NOW HERE IS SOMETHING EVERY IT PROFESSIONAL NEEDS…

If you manage a network, you know that invariably the same person who doesn't pay attention to instruction about storing vital files on central servers is also going to be the one to infect their computer by bringing a flash drive from home. Then it's up to you to retrieve their important files safely from the infected PC.

In a situation like this, the Data Rescue Engine can be your knight in shining armor—its mission is to rescue files and vanquish malware.

File rescuer.

Just plug the USB flash drive containing Data Rescue Engine into the PC's USB port, then use the on-screen menus to neatly lift files our of the infected PC and store them in an encrypted, password-protected folder on the Data Rescue Engine flash drive. It even compresses files.

Malware fighter.

Data Rescue Engine doesn't' just rescue files—it actively seeks, destroys, and blocks malware, doing battle with viruses, Trojans, keyloggers, spyware, adware, rootkits, zombies, botnets, and blended threats. It spots threats that normal agent-based anti-virus technology may overlook. It can even detect when malware uses an operating system or an application and distinguishes between user action and malware activity.

Always ready for action.

The Data Rescue Engine resides in a flash drive you keep in a PC's USB port. It updates itself daily over the Internet with malware definitions from the Data Rescue Engine upgrade server.

When the worst happens and malware strikes, take Data Rescue Engine and plug it into the USB port of the infected computer. Follow the easy on-screen menus to start rescuing files. It logs its activities in an exportable file.

Source: https://bboxblog.wordpress.com/2010/11/04/now-here-is-something-every-it-professional-needs%E2%80%A6/