DISK PROTECTION

HARD DISK ENCRYPTION

- Centrally controlled rollout throughout the organisation
- Reliable and fast initial encryption of the entire hard disk or individual partitions
- Multi-user, multilingual PBA with fast pre-boot authentication (PBA) for Legacy BIOS and UEFI (incl. UEFI Secure Boot)
- Integration into Microsoft Active Directory with single sign-on from the PBA to the operating system
- Network unlock simplifies the user logon and recovery procedures, and enables self-service devices such as ATMs to be completely encrypted
- Extensive emergency procedures in case of forgotten passwords or PINs, forgotten or lost Smart Cards

DRIVELOCK ENCRYPTS YOUR DATA – SECURELY AND QUICKLY

Accidental disclosure of sensitive business data and the loss or theft of mobile devices such as laptops, tablets and smartphones cause millions of dollars in damage to businesses every year. The most effective and simplest protection is the encryption of data. The cost of the loss is then limited to the material value of the USB stick or laptop, while the data is useless for the finder. DriveLock provides state-of-the-art solutions through a unique combination of data encryption on hard disks/partitions, external removable media, as well as through central and local directories and shared cloud directories.

DRIVELOCK'S ENCRYPTION MODULES WORK SEAMLESSLY WITH EACH OTHER. IN DETAIL THESE ARE:

- **DriveLock Disk Protection:** Transparent Full Disk Encryption (FDE).
- **DriveLock File Protection:** Transparent file and folder encryption (FFE)
- **DriveLock Encryption-2-Go:** Transparent encryption of removable media such as USB sticks, CD/DVD or removable disks (part of DriveLock Smart DeviceGuard)

DriveLock Disk Protection offers you an encryption method that is the ideal complement to our interface and application control:

- Transparent and unobtrusive, without affecting the work process or the user.
- All legal requirements of your company can be depicted.
- The end user is not affected in any way during his daily work processes.
- The DriveLock hard disk encryption always remains in the background.

Through a complete encryption of local partitions and a pre-boot authentication (PBA) **DriveLock Disk Protection** helps to ensure that the confidentiality of the stored data is maintained in the event of loss or theft of the laptop or desktop, and also ensures a secure, trustworthy startup of the computer (secure boot).

This ensures that the operating system itself and other third party security solutions are initialized and started in the intended manner.

- Support for AES-NI support, FIPS 140-2 certified encryption module, supported login policies in the PBA:
  - User Name / Domain and Password
  - Two factor authentication via PIN and cryptographic Smart Card or Token
  - Secure network unlock when the central DriveLock Enterprise Server (DES) is accessible.
- Supports Windows XP SP 3, Windows 7, Windows 8/8.1, Windows 10 (SAC and LTSC), Windows 10 in-place upgrade and Windows Hibernation.
- Configurable encryption algorithms (XTS-AES-256/128, AES-CBC 256/128, Blowfish, IDEA, etc.)
- Integration into Microsoft Active Directory with single sign-on from the PBA to the operating system: The user only needs to enter his login data or his PIN in the PBA. DriveLock ensures that the subsequent login to the operating system is performed automatically, and that the login details of the operating system and PBA remain synchronized.
- You can optionally utilize the secure logon policies which are implemented in your operating system to logon with the secure pre-boot authentication.

- The network unlock simplifies the user logon and recovery procedures and makes it possible to completely encrypt “self-service devices” such as ATMs, which must be able to boot completely without a user interaction after a power failure.
- Extensive emergency procedures in case of forgotten passwords or PINs, lost or forgotten smart cards or non-launching operating system, both online and remote through challenge response procedures
- Proven and fast data recovery capabilities without a forced decryption
- Central management of recovery keys
- In the event of a loss or theft, the data can be deleted remotely or time-controlled („remote kill“).

THE CENTRAL DRIVELOCK COMPONENTS DRIVELOCK MANAGEMENT CONSOLE (DMC) AND DRIVELOCK CONTROL CENTER (DCC)

These central DriveLock components provide the essential services for all DriveLock function modules:

- Central reporting and forensics
- Central data analysis
- Connection to SIEM systems
- Option to anonymize entries in log events
- Extensive recovery options
- Centralized key storage
- Connection to Microsoft Active Directory for e.g. the import of users and computers

All in all, the **DriveLock Product Suite** with its individual encryption modules which are based on one another, offers a perfect implementation of the three basic pillars of IT security

- Confidentiality,
- Integrity and
- Availability

DriveLock keeps your company data confidential through a secure and fast transparent encryption.

DriveLock Disk Protection‘s secure system boot will provide you with an ample integrity for your work environments, and the extensive and extremely flexible disaster recovery processes will ensure that your systems and data remain highly available, even though they are very efficiently protected by DriveLock.