

Temporary Virtualized Desktops on Encrypted Flash Drives Enable IT Departments to Provide Contractors with Limited Access to Corporate Data

A growing trend toward using contractors and trusted partners presents significant risks for organizations. Deploying virtualized portable desktops on secure IronKey flash drives reduces the cost and complexity of providing independent contractors with a work environment while meeting the need to protect critical IT system data and limit access to confidential corporate information.

In addition to protecting data with military-grade encryption, the IronKey solution enables administrators to implement security policies and manage drives remotely. IronKey centralized management services include the ability to remotely deny access to drives in the field, or even destroy all data on a drive. This capability enables administrators to limit the time that a contractor has access to data and applications on virtualized desktops.

In addition, the IronKey solution helps customers realize other important benefits when deploying virtualized desktops to contractors or partners. These include:

Speed — Portable desktops require high performance because they are constantly reading and writing. IronKey drives use ultra-fast dual channel flash memory, which delivers 10x speed compared with conventional flash drives. Additionally, operation of virtual desktops is faster because the host PC does not have to communicate with a remote server.

Reliability and Survivability — IronKey drives are waterproof far beyond military specifications, and all internal components are housed in a rugged metal enclosure. Commercial-grade SLC memory chips last 10-20 times longer than the memory used in conventional flash drives.

Security — Security is a paramount concern when a complete desktop resides on a thumb-sized device. All data on an IronKey drive is encrypted in hardware using AES 256-bit encryption in CBC mode.

Secure Access — IronKey Enterprise devices support One-Time Password technology such as RSA SecurID®, which means you can reduce cost and complexity by consolidating portable data storage with the functions of a two-factor authentication token in a single device. Additionally, each IronKey drive comes with a unique digital certificate, making it easy to grant network access using simple strong authentication.

Active Anti-Malware — A comprehensive set of malware defenses—including hardware-level defenses against AutoRun worms and other threats—stop malware from spreading from untrusted machines via USB storage to corporate or government PCs and networks.

IronKey drives are also device independent—they work on Windows, Linux, and Macintosh computers—and work without the need to install software or drivers, making it easy for contractors to work on any computer.

