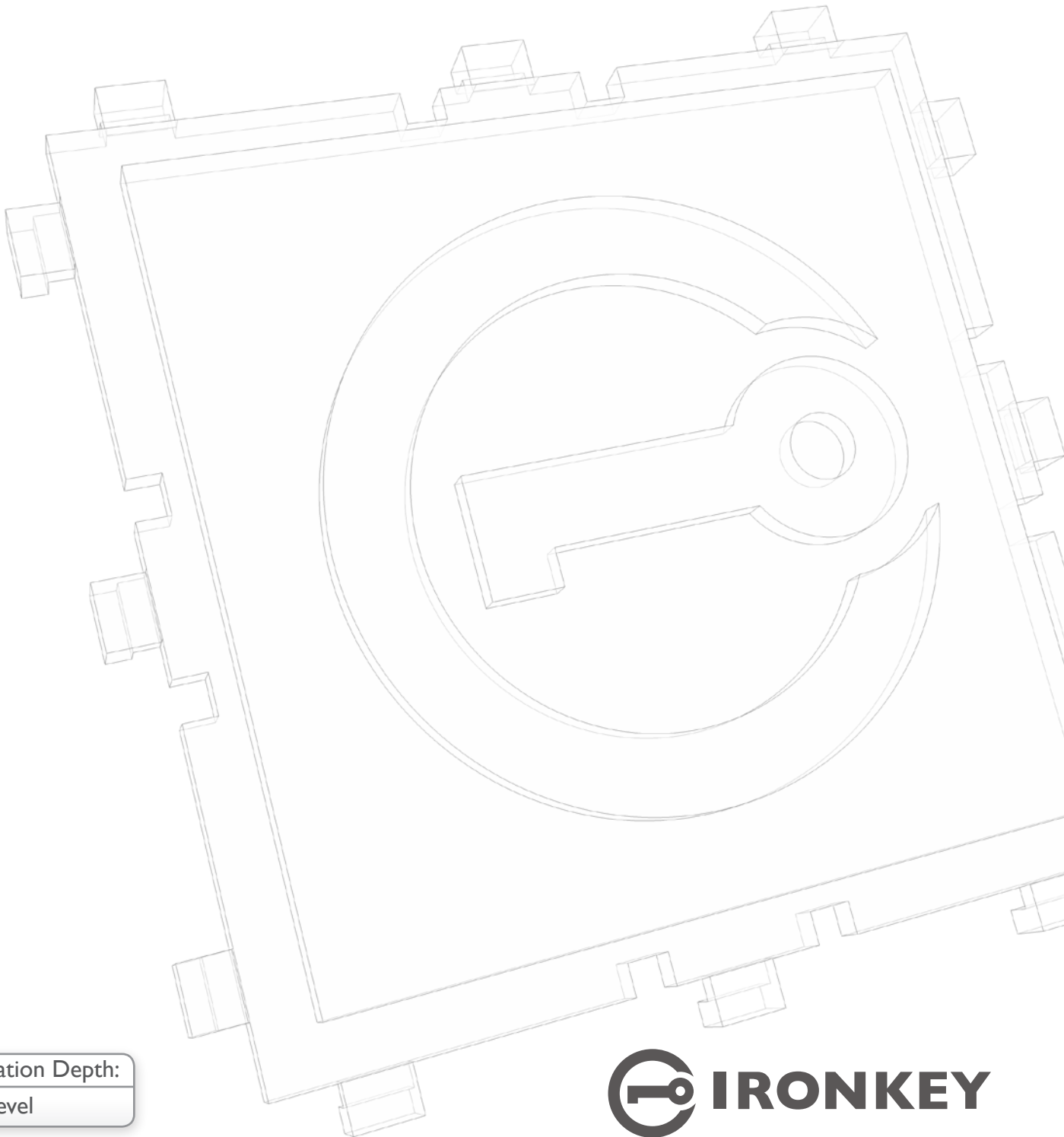


Benefits of Secure USB Flash Drives

An IronKey Whitepaper
September 2007



Information Depth:
High-Level



For more technical information, please see the whitepaper: *“Benefits of Hardware-Based Encryption.”*

78% of surveyed business professionals said USB flash drive are an organization’s greatest IT threat².

72% of surveyed decision-makers said that data loss from USB flash drives is their top endpoint security concern⁴.

Traditional flash drives are missing important security features, such as hardware encryption and authentication.

Introduction

According to industry analyst Gartner, over 100 million USB flash drives were sold in the last year¹. With 86% of recently polled IT executives saying that USB flash drives are used at their companies to store data and exchange it between computers², and 65% of polled IT managers saying that they use USB flash drives on a daily basis³, it is clear that USB flash drives have become an integral part of the corporate IT environment. USB flash drives are widely used for:

- » Backing up laptops
- » Allowing employees to carry work or email from office to home
- » Carrying sales presentations
- » Copying patient records and legal documents
- » Moving company files between computers

Without proper security controls, this proliferation of removable media devices increases the risk of loss or theft of important corporate data. Unprotected USB flash drives have become the new and greatest IT threat to organizations, according to 78% of surveyed business professionals in a variety of industries².

Security Concerns Regarding USB Flash Drives

The USB flash drive’s widespread usage and utility make it highly likely that it will remain a versatile tool in corporate environments for years to come. However, without additional security measures, unprotected flash drives have the potential to violate corporate security policies and to provide a means for data leakage and disclosures.

Additional studies support these concerns about the security of USB flash drives. In November 2006, Forrester Consulting fielded a commissioned online survey of 151 decision-makers at North American companies⁴. Respondents had specific responsibilities for information security and/or data security policy and strategy at companies with annual revenues of more than \$200 million, and 59% of the respondents came from enterprises with more than \$1 billion in revenue. Here are some of the findings from the survey:

- » More than half of respondents (52%) have lost confidential data through removable media such as USB drives in the past two years.
- » Data loss prevention is a major priority for nearly all respondents (95%).
- » Intellectual property, customer data and company financials are the top three concerns for data loss at the endpoint.
- » Data loss via USB drives and other removable media is the top concern (72%) for endpoint security, followed by Trojans, spyware and other threats.

These concerns are due in large part to the fact that traditional USB flash drives have not been designed with security in mind. Flash drives are missing a number of essential security features that are becoming increasingly important for today’s enterprises, for example:

- » The data is not encrypted, and so it can be seen by others
- » If it includes an onboard software encryption program, the protection is usually not enforceable and can be circumvented by malware (see IronKey’s whitepaper *“The Benefits of Hardware-Based Encryption”* for more information).
- » Access to the device does not require any authentication, which means anyone who has the device can access the unencrypted data

These security threats, which traditional flash drives do not protect against, could lead to serious financial repercussions and can inhibit compliance with many regulatory requirements such as Sarbanes-Oxley, HIPAA and GLBA. Examples show up in the news on a regular basis, such as:

In July 2007, a man was accused of 16 felony counts of first-degree computer trespassing for putting highly sensitive files onto a USB thumb drive and trying to leak them to newspaper reporters⁵. He allegedly stole documents that could cost Boeing \$5 billion to \$15 billion in potential damages if they fell into the wrong hands.

Flash drives present a significant security challenge for large organizations. Employing additional security measures, such as encrypted USB flash drives, can be an important factor in preventing unauthorized access to, transfer of, and loss of corporate data.

Corporate Brand Concerns Regarding USB Flash Drives

Potentially just as damaging as the security breach is the impact to a company's reputation should customer data be lost or stolen on a USB flash drive. In fact, in a survey of 323 IT managers and top executives, 79% of respondents stated that every day they work with data that, if lost, would require their organization by law to publicly notify potential victims⁶. California companies are subject to SB-1386 regulations, which require notification of consumers should their data be disclosed. Similar legislation is being enacted in other states and is being considered at a federal level.

There have been numerous high-profile cases where a lost or stolen flash drive contained sensitive information, tarnishing an organization's brand. Here are just a few from recent months:

In June 2007, an intern at the State of Ohio government took home a USB device with the personal information of more than 60,000 state employees and 225,000 taxpayers on it⁷. The intern left this device in his car, where it was promptly stolen.

Also in June, a professor at Texas A&M University-Corpus Christi lost a USB flash drive containing the personal information, including social security numbers and birth dates, of about 8,000 students⁸. He was vacationing in Madagascar and brought the USB flash drive with him to do some work while on vacation.

Lost flash drives are not only a problem for companies, but also for government agencies and the military:

In January 2007, a soldier from Tennessee lost a flash drive containing personal videos while on duty in Iraq⁹. Somehow that unencrypted flash drive ended up in enemy hands, and the video resurfaced on Iraqi TV, heavily edited into fake propaganda.

Also in January, a USB stick containing confidential information about the Dutch Embassy in Warsaw including the secret entrance codes to a diplomat's home and the names of bodyguards has been left in a rental car and is now in the hands of the Volkskrant newspaper¹⁰.

Such security breaches could have been prevented had the USB flash drive had built-in security features, such as encryption and authentication.

Benefits of Hardware-Encrypted USB Flash Drives

Since USB flash drives are an important and highly useful tool for most organizations, standardizing on secure USB flash drives with hardware encryption will alleviate many of the security concerns discussed in this document.

A good example of a flash drive that provides both hardware encryption and device authentication is the IronKey Secure Flash Drive. All data written to these devices is protected from loss or theft by military-grade encryption and strong password protection. The IronKey has been designed from the ground up with security in mind and not as an afterthought, a key differentiator between it and other secure flash drives on the market.

Regulations such as SB-1386 require many organizations to publicly notify clients when a data loss occurs.

Lost flash drives are also a concern for government agencies and the military.

IronKey Secure Flash Drives offer military-grade encryption & strong password protection.

IronKey's hardware encryption is always on and cannot be disabled or tampered with.

IronKey devices do not require any software installations or device drivers to work.

IronKey devices work with a number of end-point security software systems.

Find more information about IronKey online at: www.ironkey.com

IronKey, Inc.
5150 El Camino Real, Suite C31
Los Altos, CA 94022 USA
+1 (650) 492-4055
info@ironkey.com

Hardware-encrypted flash drives utilize an additional cryptographic processor chip that performs the encryption "on-the-fly", ensuring that data is protected without requiring user intervention. IronKey's implementation of this technology ensures that data encryption is always on and cannot be disabled by the user or by malware.

IronKey Secure USB Flash Drives deliver the industry's most secure and easy-to-use solution:

- » Hardware encryption ensures high-speed transfer of large files
- » No software or drivers need to be installed on any computer
- » Users do not need administrator privileges on Windows XP or Windows Vista
- » Password protection is implemented in hardware, preventing brute-force password guessing attacks
- » Offline cryptographic attacks are prevented
- » Rugged tamper-resistant and waterproof metal case

IronKey devices can also be used in conjunction with endpoint security software installed on your computers and laptops. This ensures that only approved IronKey hardware encrypted drives can be used on your computers.

Conclusion

USB flash drive will remain an important tool in corporate environments for years to come. However, without additional security measures, unprotected flash drives can provide a means for data leakage and disclosures, and thus violate corporate security policies and regulatory requirements. The IronKey Secure Flash Drive provides a secure means for organizations to store and transport data, alleviating many of the concerns created by traditional USB flash drives.

To learn more technical detail about IronKey's hardware encryption capabilities, and why it is more secure, easier to use and offers higher performance than software encryption, please read our whitepaper "Benefits of Hardware-Based Encryption" found at <https://learn.ironkey.com>.

References

1. "USB flash drives get to work." TechWorld. Aug. 26, 2006. <http://www.techworld.com/storage/features/index.cfm?featureid=2772>
2. "Survey Says: iPods and Other Portable Storage Devices Are a Growing Threat for Data Leakage in the Workplace", Credant Technologies. July 23, 2007, <http://www.credant.com/content/view/290/105/>
3. "Thumb Drives Replace Malware As Top Security Concern, Study Finds", InformationWeek, May 7, 2007, <http://www.informationweek.com/security/showArticle.jhtml?articleID=199300021>
4. "Data Loss Prevention and Endpoint Security", Forrester Consulting and Vontu, Jan. 29, 2007. http://www.vontu.com/news/releases/575_release.asp,
5. "Ex-Boeing worker accused of downloading documents and leaking to reporters", Seattle Times, July 10, 2007, http://seattletimes.nwsource.com/html/localnews/2003783055_webboeing10m.html
6. "Survey Says: iPods and Other Portable Storage Devices Are a Growing Threat for Data Leakage in the Workplace", Credant Technologies. July 23, 2007, Page 6. <http://www.credant.com/content/view/290/105/>
7. "Stolen Backup Device Holds Info On 225,000 Ohio Taxpayers", InformationWeek. June 21, 2007. <http://www.informationweek.com/security/showArticle.jhtml?articleID=199906138>
8. "Identity theft may be problem for TAMUCC students", KRISTC.com. June 16, 2007. http://www.kristv.com/Global/story.asp?S=6667387&nav=menu192_2
9. "Soldier's Lost Data Used in Fake Video", IdentityTheft911. Jan. 9, 2007. <http://www.identitytheft911.org/alerts/alert.ext?sp=835>
10. "Civil service USB stick found", DutchNews.nl. Jan. 23, 2007. http://www.dutchnews.nl/news/archives/2007/01/civil_service_usb_stick_found.php

The information contained in this document represents the current view of IronKey on the issue discussed as of the date of publication. IronKey cannot guarantee the accuracy of any information presented after the date of publication. This whitepaper is for information purposes only. IronKey makes no warranties, expressed or implied, in this document. IronKey and the IronKey logo are trademarks of IronKey, Inc. in the United States and other countries. All other trademarks are the properties of their respective owners. © 2007 IronKey, Inc. All rights reserved. IK0030270