DATALOCKER®

DataLocker Inc. | 7007 College Blvd. Suite 240 | Overland Park, KS 66211

DataLocker's motto is "Simply Secure"

To provide easy to use, cost effective, military grade data encryption solutions to enterprises around the world.

Company at a Glance

OUR COMPANY

- Founded in 2007
- HQ in Overland Park, KS with offices in San Jose, CA; Ottawa, Canada; London, United Kingdom; and Seoul, S. Korea
- Acquired BlockMaster in June 2015
- Acquired IronKey, Enterprise Management Service & Hard Drives in February 2016
- Kansas City Chamber of Commerce Top Ten Small Business 3 of last 5 years.

OUR CUSTOMERS

- 70% of the Fortune 100 use DataLocker solutions
- Over 250,000 users worldwide
- Products are sold in over 35 countries
- Key Verticals: Government, Banking and Financial Services
- Sales Model : Channel Focused

OUR PRODUCTS

- DataLocker products are developed and engineered in house
- All products are TAA Compliant, meeting federal and military requirements
- Patented technology – Strong patent portfolio

SHOCKING STATISTICS

51% of users **stored confidential data** on flash drives.[1]

54% of respondents believed that a non-senior management employee of their organization **lost a device** within the last year.[2]

49% said a non-senior management employee had a **device stolen** in the last year.[2]

65% of **lost USBs** never got reported to management.[1]

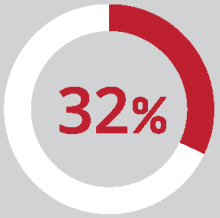
49% of **lost or stolen devices** contained confidential **emails.**[2]

38% contained confidential **files or documents,**

24% contained **customer data,**

15% contained **financial data.**[2]

LACK OF BASIC SECURITY MEASURES



of organizations are **not protecting devices and files** taken outside the office with either encryption or passwords.[2]

admit that the data could be **more adequately secured.**[2]

[1] A 2009 enterprise study by the Ponemon Institute

[2] 500 IT decision makers were interviewed in September 2015. All respondents work in organisations with at least 250 employees. 250 work in the UK, 250 in Germany. The research was conducted by Vanson Bourne. For more information, visit www.vansonbourne.com.

DataLocker Supports & Manages All Your Secure Endpoints

Encrypted Hard Drives

Encrypted Flash Drives

Encrypted Optical Media

Cloud Encryption Gateway

Central Management Platform

ONE COMPANY, 3 BRANDS, STRONG PRODUCT LINE

DATALOCKER®
SIMPLY SECURE

DATALOCKER®

- DL2 Hard Drives
- DL3/DL3FE Hard Drives
- H Series Hard Drives
- Sentry USB
- EncryptDisc
- SafeCrypt

IRONKEY™ EMS by DATALOCKER

- EMS Cloud
- EMS On-Prem

SAFECONSOLE®

- SafeConsole Cloud
- SafeConsole On-Prem

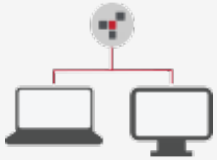
PROTECT PORTABLE DATA

- Automatic hardware encryption without any hassles or installations
- Manage devices in the field: updates, remotely disable

EASY TO USE

- Works with hardware encrypted devices including flash drives, and high capacity external hard drives.

GUARANTEE COMPLIANCE



- Not opt-in and can not be disabled
- Verify policy controls
- Scalable management (SaaS or OnPrem)

AFFORDABLE

- Total cost of ownership is less than a non-encrypted non-managed solution.

DataLocker DL Series

DL2

- Hardware encrypted external USB 2.0 hard drive with FIPS 140-2 validation for the entire device
- Up to 2TB capacity
- No software or drivers required
- TAA Compliant
- Currently deployed throughout the US military

DL3

- Hardware encrypted USB 3.0 external hard drive
- Up to 2TB in capacity.
- Requires no software or drivers
- Centrally Manageable
- Optional two factor authentication – requires two modes of authentication (password plus a physical RFID tag)

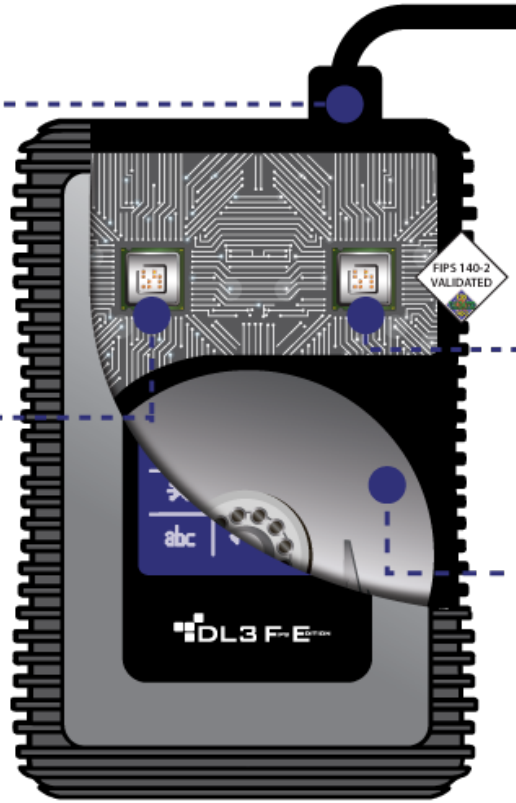
DL3 FE

- Dual Crypto, FIPS validated, hardware encrypted, USB 3.0 external hard drive
- Same exact features as the DL3
- Also deployed through the US military

DL3FE – Dual Crypto Cryptography Overview

1 Your original, unencrypted files, folders and data are transferred to your DL3 FE.

2 The DL3 CPU encrypts the incoming data with a 256-bit AES XTS mode algorithm.



3 The data is then encrypted sequentially with a FIPS 140-2 Validated 256-bit AES CBC mode algorithm.

4 Your data is written to the DL3 FE hard drive. Every bit of stored data is encrypted twice with two independent keys that never leave your device.

DataLocker H series (Formerly IronKey)

H200 BIO

- FIPS 140-2 Level 3 validated, hardware encrypted, USB 2.0 external hard drive.
- Up to 1TB in capacity.
- Centrally manageable with ACCESS Enterprise
- Fingerprint two factor authentication - Further enhance security and convenience with the biometric capabilities through an ergonomic swipe sensor

H300

- USB 3.0 encrypted external hard drive.
- Two versions: Basic and Enterprise (Enterprise version requires IronKey EMS)
- Up to 2TB in capacity.
- Centrally manageable with IronKey Enterprise Management Service or Server

H350

- FIPS 140-2 Level 3 validated, USB 3.0 encrypted external hard drive.
- Two versions: Basic and Enterprise (Enterprise version requires IronKey EMS)
- FIPS 140-2 Level 3 validation
- Up to 2TB in capacity.
- Centrally manageable with IronKey Enterprise Management Service or Server

More Encrypted Solutions

Sentry 3 FIPS

Hardware encrypted
USB flash drive

- 256 bit AES encryption
- Ruggedized design
- Fast USB 3.0 interface
- Up to 64GB capacity
- Centrally manageable with SafeConsole

EncryptDisc®

Self encrypting
optical media

- FIPS 140-2 Validated crypto engine
- No software or drivers to install
- A perfect solution for medical, legal and financial practices
- Available in CD 100 packs

Encrypted Cloud Storage with DATALOCKER SAFECRYPT®

SafeCrypt is a “cloud encryption gateway” which provides a layer of encryption between your applications and your cloud storage provider. SafeCrypt creates an easy to use virtual drive which serves as the encryption gateway. Simply point your application to the virtual drive letter and SafeCrypt fully encrypts your data before it leaves your computer and then passes it to your cloud storage service provider fully encrypted.

SafeConsole

SafeConsole enables your organization to inventory, audit, manage and kill your SafeConsole enabled encrypted endpoints.

Integrate
With Active Directory for Easy Provisioning

Identify
When and Where Your Managed Device is Used

Inventory
Manage Device Inventory, Lifecycle and Maintenance

Configure
With and Advanced Management Feature Set

IronKey EMS

Protecting your data, your mobile workforce, and your organization is easy with the IronKey EMS. You can quickly and easily establish a secure storage command center for administering and policing the use of IronKey encrypted Workspace devices for Windows To Go and Enterprise storage drives.

70 % OF FORTUNE 100 COMPANIES
AND NUMEROUS PUBLIC SECTOR AGENCIES

TRUST DATALOCKER

THOUSANDS OF CLIENTS GLOBALLY

LEGAL	ENTERPRISE	GOVERNMENT	HEALTHCARE	FINANCIAL
Whitaker Chalk Attorneys & Counselors	LOCKHEED MARTIN		Allscripts	LLOYDS BANK
GW GARFUNKEL WILD, P.C. ATTORNEYS AT LAW	GENERAL DYNAMICS		UnitedHealthcare	
EPSTEIN BECKER GREEN	Honeywell	NASA	Saint Luke's Health System	
Poyner Spruill ATTORNEYS AT LAW	NORTHROP GRUMMAN			
	KASPERSKY lab		Children's of Alabama	Deloitte.
ulmer berne llp ATTORNEYS			Banner Health	KPMG cutting through complexity
KSM KATZ SAPPER & MILLER	DREAMWORKS STUDIOS		KAISER PERMANENTE	Experian A world of insight
DEEPWATER HORIZON CLAIMS CENTER ECONOMIC & PROPERTY DAMAGE CLAIMS	Walt Disney Imagineering		QUINTILES	J.P.Morgan
	Microsoft			

United States Army

Project: ACC Rock Island – Health Information Collection

Solution: DataLocker DL2

Use Case: The US Army needed a way to encrypt, collect and transport sensitive medical records. The DataLocker Enterprise's plug and play, platform independent design allowed the Army to deploy a fail safe data encryption system without requiring any software or drivers while maintaining compliance with encryption standards (FIPS 140-2).

Results: Saved the Army hundreds of thousands of dollars and thousands of man hours in security testing and system configuration.

Walt Disney

Walt Disney Imagineering

Project: Needed to Transfer Prerelease Versions of Upcoming Films Securely

Solution: DataLocker DL3

Use Case: Walt Disney needed a way to encrypt, collect and transport sensitive prerelease films. DataLocker's agnostic solution (works for Macs or PCs) allowed Disney to safely share and transfer prerelease versions of upcoming films. USB 3.0 speeds paired with an SSD option allows faster more reliable data transfers for all their studio needs.

Results: Disney felt this was an inexpensive way to prevent a costly leak and exposure of sensitive information like the one Sony experience in 2014.

Price Waterhouse Coopers

Project: Needed a way to manage and protect thousands of USBs worldwide

Solution: DataLocker Sentry and SafeConsole

Use Case: As a global professional services firm, with thousands of consultants working offsite with confidential client data that needs to be shared and carried around at all times, having a centralized management system that allows administration and control of USB devices was critical. SafeConsole was easy to deploy and works with many leading providers of encrypted storage devices. Lost data could easily mean a lost deal and severe damage to the reputation of the company.

Results: Deployed to thousands of users

DataLocker SafeConsole

Saint Luke's Health System

Saint Luke's Health System

Project: Needed secure, low-cost method of delivering and transporting medical records including diagnostic imagery

Solution: DataLocker EncryptDisc

Use Case: Saint Luke's Health System needed a way to provide patient records (like MRIs, etc.) in a HIPPA compliant manner. They chose DataLocker EncryptDisc because the solution allowed them to easily burn sensitive information to optical media (CD/DVD) without any special software or drivers. DataLocker also printed custom labels for the Healthcare company to keep with their brand image.

Results: Medical records were encrypted and put onto optical media at a cost that was 90% less than an encrypted USB flash drive.

Top Ten Multinational Law Firm

Project: Needed a secure method of collecting and transporting large volumes of sensitive client data from its client's site to the firms e-discovery department

Solution: DataLocker DL3FE Encrypted Hard Drive

Use Case: The device uses a high speed USB 3.0 interface and is platform independent requiring no software or drivers. Hardware based encryption allowed the law firm to encrypt client data "on the fly" without having to install any software on the clients system. Read-only feature ensures drive contents are not compromised by users.

Results: Transfer was completed in less that 1/10th (10 hours vs 120 hours) of the time saving and saved $10,000 in direct cost. The client was 100% satisfied that the collected data was fully secured and accounted for.