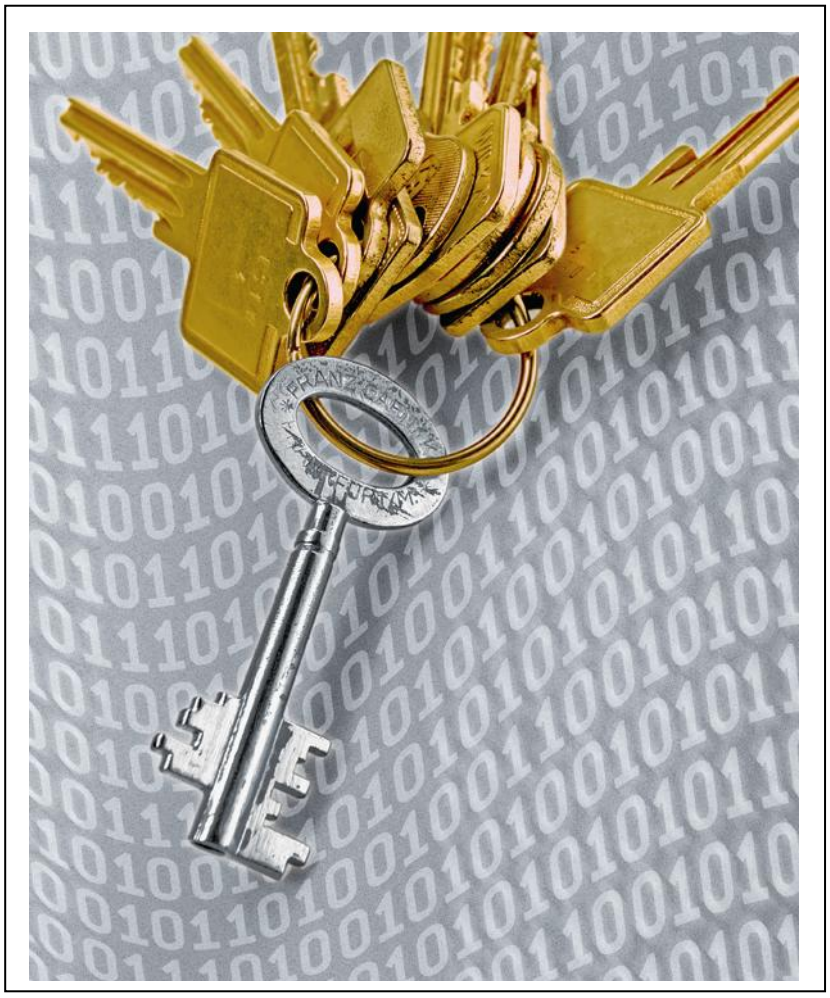
DriveLock™ 5 in Terminal Services Environments

Whitepaper



CenterTools Software GmbH

© 2007

Copyright

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred. Complying with all applicable copyright laws is the responsibility of the user.

© 2007 CenterTools Software GmbH. All rights reserved.

CenterTools and DriveLock™ and others are either registered trademarks or trademarks of CenterTools GmbH or its subsidiaries in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

DriveLock™ 5 Features

One of the new features of DriveLock™ 5.0 from CenterTools is the extension of its proven endpoint protection mechanism to terminal services environments. The new DriveLock™ Terminal Services Edition extends DriveLock's protection to Windows Terminal Services or Citrix Presentation Server / Desktop Server environments.

DriveLock™ increases security in a terminal services environment by providing the following features:

Terminal Services Drive Control

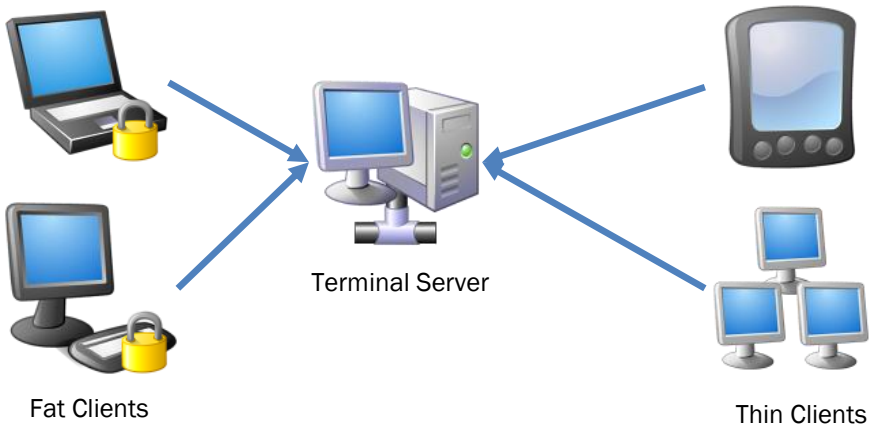
The Terminal Server Edition extends DriveLock's control of removable devices to terminal services client sessions. This drive control allows you to securely and flexibly control the use of drives within Terminal Services client sessions, including local fixed and removable drives on client computers and thin clients.

Application Launch Filter

DriveLock™ 5.0 gives you control over which applications can run on a client PC or within a terminal server client session. This means that you get complete control over which applications are running in your network. It's a revolutionary way of protecting computers against attacks, including zero-day attacks for which no patches are available yet.

Threats in Terminal Services Environments

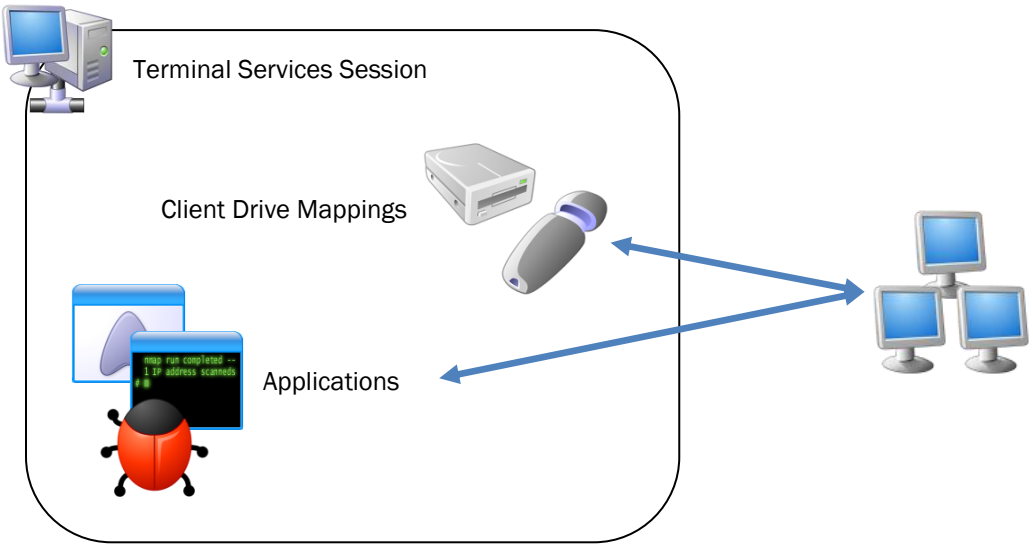
A typical terminal services environment consists of a mixed infrastructure of computers. Fat client systems (such as desktop or notebook computers) are typically used by employees to access applications that are not running on their PCs or for remote access to applications. Thin clients (such as Wyse terminals) are typically used to provide users with a complete work environment that is centrally controlled and administered.



Thin clients and fat clients both access terminal servers but they have different levels of protection against security threats. While fat clients can run DriveLock™ to protect against various threats, there is no comparable product that runs on thin clients.

Since thin clients typically are not able to run any third-party software locally, DriveLock™ can't be installed on a thin client. Instead it is necessary to protect the terminal server computers against endpoint threats. DriveLock™ Terminal Services Edition provides this protection. It protects terminal servers in the same manner as the other DriveLock™ editions and additionally extends this protection to all terminal services sessions.

Regardless of the protocol used to connect (RDP or ICA), DriveLock controls client drive mappings and the use of applications within client sessions.



Client Drive Mappings

Terminal services products allow administrators to map local client drives into a terminal services (TS) session. These drives are then available to the user inside the TS session. If the TS session is accessed using a fat client with the DriveLock™ Agent installed, all drive locking rules are enforced, whether a device is accessed locally or from within a TS session. However, when using a thin client, there is no locally installed DriveLock™ Agent. As a result, all fixed and removable drives are mapped into the TS session without any protection. DriveLock™ Terminal Services Edition controls all client drive mappings on a terminal server to ensure that the use of drives on thin clients is also protected.

Controlling client drive mappings with DriveLock™ is largely identical to controlling any other type of drive, but due to technical constraints there are some differences:

- Client drive mappings can be controlled based on users, groups and the protocol used, but currently it is not possible to assign separate permissions for reading and writing data
- Whitelist rules can't be based on vendor and product identification as this information is not available inside a TS session. Instead, rules are based on the drive letter used inside the TS session. This allows administrators to assign different permissions for different types of drives, such as CD-ROM drives or USB-connected drives.
- File filtering and auditing are not yet available for client drive mappings. This functionality will be includes in the next version of DriveLock™.

Whitelist rules need to be based on virtual drive letters because no detailed information about drives available inside the TS session. To ensure correct rule enforcement, administrators should use thin client management software to ensure consistent drive mapping. For example, the USB

port of thin clients should always be mapped to the same virtual drive letter. By using this technique it is possible to achieve granular control over all drives that are connected to thin clients.

Applications

If entire desktops are published to end users, each user can run any application that is available on a terminal server as well as any application located on a mapped client drive. To prevent the execution of unwanted applications, DriveLock™ Terminal Services Edition contains the Application Launch Filter. This feature allows you to control who can run which application and at what time of the day.

The Application Launch Filter intercepts the startup of all applications, calculates a hash of the executable file and then compares this hash against all available whitelist and blacklist rules. An application is only allowed to start if the Application Launch Filter rules allow it.

In terminal services environments the Application Launch Filter should be run in whitelist mode to ensure that only whitelisted applications can be run on the terminal server. This matches the most common use of terminal servers, which is to give users access to a tightly controlled computing environment that only consists of a few selected applications.

Built-in Solutions vs. DriveLock™

DriveLock™ Terminal Services Edition enhances some existing functionality in terminal services products. In addition, DriveLock allows administrators to maintain a single set of rules that applies to users whether they are using a PC or a terminal services session.

The following comparison chart compares the different levels of protection provided by DriveLock™ and the supported terminal services products.

Feature	DriveLock Terminal Services Edition	Windows 2003 Terminal Services	Citrix Presentation Server
Client drive mappings	✓	**Partial**	**Partial**
Per user control	✓	✓ (in Active Directory)	✓ (in Active Directory)
Per group control	✓		
Per protocol control	✓	✓ (TS Configuration)	✓ (TS Configuration)
File auditing	With the next version of DriveLock		
Whitelist Rules	✓		
Time constraints	✓		
Applications	✓	**Partial**	**Partial**
Based on MD5 hash	✓	✓ (GPO)	✓ (GPO)
Based on special rules	✓ (all OS files, all files, Windows updates)		
Predefined rules for frequently used apps.	✓		
Per user control	✓	✓	✓

Feature	DriveLock Terminal Services Edition	Windows 2003 Terminal Services	Citrix Presentation Server
Per group control	✓		
Time constraints	✓		
Combination of blacklists and whitelists	✓	Only blacklists	Only blacklists
User notifications	✓		
General features			
Administration	Central, one console	Distributed, multiple consoles	Distributed, multiple consoles
Centralized incident reporting	✓ (Security Reporting Center)		
Protection of local server resources	✓		
Protection for all computer	✓		

Various management products are routinely used to manage thin client resources. These products do not provide granular control of client drive mappings (for example, based on user and group). However, they can enforce consistent virtual drive letter mappings, which ensures that DriveLock policies can be applied correctly and consistently.

Third-party software may also be used to configure or provision Terminal Services environments. Any feature comparison between such products and DriveLock™ should focus on security features, as DriveLock™ is not a configuration or provisioning solution but a security tool Generally, DriveLock™ and provisioning tools complement each other.