When It Makes Sense to Move to Desktop Virtualization: Seven Key Indicators

WHITE PAPER

vmware®

Overview

Consolidating your datacenter through server virtualization with VMware® vSphere® has provided you with many benefits, including saving physical space, reducing power and cooling costs, lowering management costs and more. Now, you can apply the same basic strategy to dealing with end-user systems by virtualizing desktops—and reap many benefits.

With the quantity and growing variety of devices that you must purchase, secure, manage and upgrade, it may be time to consider implementing a virtual desktop infrastructure (VDI) with VMware® Horizon View™. This approach delivers a rich, personalized, virtualized desktop computing experience for users, and it centralizes and automates management for administrators.

The question is: How do you know when it's time to move to VDI? Seven key indicators are signs that your organization is ready for the benefits of desktop virtualization.

1. Your users are increasingly embracing Bring Your Own Device (BYOD), working from remote locations and requiring remote access to your organization's data.

From smartphones to tablets to laptops, employees are increasingly mobile and determined to stay connected with work on their terms. By providing users with their own virtual desktops, you ensure that they can access the data they need to be productive from whatever device they choose, wherever they are.

Devices that users provide may not meet company performance or security standards, and IT staff cannot be expected to manage them all. A simpler solution is to use desktop virtualization to manage mobile devices, which can alleviate many of the headaches that IT staff experience with BYOD. VDI allows users to access their work from any device while eliminating IT concerns about what those devices are, because administrators ensure virtual desktops meet your performance and security standards.

With VMware Horizon View Client for Windows®, Mac OS®, Linux®, iOS and Android™, users can access their personal virtual desktops from a wide variety of devices. Local Mode further lets mobile and offline users download encrypted virtual desktops to their local devices so they can access data securely without a network connection.

2. You are concerned about security.

Every laptop or desktop is a potential liability when it comes to keeping data secure. While laptops allow employees to work remotely from home, in a coffee shop, or on a business trip, their portability makes your organization's data vulnerable to loss or theft. Even desktop systems that do not leave the office may be at risk of access or theft by those looking to get their hands on sensitive information. Organizations spend a great deal of money and effort to prevent data loss from endpoint devices. They invest in technologies such as hard-disk encryption, trackers, data loss prevention software and more. In a virtual desktop environment, important data resides on servers and storage in the secure datacenter, rather than on devices themselves. This approach provides much greater security for your important data. Furthermore, using other products, such as VMware ThinApp®, in conjunction with VMware Horizon View lets you isolate applications from operating systems, so users can continue working with legacy applications on current virtual desktops without any need for expensive migrations. Adding complimentary security products, such as VMware vShield Endpoint, can remove the burden of antivirus and antimalware solutions from end-user devices and centralizes those challenges, which allows IT to monitor devices and more simply manage antivirus tools.

System administrators can maintain better control of data and those who have access to it in a VDI environment. If a user is no longer authorized to access corporate data, IT staff can easily revoke access to that user and prevent any damage to or loss of sensitive data that might occur in a traditional endpoint environment.

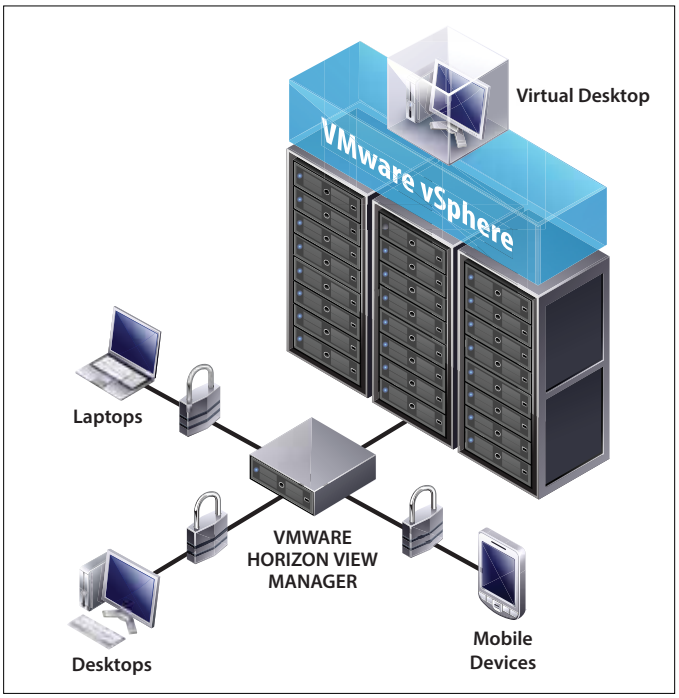

Figure 1. Virtual Desktop Infrastructure with VMware Horizon View Overview

3. You want a common desktop experience.

You know how your business operates and the tools that your employees need for success. Standardization is often the key to repeatability and quality assurance of a product or service. No matter the applications they use, users get a common desktop experience with VDI. Desktop virtualization ensures each user has access to the applications, programs and data that corporate policies dictate. Because IT staff create virtual desktops from a single image, it is easy for them to deliver updates and OS refreshes. Instead of physically handling each device, administrators need only update an image and recompose the desktop to refresh the corporate image, update drivers and applications, and deliver the desktops to employees.

The common desktop experience can also increase productivity. No matter where a user accesses his or her virtual desktop, the experience remains the same. Users can access all their data all the time, without fear of forgetting to send a file to work from their home systems.

4. You face compliance requirements.

Strict regulatory requirements apply to some data, such as medical records. Regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act establish national standards for the privacy and security of health information—and enforce them with stringent penalties. Similarly, the Sarbanes-Oxley Act of 2002 enacts strict security guidelines and defines best practices for how management and accounting firms must certify the accuracy of their financial data. Penalties for non-compliance can include up to a 10-year prison sentence and fines of up to $15 million. Because VDI centralizes data in the datacenter, it's much easier to make sure data complies with these regulations and to make any changes the regulations require. By implementing secure virtual desktops, administrators can make changes quickly in one spot, rather than going through the arduous process of finding and making changes to copies of the data on countless endpoint devices.

Diverse endpoint devices have also proven difficult and time-consuming for IT staff when they have to track the many security patches and data backups these regulations require. Desktop virtualization with VMware Horizon View can lower the cost of regulatory compliance by providing administrators a simpler, more accurate way to track patch and backup information, all of which occurs from VMware Horizon View Manager.

5. You want maximum agility and business continuity.

Endpoint devices can suffer any number of traumas, and downtime resulting from endpoint failure can be expensive. Whether a laptop or tablet is lost or stolen, suffers damage from an accident, or simply fails, with a traditional infrastructure the result is the same: the user cannot access his or her work from that device. Even in cases where the system eventually recovers, downtime can cripple an urgent project and tie up IT staff as they try to repair the device. With a virtual desktop, users can pick up right where they left off and continue business as usual from another device, without losing any work.

Desktop virtualization with VMware Horizon View enables you to respond to changing dynamics in your organization quickly and with ease. From adding contractors to handling mergers and acquisitions, VDI lets you scale up and down on demand, removing the long and expensive procurement processes that are typical with traditional endpoint management models.

6. You want to ease desktop management and upgrade headaches.

With desktop virtualization, desktop management has never been simpler. In a traditional environment, IT staff would either need to physically access each endpoint device or work with complex software and scripts to remotely manage updates, such as rolling out a new version of an application, installing and configuring the application, and ensuring that it is working properly. On a large scale, this effort not only monopolizes the time of IT staff, it also decreases user productivity as the upgrade happens. VMware Horizon View reduces endpoint upgrade and maintenance time, because IT staff can quietly upgrade applications on virtual desktops from the datacenter.

VMware Horizon View offers a number of additional features that simplify desktop management. VMware Horizon View Manager provides a common interface for desktop provisioning, resource allocation and image management, which makes it easy for administrators to deploy, customize and set policies for virtual desktops. VMware Horizon View Composer handles advanced image management, allowing speedy linked-clone deployment. Administrators can also monitor the performance of both individual desktops and the infrastructure as a whole to troubleshoot issues and optimize resource utilization using VMware vCenter™ Operations Manager for Horizon View.

7. You accommodate an ever-changing workforce composed of both contractors and employees.

Regular employees are not the only ones who need to work with company data. Interns, contractors, and other temporary workers might need access to some of your data alongside permanent employees, but they may not require full access to all sensitive information. Desktop virtualization with VMware Horizon View gives IT easy control over who can access what data and when. VMware Horizon View Manager allows administrators to customize desktops and set policies that limit permissions to groups and individuals within the organization. Because virtual desktops are dynamic, they can be persistent or disposable, making them an ideal fit for both permanent employees and short-term contractors. As your workforce grows and contracts, administrators can quickly and easily create new desktops or dispose of them as the situation requires.

Conclusion

If any of these indicators are present in your organization, it's time to give desktop virtualization a look. Traditional endpoint environments can be difficult to manage and can present a number of security risks that your organization cannot afford. Virtualizing desktops with VMware Horizon View can help you secure and manage user-provided devices as BYOD gains popularity, deliver a common desktop experience to end users, increase security and bolster regulatory compliance, maximize agility and business continuity, ease desktop management, and better accommodate all the users in your ever-changing workforce.

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com