

## FILE PROTECTION



## FILE ENCRYPTION

- ▶ Local, central, mobile or in the cloud
- ▶ The **DriveLock File Protection** offers a unique file-level, user or group-based encryption – it's easy to configure and meets all the requirements for a cost-effective, enterprise-wide deployable and solution.
- ▶ With **DriveLock**, the responsibilities of system and security administrators can be separated. The network administrator is therefore no longer the central role in the company that has access to all data.
- ▶ It doesn't matter if you have data on the local computer, on a central directory of a server in the company, on an external USB disk or on a cloud-based service such as Dropbox, Microsoft OneDrive or Google Drive.
- ▶ Support of
  - Google Drive
  - Microsoft OneDrive
  - DropBox
  - and many other technically similar cloud-based services.
- ▶ Support of a logon with the user name and password, as well as with X.509 certificates from the Microsoft certificate store, or the Mac OS X keychain for logging on to DriveLock File Protection.
- ▶ Efficient recovery and emergency procedures in case of a forgotten password, forgotten or lost smart card or token.

## 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)

With **DriveLock File Protection**, confidential and sensitive information is securely encrypted, and can only be used in plain text by authorized persons or groups.

The **DriveLock architecture** allows files or directories to be protected both centrally and locally at the level of departments, business units or teams to be set up quickly and easily - without the support of the IT administrator - and thus enables the access management to your own encrypted directories. This saves time and reduces costs.

**DriveLock File Protection** encrypts sensitive information reliably and - thanks to the support of hardware-based encryption (AES NI) - quickly.

## 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.