# DriveLock Device Control: Protects and controls external media

**In this digital era, data protection and security are becoming increasingly important issues for companies. Increasing demands are being placed on today's IT security solutions. Mobile removable media and USB sticks continue to play a major role when it comes to transferring data from one computer to another. We are committed to protecting your data, devices and systems.**

The number of Cyber Attacks is continually increasing. Attackers are more inventive and always finding new ways to ensure their attacks have an even greater impact on their targets. In 2019 alone, there were over 1 billion malware variants, each with devastating consequences. Traditional attacks primarily involve installing or running external malware on the target system. External media and devices can play a pivotal role in such transfers. Research shows that 80% of workers have already copied data from or to **USB drives, mobile phones and other devices (such as external hard drives)** via USB ports without considering its consequences. In the medical field, scans are often passed between doctors via USB drives. By using this method, malware can quickly latch itself on to a device and then be transmitted across multiple systems, for example, through a so-called Bad USB attack. But how can a company monitor or even prevent these occurrences? Is there a way to enforce permissions on certain removable media and to automatically encrypt data when copying to USB drives? How can companies control wireless data transmission via Bluetooth?

## Device Control - Control and protection of mobile data carriers

Our device control solution monitors external data carriers and data flow. It prevents sensitive data from reaching external storage media such as USB drives, or data from being easily transferred and read. It checks each connected device and if necessary, will lock that device out. Our solution will only allow the use of authorised external media.

## Rules define the permissibility of actions

When an employee connects a device to the USB port, the computer recognises what type of device it is (whether it is an external hard disk or USB drive, etc.). As such, DriveLock can be used to control which USB media are allowed connection to the computer. Another rule could be to allow the connection of USB devices, but to give the users read-only permissions so that they are not allowed to write any data to the devices.

## Advantages of interface control

- PROTECTION AGAINST MALWARE ON AND THROUGH EXTERNAL DATA CARRIERS AND DEVICES
- CONTROL WHO HAS COPIED WHICH FILE TO WHICH MEDIA
- PROTECTS DATA ON EXTERNAL MEDIA BY MEANS OF ENCRYPTION
- AUTOMATIC LEARNING FROM CONNECTED DEVICES
- TRAINS EMPLOYEES IN THE SECURE HANDLING OF DATA CARRIERS
- REPORTING FOR VERIFICATION

## Cyber Threats - Status Quo

- MORE THAN 50% OF COMPANIES WORLDWIDE HAVE BEEN THE TARGET OF CYBER ATTACKS
- REMOVABLE STORAGE DEVICES AND EXTERNAL HARDWARE ARE ONE OF THE MOST FREQUENT SOURCES FOR INTRODUCING MALWARE
- USB DEVICES FACILITATE DATA THEFT AND DATA LOSS

DriveLock

### Advantages of DriveLock Device Control

DriveLock Device Control manages all removable media and external devices. All variants of a company policy are conceivable and can be adapted for this purpose: from monitoring a company policy, through to enforcing strict guidelines. The quick roll out of all settings based on policies means the implementation of DriveLock Device Control is a breeze.

### Control of external drives:

- Flexible control of all externally connected media:
  You determine who can use which drives at what time.
- Integrated data flow control through data type checking:
  You define who is allowed to read or copy which files.
- Extensive audit of file operations: You are able to monitor who has copied which file to what media and when this was done.

### Control of network drives:

- Additional security for network shares or WebDAV-based drives:
  You define who is allowed to use which drives at what time.
- Integrated data flow control through data type checking: You decide who is allowed to copy which files to what destination.

### Granular setting options

In addition to the basic guidelines for all devices, rules can be used to configure all settings according to various criteria. From user groups via times of day through to network locations, there are no limits to the flexibility here.

### Shadow copies and forced encryption

DriveLock supports the creation of shadow copies in addition to completely verifying the use of external media and logging the data flow. It is also possible to force data encryption when it is written to external media.

### Control of the data volume

DriveLock allows you to control the volume of data transferred between the removable storage device and the endpoint device.

## DriveLock - Features

+ ONLY AUTHORISED DEVICES AND EXTERNAL DRIVES ARE PERMITTED
+ CONTROLS BLUETOOTH CONNECTIONS FROM EXTERNAL DEVICES TO THE COMPUTER VIA SELF CONFIGURATION SETTINGS
+ PREVENTS FILE TRANSFERS OVER UNENCRYPTED OR UNAUTHORISED MEDIA
+ ALLOWS CONTROL OF WHICH USERS CAN COPY WHICH FILE TO WHAT MEDIA
+ ENCRYPTS EXTERNAL USB MEDIA ON DEMAND
+ ENABLES CONTEXTUAL AWARENESS CAMPAIGNS
+ FORENSIC ANALYSIS & REPORTING

## Additional features

+ PREDEFINED FILE FILTER GROUPS OF THE MOST COMMON FILE TYPES
+ OFFLINE SHARING VIA UNLOCK ACCESS CODES
+ REMOTE ACCESS TO AGENTS AND DISPLAY OF CURRENTLY VALID SETTINGS
+ MULTILINGUAL, SELF-CONFIGURABLE USER MESSAGES
+ SECURE SHARING OPTIONS AND USER-FRIENDLY SELF-SERVICING

### DriveLock: Expert in IT and data security for more than 20 years

The German company **DriveLock SE** was founded in 1999 and is now one of the leading international specialists for cloud-based endpoint and data security. The solutions include measures for prevention, as well as for the detection and containment of attackers in the system.

**DriveLock is Made in Germany, with development and technical support from Germany.**

DriveLock SE • Germany • France • Australia • Singapore • Middle East • USA
sales@drivelock.com • www.drivelock.com