

DeviceLock Virtual DLP: Overview & Scenarios

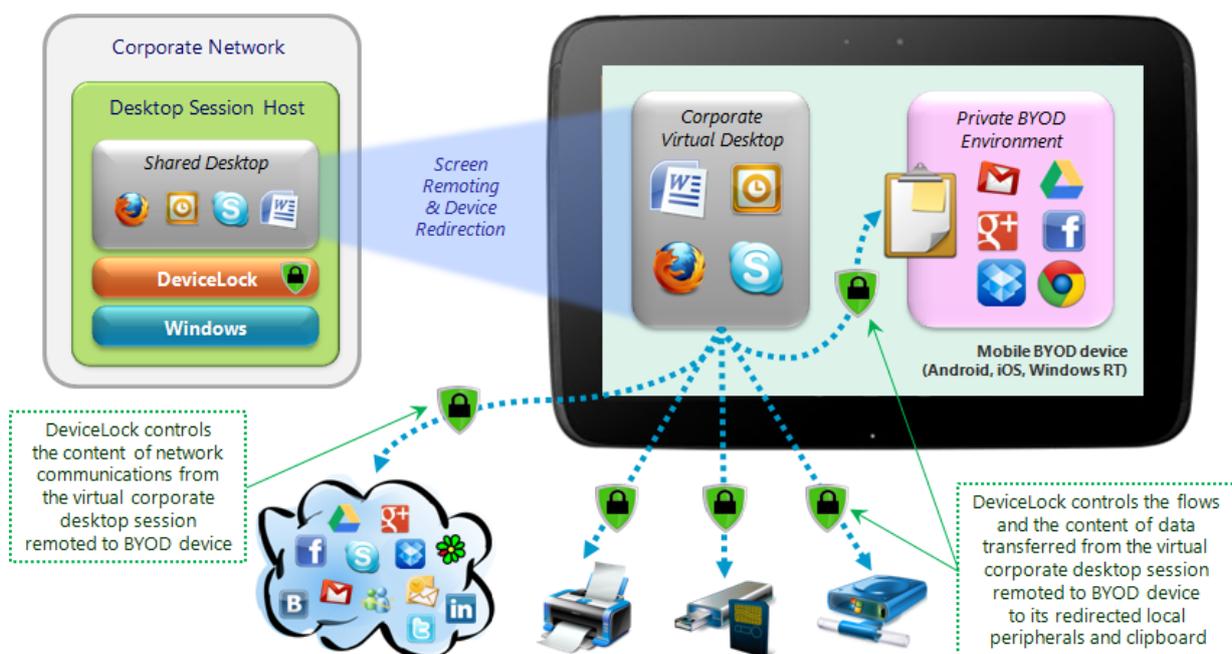
DeviceLock Virtual DLP Overview

DeviceLock's Virtual DLP feature extends the reach of DeviceLock data leak prevention capabilities to a variety of virtual computing scenarios:

- **Session-based application virtualization** based on applications that run centrally in sessions on a terminal server while their GUI displays are delivered to terminals or BYOD devices via remoting protocols (e.g. RDP, ICA, PCoIP, HTML5/WebSockets, etc.).
- **Session-based desktop virtualization** based on desktops that run centrally in sessions on a terminal server while their displays are delivered to terminals or BYOD devices via remoting protocols.
- **Hosted virtual desktops (HVD), a.k.a. virtual desktop infrastructure (VDI) services**, based on centrally hosted Windows desktops each of which runs in a separate virtual machine (VM) above a hypervisor on a virtualization host server.
- **Desktop streaming** based on delivering centrally provisioned desktop images to remote computers where they run in guest VMs above the local hypervisor.
- **Local desktop virtualization** based on Windows desktop images that are provisioned locally on a standalone computer and run there in guest VMs above the hypervisor.

How Virtual DLP Works with Remote Virtualization

By its technological nature, the remote virtualization category comprises session-based application and desktop virtualization, as well as VHD/VDI solutions. DeviceLock Virtual DLP supports remote virtualization solutions from major vendors including Microsoft RDS, Citrix XenApp, Citrix XenDesktop and VMware Horizon View.



The inherent capabilities of these platforms to strongly isolate the *remoted* virtual corporate environment from the *native* mobile OS on BYOD devices are complemented by a flexible set of content-filtering and contextual controls enforced by DeviceLock Virtual DLP over data flows between

centrally hosted virtual desktops or applications and redirected peripherals of terminal BYOD devices that include removable flash drives, printers, USB ports, as well as the clipboard. DeviceLock controls device, port and terminal clipboard redirections via Microsoft RDP, Citrix ICA, VMware PCoIP, HTML5/WebSockets remoting protocols.

In addition, the user’s network communications from within the terminal session are controlled by the DeviceLock DLP inspection mechanisms per protocol. What’s more, for all Virtual DLP scenarios listed above, DeviceLock provides centralized event logging and data shadowing.

By using DeviceLock Endpoint DLP Suite in BYOD implementations based on virtualization platforms, organizations can more reliably protect virtual corporate environments that are sessioned on employees’ personal devices against data leakage while maintaining a transparent user experience in their business activities. If configured accordingly, IT security departments can monitor, inspect, and filter the content of all data exchanges between the protected virtual workspace and the personal part of the BYOD device, namely its storage, local peripherals, and the network – i.e., those destinations outside of the corporate border that should by default be treated as untrusted and insecure.

DeviceLock Virtual DLP controls enforced on the edge of virtual platforms ensure that data from the corporate IT environment and the host BYOD environment are not intermingled. All necessary business-related data exchanges between the two environments are allowed based on least-privilege contextual parameters and DLP content policies, while employees maintain full control over the device platform, personal applications, and their private data. In addition, the employee remains fully responsible for the device maintenance and support, which provides a distinct advantage over the conventional BYOD Mobile Device Management (MDM) approach, whereby the enterprise can be responsible for causing problems with the personal device and its owner’s private data.

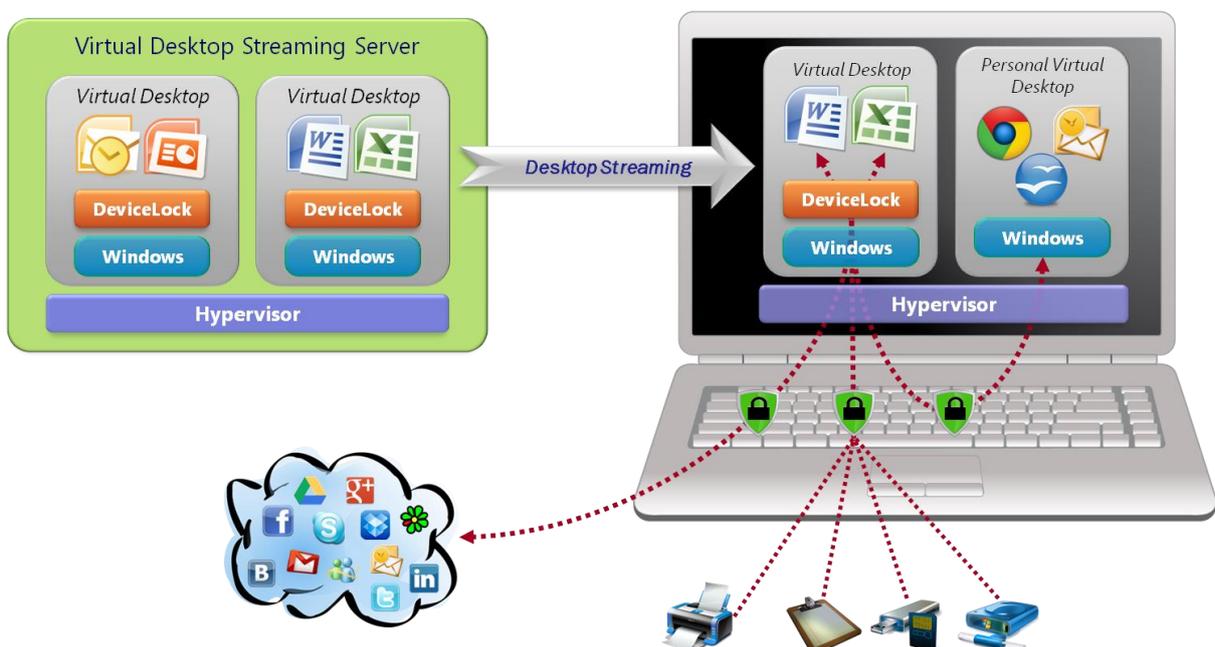
DeviceLock has been verified by Citrix and VMware to work with Citrix XenDesktop, Citrix XenApp and VMware Horizon View solutions. Microsoft RDS is also fully supported, as well as other remote virtualization solutions based on RDP, ICA, PCoIP and HTML5/WebSockets protocols.

Best of all, the DLP protection delivered by Virtual DLP to BYOD solutions based on desktop and application virtualization is universal and works for all types of BYOD devices. These can include mobile platforms, such as iOS, Android and WindowsRT, thin terminal clients with Windows CE, Windows XP Embedded or Linux, as well as any computers that run OS X, Linux, or Windows.

Organizations standardized on any virtualization platform for their BYOD strategies will benefit greatly from deploying the DeviceLock Endpoint DLP Suite, since it is the most effective, straight-forward and affordable way of implementing comprehensive endpoint DLP services for any type of BYOD devices.

How Virtual DLP Works with Local Virtualization

The fact that DeviceLock is a Windows application and runs within the Windows OS environment that it protects governs how DeviceLock Virtual DLP works with local virtualization solutions generally comprised of desktop streaming platforms (such as Windows Thin PC, Citrix XenDesktop, VMware Workstation, and VMware vSphere), as well as pure local desktop virtualization products (such as VMware Workstation, VMware Player, Oracle VM VirtualBox, and Windows Virtual PC).



Running within the virtual Windows desktop, the DeviceLock agent enforces centrally defined DLP policies to protect data access and transfer operations of VM's applications and users to local and shared peripheral devices as well as the Windows clipboard. Equally controlled are local data interactions with another virtual machine on the same BYOD endpoint – in most cases, a personal virtual desktop.

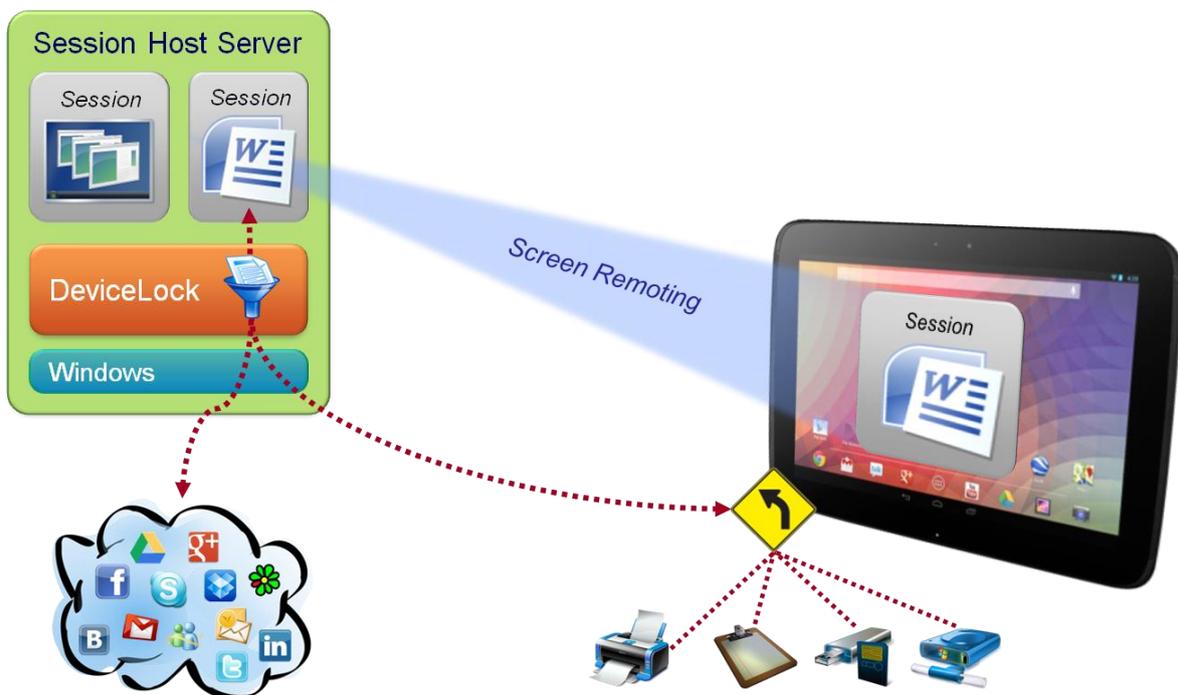
In addition, the DeviceLock agent controls network communications of applications and users from the corporate virtual desktop out to the Internet and even out to the internal corporate network.

Virtual DLP Use Scenarios

The use-case scenarios presented below are aimed at explaining how Virtual DLP complements Windows desktop/application virtualization solutions to deliver content-aware and contextual DLP protection to various corporate virtualization deployments.

Scenario 1: Virtual DLP for Session Virtualization – Simplified Diagram

This is a simplified diagram of the vDLP scenario for session-based virtualization that enables remote access to virtual desktops and applications centrally hosted on terminal servers in Microsoft RDS, Citrix XenApp and XenDesktop, or VMware Horizon View solutions.



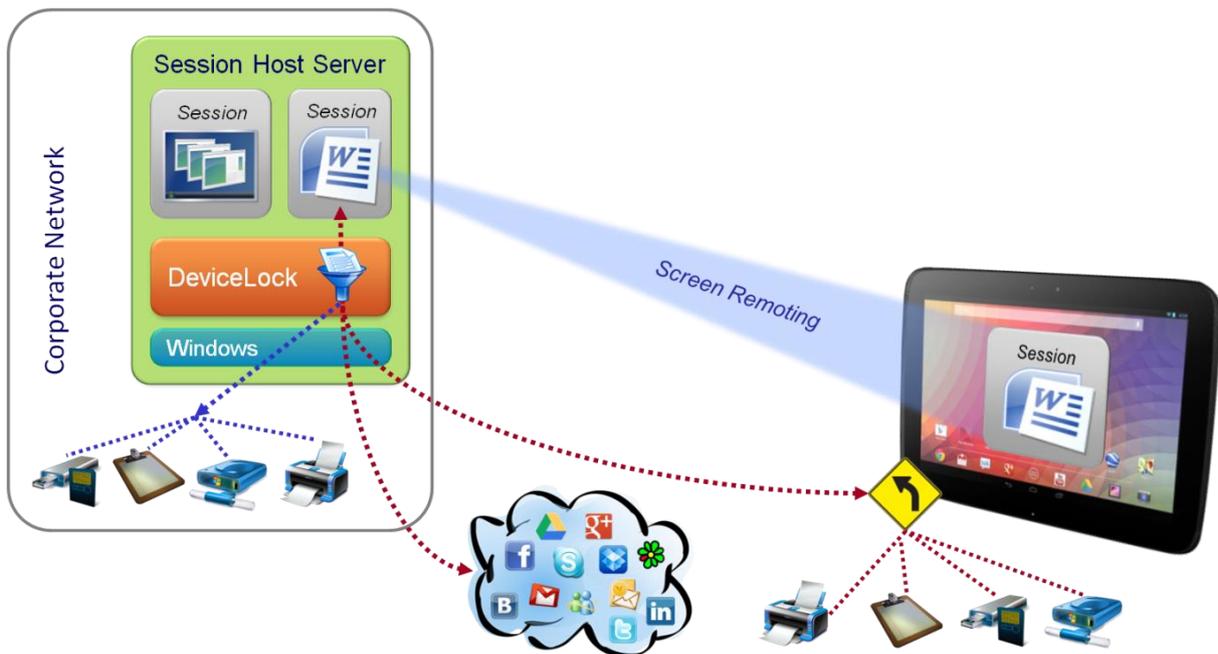
- In this Virtual DLP scenario, a native terminal client software (for RDP, ICA, PCoIP remoting protocols) is used on the BYOD device for providing user access to remote corporate desktop or applications in the terminal session.
- From the remote BYOD device (e.g. Google Nexus 10), its user starts Citrix Receiver (or any other RDP/ICA/PCoIP remoting protocol client), which connects the user to a session on the corporate terminal server (e.g. Microsoft RDSH) where hosted business applications (in this case MS Word) assigned for this user run. Note that another session on the terminal server is shown with a pool of virtual desktops running. This is shown in order to positively address the question whether the DeviceLock protected scenario covers remote access to session-based virtual desktops.
- To increase user's productivity while working on the BYOD device, locally connected peripherals and the clipboard of the BYOD device are redirected to the terminal session on the server. This generally enables the user to save or print documents to the BYOD flash drive or a locally connected printer, as well as copy and paste data from the BYOD device to the document the user is editing in MS Word within the terminal session.
- At the same time, the content of the documents and data transferred via redirected devices and the clipboard shall comply with the acceptable data use policy (i.e. the corporate data security policy, government or industry regulations such as HIPAA, SOX, etc.).

- To ensure compliance, once the data transferred via redirected peripheral devices and the clipboard of the BYOD endpoint reach the terminal server, the DeviceLock agent intercepts them and in real-time checks whether the context of specific data transfer operations and the content of data being transferred comply with the DLP policy specified for this user and the BYOD device. If a policy violation is detected, the analyzed data transfer operation is blocked. In addition, relevant logging, shadowing, and alerting actions can be generated to facilitate the incident management, post-analysis forensics, and auditing tasks necessary for verifying compliance.
- As the specified DLP policy precisely interprets the acceptable data use policy, the DeviceLock solution's granularity and flexibility of control ensures that all legitimate business-related data transfers between the virtual corporate environment in the terminal session and the personal part of the BYOD device are performed transparently for the user such that business productivity is optimized while being secure
- At the same time, all data transactions that trigger DLP policy violations are blocked to keep the security of corporate data uncompromised.
- DeviceLock enforces contextual and content filtering controls over the user's network communications from within the virtual corporate environment in the BYOD device. In this scenario, the user may decide to send an unauthorized document via email to a colleague directly from the MS Word application. DeviceLock will monitor and analyze the context of this operation (whether the user is allowed to send emails to this colleague at all) and the content of the document being sent. In case the sending of this document violates the corporate acceptable data use policy, the transaction will be blocked with relevant event logging, data shadowing, and alerting actions assigned for this type of violation.
- It is not shown on the diagram, but the setting for the DeviceLock agent on the terminal server is typically managed from the DeviceLock MMC snap-in that runs within the Microsoft Group Policy Management Console used with Microsoft Active Directory deployments.

Scenario 1: Virtual DLP for Session Virtualization – Complete Diagram

This diagram fully encompasses the previous simplified one but additionally shows that DeviceLock can simultaneously control data transfer operations that the user may perform from the application (MS Word) in the terminal session with peripheral devices accessible from the terminal server locally or in the corporate LAN (office network).

These devices include local and mapped drives, local and network printers, removable storage devices, as well as any other devices controlled by DeviceLock. In addition, copy/paste data operations via the local Windows clipboard in the terminal session are granularly controlled. Therefore, this diagram is more comprehensive than the previous one.



Scenario 2: Virtual DLP for Session Virtualization with HTML5 Browsers

This simplified diagram shows a vDLP use case in a session virtualization scenario where HTML5 web browsers are used instead of native terminal software clients (such as Citrix Receiver).



From the DLP implementation architecture standpoint, this scenario basically corresponds to the simplified vDLP scenario of session virtualization depicted on diagram 1. Through the remoting protocol, the user is provided with remote access to a centralized corporate desktop (in this case) that runs in a terminal session on the terminal server.

The main reason for separately presenting this scenario is that no native terminal client software has to be installed on the BYOD device. Instead, any standard HTML5 web browser can be used, which plays the role of a zero-install terminal client. Most popular web browsers support the HTML5 standard, and these include Firefox, Chrome, Safari, Opera, and Internet Explorer 10. Secure HTML5 web browsers, such as Citrix @WorkWeb, can be used as HTML5 terminal clients as well.

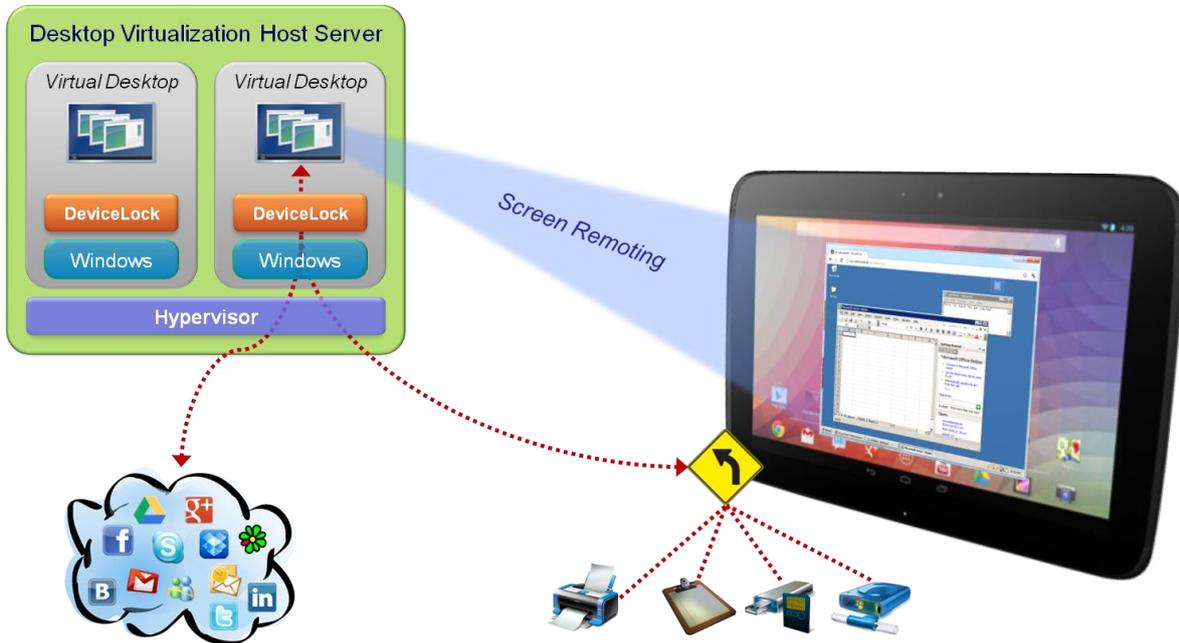
As a result, it is no longer necessary for organizations to spend time, money, and labor resources to deploy and manage native terminal session clients. Because of the anticipated simplicity for end users and savings for IT organizations, this scenario is becoming very popular on the market.

There is another technical difference between this scenario and the scenario with native terminal clients (from diagrams 1 and 2). In this case an additional architectural component, a RDP-HTML5 proxy server, has to translate native remoting protocol (e.g. RDP or ICA) to the HTML5/WebSockets protocol used by HTML5 web browsers for remoting the session.

It is important to note that the DeviceLock vDLP implementation is neutral to this protocol conversion and fully supports this virtualization scenario. The reason is that the DeviceLock agent enforces its DLP controls over the data transferred in the terminal session before that data gets encapsulated in the remoting protocol.

Scenario 3: Virtual DLP for Hosted Virtual Desktops

This simplified diagram shows a vDLP use case in a virtualization scenario where virtual desktops are hosted centrally, but not as desktop pools in sessions on a Terminal Server (diagrams 1-3). Instead they run as separate virtual machines on a hypervisor in a Desktop Virtualization Host Server.



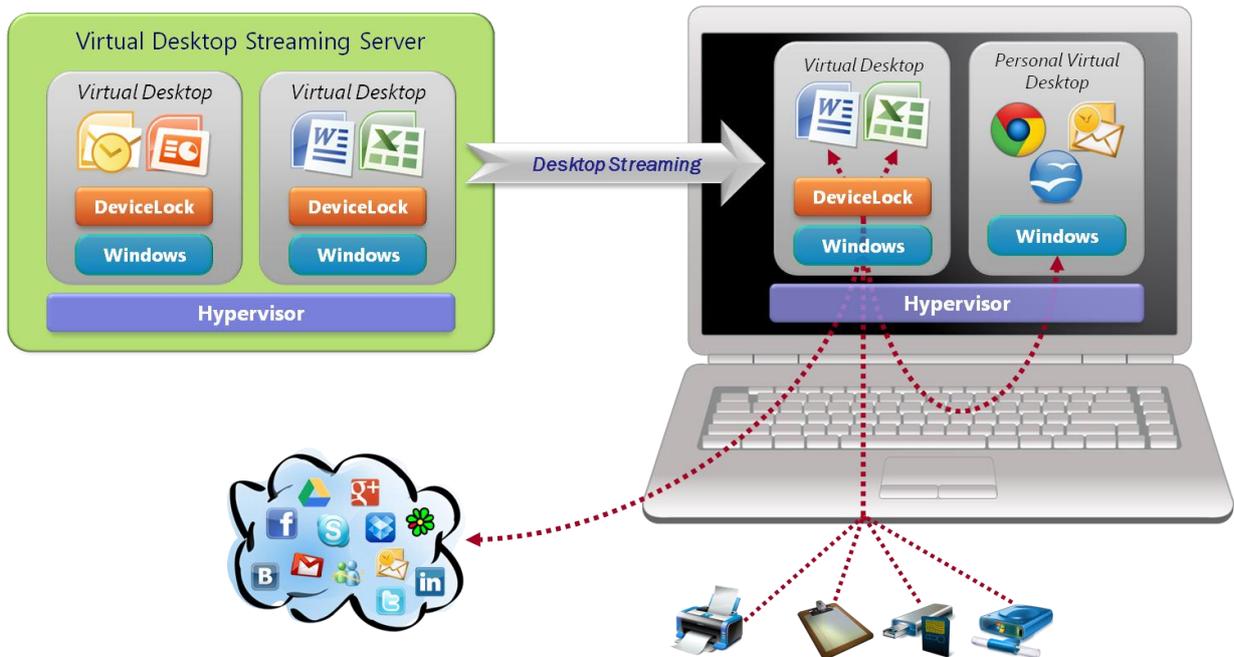
- From the remote BYOD device (e.g. Google Nexus 10), its user starts Citrix Receiver (or any other RDP/ICA/PCoIP remoting protocol client), which connects the user to a remote virtual desktop on the corporate Desktop Virtualization Host Server (e.g. Microsoft RDVH) where the virtual desktop assigned for this user runs as a virtual machine above the hypervisor.
- To increase user’s productivity while working on the BYOD device, locally connected peripherals and the clipboard of the BYOD device are redirected to the remote virtual desktop on the server. This enables the user to save or print documents to the BYOD flash drive or a locally connected printer, as well as copy and paste data from the BYOD device to applications that the user starts on the remote desktop.
- At the same time, the content of the documents and data transferred via redirected devices and the clipboard shall comply with the acceptable data use policy (i.e. the corporate data security policy, government or industry regulations such as HIPAA, SOX, etc.).
- The important difference of this scenario is that the DeviceLock agent is installed and runs in every virtual desktop instance hosted centrally at the Desktop Virtualization Host Server.
- Once the data transferred via redirected peripheral devices and the clipboard of the BYOD endpoint reach the virtual desktop,
- the DeviceLock agent intercepts them and in real-time checks whether the context of specific data transfer operations and the content of data being transferred comply with the DLP policy specified for this user and the BYOD device. If a policy violation is detected, the analyzed data transfer operation is blocked. In addition, relevant logging, shadowing, and alerting actions can be generated to facilitate the incident management, post-analysis forensics, and auditing tasks necessary for verifying compliance.
- As the specified DLP policy precisely interprets the acceptable data use policy, the DeviceLock solution’s granularity and flexibility of control ensures that all legitimate business-related data transfers between the virtual corporate environment in the terminal session and the personal part of the BYOD device are performed transparently for the user such that business productivity is optimized while being secure
- At the same time, all data transactions that trigger DLP policy violations are blocked to keep the security of corporate data uncompromised.
- In addition, DeviceLock enforces contextual and content filtering controls over user network communications from within the virtual corporate environment.
- For simplicity, DeviceLock’s central management components are not shown on the diagram.

Scenario 4: Virtual DLP for Streamed Virtual Desktops

This diagram shows a vDLP use case in a virtualization scenario where full virtual desktop images are configured on the central Virtual Desktop Streaming Server and then streamed down to the remote BYOD endpoint computer.

Virtualization solutions supported in this scenario include Windows Thin PC, Citrix XenDesktop, VMware Workstation, VMware vSphere.

On the target computer on the right, the streamed Windows desktop runs as a separate virtual machine on the local hypervisor (such as Citrix XenClient, Windows Virtual PC, and Windows Client Hyper-V).



From the DLP implementation architecture point of view, this scenario requires that the DeviceLock agent is installed in every virtual Windows image streamed to the target BYOD endpoint.

After the desktop image has been delivered to the endpoint, it starts running there locally as a virtual machine. The DeviceLock agent runs within the virtual Windows desktop and enforces necessary DLP controls to protect data access and transfer operations of VM's applications and users to local and shared peripheral devices, and the Windows clipboard.

Equally controlled are local data interactions with another virtual machine on the same BYOD endpoint – in this case, a personal virtual desktop.

In addition, the DeviceLock agent controls network communications of applications and users from the corporate virtual desktop to the Internet and the corporate network.

As a result, in this scenario the DeviceLock agent prevents data leaks from the corporate virtual desktop to the Internet and to the rest of personal computer, which is not controlled by the organization and should be otherwise considered as an unmanaged endpoint and insecure BYOD environment without DeviceLock DLP managing the image.

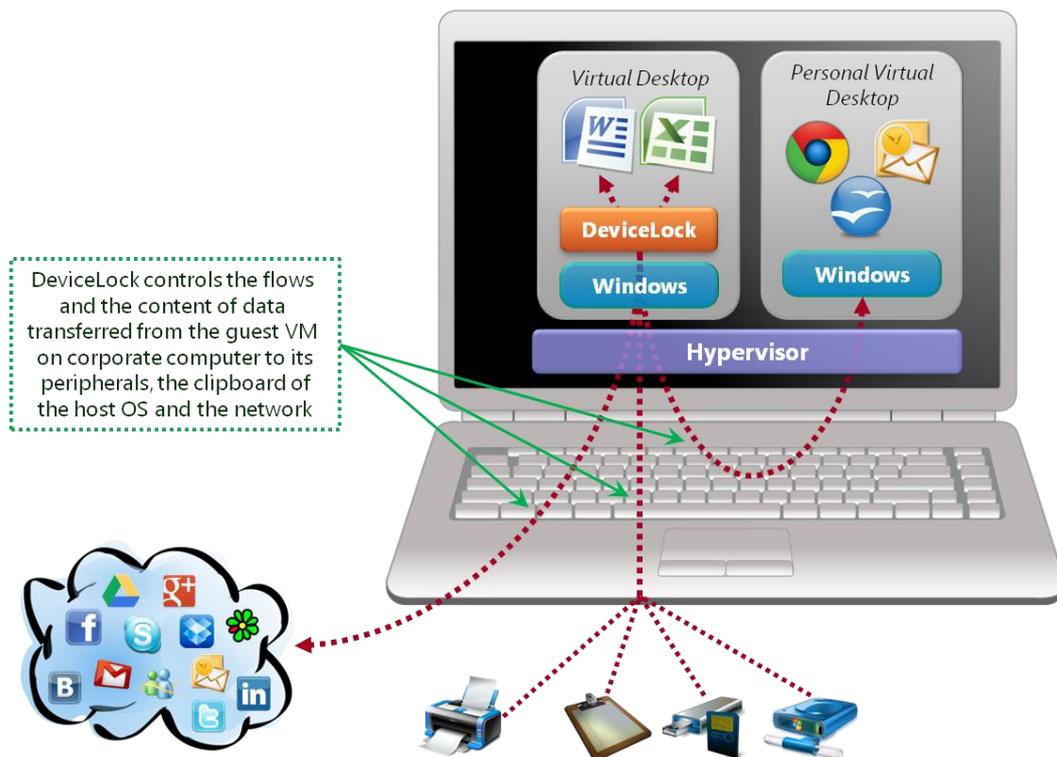
Scenario 5: Virtual DLP for Local Virtual Desktops

This diagram shows a vDLP use case in a virtualization scenario where the virtual desktop that runs on the target computer is provisioned locally.

This is the only difference between this scenario and the previous one - Virtual DLP for Streamed Virtual Desktops.

DeviceLock Virtual DLP works in any virtualization solutions that support this scenario, for instance, VMware Workstation, VMware Player, Oracle VM VirtualBox, Windows Virtual PC, etc.

On the target computer on the right, the virtual Windows desktop runs as a guest virtual machine on the local hypervisor.



This scenario requires that the DeviceLock agent is installed in the guest (corporate) Windows VM at the target BYOD endpoint.

The DeviceLock agent runs within the virtual corporate Windows desktop and enforces necessary DLP controls to protect data access and transfer operations of VM's applications and users to local and shared peripheral devices as well as the Windows clipboard.

Equally controlled are local data interactions with another virtual machine on the same BYOD endpoint – in this case, a personal virtual desktop.

In addition, the DeviceLock agent controls network communications of applications and users from the corporate virtual desktop to the Internet and the corporate network.

As a result, in this scenario the DeviceLock agent prevents data leaks from the corporate virtual desktop to the Internet and to the rest of personal computer, which is not controlled by the organization and should be otherwise considered as an unmanaged endpoint and insecure BYOD environment without DeviceLock DLP managing the virtual machine.

Virtual DLP for Small-Medium Business

As a significant portion of small and medium-sized (SMB) companies generally cannot afford expensive desktop virtualization solutions, they often use a free single-session RDP server (a.k.a. “Remote Desktop Connection”) that is built into any Windows Professional and higher versions. This provides SMB employees with remote access to corporate physical desktops from their personal BYOD devices. This session-based virtualization scenario requires an equally high level of data leak prevention for the remotely accessed physical desktop as for other types of desktop and session virtualization solutions based on terminal servers or VDIs.

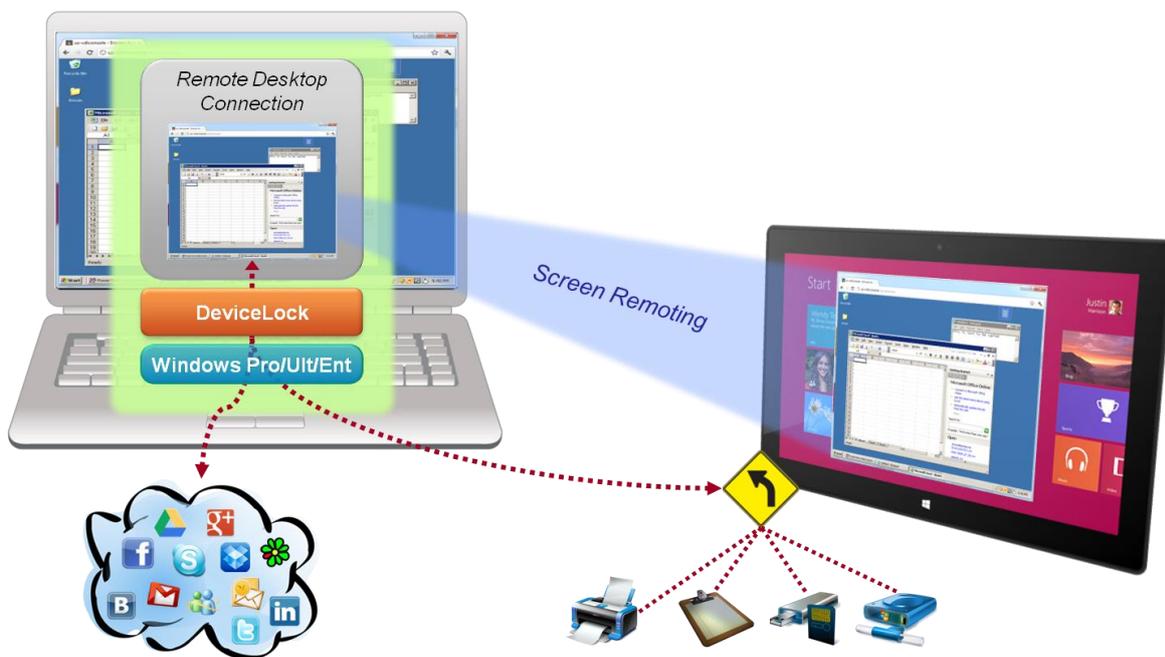
This desired functionality is exactly what Virtual DLP enables for the remote session to the desktop once the DeviceLock agent is installed at this computer. Remarkably for SMBs, the Virtual DLP licensing for a single terminal session from a DeviceLock DLP protected *desktop* (as opposed to *terminal servers* with DeviceLock¹) is included in the DeviceLock license acceptable usage and does not require additional investments from DeviceLock customers.

This licensing flexibility enables those DeviceLock customers that have upgraded to DeviceLock version 7.2 or above to *immediately and without additional expenses* extend the reach of their DeviceLock-based endpoint DLP solutions to employee’s mobile BYOD devices of any type.

The following subsections show three typical low-cost session virtualization scenarios for providing Virtual DLP-protected remote access to physical desktops.

Scenario 1 for SMB: Remote Access to Desktop from Windows RT or Macintosh

In this scenario, vDLP protects remote access to a Windows computer from a BYOD tablet with Windows RT or a Macintosh (Mac).



As Windows RT has a built-in RDP client, as well as Microsoft offers free Remote Desktop Connection Client for Mac, this scenario does not require any additional investment from DeviceLock DLP customers (“Free Virtual DLP for BYOD”).

¹ The free single-session Virtual DLP license is not applicable to terminal servers or virtual desktop host servers where DeviceLock is used for preventing data leaks from more than one virtual desktop or terminal session accessed remotely. In this case, multi-session Virtual DLP licenses must be acquired for the maximal number of protected terminal sessions on the server.

Scenario 2 for SMB: Remote Access to Desktop from iOS or Android

In this scenario, vDLP protects remote access to a Windows computer from any type of mobile BYOD device – such as those running iOS (iPad), Android tablets, as well as any other endpoint computers.



From the implementation standpoint, an RDP client software native to the BYOD device platform has to run on the device. An example of such an RDP client is PocketCloud Remote Desktop from Wyse. With the average price of RDP clients for mobile platforms in the \$8-15 range, this variant is a “low-cost Virtual DLP for BYOD” solution that can be attractive for SMBs.

Scenario 3 for SMB: Remote Desktop Access from HTML5 Browser

In this scenario, vDLP protects remote access to a Windows computer from any type of mobile BYOD device by using an HTML5 browser as a terminal client.



From the implementation standpoint in this case, a RDP-HTML5 proxy server should run on the Windows desktop to translate native remoting protocol (e.g. RDP or ICA) to the HTML5/WebSockets protocol used by HTML5 web browsers for remoting the session.

The examples of RDP-HTML5 proxy software products are Citrix Receiver for HTML5, Cybele ThinRDP, Ericom AccessNow, Remote Spark's SparkView, etc.

With the average street price of RDP-HTML5 software proxies in the range of \$25-50, this variant is also a "low-cost Virtual DLP for BYOD" solution for SMB customers.