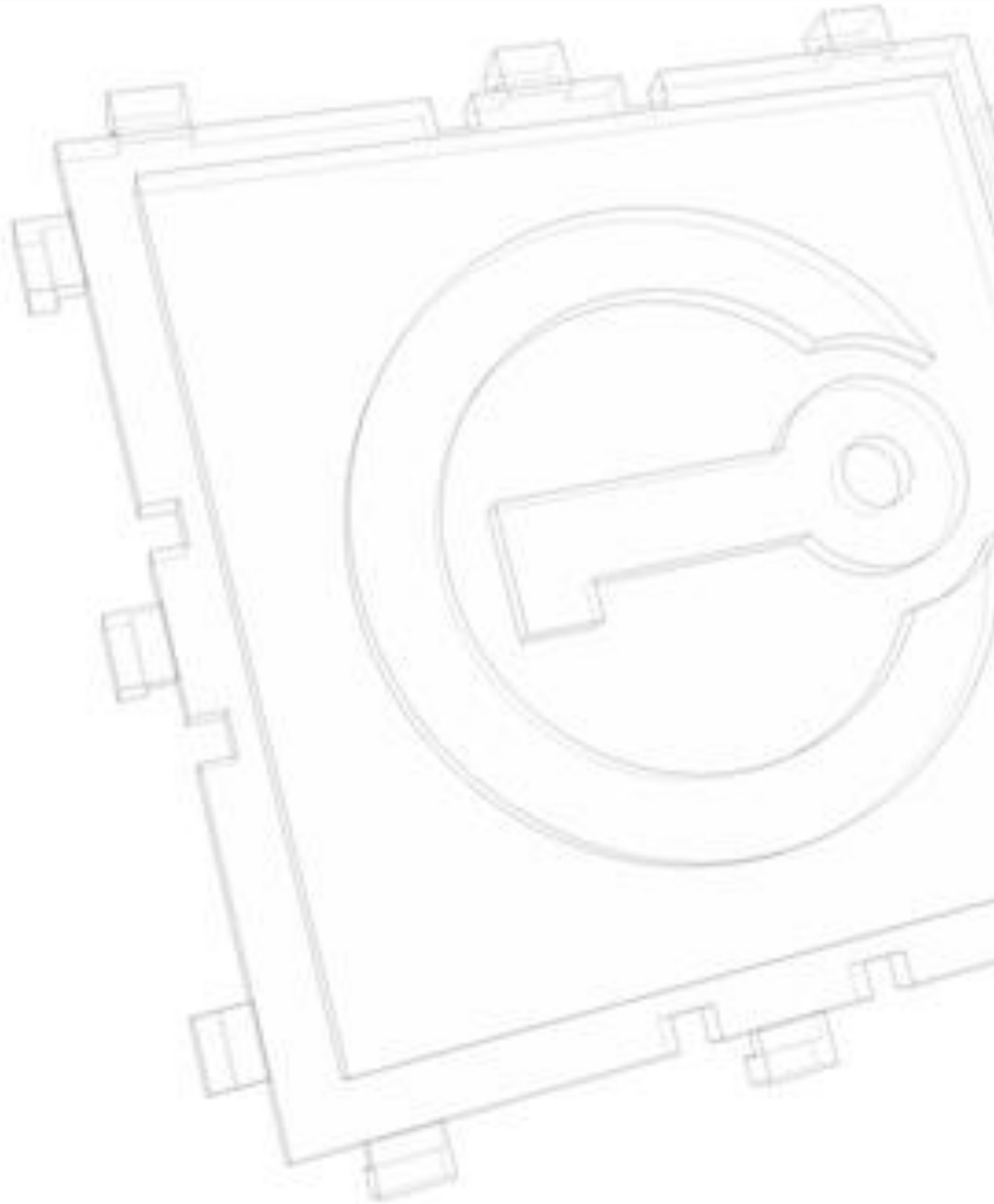


# IronKey Silver Bullet Service Business Brief

Disable or Terminate Rogue USB Drives—with Extreme Prejudice



# IronKey Silver Bullet Service

## Disable or Terminate Rogue USB Drives—with Extreme Prejudice

Owing to their grass roots popularity among end users, USB flash drives, also known as thumb drives and memory sticks; have rapidly become ubiquitous throughout business and government. Over 85 million of these devices were sold in 2007. However, while workers may be enamored with the convenience, portability and low cost of these devices, IT security professionals increasingly recognize the risks they pose. Encryption provides a first line of defense against data loss from flash drives, but it is not enough. Larger organizations require an enterprise approach to securing confidential data on flash drives, which includes centralized management and policy-based control of devices in the field. These controls—together with encryption—can provide effective protection against malicious and careless users.

**“39%** of enterprise users have lost flash drives or laptops and **72%** have failed to report the lost device promptly.”

IronKey has spent years researching and developing the world’s most securing USB flash drive. Recognizing the needs of the enterprise, IronKey has enhanced this data protection with the industry’s most advanced management environment. A key component is the IronKey Silver Bullet Service™—the only remote *deny, disable, destruct* capability for managing USB flash drives over the Internet.

**A Gartner research study found that 22 % of USB flash drives are sold to enterprises and about 80–90 % are not encrypted.**

## Beyond Encryption — The Insider Threat

While an IronKey drive provides virtually unbreakable protection against unauthorized access to data stored on the device, authorized users often comprise a significant security risk. These insider threats typically include:

**“26% of enterprise data breaches are caused by malicious insiders**

- Users who write down passwords on a piece of paper and store it in their briefcase with their encrypted drive or write the password on the device itself
- A knowledge worker or executive who quits and takes a job with a competitor but refuses to return their encrypted drive
- A user who is suspected of storing offensive or inappropriate material on an encrypted drive and refuses to divulge the encryption password
- An insider attempting to steal confidential data by removing it from a facility on an encrypted flash drive (thereby attempting to circumvent controls in place on the network)

*Sidebar:*

**“51% of users store confidential information on USB flash drives.”**

### Lock Out Users or Neutralize Drives Remotely

IronKey Silver Bullet Service gives administrators flexible, comprehensive control over drives deployed in the field—inside and outside the firewall.

In the event a drive’s security posture becomes compromised—whether it is lost, stolen or in the possession of a user who has been terminated or deemed an insider threat—the Silver Bullet Service provides several options to prevent access to data on the device. By setting a policy requiring all drives to communicate with the IronKey Enterprise online service before allowing access to data, the administrator can:

**Deny** —Prohibit a user from accessing the files on the IronKey device, even if they know the password. Access to the device is denied until it can verify status with the management service. This prevents an unauthorized user from accessing the data on an IronKey drive unless the user’s status is current and valid.

**Disable** — The next time the device connects to an internal or external network, the

Silver Bullet Service disables the device by locking out the user completely. This disabled state cannot be undone unless the administrator manually changes it back. Generally, this option is used for employee termination, access control change, or even lost/stolen devices (where a destruct is considered too severe an option).

**Destruct** — Instructs the IronKey device to initiate its self-destruct sequence, which destroys the encryption keys and shreds flash memory—using patent-pending IronKey Flash Trash™ technology—so that even the administrator cannot recover the data.

### **How it works**

IronKey Silver Bullet Service is implemented as a security policy in the IronKey Enterprise management system. The administrator can set a policy requiring the IronKey device to validate with the server before allowing the user to log on and access data. Then, the device must call home to the server every time it connects to a network (or as often as the administrator chooses, based on the policy setting). The device asks the service if the user is valid and the server sends a signed response—affirmative or negative. To prevent spoofing and man-in-the-middle attacks, the signed response is verified in hardware on the device. At this point, if the drive has been lost, stolen, or otherwise compromised, the Silver Bullet Service can allow access, deny access, disable the drive, or destroy the data.

**In 2007, 85 million  
USB flash drives  
were sold, but only  
a few of those  
buyers thought  
about the drives'  
security  
implications.**

### **Tracking and Audit**

Administrators often need to have forensic knowledge of device activities or prove that data on a device has been rendered inaccessible. This includes avoiding the costly remediation required by privacy laws such as California's SB1386. The IronKey Silver Bullet Service gives the administrator a provable audit trail showing which machine it connected to before the disablement and where it was physically when it received the command.

**“Customer data stolen by an employee is misused more frequently than data obtained through an external breach.”**

The IronKey Silver Bullet Service provides rich tracking and auditing, which can include confirmation that all data on a device has been deleted (even when the device subsequently self-destructs).

**Conclusion**

Companies and government agencies are rushing to deploy encryption technology to protect against lost and stolen digital assets. Portable storage devices, laptops, smart phones, and flash drives all require encryption, but encryption without adequate management can be a dangerous tool. Malicious or careless insiders can compromise data security with thumb-size devices and inflict billions of dollars in damage. This is why encryption without control is not enough. IronKey extends mobile data protection with important features such as the ability to seek out and disable or destroy rogue devices.