

## Virtualized Portable Desktops on Encrypted Flash Drives Provide Data Protection and Secure Access for Remote Workers

From senior management to the rank and file, more and more employees are taking work home. In fact, Gartner estimates that half of all C-level executives perform 80 percent of their work on machines other than the standard corporate-issued PC. Rather than viewing this trend as a security risk, IT departments can turn it into an advantage. Deploying virtualized desktops on encrypted IronKey flash drives allows employees to work at home while delivering better security and greater control over desktops. This solution can also achieve cost savings by eliminating the need to issue laptops to whole classes of enterprise users.

State-of-the-art IronKey features like “always-on,” military-grade encryption and online identity protection prevent employees from accidentally compromising critical corporate data. This security works whether they are working on a corporate PC, a shared computer at a hotel, or their home computer.

In the event a drive is lost or stolen, no one can access the contents without the proper password. In fact, the entire virtualized desktop and stored files are more secure on an IronKey drive than on an encrypted PC hard drive. Unlike PCs, which are vulnerable to cold boot attacks because they store encryption keys in RAM, IronKey stores encryption keys in hardware. The keys never leave the onboard cryptographic processor, which is shielded against physical and electromagnetic attacks. Encryption in hardware also protects against brute force password guessing and other online threats.

To ensure that malware does not jump to the flash drive and then spread to corporate or government PCs and networks, IronKey drives employ active anti-malware defenses. These include hardware-level protections against AutoRun worms and other malicious code. A Read-Only mode also allows the drive to mount on untrusted computers without risk of infection.

The IronKey solution helps customers realize important benefits when implementing disaster recovery plans, including:

**Speed** — Portable desktops require high performance because they are constantly reading and writing. IronKey use ultra-fast dual channel flash memory, which delivers 10x speed compared with conventional flash drives. Additionally, operation of portable 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 used in IronKey drives 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 military-grade 256-bit encryption. Additionally, IronKey management services allow you to set a range of security policies on drives, and remotely disable or destroy drives—including the entire virtualized infrastructure—in the event the drive is lost, stolen or in the hands of a high-risk user.

**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

