Device Control
Intelligent Device Control

FLEXIBLE, SIMPLE AND EFFICIENT

▶ **Easy configuration of integrated devices through Machine Learning.**

▶ **Only desired devices and external drives will be allowed.**

▶ **Proactive blocking of CD/DVD writers.**

▶ **Prevents file transfer via unencrypted or unauthorized media.**

▶ **Allows control over who has copied which file to what media.**

▶ **Automatically and securely encrypts external USB data devices upon request.**

▶ **Trains employees regarding the safe handling of data and external data devices.**

▶ **Extensive forensic analysis and reporting options.**

FLEXIBLE, YET SIMPLE AND EFFICIENT

USB sticks continue to be a popular medium to exchange data. Despite various cloud sharing services such as Dropbox, USB sticks continue to be used frequently. Employees also use corporate USB ports to charge mobile phones or other devices. This makes it possible for Ransomware to infiltrate a device, machine or network. Numerous studies show 80% of employees have copied data from or to a USB stick, or connected devices to the USB port for charging without taking the consequences into account. Potentially exposing confidential company data to the public or a third-party. This may result in opening the companies machine or network to attacks from malware, or Trojans that could cause considerable damage including further criminal activities like extortion.

HOW IS A COMPANY ABLE TO EFFECTIVELY MONITOR OR PREVENT THESE INSIDER THREATS?

How can a company create the mandatory automatic encryption of connected USB sticks? The answer is very simple: **DriveLock Device Control** controls all removable media and devices – A customized policy can be created based on machine, user, device or companywide policy. Ensuring compliance through direct policy deployment or deep AD/GPO integration.

CONTROL OF EXTERNAL DRIVES

▶ Flexible control of all externally connected media: You can determine who is allowed to use which drives at what time.

▶ Integrated data flow control including data type checking: You can decide who is allowed to read or copy which files.

▶ Extensive audit of file operations including shadow copies: You are able to monitor who has copied which file to what media and when this action was conducted.

NETWORK DRIVE CONTROL

▶ Additional security for network shares or WebDAV-based drives: You can determine who is allowed to use which drives at what time.

▶ Integrated data flow control including data type checking: You can decide who is allowed to copy which files to what destination.

EXCEPTIONS, MULTIDIMENSIONAL

In addition to the basic guidelines for all types of devices, you can also use exception rules (whitelists) to permit device connection events based on company guidelines. Here, a total of 17 configurations are available - from users and groups to the time of day and network location, the flexibility is limitless.

ADDITIONAL FEATURES

▶ Maximum flexibility through extensive configuration options.

▶ Predefined file filter groups including the most common file types.

▶ Offline sharing via unlock codes.

▶ Remote access to agents and display of the currently applied settings.

▶ Proactive prevention of the CD/DVD writer use.

▶ Multi-lingual, self-configurable user messaging.

▶ Secure sharing options and user-friendly self-service.

PORTABLE ENCRYPTION – DRIVELOCK ENCRYPTION 2-GO (ADD-ON)

To provide you with an access option to your encrypted containers or files located on external drives from Windows and Mac computers without DriveLock, we developed DriveLock Encryption-2-Go.

Encryption-2-Go offers the functionality to securely encrypt files on removable storage devices, either with an encrypted container or on the file and directory level. This can either be selected by the end user or specified by the DriveLock Administrator.

With DriveLock Encryption-2-Go it is possible to connect or disconnect encrypted containers as normal drives.

Directory level encryption, for example, enables the comprehensive encryption of all files on a removable storage device, as well as the provision of a separate directory in plain text, by means of which the end user can export files in a controlled manner.

On computers without DriveLock the encrypted data can be decrypted with „DriveLock Mobile".

Thereby, this application does not have to be installed (with administration rights) but can simply be started as a standalone application.