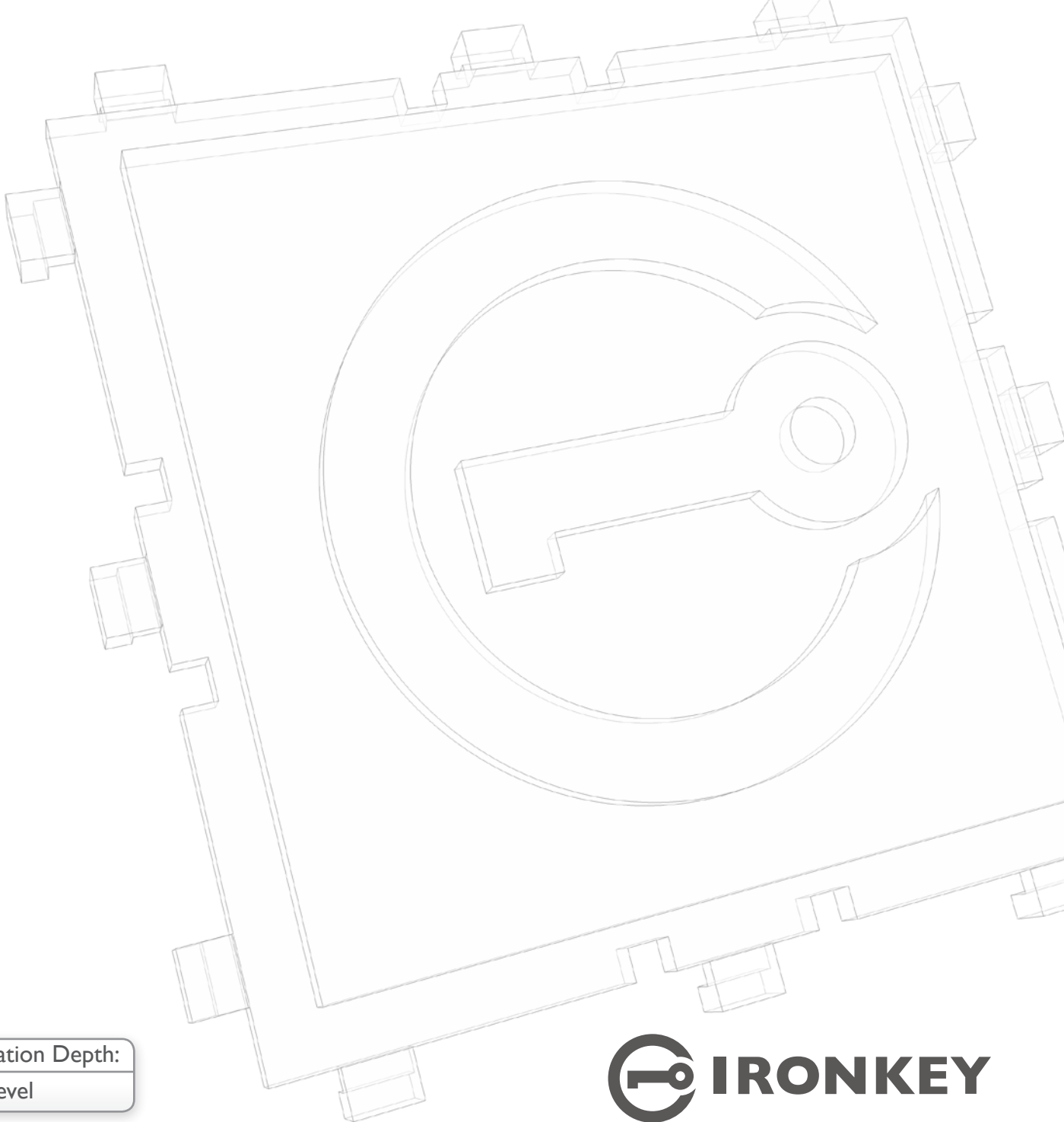


Enterprise Security and Management of IronKey USB Devices

An IronKey Whitepaper
October 2007



Information Depth:
High-Level



75% of Fortune 1000 companies fell victim to data leakage in 2006, with an average recovery cost of \$5,000,000⁴.

Also see IronKey's whitepaper on "The Benefits of Hardware-Based Encryption" for more information about IronKey devices.

Today's enterprise IT administrators face a number of challenges in managing an enterprise's portable data devices.

Introduction

Enterprise security managers' concerns about the security of USB flash drives continue to grow. Over 250 million USB flash drives were sold in the last three years¹. With an average storage capacity of approximately one gigabyte, these devices represent one of the most difficult to control and potentially costly security risks today's organizations face. A recent survey¹ of 300 United Kingdom IT professionals found that on average 31% of employees within a company are using USB flash drives in the office. Two-thirds of IT professionals who used the devices at work (employees who certainly ought to understand these risks) admitted that they did not protect them with encryption even though they were aware of the associated dangers². Uncontrolled usage of portable data storage devices has resulted in real-world repercussions, as approximately 75 percent of Fortune 1000 companies fell victim to data leakage in 2006³, with an average cost of recovery that exceeded \$5,000,000⁴.

IronKey Secure USB Flash Drives represent one of the most secure and easy-to-use solutions to the problem of physical USB device security. However, physical security of USB flash drives is only one issue IT managers face. With thousands of flash drives being used in an organization, managing the usage and policies of devices presents an equally significant challenge.

Common Concerns Among Enterprise Security Managers

Figure 1 visually represents common areas of concern that are unique to enterprise management of portable data devices.

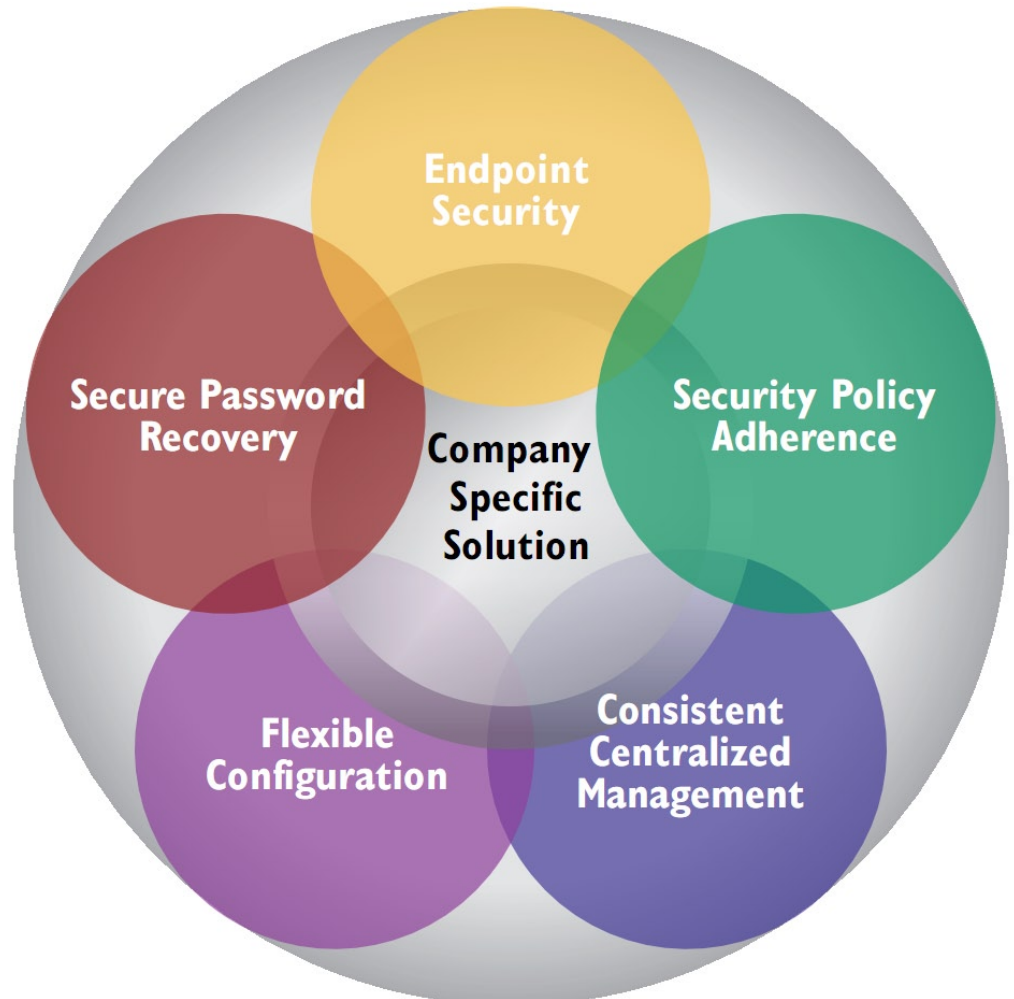


Figure 1. Management Requirements of Portable Data Devices in Enterprises

Endpoint Security

The data on portable storage devices should ideally be protected from a myriad of known attacks, regardless of whether the device is being used correctly by its assigned owner or being tampered with by an intruder. The devices must also integrate easily with endpoint security software that authorizes which devices can be safely integrated with the existing network or PC.

Security Policy Adherence

Portable devices must reside under and support the organization's existing security policy umbrella. This means that data access must be controlled by the same password policies and external devices must be subject to the same on-the-wire security policies.

Secure Device Recovery

Even if an enterprise's portable devices have been secured against a multitude of potential attacks, a forgotten password to a specific device could render the device inaccessible and result in loss of critical company information if there is not a secure means for device recovery. Examples also include accessing data on the device when an individual is no longer with the organization and changing the device owner's password for repurposing the device.

Since forgotten passwords constitute upwards of 30% of all help desk requests⁵, data loss due to a forgotten password is a potentially significant problem for enterprise IT managers. However the ability to recover forgotten passwords carries its own set of security risks, and ensuring proper authentication, authorization and access are crucial. For example, even with military-grade device security, a disgruntled insider could gain access to the data on all of an organization's flash drives if the passwords are stored in a central database for administrators.

Flexible Configuration

How endpoint devices may be used needs to be subject to policies and processes unique to a specific organization. Security managers must be able to control what software can be used on specific devices, how that software is configured for use. Equally important, the IT organization must control who is allowed to administer which policies on which devices.

Consistent, Centralized Management

The flip side of flexible configuration is consistent management, and the two sides represent a balance of competing needs:

- » The need to ensure that a minimum set of security standards can be established and automatically enforced across an entire group of portable devices.
- » The need to allow flexible implementation to conform to the policy of a specific user group.

With multiple groups using portable devices throughout an organization (e.g. divisions, departments, teams), consistency of device policies becomes a critical concern. If a company has a seven character minimum for password length, then an enterprise administrator must be capable of enforcing that policy across all departments within their span of control.

Another aspect of consistent management involves cost. Consistent management is ineffective if the cost of administration is too high to make it practical. With hundreds or thousands of devices in a given user group, device management must have a centralized control console. Provisioning cannot be practically handled by already overburdened IT staff. Simple, yet secure self-provisioning of devices by end users is a practical solution for this issue.

Forgotten passwords (more than 30% of all help desk requests⁵) could result in data loss if the password was to an encrypted flash drive.

IT administrators need to balance system configuration with ease-of-use, cost, and consistent policy enforcement.

IronKey: Enterprise Edition

To deal with these issues, IronKey has developed the IronKey: Enterprise Edition, which provides an easy-to-use, scalable and secure solution for enterprise IT managers to customize the IronKey devices for their organizations. Available as a managed security service, it reduces deployment costs and enables global rollout to anyone with Internet access.

The IronKey: Enterprise Edition includes all the security features of the standard edition of the IronKey Secure Flash Drive, and more.

Unique Features of the IronKey: Enterprise Edition

IronKey developed the Enterprise Edition to specifically address the concerns IT managers have about managing thousands of IronKey USB flash drives, potentially deployed in hundreds of locations around the world. The Enterprise Edition builds on top of the core feature set of the IronKey Secure Flash Drive, which includes:

» **Hardware Encryption of Flash Drive Data.**

All IronKey flash drives have high-speed hardware AES encryption that protects all data stored on the device. No software or drivers need to be installed and no local administration rights are required.

» **Hardware-Based Device Password Verification.**

To unlock an IronKey device, the user must enter their device password. This is verified in hardware by the IronKey. If a user enters the incorrect password too many times, the device self destructs by erasing all the user's encrypted data.

» **On-Board Cryptographic Authentication.**

The IronKey is pre-configured with a unique cryptographic key that is pre-installed during manufacturing. This can be used for strong authentication to enterprise websites. Developers can also access the device's cryptographic functions for custom applications by using IronKey's PKCS#11 interface.

The Enterprise Edition introduces the following new technologies and features:

» **Centralized Device Management via an Online Service.**

IronKey: Enterprise Edition has a straightforward and cost-effective interface for managing tens, hundreds or thousands of devices through a centralized management console. The Admin Console is delivered as an on-line service, reducing overall deployment times and maintenance requirements. The service-based offering also scales easily as more IronKeys are deployed.

» **Creation & Enforcement of Corporate Password Policies on the Device.**

IronKey: Enterprise Edition allows you to configure policies for device password strength through the central Admin Console.

» **Configuration of IronKey Applications and Services.**

You may configure which on-board IronKey applications and services are enabled for your users. You can allow or prohibit the use of the on-board Mozilla Firefox web browser, the IronKey Password Manager, IronKey's Secure Sessions (secure web surfing service), and IronKey's encrypted online password backup services.

» **Creation and Enforcement of Self-Destruct Policies.**

IronKey: Enterprise Edition allows you to configure the number of times a password can be entered incorrectly before the self-destruct feature is activated.

» **A Secure yet Practical Method for Unlocking Employee Devices.**

IronKey: Enterprise Edition provides you with a secure mechanism for recovering device passwords for regulatory compliance or in the case of termination.

» **Flexible Configuration of Administrative Roles and Privileges.**

Adding and managing enterprise administrators is simple. Centrally grant and revoke the ability for administrators to establish device policies and the ability to recover the end user passwords.

» **Self-Service Device Policy Provisioning.**

Administrators can choose to allow users to provision their own devices, thus avoiding a device deployment headache for the IT staff. After an administrator

identifies which users will receive an IronKey, an email with an activation code is automatically sent to each new user. Users enter that activation code into their IronKey upon initialization, and, once the activation code is verified, the device downloads its policy and walks the user step-by-step through the device setup process.

» **Integration with Endpoint Security Systems.**

IronKey: Enterprise Edition has been designed to integrate seamlessly with many of the industry's leading endpoint security software products. Additionally, every IronKey has a unique serial number and product ID, making it easy to manage and apply usage policies within endpoint security solutions.

Secure Device Recovery

The ability to securely access and recover your organization's devices is one of the strongest benefits of IronKey: Enterprise Edition. Other devices on the market use backdoor passwords (a common password that will unlock all devices) to gain access to a device when the user has forgotten the primary password for that device. But backdoor passwords represent a number of unwarranted security risks:

- » Backdoor passwords can be guessed and brute-force attacked.
- » Securely managing a database of backdoor passwords is difficult – one or more administrators have easy access to every device's password.
- » Backdoor passwords make it difficult to revoke administrator privileges because the password remains valid regardless of whether an administrator has been terminated or not.
- » Backdoor passwords are subject to password replay attacks

IronKey has taken a unique and much more secure approach. IronKey: Enterprise Edition uses a special recovery tool and patent-pending PKI-based device recovery to ensure that devices can be recovered without using a backdoor password or allowing anyone other than the device's owner to see the device password. Moreover, administrators can gain access to an IronKey from their organization that has been abandoned (e.g. by a former employee who is no longer available) or previously lost.

To do this the Enterprise Edition strongly encrypts the device password in such a way that only that specific enterprise can decrypt it. Additionally, it encrypts it again so that only an approved administrator's IronKey can decrypt it. That way, unlocking a device requires that you:

1. Are an active administrator with appropriate privileges in the correct enterprise
2. Have full access to an approved administrator's IronKey

This approach removes the threats associated with revoked administrators, backdoor passwords, and other forms of unauthorized access to user passwords. Additionally, this technique maintains IronKey's standard for ensuring that IronKey and its employees cannot access your enterprises' devices.

This entire process has been designed to be the most secure way for administrators to recover their users' secure flash drives. It leverages the power of the IronKey Cryptochip for hardware encryption and relies on the integrity of known, trusted and proven cryptographic algorithms, including AES, RSA, and SHA.

The Benefits of a the Managed Security Service

The IronKey: Enterprise Edition works with the IronKey online service to allow administrators to manage their devices without having to install and integrate complex enterprise software. The benefits of device management as a service include:

Unlike systems that rely on backdoor passwords to recover devices, IronKey's services rely on strong, proven cryptographic algorithms.

IronKey's Secure Device Recovery removes the threats associated with revoked administrators and backdoor passwords.

IronKey's enterprise services can ease the burden on IT staff without straining end-users with complicated software.

» **Easy to Trial and Deploy.**

There is no complex enterprise software to purchase and install. IronKey: Enterprise Edition's online device management is straightforward to pilot, test and roll-out.

» **Activate IronKeys Anywhere, Anytime.**

If an enterprise installs a management tool on its network, it can be difficult to manage USB flash drives that are used on remote networks. USB flash drives are typically employed to move data between networks and are often used outside of the enterprise's main corporate Intranet. For example, many USB flash drives are used from home networks, remote offices, wireless access points and third-party intranets. Because IronKey's secure management servers are available on the Internet, administrators can manage devices no matter where they are used, using two-factor authentication that does not require a VPN connection back to an internal enterprise server.

» **Scalability.**

As a hosted service, IronKey: Enterprise Edition scales as your organization grows and changes. It is equally well suited for large enterprises as it is for small and medium businesses.

» **Ability to Deploy New Services.**

IronKey's online service is available to any Windows XP or Vista computer* with Internet access. It allows IT administrators to reliably deploy new features as they are rolled out.

» **Reduced Cost of Ownership.**

IronKey's IT staff ensures that the service is online 24x7**. They are constantly managing network performance and availability. The team also manages service upgrades and the rollout of new features. All of this reduces the burden of IT administrators and the total cost of ownership of the managed solution.

The IronKey: Enterprise Edition has been designed from the ground up with security in mind (*secure by design*).

The Security Architecture of the Enterprise Managed Service

The IronKey: Enterprise Edition has been designed from the ground up with security in mind:

» **Network Security of the Service.**

IronKey's enterprise services have been designed by security architects with a background in managing the security of banking and payment systems. Best practices are used in network design, firewalls, IPS, event monitoring and cryptographic key management. All access to the systems is through two-factor authenticated encrypted communications.

» **Hardware Cryptographic Authentication of Devices to the Service.**

All user and administrator IronKey devices authenticate themselves to the management service with on-board hardware encryption. This allows the service to ensure that administrators and users are authenticated and have the appropriate permissions.

» **Encryption of All Communications with the Service.**

All communications with the service are encrypted and strongly authenticated to mitigate spoofing, man-in-the-middle, phishing and pharming threats.

» **Anti-Phishing Technology.**

User and administrator accounts have the latest anti-phishing technologies to authenticate users, including two-factor cryptographic mutual authentication, shared secret images, shared secret questions and device fingerprinting.

» **Cryptographic Architecture of Secure Device Recovery.**

Unlike "backdoor password" systems, the IronKey device key recovery system uses strong public-key cryptography to encrypt and recover device passwords.

* Note: Mac OSX and Linux support in development.

** Note: 24x7 uptime as defined in IronKey's Service License Agreement

Secure Device Recovery is designed so that there is no way for IronKey or its employees to unlock your enterprise's devices.

Encryption methodologies (which require both the appropriate administrator and the IronKey server to unlock a user's IronKey) enable the management server to revoke administrator recovery abilities, mitigating the threat of rogue administrators. Replay attacks are similarly prevented. This approach also prevents the single-point of failure issues that can result from backdoor-password approaches. Finally, only administrators with authorized administrator IronKey devices can recover device passwords – there is no way for IronKey or its employees to unlock devices or recover device passwords.

» **Secure Cryptographic Key Management.**

The IronKey online service uses FIPS compliant Hardware Security Modules (HSMs) to manage encryption keys, preventing theft or cloning of the keys. The system is architected that even if these keys were compromised, it cannot compromise the security of enterprise devices.

Conclusion

The security experts at IronKey have gone to extreme lengths to ensure that the IronKey: Enterprise Edition meets the common security, deployment, and usability/maintenance needs of IT managers demand, while maintaining the overall security of the IronKey enterprise services at the same unmatched level as the IronKey hardware.

If you should need more technical information than is provided in this whitepaper, please contact your IronKey representative.

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>.

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

References

1. Unworth, Joseph. "Forecast: USB Flash Drives, Worldwide, 2001-2011", Boston: Gartner/Dataquest, October 2007.
2. Pointsec as quoted in *Outlaw News*, June 13, 2005.
3. 2006 CSI/FBI Computer Crime and Security Survey, http://li.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
4. Ponemon Institute, 2006 Cost of Data Breach Study, http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf
5. Marianne McGee, "The Top Reason Users Call the IT Help Desk", InformationWeek, March 1, 2007, <http://www.informationweek.com/news/showArticle.jhtml?articleID=197700628>. Also ContactCenterWorld, January 15, 2003.

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. IK0039084