Technical Insight Report

Establishing a Secure Manageable Remote Work Environment

Using Open Source VirtualBox to Instantiate Corporate-approved, Encrypted VMs

By John Webster

November 2020

Evaluator Group

Enabling you to make the best technology decisions

ORACLE

Introduction – Remote Work Gains Permanent Traction

The post-COVID-19 reality for enterprise IT is now settling-in. Business executives need to give workers the ability and flexibility to work from a preferred location while fostering collaboration and motivation. Uncertainty is now a facet of the business climate and it is best to be prepared for potential disruptions down the road.

In order to cope with COVID-19, enterprises adapted – essentially overnight - to a workforce that was, practically speaking, entirely remote. And they did it by deploying resources they found to be immediately accessible. These included the extensive use of a well-established technology known as Virtual Desktop Infrastructure (VDI), coupled with immediately available cloud resources and Virtual Private Network (VPN) connectivity. Doing so allowed business users to conduct critical, day-to-day operations with little to no lapse in productivity while enterprise IT was able to control the remote workplace environment. VDI also added much needed layers of security and manageability vs. simply connecting remote user devices (laptops, desktops) over VPN links.

In this Evaluator Group Technical insight report, we look at the technologies now in use to support a remote workforce that preserves aspects of the office environment that fostered productivity. As mentioned, one immediately available solution is to simply replace office desktops with remote laptops connected via (VPN) connection. However, this solution might not be sufficient for many critical business applications as it engenders a host of enterprise security and data governance-related issues as well as creating a complex and error prone environment for managing remote devices. Using VDI as an alternative enabling technology addresses these issues.

Here we review Oracle's VM VirtualBox solution as an example of a VDI platform that combines open source development with Oracle extensions and support while simplifying remote device management an addressing enterprise IT's security and data governance mandates.

The COVID-19 Effect

In September of this year, the Evaluator Group conducted a survey of IT professionals who are still coping with the impact of COVID-19 on their IT organizations. We found that only 6% of them planned to be fully back in an on-site office environment by the end of 2020. The vast majority of them were planned to continue to work from home or commuting to the office on a part time/hybrid basis (see Figure 1. Below).

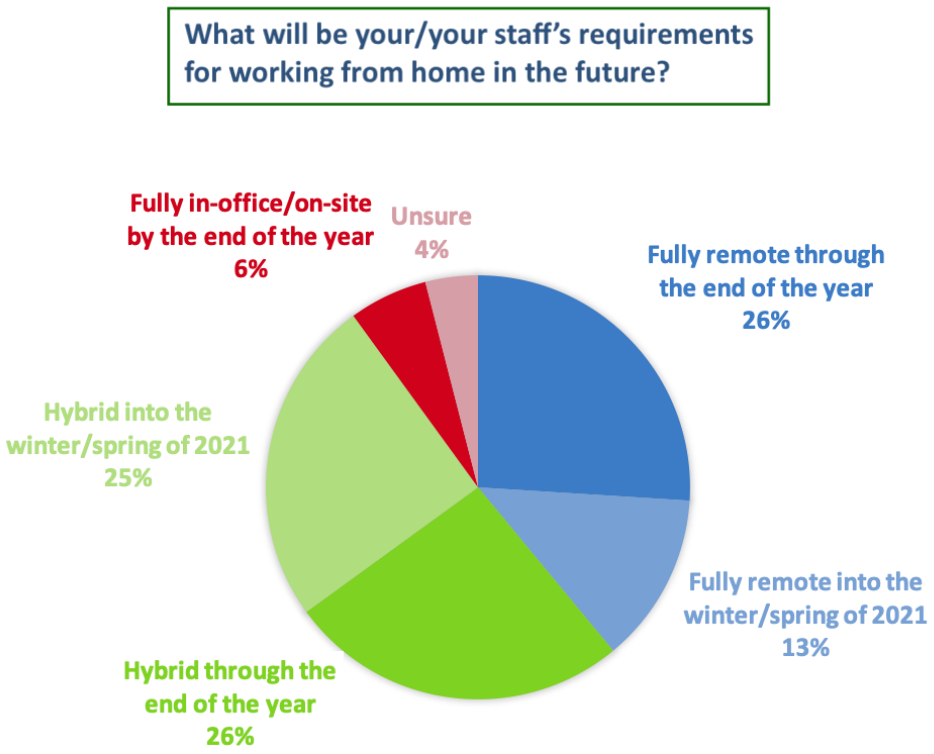

Figure 1. IT staff requirements for working from home in the future

In order to cope, they have deployed resources they found to be immediately accessible. These included the extensive use of Virtual Desktop Infrastructure (VDI) and public cloud resources. Doing so allowed business users to conduct critical, day-to-day operations with little to no lapse in productivity while enterprise IT was able to control the remote workplace environment.

Using VDI to Address Risk Exposure and Management Complexity

The shift to a remote workforce means that the devices used to access business applications are out "in the wild." This forces IT to question the extent to which they can trust a remote access system that in many cases encompass thousands of new devices. The attitude of many enterprise IT professionals toward the resulting risk potential can be summed up in a comment made to us by one of them: "We're in the open, hackers and bad actors are in the dark, always trying something new. Our job is to defeat them every time."

As a significant percentage of a company's workforce is still remotely accessing and using IT resources, we see that an expanded set of user devices is now exposed to malware, phishing attacks, and other security breaches. What the bad actors look for are new ways to hack into enterprise IT. Remote workers open up an expanded set of targets. They need not only to be using secure access points but also be trained on topics like phishing and ransomware. Some of our respondents reported that the saw

a 50% increase in such attacks through March and April of 2020 alone.

Enterprise IT professionals we surveyed reported the following IT initiatives as being most positively impacted by COVID-19 over the last six months:

1. Increased cybersecurity measures
2. Adoption/deployment of VDI
3. Implementation/expansion of public cloud resources

VDI is now a well-known technology used to deploy virtual as opposed to physical desktops. The advantages of using VDI to support an increasingly mobile workforce include:

- Rapid remote business user deployment on a user's preferred device
- Ease of remote user access
- Standardized access control
- Strict adherence to company security and business governance policies
- Centralized, efficient updating and management of up to thousands of remote workstations

Deploying VDI allows IT to distribute a standard and consistent platform for remote work that can be run on remote user devices, no matter the operating system, for which security features are already "baked-in." Training becomes easier as well when all remote users have and see the same environment with the security measure implemented.
In addition, they identified other issues that VDI could address including:

- *Complexity* resulting from differing access points, platforms, operating systems versions, and applications across potentially thousands of devices. Using a VDI implementation that was supported on a wide range of remote user devices allowed them to create and deploy from one to a few consistent desktop images that could be easily updated as necessary.
- *IT governance* policies that must be adhered to by remote workers as if they were working from office locations. These policies could be implemented in the VDI image that is distributed to all remote devices, assuring consistent adherence and preventing the possibility of exposing sensitive corporate data.
- *User errors* that create exposure to disruption and data loss as users adapt to their new and potentially unfamiliar work from home environments. A VDI image that delivered the same user experience on a device that the user was familiar with reduced the exposure to user errors that could result in data loss and security vulnerability.

Simply using Virtual Private Network (VPN) connections without VDI does not begin to address the issues noted above and our survey respondents generally avoided this approach. Workloads that were not suited to simple VPN connectivity included applications that generated sensitive data and critical transaction-oriented applications. However, they reported that VDI gave them the ability to quickly distribute remote access points that were locked-down and secure. In addition, VDI allowed them to

impose centralized measures aimed at compliance with their organizations' security and data governance policies.

Oracle VM VirtualBox – Addressing Risk and Complexity Issues

Oracle VirtualBox[1] is cross-platform, open source virtualization software that allows users to run multiple operating systems on the same computing device – from server clusters to a single laptop. When installed on a laptop or desktop, it can be used to deliver a preconfigured VDI image to remote users. As such, enterprise IT customers can deploy Oracle VirtualBox as a VDI solution consisting of all open-source components.

Features that make Oracle VM VirtualBox attractive as a VDI platforms include:

- Supports a wide range of Windows, Linux, Solaris, Mac, Unix, and OS2 versions of virtual machines (or as guest OS)
- The same VDI is supported on Linux, Windows, Mac OS and Solaris platforms as a host OS
- Deployment of a secure image remotely under the same or different OS (i.e. Linux VirtualBox on a MAC OS laptop)
- Role-based application access restrictions can be applied as well as access to datasets encompassed by restricted applications
- "Drag and drop" content between host and guest OS
- User-defined encryption keys to secure remote connections via 256-bit encryption keys
- VM and disk image encryption to secure against exposure to device loss or theft
- Ability to lock content sharing and copy/paste operations between the host and guest OS, so that data cannot be downloaded to, or copied to the local device
- Easy to learn and understand GUI for business application users
- Scriptable Command Line Interface (CLI)
- Web service API for remote control of a VirtualBox desktop by authorized clients
- Support for workloads of up to 32 virtual CPUs
- Vagrant Boxes for the rapid and automated provisioning of development VMs with pre-configured software
- Import and export via GUI of virtual machines in standard OVF format, on-premises or in the cloud.
- Single-click upload or download of a virtual machine for Oracle Cloud Infrastructure.

[1] https://www.oracle.com/virtualization/virtualbox/

- Shared storage between VMs deployed on single device allowing applications which depend on the same data to run on a single device without needing NAS or SAN or other enterprise shared storage.

Using VirtualBox, an enterprise IT administrator creates a “gold image” of a corporate desktop to be used by a remote business application user. The gold image is then distributed via download and installed on remote devices. This process can be used with restricted or critical applications that are not designed for remote employee access. With VirtualBox, these applications can be deployed as a secure image on any client, run in isolation from other applications, and run under a different OS (see figure 2. below).

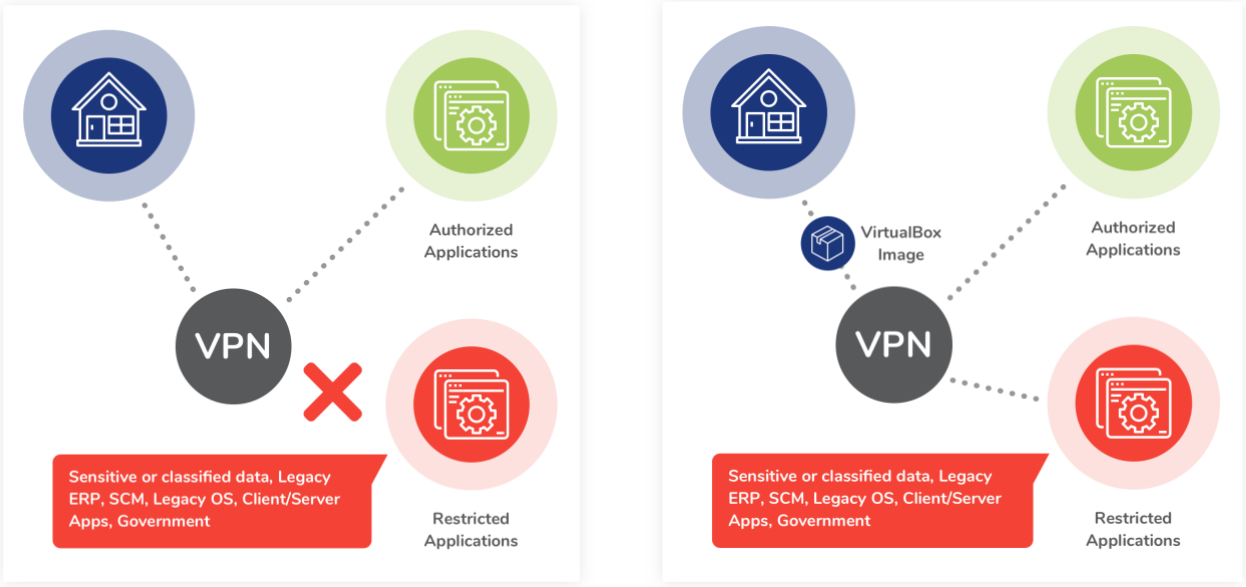

Figure 2. Remote employee access to restricted applications without Oracle VirtualBox (left) and with Oracle VirtualBox (right) Source: Oracle

Subsequent releases of the gold image to fix security issues as they come up for example are distributed and installed in the same way. This methodology ensures that remote workplaces are deployed consistently, simplifying the management of potentially thousands of remote devices, and greatly reducing exposure to errors that could be created in the process. It also gives enterprise IT a quick and consistent way to implement corporate security and governance policies within a work-form-home environment. And if needed, administrators can create standard images for most business users plus another one that is more secure for workloads with higher sensitivity. To further address security concerns, administrators can use Virtual Box to encrypt VMs prior to distribution to any remote desktop or laptop device.

Oracle VirtualBox Base is free for use under a GPL V2 license[2]. The Base package consists of all of the open-source components and users are free to modify and distribute the code. However, Oracle also offers an Extension Pack licensed under the VirtualBox Personal Use and Evaluation License (PUEL)[3] that includes the following features that will be particularly attractive to remote desktop/laptop users as well as IT administrators tasked with managing these devices:

Host webcam passthrough – a critical feature for the enablement video conferencing applications (Skype, Zoom, etc.) that have brought user groups together in a collaborative atmosphere while working from home.
Cloud development and migration – applications developed for VirtualBox VMs can be uploaded to or downloaded from Oracle Cloud without modification.
VirtualBox Remote Desktop Protocol (VRDP) – a backwards-compatible extension to Microsoft's Remote Desktop Protocol (RDP) that can be used by an IT administrator to control remote VDI instances.
Virtual USB 3.0 device support – allows users to have USB 2.0/3.0 devices connected to VirtualBox VMs. In addition, when Oracle VM VirtualBox acts as a VRDP server, it is also possible to use USB devices remotely on RDP clients.
VM and Disk Image Encryption– for the encryption of VirtualBox-related data stored on the remote device. This feature is critical to ensuring that if the remote device is lost or stolen, the VirtualBox image and its data will remain inaccessible.

Commercial licenses and technical support by Oracle is provided by purchasing Oracle VM VirtualBox Enterprise which includes:

- Commercial use license and 24x7 support from Oracle for the Base Package and Extension Pack
- Multiple remote desktop connections (VRDP) to virtual machines
- Centralized, tracking of VirtualBox Extension Pack downloads and installation compliance
- Esurance that all VirtualBox instances are on the latest release and have the latest security patches

Conclusion

What business executives need now is to give workers the ability and flexibility to work from a preferred location – be it local or remote – while fostering collaboration and motivation in either situation. Uncertainty is now a facet of the business climate and it is best to be prepared for potential disruptions down the road. Because VDI can be deployed quickly and consistently, it can and will be used in circumstances similar those presented by COVID-19 which in many ways mimicked a disaster that IT had

[2] https://www.virtualbox.org/wiki/GPL
[3] https://www.virtualbox.org/wiki/VirtualBox_PUEL

to immediately recover from. Therefore, it is no surprise that our survey revealed that the organizations with comprehensive and often tested disaster recovery plans were the best prepared to handle work from home mandates. Many of these same organizations turned to VDI to bring their remote workforces back quickly and efficiently to productivity.

For IT administrators, Oracle VM VirtualBox can be effectively used as a secure, open source VDI solution that is lighter weight than others available. It allows business users to quickly continue to access business critical applications without the need for time consuming and costly modification. With VirtualBox, business users utilize their preferred desktop/laptop systems by being deployable on Microsoft Windows and Mac OS machines as well as on Linux and Solaris x86. At the same time, VirtualBox can be customized by IT administrators to fit their specific environments while being responsive to corporate security and IT governance requirements. VirtualBox comes with continued open source community development and support from Oracle. Therefore, we can expect to see community growth and feature enrichment as time goes on.

We believe that VDI will become the preferred environment for hosting an at-home workforce because security enforcement is more effective, management can be centralized and automated, and supporting infrastructure can be ramped up and down quickly. Therefore, the ability to support VDI at scale will become a permanent fixture of enterprise IT strategies. Along the way however, IT administrators will be considering the most effective ways to scale and manage VDI environments going forward. Open source Oracle VM VirtualBox gives enterprise IT professionals a full featured solution that is consistent with today's work from home support strategies.

About Evaluator Group

Evaluator Group Inc., an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.