Q: What is your USB Port Strategy?

Block

Q: What do you use? Are you happy with the solution?

YES

NO

Open/Allow

Q: Are you concerned? Data breach, compliance, fines...

YES

NO

Try a simple solution to block your USB ports

PortBlocker

Q: Does your organization allow USB removable storage? Do you allow Data to be transported in & out of your network or office?

YES

NO

Try Encrypted Virtual Drives

SAFECRYPT

Q: How do you secure your removable storage devices?

YES

NO

Other Encryption

None

READ

Software vs Hardware Encryption

Q: Would you like to manage your encrypted USBs? Enforce policy, password reset, remote kill, audit activity ...

YES

NO

READ

Benefits of Centrally Managed Secure USB Drives

Try DataLocker Hardware Encrypted Flash/Hard Drives

DL4 FE

Sentry ONE

Sentry K300

DL3/DL3FE

H300/H350

Try Central Management

SAFECONSOLE®

Fast & easy deployment

Server on site requirement?

Cloud Version

On-Prem Version

Try On-Board Anti-Malware for Encrypted Drives

Powered by McAfee

SAFECONSOLE®

Cloud Version | On-Prem Version

PortBlocker
License Per Workstation
1 year or 3 year

DeviceControl
License Per Device
1 year or 3 year

SAFECRYPT
License Per Virtual Drive
1 year or 3 year

Powered by McAfee
License Per Device
1 year or 3 year

DATALOCKER®
Encrypted Flash Drives
Capacity Range 4GB - 256GB


Sentry K300


FIPS 140-2 Validated
Sentry ONE
Sentry ONE Managed

DATALOCKER®
Encrypted Hard Drives
Capacity Range 500GB - 15.3TB SSD


DL3


H300 Basic
H300 Enterprise


H350 Basic
H350 Enterprise


FIPS 140-2 Validated
DL4 FE


DL3 FE

Risks

Unmanaged USBs create a gap in enterprise security architecture

- Confidential and sensitive information risk exposure if device is lost or stolen
- Potentially put organization at risk

Non-compliance can cost you in fines and reputation

- GDPR fine up to 4% of worldwide TO or €20 M fine
- Data breach disclosures are required - long term damage to your reputation and brand

Regular un-encrypted USB Devices = Data Hoarders

Solutions

Secure data and gain control while protecting productivity

- Manage your endpoints: authorize only approved USB devices
- Protect your portable data: hassle-free automatic hardware encryption
- Guarantee compliance (GDPR/SOX/HIPAA etc) via audit logs and always-on security
- Manage your secure USB devices - like any other IT asset: control access,enforce policies, and simplify compliance auditing
- Encrypt and manage your virtual drive

Request a FREE Evaluation

https://datalocker.com/evaluation-request/

30 Day Free Trial
Terms & Conditions Apply

Why DataLocker?

Hardware encrypted devices are simple to manage anywhere in the world

Wide range of devices to fit all budgets and requirements

Easy to deploy Saas/Cloud version saves internal resources (On-prem optional)

Device Security Features:

- Military grade encryption AES 256-bit
- Actively detects & responds to threats
- Multi-platform compatibility
- FIPS 140-2 validation
- Tamper proof design
- Brute force protection

Administrators can control policies: mass and automated deployment = lower opertaional cost