Introduction

This document details the risks that can affect a virtual desktop platform and describes different techniques to secure platforms of this type.

Different methods are used to secure virtual or physical desktops. Virtual desktop technology introduces new challenges in security issues. Although some practices are common for physical and virtual environments, it is necessary to implement new techniques and security measures.

Internet usage control

To undertake a migration from traditional workstations to VDI platforms with success, many of the management processes are centralized, such as, for example, user and system policies.

The use of these policies allows to improve the security in a VDI platform, centralizing the control of the user's environment. Here are some policies that make virtual desktops secure:

- Make documents that can be downloaded
- Store properly the downloaded files to have a better visibility of these latter
- Control the execution of scripts
- Determine the longevity of the temporary files of browsers

Virus isolation

Using virtual desktops based on templates, the virtual desktop returns to its initial state each time a user logs out.

It is also possible to perform a centralized emergency shutdown of infected virtual desktops forcing users to log out.

Subsequently, these desktops can be restarted in isolated environments in order to eliminate the virus from the network.

For the detection of viruses in a VDI environment, administrators of the platform will have to take into account that carrying out disk scans in search of viruses in the usual way (in a given time over the whole platform) can suppose the complete collapse of all the platform due to the tremendous load of IOPS to which it is subjected to storage.

Here are some security recommendations for VDI platforms:

- Use downloads and scans in search of viruses in a random way limiting the number of desktops that perform this task simultaneously
- Use the different functionalities of the antivirus products to pre-scan, approve and ignore files of the base template (golden image) on which the virtual desktops will be deployed
- Scan only and exclusively those files that are created or modified in the virtual desktop. Each of the antivirus manufacturers has specific functions for VDI platform base templates

Common risks

The table on the next page shows some security risks, their characteristics on a traditional platform and a virtual platform, as well as a series of operational recommendations to take into account when implementing desktop virtualization.

Security risk	Physical Desktops	Virtual Desktops	Recommendations
Virus in local disk	A complete periodic scan of the disks finds viruses that were not detected with the real-time scan	Full scans are not necessary and can lead to drops in platform performance	Use the pre-scan features of the antivirus
Virus in network unity	Most of the files are on local disks and some on file servers, being scanned separately	VDI platforms host a large amount of data in shared resources (profiles, shared resources, folder redirection) with which a greater number of files are scanned in the servers	It is necessary to assume that there will be a greater IOPS load on the file servers. Assign greater resources or priority to the storage where these file servers are located during the scanning of these
Internet downloads	Difficult to find	Use of GPO policies to offer improved control	Focus on entry points (gateways, firewalls) and policies and not on desktops
System isolation	A necessary method but one that consumes a large amount of time to deal with the infection	It allows the isolation of the system and forces the start of the desktops to allow the users to work	Prepare a base template for this type of scenario
Firewalls and Access policies	Activation of Windows Firewall to protect the desktop when it is out of the office	Even if the user or the connection device is mobile, the virtual desktop is hosted in the Data Center	Focus efforts on the security and gateway of the Data Center
Data Loss Prevention (DLP)	DLP is used to scan and protect the sensitive data of the entity	The same tactic is used as in physical desktops with the addition that it is possible to control USB device connections	VDI does not eliminate the need for DLP
Disk encryption	Prevents the theft of information when the disk drives are removed or the laptops go astray	Encryption is not necessary because virtual desktops are hosted in the Data Center, which is a controlled environment	It is not necessary to invest in disk encryption

Security problems in virtual desktop platforms

On virtual desktop platforms, a series of security issues are detected:

- Many entities allow their users to work with administrator rights in their desktops, this practice being a security hole, since it facilitates the installation of any software (safe or not) in the desktops. In addition, when users open a session with administrator rights, viruses can cause much more damage to systems
- There is a belief that using virtual desktops it is easy to revert them to the original state of the base template, which does not require the use of security and antivirus systems
- Since the virtual desktop is running in the Data Center, the user environment is in a secure network from a secure connection, although it is not known what the user does within his session

To limit these problems, it is recommended:

- Do not allow users to open sessions on their desktops with administration rights
- In terms of security and management tools, a traditional platform and a virtual desktop platform are quite similar. If antivirus tools and security policies are used in the traditional environment, it is necessary to use the same tools in the virtual desktop environment, even if the management techniques are somewhat different
- When using VDI platforms, the virtual desktops are in the same environment as the production servers. If VLANs and firewalls are used, it is necessary to ensure that these servers are separated from the desktops

Use VDI optimize security

A mainframe is one of the most secure systems, since the terminals interact with the system using connection protocols, with which bidirectional file transfer is impossible.

This concept can be applied to VDI environments, existing virtual desktops in a trusted environment such as the Data Center, to which users connect from more or less intelligent devices.

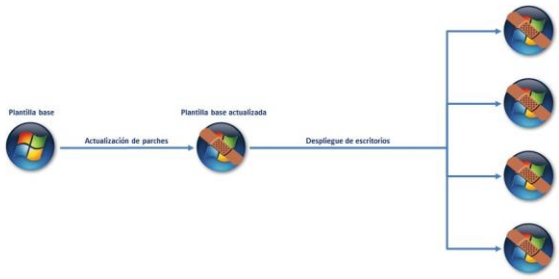
Here are some of the reasons why VDI allows you to secure a user post environment:

Configuration of devices. Many security rules are defined when a base template is configured to deploy virtual desktops and these are not usually modified later.

It is also necessary that in a virtual desktop platform each desktop is configured according to a series of security rules defined by Group Policy.

Centralizing this type of configuration, the security of all the desktops is significantly improved.

Patch update. The use of template-based virtual desktops saves a lot of time compared to a traditional platform. Performing the application and updating patches on the base template ensures that patches are applied correctly on all desktops.



To properly perform the application of patches on the base template, the following considerations must be taken into account:

- What patches are necessary and what base templates are applied, patches for 32-bit, patches for 64-bit, OS version, etc
- At what point the patches in the base template are applied
- Make sure that the appropriate patches are applied to each base template and they are executed correctly
- With what patches system reboots are necessary

Applying patches in a traditional environment requires a significant amount of time, effort and bandwidth.

Using virtual desktop platforms, the application and patch management is simplified, since all the necessary patches are applied to the base template on which the virtual desktops will later be deployed.

Firewall rules. The firewalls that exist in Windows operating systems offer a first barrier to protecting the system and data.

The easiest way to configure firewall policies and exceptions is to make this configuration in the base template and perform a subsequent deployment of it. These changes in policies and exceptions can be done almost immediately, ensuring that all desktops receive the necessary changes.

Application Control. A desktop that is considered secure can have if users can bypass security policies by installing applications on their desktops. If these applications have not been patched and configured correctly they can become a gateway for hackers and users can install unwanted applications with malware or spyware.

Using virtual desktop platforms is a good way to ensure which applications are allowed on the desktops.

Users not having administrator rights in their virtual desktops means that they cannot install applications and, although it is not a popular decision, it is essential in the security of the user position, allowing only the applications installed in the base template to be executed. In the worst case, if an application is not allowed to be installed, at the next session start it would be deleted.

Support and professional services

VirtualCable markets UDS Enterprise through a subscription model, including support and updates, depending on the number of users.

In addition, VirtualCable offers professional services to install and configure UDS Enterprise and other virtualization technologies.

For more information, visit www.udsenterprise.com or send us an email at info@udsenterprise.com

Sources:

Physical vs. virtual desktop security: It's just not the same, Eugene Alfaro.
The top 5 ways that VDI can help improve your enterprise's security, Eric Schultze.