Whitepaper

DriveLock in Terminal Services Environments

Technical Article

DriveLock SE 2019

Contents

1 DRIVELOCK FEATURES 2

1.1 TERMINAL SERVICES DRIVE CONTROL 2

1.2 APPLICATION LAUNCH FILTER 2

1.3 THIN CLIENT DEVICE INTEGRATION 2

2 THREATS IN TERMINAL SERVICES ENVIRONMENTS 3

2.1 CLIENT DRIVE MAPPINGS 4

2.2 APPLICATIONS 5

2.3 ENCRYPTION 5

3 BUILT-IN SOLUTIONS VS. DRIVELOCK 6

1 DriveLock Features

One of the features of DriveLock is the extension of its proven endpoint protection mechanism to terminal services environments. The DriveLock Thin-Client License extends DriveLock's protection to Windows Terminal Services or Citrix XenApp / XenDesktop environments.

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

1.1 Terminal Services Drive Control

The Terminal Server support extends DriveLock's control of removable drives 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.

1.2 Application Control

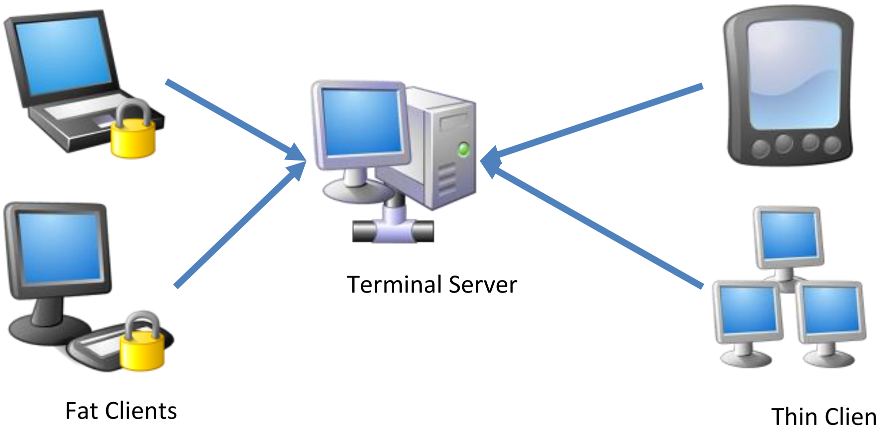
DriveLock™ gives you control over which applications can run on a client PC or within a terminal server client session. This means that you get complete control over which applications are running in your network. It's a revolutionary way of protecting computers against attacks, including zero-day attacks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

1.3 Thin Client Device Integration

DriveLock is able to control drives of thin clients based on the same parameters (vendor, product, serial number) as on fat clients. This is done using a piece of software ("virtual channel") which is running on the thin client. This virtual channel communicates with the DriveLock Agent on the server to provide this tight integration. Virtual channel is available for Windows-based thin clients and already integrated in all IGEL thin clients.

2 Threats in Terminal Services Environments

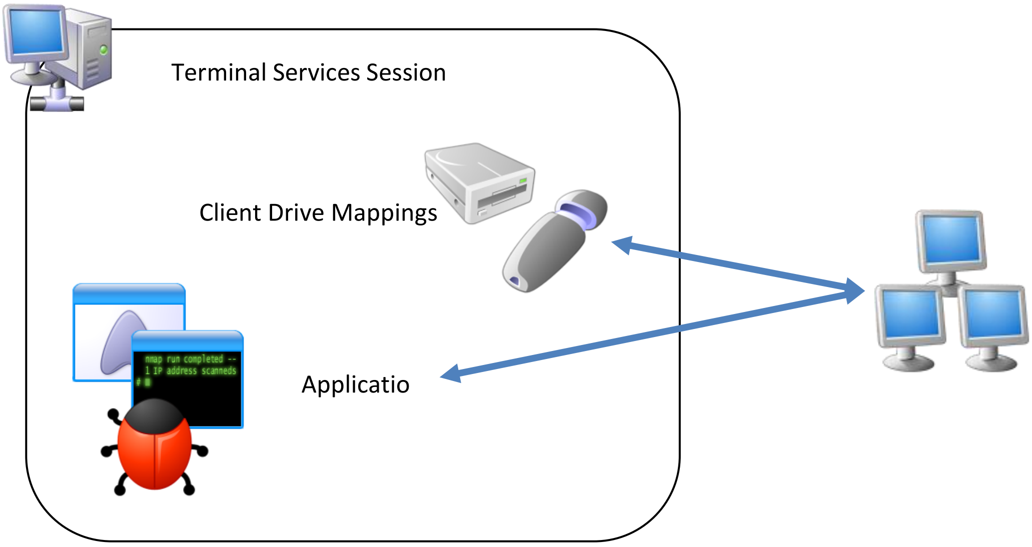
A typical terminal services environment consists of a mixed infrastructure of computers. Fat client systems (such as desktop or notebook computers) are typically used by employees to access applications in a terminal services environment that are not running on their PCs. Thin clients (such as IGEL terminals) 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 locally 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 Agent can’t be installed on a thin client. Instead it is necessary to protect the terminal server computers against endpoint threats. The DriveLock Agent provides this protection. When installed on terminal servers it protects these servers in the same manner 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.



2.1 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 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:

- Whitelist rules can't be based on vendor and product identification, if no virtual channel is installed / available on the thin client as this information is not available inside a TS session. In that case, 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.
- When no virtual channel is available, removable drives can be tagged using volume identification files. DriveLock can be configured so that these files are automatically created on fat clients and pre-filled with the hardware identification of the drive.

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 enforce consistent drive mapping. For example, the USB port of thin clients should then 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.

With the additional file filter it is possible to restrict file type usage on client drive mappings and to do auditing on these files a user had copied.

2.2 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™ 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.

2.3 Encryption

For Terminal servers, it is to note that the encryption rule does not apply to the physical drive of the Terminal Server, but on the drive submitted. For this, a basic rule for the drives should be created. See "drives-> drive-whitelist rules -> new-> terminal server rule". Under this, the encryption can be switched on.

You can use the container-based encryption in Terminal Server environments only.

3 Built-In Solutions VS. DriveLock

DriveLock 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	Windows 2008 Terminal Services	Citrix XenApp
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	✓		
Shadowing	Planned		
Whitelist Rules	✓		
Time constraints	✓		
CDM	✓	**Partial**	**Partial**
Hardware Identification • Virtual channel • Volume Identification FIles	✓		
Encryption	✓		
Enforced Encryption	✓		
Applications	✓	**Partial**	**Partial**
Based on MD5 hash	✓	✓ (GPO)	✓ (GPO)
Based on special rules	✓ (all OS files, all files, Windows updates)		
Based on certificate	✓		
Based on File Drives	✓		
Predefined rules for frequently used apps.	✓		

Feature	DriveLock	Windows 2008 Terminal Services	Citrix XenApp
Per user control	✓	✓	✓
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	✓ (DriveLock Control 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 ensure that DriveLock policies can be applied correctly and consistently when no virtual channel is available.

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.