



Heidi Rosenberg
Nadel Phelan, Inc.
+1-831-440-2405
heidi@nadelphelan.com

IRONKEY AND TRESYS DELIVER COMPREHENSIVE SOLUTION FOR MALWARE PROTECTION ON USB STORAGE DEVICES

*Integration of Data-at-Rest and Device Sanitization Solutions
Delivers Unprecedented Malware Protection to Mission Critical Environments*

LOS ALTOS, Calif., Aug. 18, 2009 – IronKey, maker of the world’s most secure flash drives, and Tresys Technology, a provider of technology and services for customers with high security requirements, today announced the integration of IronKey’s FIPS 140-2 Level 3 validated secure flash drives with Tresys’ FiST (File Sanitization Tool). This integration provides end-to-end protection for USB devices and data without fear of corruption by common viruses or highly targeted malware attacks.

USB flash drives play a critical role in data sharing across networks that include the U.S. Government and its coalition partners. Recent cyber attacks have used USB devices to propagate various forms of advanced viruses and malware across these systems and networks and the potential exists for additional attacks via USB connections. As a result, their use has been restricted and even banned in some environments.

IronKey’s family of intelligent encrypted USB devices delivers the most secure data-at-rest solutions on the market. Always-on hardware encryption safeguards the most sensitive data on the USB device, ensuring that only authorized individuals have access. IronKey’s active malware defenses start with a trusted supply chain and maintain cleanliness with clean AutoRun protection, Read-only mode and trusted network restrictions.

Tresys’ FiST is an appliance-based kiosk that accesses a USB device and its data in a virtual, controlled and isolated environment to safely handle malicious content without the risk of infecting either the kiosk or other USB devices. FiST conducts deep content inspection and analysis and detects, removes and stores (for forensic analysis) malicious hidden content, viruses and malware from USB devices. In addition, the kiosk includes a simple, single-purpose user interface, secure erasure of USB devices and software for forensic capture.

“Combining IronKey and Tresys technologies provides a secure second source for validating that IronKey devices are free from malware,” said Steve Ryan, senior vice president of business development at IronKey. “The risk of data compromise on the flash drive itself and the risk of introducing or propagating malicious instructions into an environment via a USB device are now obsolete and can be verified prior to any use on PC’s and networks. With this integration of IronKey and Tresys, users can be completely assured and confident that it is safe to use IronKey devices to move data between highly secure computers and networks.”

“Tresys Technology was founded on the premise of solving the most complex security challenges through innovation and the implementations of advanced security technologies for practical use,” said Gary Latham, executive vice president at Tresys Technology. “By integrating our offering with IronKey’s secure line of USB devices, we are able to provide customers with a complete solution to protect against cyber threats. This integration provides end-to-end protection for USB devices and their data without fear of corruption by common viruses or highly targeted malware attacks.”

About IronKey

IronKey's award-winning products and services combine the world's most secure flash drive with the world's most powerful USB management software. IronKey's USB flash drives bring the power of authentication, encryption, identity management and privacy to businesses and consumers in 23 countries. IronKey's management software and associated services allow enterprises of all sizes, government agencies, the military, and other organizations to take back control of the mobile data that has been leaking out of their organizations due to the uncontrolled proliferation of USB drives. With IronKey, organizations centrally administer, remotely manage, and enforce policies on thousands of devices located anywhere in the world. Thousands of customers, including Fortune 500 companies, government agencies, military organizations, banks, healthcare providers and law firms that handle some of the most sensitive security information in the world trust IronKey to protect business critical data. All IronKey products are FIPS 140-2 validated. For more information, please visit www.IronKey.com.

About Tresys Technology

Tresys innovates and applies advanced technologies to quickly solve the needs of customers who require agility and responsiveness to meet their security requirements. Leveraging secure open source software, our products and services support the most sensitive security missions around the world. As a result Tresys enjoys a distinct reputation for shifting the way governments and businesses approach security. For more information, visit: www.tresys.com.

#