

Key drives a security risk? Not when they're made like this.

- By [John Breeden II](#)
- Feb 13, 2012

A rugged plan for your agency is like a power protection or a security plan. You need to make sure that every aspect is covered. And given that most of us have home bases in areas that do not require rugged gear, the focus is probably going to be on moving data from place to place.

One of the best ways to do this, if you don't need a full notebook, is a key drive. Once the scourge of security plans, the humble key drive has grown up a lot lately, to the point where it can become the preferred method of rugged data transfer. The CE-Secure Vault from CMS Products fits this role nicely. Based on our testing, it can keep your data safe from both the elements and hackers.

On the surface, the CE-Secure Vault we tested looks like a normal 16G key drive, though the frame is actually made of rugged aluminum. There are also higher and lower drive sizes available, though the physical size of the device is the same. The drive will work with Windows 7 and XP, Mac OS X 10.5 and 10.6, and 32- or 64-bit systems, so pretty much anywhere.

CMS Products CE-Secure Vault

Performance: B

Features: A

Ease of Use: A

Value: B

Price: \$109 for 4G, \$149 for 8G, \$269 for 16G, \$449 for 32G unit

Pros: Very rugged; encrypted AES 256.

Cons: Slow to write to the drive due to encryption.

Related coverage: [At last a key drive the government can love](#)

When you first put the Vault into a computer, you are prompted to set up the security password. This needs to consist of at least one capital letter, one lowercase letter and one alphanumeric character and be eight characters long. In addition to the password, you are able to set up a hint in case you forget. And we were not allowed to make the hint the actual password, so users can't shoot themselves in the foot right off the bat.

We tested for rugged but started with security. Everything that goes onto the drive is automatically encrypted to AES 256. If you don't first enter the password, you won't be able to see anything that is on the drive, other than the program that launches the password application, which will automatically open when the drive is inserted but can be manually triggered as well.

Precautions have been made to make the password interface more secure, which has been a weak point traditionally for key drives. For one, if the wrong password is entered 20 times, the drive is

disconnected from the host system to prevent brute force dictionary-type attacks. Also, if a drive is left in a machine too long, it will disconnect, which means a user has to re-enter the password to keep working.

If you are using the drive the whole time, this won't happen, but it can time out so you don't leave unsecured data on the drive in a machine with bypassed security while heading off to lunch. And, of course, if you pull the drive and reinsert it, you will have to enter the password once again.

Finally, the Vault is configured so it leaves no footprints on a host computer. So although it's not recommended, in a pinch you could use a public terminal to access the drive and not have to worry quite so much about it being a security breach.

A slight disappointment

The one slight disappointment we had with the Vault in terms of raw performance was with transfer times. Pulling data from the drive takes almost no time at all. However, because of the encryption process, it takes a long time to write data to the Vault.

Our 2G test file could be pulled from the Vault in 17 seconds, which is right on the mark in terms of what we would expect to find in any key drive using a USB 2.0 port. However, writing that same file to the drive took much longer. In fact, it took three minutes, 18 seconds. Once the data is there, you can access it normally. We even streamed a movie off the drive with no problems. But getting data to it initially takes time.

The Vault easily met the 810f mil-spec level for rugged. It dropped from heights up to 48 inches with no damage whatsoever and all data remaining secure. The one slight cosmetic problem it faced was that the CMS faceplate, which is apparently only held on by very thin strip of glue, popped off in a three-foot drop. No big deal, but CMS might want to invest in an extra dab of glue.

It goes beyond mil-spec in terms of waterproofing. We sunk it into a fish tank full of water and left it there for four hours. After a quick toweling off, we inserted it into a computer where it asked us for the password like nothing happened. And all the data was intact. It also had little problem with temperature, spending the night in an environment where it was a few degrees above freezing and a couple hours in the GCN Rainforest Test Environment where it got up to 120 degrees Fahrenheit, with very high humidity. The data never suffered, and the drive itself didn't even get scratched.

The one thing it didn't do, which we have seen other drives tout as a feature, is erase data if the password isn't entered after a certain number of tries. Although the Vault will disconnect from a computer to halt a brute-force attack, the data itself remains in place. But it really comes down to the level of security you want or need. Probably just as many people have lost all their data due to a misplaced password as have been saved by a feature like that.

With strong encryption, smart protection of the password interface, and solid fortification against the elements, the CE-Secure Vault is a great choice for keeping your secrets safe as well as dry. It's a vault that fits nicely in your pocket.