DeviceLock

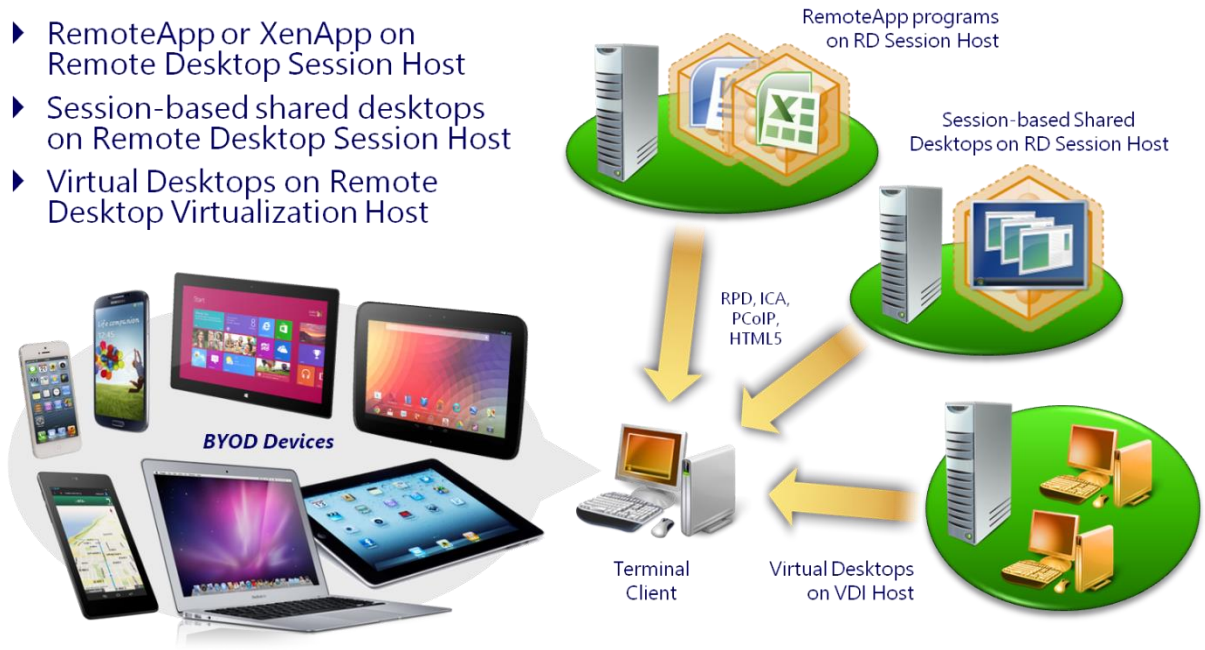
DeviceLock Virtual DLP for Remote Virtualization-Based BYOD

Remote Virtualization in Corporate BYOD Programs

Currently, more and more organizations use various remote virtualization solutions to reduce operational IT expenses and simplify IT maintenance and support processes. There are basically three types of remote virtualization scenarios.

The first is when user applications run in sessions on a terminal server while their screens are transferred to terminal clients via remoting protocols, such as Microsoft RDP, Citrix ICA, Terradici PCoIP and HTML5/WebSockets. The second and third scenarios enable users to virtualize and remotely access entire desktops – either via shared desktop sessions, or running every user desktop in a separate virtual machine on the VDI host server.

Remarkably, remote virtualization solutions enable employees to access business applications or corporate desktops not only from organization-owned workstations and terminals but also from any employee-owned Windows or Linux PC, Mac, or even mobile devices such as tablets and smartphones – in essence, from any bring-your-own-device (BYOD).



This is why organizations facing the challenges of the BYOD trend generally decide to implement BYOD programs based on remote virtualization platforms they already use, such as Microsoft RDS, Citrix XenDesktop/XenApp and VMware Horizon View.

There are many compelling reasons for this choice over reliance upon MDM solutions as follows:

- First and foremost, with BYOD based on remote virtualization platforms, organizations do not have to incur the labor overhead and responsibility of maintaining the entire BYOD device's corporate and personal environments, applications, and data. When using current MDM solutions, it is unavoidably necessary to maintain the entire BYOD device, which requires much more labor resources and creates more business risks for the organization.
- Secondly, in case of BYOD based on a remote virtualization approach, employees simply use Windows and familiar business applications while working in the corporate environments from their BYOD devices. As a result, organizations should not additionally maintain the corporate store of native apps for multiple mobile OS's – which is required in the case of MDM solutions.

Usually, maintaining such a corporate appstore is a daunting task that requires significant and specialized IT resources.

- Third and perhaps the most important reason: organizations that implement BYOD programs based on their existing virtualization platforms need not additionally pay for modestly effective MDM solutions.

In fact, the very nature of remote virtualization is intrinsically suitable for BYOD. With practically nothing to manage on employee-owned BYOD devices (except probably a terminal client requester software and perhaps an authorization certificate) and no corporate data stored there, organizations do not truly need to maintain and support these devices, which saves them money, deployment time, and resources. It is the BYOD owner who has to take care of their device, which was the original rationale for adopting BYOD in the first place. As a result, organizations are not responsible for any problems with the owner's private data and personal applications on BYOD devices, which is the major conflict and challenge with conventional MDM-based BYOD solutions.

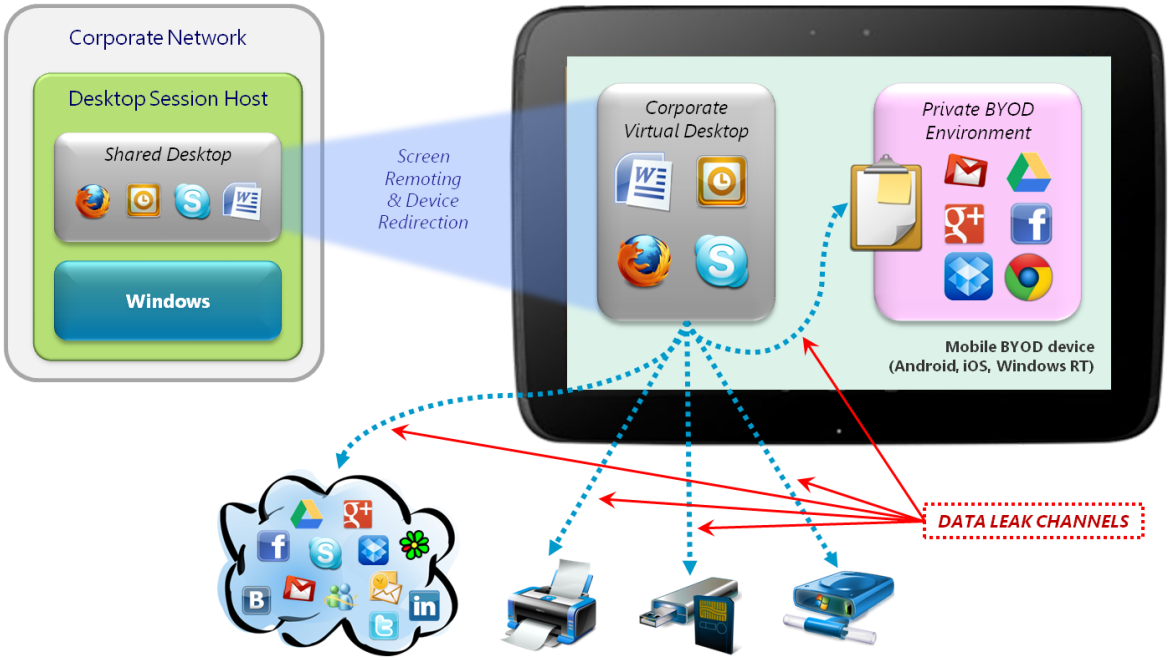
It cannot be overlooked that with a virtualization approach rather than MDM, the employees are happy that no one other than them maintains full control over their own devices, private data, and personal apps.

As a result of the many benefits for the enterprise and desired convenience for employees, remote virtualization is the superior approach to implementing BYOD programs in organizations that already use virtualization platforms such as Microsoft RDS, Citrix XenDesktop, or VMware Horizon View.

Data Security Challenges of Remote Virtualization in the BYOD Context

From the data security standpoint, the corporate virtual environment (desktop/application) in the terminal client or HTML5 browser on the BYOD device can be reliably isolated from its uncontrolled and untrusted native OS, private user data, and their personal applications. This isolation is even stronger than hardware-based, because corporate applications and virtual desktops physically run in the terminal session or virtual machines on the host server and ONLY their screens are displayed via remoting protocols to the BYOD device, while just user keystrokes and pointer movements are sent back.

However, to more productively work on BYOD devices, employees should be able to use locally connected peripherals, such as USB drives, removable storage, and printers from within the virtual session or desktop. It is also often required to copy data via the clipboard between applications in the corporate virtual environment and their personal apps that run natively on the BYOD device. Remote virtualization solutions enable these productivity capabilities by redirecting BYOD peripherals and the clipboard via remoting protocols to the session host.



While this redirection is strongly desired for employee productivity, at the same time it literally "perforates holes" in the full isolation between the corporate-protected virtual environment and the private untrusted part of the BYOD device. Without proper contextual and content-aware controls, each redirected peripheral becomes a wide open data leak channel from the virtual desktop or application session.

For example, from a business application in the virtual desktop, the user can save a file with sensitive corporate data to a flash memory card connected to the BYOD device, and then accidentally or intentionally publish this file to the Internet. Or, the user can print a confidential document from the corporate repository to a home printer connected to their personal tablet to cause a hardcopy data breach.

Indeed, today's remote virtualization solutions can be configured to *fully* block a local device redirection – but that would essentially interrupt the user's normal business productivity processes and therefore would just be impractical and result in a little-used or failed BYOD project.

The same is true for the network channel from the virtual desktop, which is used by employees for communicating with colleagues, partners, and clients via email and instant messengers, as well as accessing corporate applications and file storage in the cloud. Network communications must be enabled, but remote virtualization solutions themselves do not support the function of controlling which data and content are flowing through these channels out to the wild.

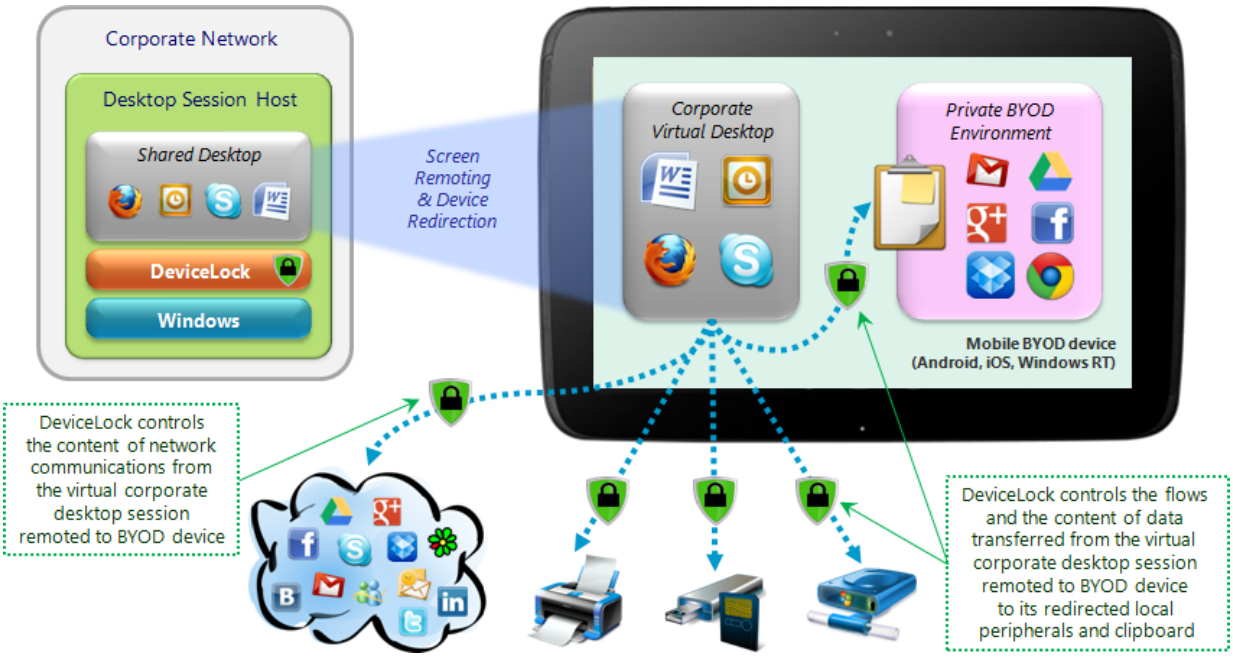
DeviceLock Virtual DLP – An Endpoint DLP for Remote Virtualization-Based BYOD Programs

DeviceLock's Virtual DLP features extend the reach of DeviceLock data leak prevention capabilities to a variety of virtual computing solutions based on remote virtualization technologies.

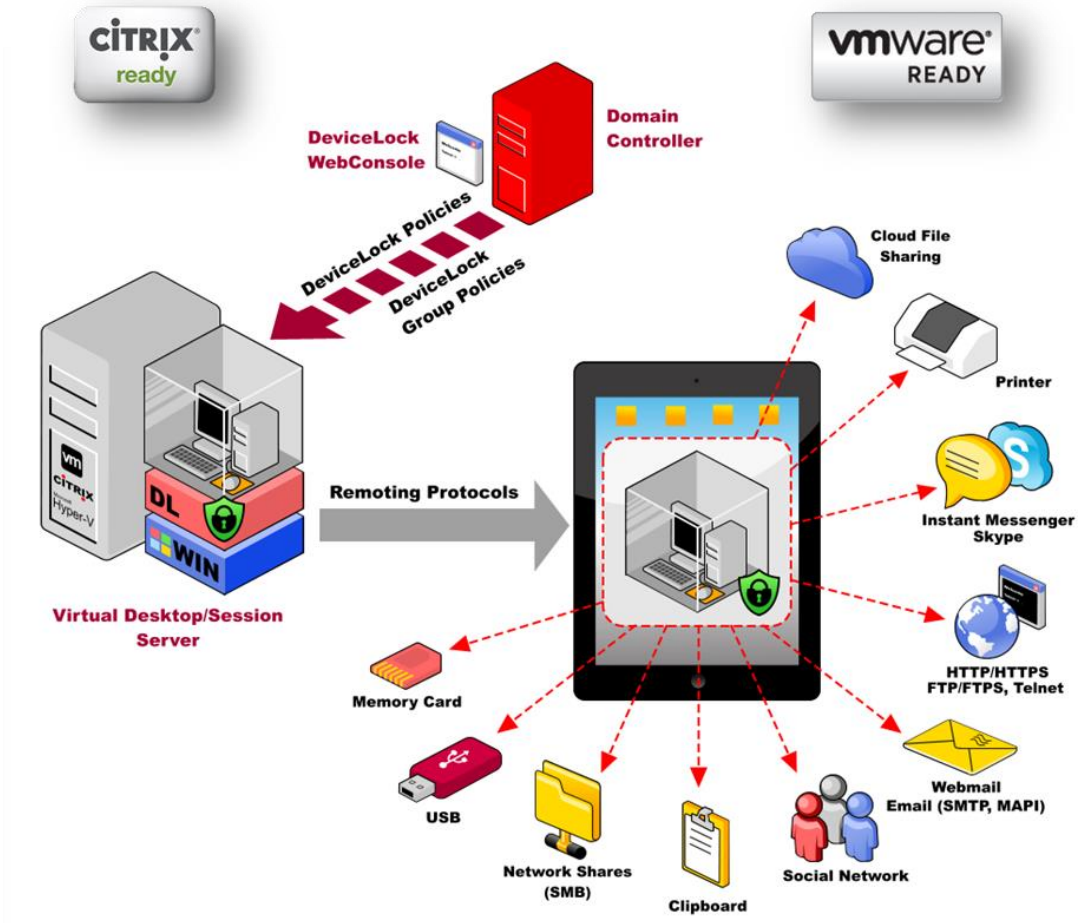
These include *session-based applications*, *session-based desktops*, as well as *hosted virtual desktops* (HVD) a.k.a. *virtual desktop infrastructure* (VDI) services implemented on virtualization platforms from major vendors: Microsoft RDS, Citrix XenDesktop, Citrix XenApp, and VMware Horizon View.

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 like removable flash drives, printers, USB ports, as well as the clipboard. In addition, user network communications from within the terminal session can be controlled by the DeviceLock DLP mechanisms.

Centralized event logging and data shadowing are also fully supported for all DeviceLock Virtual DLP scenarios.



As a result, by using the DeviceLock Endpoint DLP Suite in BYOD implementations based on virtualization platforms from Microsoft, Citrix, VMware, and others; organizations can fully control virtual corporate application and data environments accessed by employees' personal devices. In addition, they can monitor, inspect, and filter the content of all data exchanges between the protected virtual workspace and the rest of the BYOD device, its local peripherals, and the network – i.e., all those destinations outside of the corporate border that should be treated by default as 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 DLP policies. Employees otherwise maintain full control and responsibility over the device platform, personal applications, their private data, and the device maintenance and support. All of which provide a distinct advantage over the conventional BYOD-MDM approach, whereby the enterprise can be responsible for causing problems with the personal device and its owner's private data.



Best of all, the DLP protection delivered by Virtual DLP to BYOD solutions based on desktop and application virtualization is universal and works for any and all types of BYOD devices that support a terminal connection and browser. 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. DeviceLock Endpoint DLP Suite has been verified by Citrix and VMware to work with Citrix XenDesktop, Citrix XenApp and VMware View solutions. Microsoft RDS is also fully supported, as well as other remote virtualization solutions based on RDP, ICA, PCoIP and HTML5/WebSockets protocols.

Organizations standardized on any virtualization platform for their BYOD strategies will greatly benefit 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.