

# CenterTools DriveLock™ 5.5

*DriveLock™ helps you solve common security challenges*

**DriveLock**  
Intelligent control of mobile devices

Uncontrolled use of mobile devices, applications and network connections can lead to theft and disclosure of confidential data and may disrupt network operations. A lost or stolen computer can create severe liability issues for your company. Businesses increasingly recognize the need to take control of their network endpoints. DriveLock™ can help you solve many common security-related challenges.

"I need to prevent the use of mobile devices for stealing confidential data."

- DriveLock gives administrators granular control over who can use which mobile storage devices.
- Configure separate Read and Write permissions for different types of documents.

"I need to prevent accidental data disclosure due to lost or stolen storage devices."

- Administrators can enforce the use of encryption of all data copied to mobile storage devices.
- Encryption can be completely transparent to users.
- Encryption can be used with any removable storage device; no need to buy special hardware.

"Users must be able to access encrypted data on any computer."

- The *Mobile Encryption Application* gives access to encrypted data on computers without DriveLock.
- No software installation or license are required to use the Mobile Encryption Application.
- Users access data using a personal password chosen when drive encryption was set up.

"I need to secure data on a local hard-drive and prevent exposure if lost or stolen."

- DriveLock Full-Drive Encryption encrypts the full hard-drive including the system partition.
- You can enforce strong two-factor authentication without authentication back to the server infrastructure.
- FIPS 140-2 certification is essential along with AES-256 level encryption to assure security standards are met.

"I need to eliminate threats and instability caused by the use of unauthorized devices."

- DriveLock gives administrators granular control over most types of devices.
- Whitelists can allow the use of company-approved devices.
- Easy device discovery detects current and historic device usage, even on computers without DriveLock.

"To comply with policies and regulations, I need to monitor mobile device usage."

- DriveLock keeps a detailed record of all device use and file copy operations
- Shadowing maintains an exact record of copied data that can be used for forensic analysis.
- The *Security Reporting Center* consolidates all auditing data and lets administrators create detailed reports.

"I need to ensure that users can only connect to authorized networks."

- DriveLock ensures that only approved networks can be used. (Active Directory site, wireless SSID, etc..)
- Device and application rules can be configured to apply to selected networks only.
- DriveLock can prevent the use of wireless networks while the computer is connected to a wired LAN..

"I need to prevent the use of unauthorized applications."

- The *Application Launch Filter* gives granular control over who can run which application.
- Blacklists prevent users from running known dangerous applications.
- Whitelists limit users to approved applications, stopping almost all malicious software dead in its tracks..

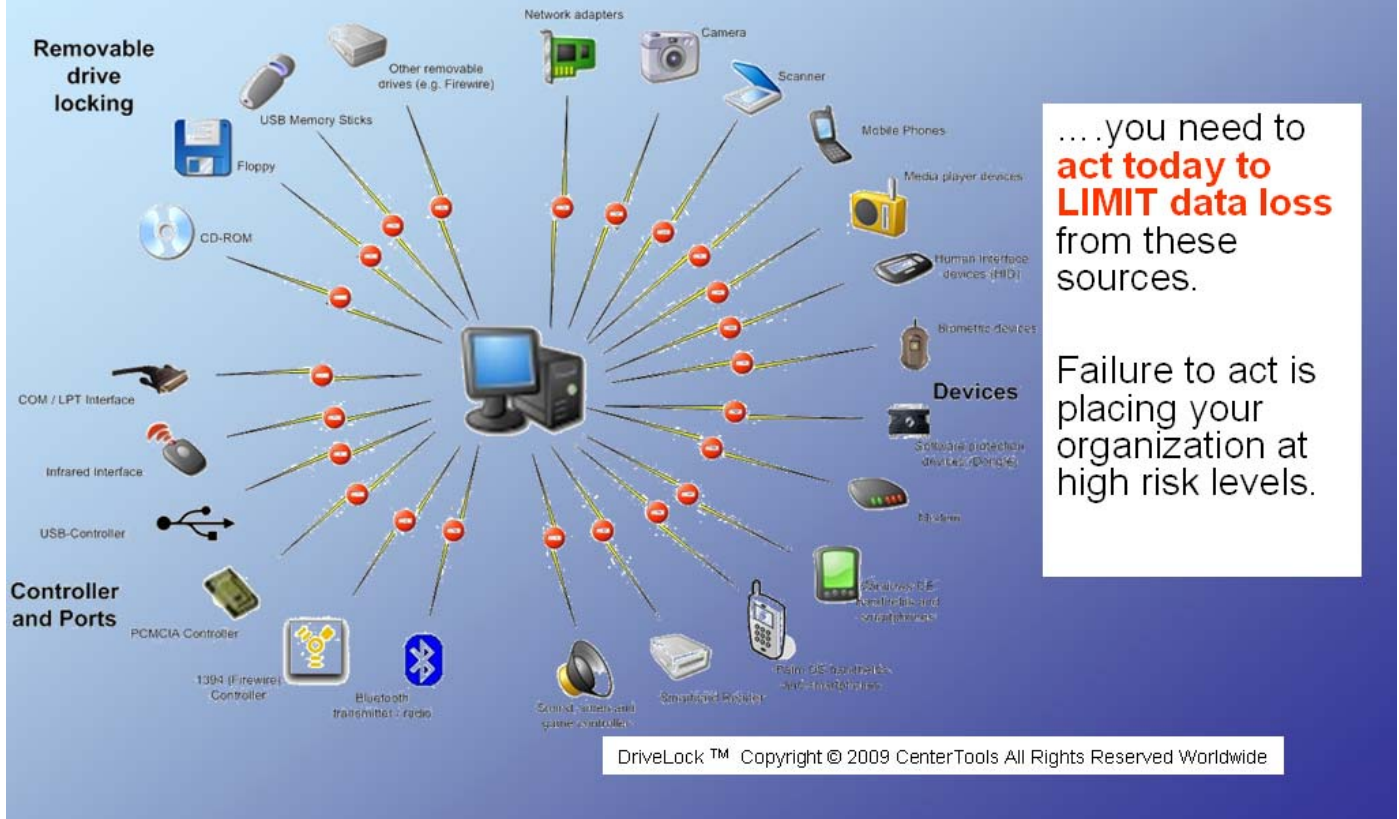
"Device and application control must integrate into our existing infrastructure."

- No dedicated servers or other central resources are required to distribute and enforce DriveLock policies.
- DriveLock seamlessly integrates with Active Directory and Novell networks.

"Network and Security Tools must be easy to implement and easy to administer."

- DriveLock tools use the familiar Microsoft Management Console, are intuitive and easy to learn.
- Customizable messages notify users when a device is blocked.
- Whitelists can be based on device discovery for quick and easy creation of usage rules.

# To **CONTROL** access to these wide range of devices



...you need to **act today to LIMIT data loss** from these sources.

Failure to act is placing your organization at high risk levels.

To read more about DriveLock™ or to download a fully functional trial, visit <http://www.pcprofile.com/USBScanner.htm>



CenterTools DriveLock™ is available from;



PCProfile  
Adelaide South Australia  
Timezone GMT +0930  
Contact via Cell/Mobile +61 (0) 448 650 227  
Fax +61 (0) 8 8265 1961  
email : [pcprofile@pcprofile.com](mailto:pcprofile@pcprofile.com)  
<http://www.pcprofile.com/USBScanner.htm>