

Virtualized Portable Desktops on Encrypted Flash Drives Enable Secure and Reliable Disaster Recovery

IT groups implementing disaster recovery programs must consider all possible scenarios—from natural disasters such as a flood, fire, earthquake or epidemic to a manmade catastrophe such as a terrorist attack. Deploying portable virtual desktops on secure IronKey flash drives enables organizations to ensure rapid recovery and continuity of operations. Workers can have access to a complete desktop—including OS, applications and sensitive data—and quickly resume their activities, even if public or corporate networks are rendered inoperable by the disaster.

IronKey is the world's most secure USB flash drive. The IronKey solution provides military-grade encryption in hardware, active anti-malware defenses, remote management (including the ability to terminate lost or stolen drives), and strong authentication capabilities. Virtualized emergency desktops loaded on secure IronKey drives provide excellent mobility and easy remote access—without exposing organizations to risks such as data loss or the spread of malicious code. Rugged, waterproof IronKey drives also provide superior reliability and survivability.

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 uses ultra-fast dual channel flash memory, which delivers 4-5x 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. They also employ commercial-grade SLC memory chips, which 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. 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 a 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 fast and simple for employees to resume work on any computer.

