BITLOCKER MANAGEMENT

Advanced Microsoft hard disk encryption

comfortable - comprehensive - safe

- enables a centralized configuration and company-wide implementation of encryption policies
- supports all common BitLocker authentication methods with TPM and password
- provides an overview of the encryption status of individual devices at any time via the compliance dashboard
- secure and central management of BitLocker recovery keys
- support for BitLocker To Go for the controlled encryption of external mobile drives and media
- powerful pre-boot authentication (DriveLock PBA) also enables additional authentication methods, remote decommissioning of stolen devices and emergency logon

Why should you apply hard disk encryption?

Data protection is a key priority for companies in the digital age. The loss of confidential information doesn't just represent financial damages, but also a loss of reputation and trust. Protecting data through hard disk encryption is the easiest way to **prevent data loss, manipulation or theft**. Hard disk encryption is recommended for both desktop clients and notebooks, especially for data with high protection requirements.

Hard disk encryption is also one of the key components for a **Zero Trust security approach**. Within the framework of this security concept, sensitive information should always be encrypted, and a decryption should only be possible through authorised access.

DriveLock BitLocker Management

Microsoft provides BitLocker hard disk encryption free of charge for many versions of Windows. But with increasing regulatory requirements, BitLocker encryption alone is often insufficient.

DriveLock BitLocker Management will manage your existing BitLocker installation and also **add some key features:**

- central configuration of BitLocker disk encryption independent from the Active Directory (AD) - even for computers without an AD connection
- DriveLock's advanced web-based management console to manage and analyse the system environment security status throughout the entire computer life cycle
- secure one-time recovery with an automatic key exchange

We also support the encryption of external data carriers with BitLocker To Go.

Important Add-on: DriveLock PBA for BitLocker

The optional, custom-developed pre-boot authentication (DriveLock PBA for BitLocker) not only enables a secure boot process, but also **expands the limited functionality of BitLocker's own PBA.** Thus, the confidentiality of stored data is maintained even in the event of loss or theft of the notebook or desktop.

The BitLocker PBA is thereby replaced by the DriveLock PBA. The operating system itself as well as other third party security solutions can be initialized and started without interference.

Our DriveLock PBA solution offers significant advantages over BitLocker PBA:

- Login with Windows user name / domain and password
- Two-factor authentication using cryptographic smartcards or tokens
- Single-Sign-On to the Windows operating system possible
- Self-service emergency login in case of forgotten access data
- Network unlock: Secure automated activation when connected to the central DriveLock Enterprise Server
- User synchronization with Microsoft Active Directory for initial deployments or update processes
- Customizable login screen
- Support for a wide range of international keyboard layouts
- On-screen keyboard for logging on to touch-enabled Windows devices such as Microsoft Surface

By the way, did you hear about a highly innovative feature:
BitLocker Management from the cloud?

DriveLock Managed Security Services enable a BitLocker management from the cloud. You will benefit from:

- **cost advantages**
- **rapid deployment & automatic updates**
- **predefined security policies**

You can find more information at drivelock.com/managed-security-services/

The advantages of DriveLock BitLocker Management at a glance

- Reduced administration effort through a centralized management of policies, decommissioning and recovery measures
- Advanced authentication methods: Smartcards, tokens, network startup and Single-Sign-On
- 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 the BitLocker Management from the cloud

Everything from a single source:
DriveLock offers BitLocker Management as a building block of its Zero Trust Platform to implement a comprehensive security strategy.

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