

Seagate Maxtor BlackArmor: Armor for Your Mobile Data

Categories: [News & Events](#), [Security & Spyware](#)

Tags: [encryption](#), [storage](#), [usb](#)



At CES this past January [Seagate announced](#) the Maxtor BlackArmor encrypted portable drive. Perfecting the product took a bit longer than they expected, but it should be released in May and widely available by June. Staples will have exclusive retail distribution rights, while CDW will handle online sales.

Executive Director Jon van Bronkhorst "totally loves" the product. "It's not about capacity, it's not about backup, it's not about expansion - it's

all about security," he said. "It mounts like a drive and acts like a drive, but without the password it's a brick". The USB 2.0-compatible drive offers 160 GB of storage protected by 128-bit AES hardware-based encryption. Once you enter your password you have full, speedy access to the data.

Van Bronkhorst pointed out that the user is responsible for choosing and remembering a strong password. There's no back door; if you lose the password your only recourse is to format the drive and start fresh. He explained that Seagate considered offering a biometric option, but biometrics generally need some kind of back door in case the scanner fails.

The product ships with Maxtor backup and synchronization software for installation on your home system. On the home system the device works in "host mode"; anywhere else it's in "traveler mode". The biggest difference is that it's only possible to erase the drive in host mode. If somebody steals or borrows the drive, they can't get your data and they can't erase the drive and make it their own.

The device is small - 131mm x 84mm x 16.5 mm - and it weighs just 208 grams.

Best of CES Storage Device: Maxtor BlackArmor

January 9th, 2008 by Jeffrey L. Wilson

There's security and then there's near-impenetrable security. The sleek and sexy [Maxtor BlackArmor](#) takes the prize as the Fort Knox of the storage world, as the first external hard drive to back up and secure your data using Seagate's [DriveTrust hardware encryption](#).

If you're wondering about the thoroughness of the government-grade AES protection, how's this for a kicker? If you somehow lose or forget your password, you'll have to perform a "secure erase" to wipe the drive clean in order to gain access.

