CENTRALIZED BITLOCKER MANAGEMENT WITH DRIVELOCK

- Centralized configuration and integrated implementation of the BitLocker encryption policy
- Support of authentication methods like smartcard, token or network start
- Support of all common BitLocker authentication methods
- Compliance Dashboard: Encryption status of individual devices always in the view
- Secure and central management of BitLocker recovery keys
- Lost or stolen devices are voided when the network connection is reestablished
- Prevention of unauthorized access to decommissioned or recycled endpoint devices

Centralized BitLocker Management with DriveLock

The free BitLocker encryption is a great advantage for Microsoft customers, and makes an important contribution to improved IT security for companies. But with increasing regulatory requirements, BitLocker encryption alone is often insufficient. A management console is a mandatory component to properly manage these features.

By integrating BitLocker management into the DriveLock portfolio, users are provided with an easy-to-use interface to manage all the functions through a single DriveLock console.

This provides DriveLock with important additional functions to supplement the BitLocker functionalities.

In particular, this includes expanded configuration options, the centralized configuration, and thus the holistic, company-wide implementation of encryption guidelines. In addition, administrators are always provided with a clear overview of the encryption status of individual devices via the Management Console.

BitLocker management with DriveLock enables a centralized reporting and hardware management as well as an integrated challenge/response-based helpdesk.

DriveLock offers additional critical security features with its pre-boot authentication and supports authentication methods such as smart card, token or network start. These are relevant functions for a compliant protection of your end devices.

DriveLock Managed Security Services enable a BitLocker management from within DriveLock, significantly reducing your administrative overhead.

Your advantages:

Reduced administration effort through a centralized management of

- policies,
- decommissioning
- and recovery measures
- Advanced authentication methods: Smartcards, token, network start
- Compliance Dashboard: Always a clear overview of the encryption status of individual devices
- Integrated reporting & forensics functions
- Supports multi and roaming users
- DriveLock Managed Security Services enable a BitLocker Management directly from the DriveLock Cloud