USB Alert:
Locking Down Your Data

While USB drives have revolutionized data transfers, they've also introduced grave security risks. With their extreme portability, USB drives can turn up anywhere and everywhere, from jacket pockets to parking lots—putting data at risk. How can IT deal with these risks, without completely forbidding USB drive usage and all its convenience?

What's the worst that can happen?

USB drives can introduce risk in many ways:

LOST

>22,000 USB drives end up at the dry cleaners each year[1]

FOUND

48% of people who find USB drives plug them in and click on at least one file[4]

STOLEN

A USB drive containing sensitive data for **patients** went missing from a hospital ER[2]

A disgruntled employee used a USB drive to steal banking information for **~30,000 people**[3]

How do IT pros handle USB drive security?

A Spiceworks survey of IT professionals found that while most organizations do consider USB drive security, many have not necessarily nailed it down.[5]

80% of organizations have USB policies

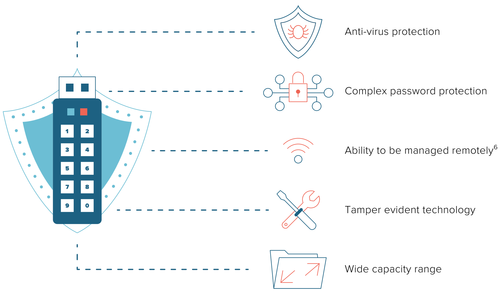
Most common policy: Limit USB drives to specific employees or departments

<20% of organizations with USB drive policies enforce the use of encrypted USBs

Yet, **1/3** of the respondents have experienced a USB drive security threat or breach in the last year.

Encrypted USBs never give up their secrets.

USB drives with encryption can be powerful tools in closing this all-too-common security gap, helping to ensure security and compliance with:



Protect yourself with Kingston.

Kingston's IronKey encrypted USB drives are designed to protect even the most sensitive data using the strictest security regulations and protocols across government agencies, medical providers, and financial institutions.

Want to learn more?

Download the White Paper

Kingston TECHNOLOGY

Sources:

1 Steve Bush, "22,000 USB sticks go to the dry cleaners," *ElectronicsWeekly.com*, January 14, 2016. www.electronicsweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/

2 Taya Flores, "IU Health Arnett reports missing patient info," *JConline*, January 5, 2016. www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/

3 Tom Brant, "Report: FDIC Employees Caused Repeated Security Breaches," *PC Magazine*, July 15, 2016. www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches

4 Elie Bursztein, "Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots," *Elie.net*, April 2016. www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots

5 Spiceworks survey of 300 IT decision-makers in the US, Canada, and Europe, on behalf of Kingston, February 2017.

6 To provide management solutions for its Encrypted USB drives, Kingston Digital has partnered with DataLocker. http://www.kingston.com/us/usb/encrypted_security/management-solutions