an excellent starting point and, hopefully, give some insight into some of the security features to look for in encrypted, secure flash drives.

With the proper knowledge and protection, flash drives can be used in a manner that highlights their benefits and reduces their drawbacks. Although secure flash drives may cost slightly more than standard flash drives, the money that you save in the long run will far outweigh the extra up-front cost.

---

i Allen, David & Svan, Jennifer. The Defense Department has banned the use of removable flash media and storage devices from all government computers, according to a series of notices put out by the services this week. Starts and Stripes. [Online] November 21st, 2008. http://www.stripes.com/news/dod-bans-the-use-of-removable-flash-type-drives-on-all-government-computers-1.85514.

ii Evans, Donald L. SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES. Gaithersburg, MD : U.S. DEPARTMENT OF COMMERCE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), 2001.

iii Keizer, Gregg. Is Stuxnet the 'best' malware ever? Computer World. [Online] September 2010. http://www.computerworld.com/s/article/9185919/Is_Stuxnet_the_best_malware_ever_.