IRONKEY ENTERPRISE

White Paper

Active Anti-Malware Protection

Self-Defending IronKey Flash Drives Stop MalWare and Viruses from Spreading to Computers and Networks

January 30, 2009

THE WORLD'S MOST SECURE FLASH DRIVE

Only IronKey—with our unique end-to-end security that extends from the Cryptochip to firmware to services—is able to deliver a complete range of anti-malware controls down to the hardware level.

Ensure That Data Stays *In* and Malware Stays *Out*

Conventional USB flash drives and other removable storage devices can allow viruses, worms and other malicious code to penetrate the IT system. Only IronKey—with our unique end-to-end security that extends from the Cryptochip to firmware to services—is able to deliver a complete range of anti-malware controls down to the hardware level. When combined with other advanced IronKey security features, these layers of protection make IronKey USB flash drives a truly portable computing environment that protects data from loss or leakage while preventing the spread of malware.

Removable storage media devices often contain Autorun.inf files, which cause the Windows operating system to automatically run a program when the device is inserted. Malware that spreads via AutoRun files typically changes a useful Autorun.inf file to achieve a malicious goal (e.g., adding a line of code that says "automatically run this virus"). This is how the Agent.btz worm spreads.

Patent-pending IronKey USB anti-worm technologies protect the Autorun.inf file from being changed, and verify that the file is in its original state before Windows executes the Autorun.inf. In the event that the file has been changed, the antiworm technology automatically repairs the file and notifies the user. As an added level of security, IronKey also allows the administrator to disable the Autorun.inf file.

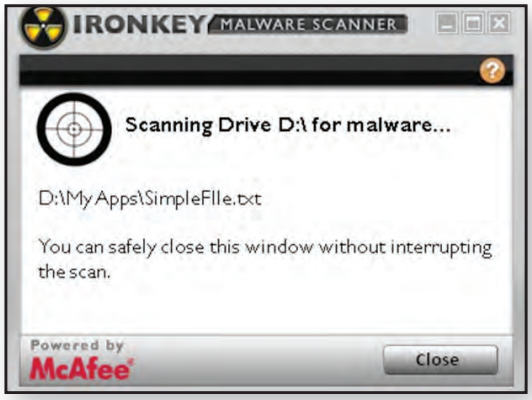
IronKey also protects against AutoRun threats on machines that your organization does not manage. For example, if a user inserts an IronKey device into an infected home computer, the device will detect and warn the user that the unmanaged machine contains a virus, and will immediately repair the AutoRun file so that the worm does not spread. This is important because malware that propagates by AutoRun files represents a particularly fast-moving threat vector. The device also notifies the user that malware was trying to change your file and instructs them to contact the system administrator.

"The number of publicly reported data breaches in the US rose by more than 40% in 2007."
ITRC

Scanning for Malware

IronKey has partnered with a best-of-breed US-based provider of anti-virus and intrusion prevention software to develop the IronKey Malware Scanner. Whenever a user plugs an IronKey Enterprise device into a computer, the Malware Scanner checks to make sure the latest version of the signature database is installed. It downloads the latest version if needed and scans the IronKey drive, automatically repairs any problems, notifies the user, and logs a report.

An upcoming IronKey release will make these reports available online so that system administrators will immediately be aware of malware threats. This approach keeps devices clean at all times using the latest anti-virus engine, and helps to prevent data leakage by eliminating USB devices as an avenue of attack.



The Malware Scanner does not require installation on the host computer, which improves portability. It does not require anything other than the standard USB driver in Windows, eliminating the need to install drivers on all machines.

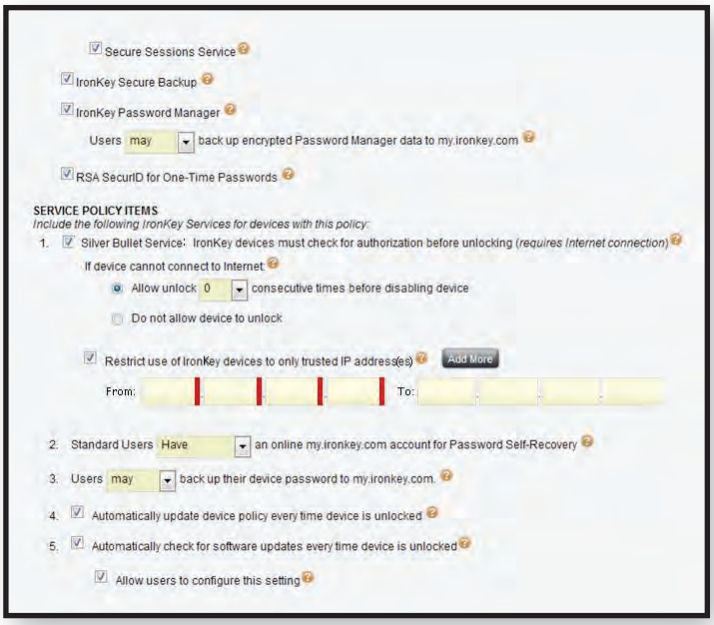
Additionally, users can scan a host computer using the Malware Scanner on the IronKey device.

Active malware defenses enable you to limit the use of IronKey devices to only trusted networks as defined address ranges.

IronKey devices will not function without secure and digitally signed and verified firmware and software.

Restricting Use to Trusted Networks

The IronKey Silver Bullet Service, which enables remote control of flash drives in the field, allows administrators to set policies regarding where a device can and cannot be used. This typically involves creating a whitelist of trusted networks as defined IP address ranges that you trust. For example, you can establish your corporate network block as a trusted network, which will allow workers inside the firewall to use an IronKey anytime. However, when working from home they will be prevented from unlocking the device unless the PC is connected to the VPN or otherwise connected to a trusted network.



Guarding Against Keyloggers and Screenloggers

The IronKey Virtual Keyboard can be toggled for IronKey applications as well as PC-based applications. It thwarts keyloggers by enabling users to click out their passwords instead of typing them out. The IronKey Virtual Keyboard has additional security countermeasures to protect against screenlogging spyware, including keyboard randomization and automatic keyboard-clearing on mouse events, which is the point where screenlogging software typically grabs the screenshot.

To prevent fraudulent updates, all firmware and software is validated in hardware using 2048-bit RSA digital signatures.

Malware-protected Software and Firmware Updates
IronKey devices can be updated remotely via a secure update service. To prevent fraudulent updates, all firmware and software is validated in hardware using 2048-bit RSA digital signatures. Making sure that all code is signed before allowing an update prevents the installation of malicious software or firmware onto IronKey devices.

Read-Only Unlock Mode
IronKey allows an end-user to unlock a device in read-only mode. This approach prevents malware from infecting a device when used on an untrusted computer because, by making it impossible to write data, malware cannot jump from an infected host computer to the drive. Administrators find this feature particularly useful when using an IronKey flash drive as a portable tool belt for anti-virus maintenance. For example, when a machine is not trusted, the IT person can unlock the IronKey in read-only mode and use the onboard tools to clean the computer without risking the drive becoming infected in the process.

Read-only Mode protects against infections and data compromises.

Secure Manufacturing Processes
Unlike many computer hardware products that are manufactured in offshore, uncontrolled factory environments, all IronKey devices are designed and assembled in the USA, which dramatically reduces the risk of hostile factories implanting malware onto silicon or memory chips during the manufacturing process.

Secure Provisioning and Quality Assurance Processes
IronKey devices will not function without secure and digitally signed and verified firmware and software. These software and firmware images are developed, security scanned, anti-malware scanned, and digitally signed at IronKey premises in the USA. All IronKey devices are inoperable until they are loaded with verified and scanned software and firmware from IronKey headquarters. This provides a security validation that is unmatched in the industry, ensuring that IronKey devices have not been tampered with in the manufacturing or supply chain process.

Over 100,000 customers trust IronKey to protect their data.

Summary

Top-Tier US-Based ASIC Security Processor Design Team

IronKey's continued innovation in the areas of intelligent security processors on very small form-factor portable storage devices—particularly USB flash drives or memory sticks—allows IronKey to deliver the world's most secure flash drive with intelligent on board anti-malware and anti-crimeware technology. IronKey has a top-tier ASIC security processor design team that develops the world's most secure, intelligent security processors for secure storage and authentication. The integration of intelligent security processors into standard USB flash drive formats provides affordable, easy to use, and effective protection against data loss, data leakage, and malware for enterprise and government customers.

IronKey Anti-Malware Initiative

IronKey is dedicated to preventing cyber-criminals from gaining access to corporate and government networks. We recently launched the industry's most comprehensive anti-malware initiative (www.ironkey.com/anti-malware) for protecting removable storage media. It includes ongoing research and development of hardware-based defenses against malware and crimeware.

FIPS VALIDATED 140-2

Designed & Assembled in the USA

CONTACT US:

www.ironkey.com
sales@ironkey.com

5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA

T 650 492 4055
F 650 967 4650