mokafive™

WHITE PAPER

Manage Your Virtual Desktop with Layers

by John Whaley, CTO MokaFive

"The problem is that desktops are monolithic. Everything—the hardware, operating system, corporate applications, user-installed applications, plugins, user data—are all mixed up together so it is difficult to manage or control one without affecting the others."

Desktop management is becoming more and more challenging. Today employees are far more tech-savvy than they were just a few years ago. This has led to greater productivity, but also increased the demands on technology. Employees need flexibility to be productive. They expect to have access to information wherever they go, whether they are in the office, at home or on the road. People want to be able to install their own browser plugins and drivers for their home printers. They expect to be able to do research on Google, network on LinkedIn, pay their bills online, and connect with friends on Facebook anytime. The distinction between work life and home life is blurred - people work from home, and do personal tasks at work.

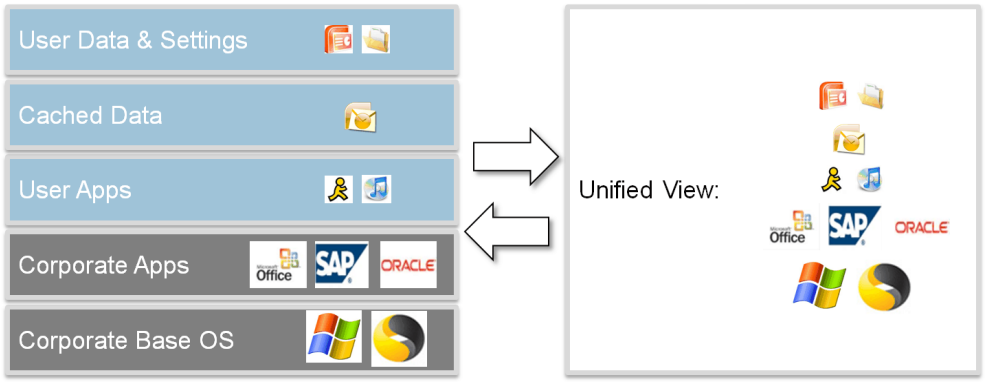
Business needs also present their own set of technology challenges. Regulations such as Sarbanes-Oxley, HIPAA, and the data breach notification laws that exist in most states, make security breaches very costly. Malware has become increasingly vicious and an attack can instantly cripple an organization and cost millions of dollars to clean up. Furthermore, the current economic climate introduces a whole other set of difficulties. Today's IT organizations have to do more with less: Budgets have been frozen and hardware refresh cycles have been extended. Additionally, there are more temporary and contract workers, which in turn introduces new provisioning and de-provisioning issues. And despite all these circumstances, IT is expected to move more quickly than ever to keep up with the accelerating pace of business.

The problem is that desktops are monolithic. Everything—the hardware, operating system, corporate applications, user-installed applications, plugins, user data—are all mixed up together so it is difficult to manage or control one without affecting the others. For example, locking down the operating system may make it more secure, but that could prevent the employee from installing an application or plugin he or she needs to be productive. To further complicate the situation, different parties are often responsible for different components. The hardware may be employee-owned, while the operating system is provided by a desktop engineering group, the corporate applications are supplied by the department, and the security updates are controlled by yet another group.

Desktop virtualization has been heralded as a panacea to these problems. By separating the software from the hardware, desktops become easier to manage. However, simply moving the desktop into a virtual machine does not solve the fundamental issue of managing the desktop, nor the fact that different parties are responsible for different parts of the desktop and these parties have conflicting concerns. Traditionally these issues have been resolved by either locking down the desktop, reducing functionality and thereby end-user productivity, or by giving each user their own unique desktop instance, which leads to image sprawl and makes them difficult to manage. But there is another way.

Virtual Layers

Just as you can use virtualization to separate software from hardware, you can similarly use virtualization to separate a desktop into virtual layers that can be managed individually. These layers are dynamically composited to provide a single unified view of the system. For example, you can separate the desktop into a layer for the operating system, a layer for targeted corporate applications, a layer for user applications and a layer for user data. Each of these layers are kept separate and can be managed individually, but to the user it looks and feels like a traditional desktop.



Managing virtual desktops with layers means you no longer need to individually manage, patch and update thousands of separate copies of the operating system—simply manage your one golden image which all users share.

Separating the desktop into layers gives you power. The fundamental power of virtualization comes from adding a level of abstraction. This allows you to easily add, remove, update and rollback individual components. It also empowers you to reuse the same components across different instances. Applying this technique within the desktop gives you flexibility and leverage on a fine-grained basis. You can use the same base operating system image for everyone and then layer customizations on top. This means you no longer need to individually manage, patch and update thousands of separate copies of the operating system. Instead, you simply manage your one golden image which all users share—saving you from a management nightmare. Likewise, any applications that are not distributed to all users—perhaps due to licensing restrictions—can be placed in a layer and targeted to only the users entitled to the application. The OS and application layers are sourced from the golden image on every boot, which means they are always up-to-date. If an image gets corrupted or attacked by malware, the user can immediately recover by restarting their desktop. This also avoids the problem commonly referred to as “Windows rot” - the tendency for a Windows installation to get slower and slower over time.

Separating the user personality into its own layer(s) apart from the system layer also allows each user to have their own customizations (if permitted) by automatically layering them on top of the standard IT-provided system image. When the user-installed applications are separated from the user documents and the user breaks their system

by installing incompatible software, they can easily recover by reverting or rolling back the user applications layer and nothing else. The rest of the system, including the latest changes to their documents, remain unaffected. Backups become much easier and more efficient as well—by simply backing up the user layer, you can get an efficient backup of just the user personality without the overhead of backing up the whole system, and thus recovering from a crash also becomes much easier. By splitting the user layer into user data (which is backed up) and ephemeral datawhich is not backed up), backups become even more efficient because they can skip temporary data such as Web caches or mail files that are also stored on the mail server.

Virtual layers are an application of a well-known principle in systems design called "separation of concerns." Separation of concerns means that you decompose a complicated problem into a set of meaningfully-distinct pieces that you solve individually, then compose the solution from the individual parts. Virtualization is the key technique that allows this separation while still providing a composite view of the whole.

Techniques for Virtual Layers

There are a number of products available today that provide the ability to separate out a Windows installation into various layers. The most basic products allow you to capture the user profile as an independent layer that can be managed separately from the rest of the system, so for example you can use the same user profile on different Windows installations. More advanced products are able to layer applications, use different policies for each layer, and even automatically capture user-installed applications into a layer.

Approaches for achieving layering can be categorized in three areas:

1. What view does the virtualization provide: isolated or layered?

2. Who can see the virtualized view: a single process, a collection of processes or the whole system?

3. What is being virtualized: filesystem, registry, services, kernel drivers?

Common techniques for layering include user profile redirection using registry hooks or reparse points, application virtualization, kernel drivers or file system filter drivers. Every product has its own set of pros and cons, but in general, the lower the layering hooks into the system, the more compatible the layering will be with a wider variety of programs and system services. Thus, layering techniques that leverage kernel components will be more compatible in general than pure user-space techniques.

The approach or product you use needs to support your desired use case. For example, if you are using a completely locked-down desktop where the user cannot install applications and can only save into the "My Documents" folder or a network share, a product that only handles the user profile may be adequate. However if you want to support more sophisticated use cases where the user personality includes installed applications, plugins, and printer configurations, you will likely need a more sophisticated product.

Isolation vs. Layering

It is important to draw a distinction between two different attributes provided by virtualization: isolation and layering. Virtualization is sometimes used to isolate processes from the rest of the system, to avoid conflicts or improve manageability. For example, with application virtualization you can bundle an installed application into a single executable that can run on multiple systems without installation or conflicting with other installed software. Application virtualization achieves this by isolating the application from the rest of the system, bundling the necessary pieces of the operating system and other libraries into a single unit. Although there are benefits to isolation, it has some drawbacks as well. Some interfaces are very difficult or impossible to adequately virtualize, such as applications that make use of kernel drivers, services, DCOM, etc., and thus are not compatible or do not work with application virtualization. In addition, because the applications are isolated, it is often difficult to get virtualized applications to integrate with each other; for example, copying-and-pasting from one virtualized application to another may not work correctly. Layering does not provide isolation but is more compatible and makes integration with other components easier.

What to Look For in a Layering Solution

When evaluating a layering solution for managing your desktops, there are a few things you should consider:

#1. Does it work with your existing administration techniques?
Even when you are using a layering solution, you will still need to integrate with your existing IT processes, tools, agents, and techniques—at least until you have moved to an entirely layered solution. A good solution should allow you to seamlessly use your existing infrastructure for patch management, updates and software distribution.

#2. Do users need to do anything differently?
Changing user behavior is even more difficult than changing IT processes. Users need to be productive, so a good layering solution should not require the users to do anything differently. Solutions where users must save their documents in a different place, complete an extra step before going offline, or are restricted from installing

plugins, will lead to frustration and lost productivity—even perhaps to the rejection of the system or finding creative ways around it.

#3. Does the solution allow different people to manage different pieces?

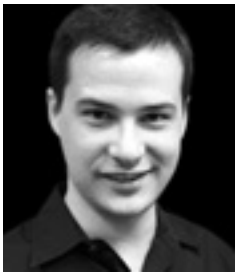
The reality of today's desktop is that different people are responsible for different pieces. A good layering solution will be separable so different people can create and manage indivdual aspects of the system without introducing extra processes or interdependencies.

#4. Does the solution amortize the cost of IT across many users?

One of the primary drivers of virtualization, and layering in particular, is the ability to do something once and have it automatically apply to a large number of endpoints in a variety of situations. A good layering solution should make it easy to manage a single layer and leverage the work you have done for other users, allowing you to scale easily, and thereby improving responsiveness and saving you time and money.

Summary

Managing virtual desktops definitely has a set of challenges. Even after moving the desktop into a virtual machine, you have conflicting requirements from users, IT and business, and the monolithic nature of the desktop means you either need to lock it down or allow customizations and suffer image sprawl. Leveraging virtualization to divide the desktop into layers allows for a separation of concerns such that the system can be decomposed into individually-managed components while still giving the end-user the unified view to which they are accustomed. Virtual layers reduce the management burden, allowing easier management and better scalability on the IT side, while simultaneously giving users the flexibility to do whatever they need to be productive.



John Whaley is responsible for the technical vision of MokaFive. He holds a doctorate in computer science from Stanford University, where he made key contributions to the fields of program analysis, compilers, and virtual machines. He is the winner of numerous awards including the Arthur L. Samuel Thesis Award for Best Thesis at Stanford, and has worked at IBM's T.J. Watson Research Center and Tokyo Research Lab. John was named one of the top 15 programmers in the USA Computing Olympiad. He also holds bachelors and masters degrees in computer science from MIT and speaks fluent Japanese.

www.mokafive.com
650-980-0960

475 Broadway St., 2nd Floor, Redwood City, California 94063