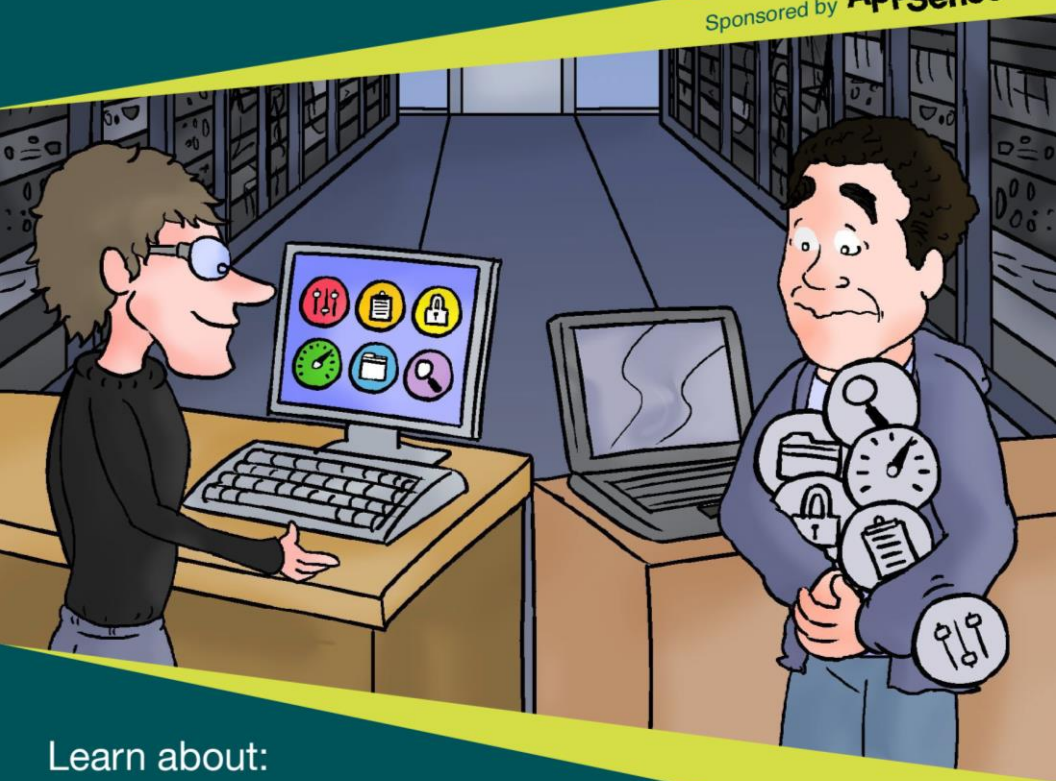
Conversational
User Environment Management

A ConversationalGeek Book

Sponsored by AppSense®



Learn about:

- Six important things to look for in a user environment management solution
- How Windows 10 impacts user environment management
- Why group policies alone are inadequate for securing your VDI environment

By Brien M. Posey (Microsoft MVP)

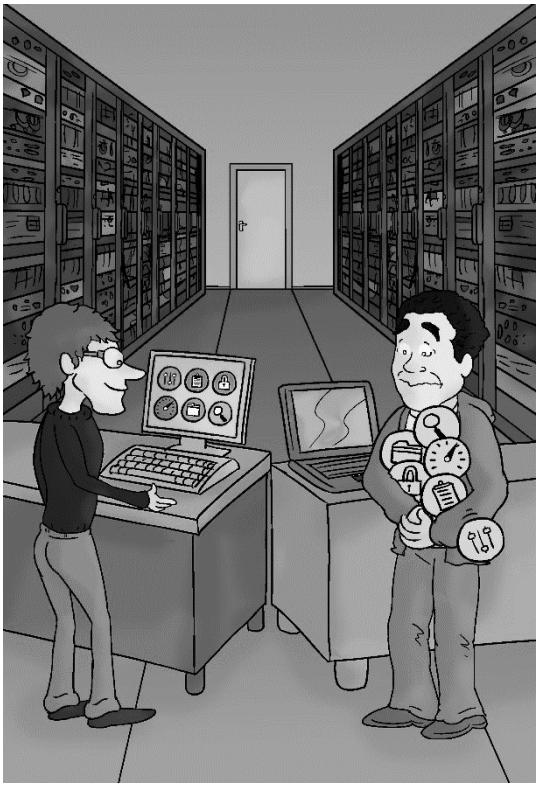
Sponsored by AppSense

AppSense is the leading provider of UEM and endpoint security solutions. AppSense user virtualization technology allows IT to secure and simplify workspace control at scale across physical, virtual, and cloud-delivered desktops.

AppSense Solutions have been deployed by over 4000 enterprises worldwide to over 8 million endpoints. The company is headquartered in Sunnyvale, CA with offices around the world.
For more information please visit www.appsense.com

Conversational
User Environment Management (UEM)

By Brien M. Posey



ConversationalGeek

Conversational User Environment Management (UEM)

Published by Conversational Geek Inc.

www.conversationalgeek.com

Trademarks

Warning and Disclaimer

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Brien M. Posey
Project Editor:	J. Peter Bruzzese
Copy Editor:	John Rugh
Content Reviewer(s):	Shanna G. Giarrano

Foreword

User environment management (UEM) is no longer a nice-to-have. It is as important a part of the user's workspace as the applications and the OS itself. Without UEM your workforce is much less productive and desktops are much less secure. With UEM you get both happy users and the security, manageability and cost savings that IT needs.

We have all seen virtualization projects succeed, or fail, based on the way user environments were managed. Many vendors now provide some UEM functionality to check that box. But is UEM really just a checkbox? We don't believe so. Buyers beware of free solutions. A desktop with partial UEM is just as naked as one without.

User environment management is composed of six tightly interdependent components for managing desktops; profile, policy, security, performance, data access and analytics. They are the "MECE" (mutually exclusive, collectively exhaustive) set of functionality that plays a key role in providing the best desktop ever.

Each component provides great value as a standalone solution, and in fact most vendors sell just one, sometimes two. We believe that the real value of UEM comes from not just the components but from the interplay between them. It's great that the doctor's printer mapped automatically when she walked down two floors. It's better that the system's real-time policy enforcement prevented a sensitive report from printing in the patient area. It's even better that the system gave the doctor just enough OS privilege to connect over a Starbucks network in the lobby but automatically terminated the sensitive patient record application on the fly and reported back to IT the files she copied on to the hard drive from that network. And on and on with each additional UEM functionality.

Comprehensive UEM not only makes the workspace better, more secure and more cost efficient, it provides the metrics of exactly how much. How much faster was that doctor's logon process? How many times did our policy prevent her from printing? How many more users were we able to add on to our current hardware? These questions are important to get our house in order and to keep it in order as the user landscape constantly shifts.

In the world of end user computing, change is not only constant, but can often be brutal. Windows 10's rapid-fire OS upgrades will stretch IT's ability to keep up. The beauty of UEM is that once the user's environment is managed it becomes future-proof and ready for any desktop transformation. An AppSense customer put it best: "The next upgrade we do was the last one we did."

We at AppSense do not virtualize the desktop. We do not virtualize applications. Our only mission is to build the best possible user environment management platform that allows you to give your users the best and most secure desktop ever.

Bassam Khan
Vice President, Product Marketing
AppSense
bassam.khan@appsense.com
@bassamkhan

Note from the Author

Welcome to Conversational UEM! I'm Brien Posey, a long time tech author, and I am going to be giving you a quick crash course on the subject of User Environment Management (UEM).

As you have probably guessed from the thickness of this book (or the lack thereof), this text isn't meant to be an exhaustive, super deep, hard core technical reference. Rather, it's me taking the time to explain some of the more important concepts in an effort to familiarize you with the subject. That way when you go shopping for a UEM solution you'll know which features and capabilities you should be looking for, and you'll understand why those features are important.

One last thing I want to be sure to mention is that this book isn't intended to be a sales pitch. Sure, the book will probably eventually have a sponsor (we can't produce these books for free), but this book is meant to teach you the basics of UEM, not to sell a product.

Brien M. Posey

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

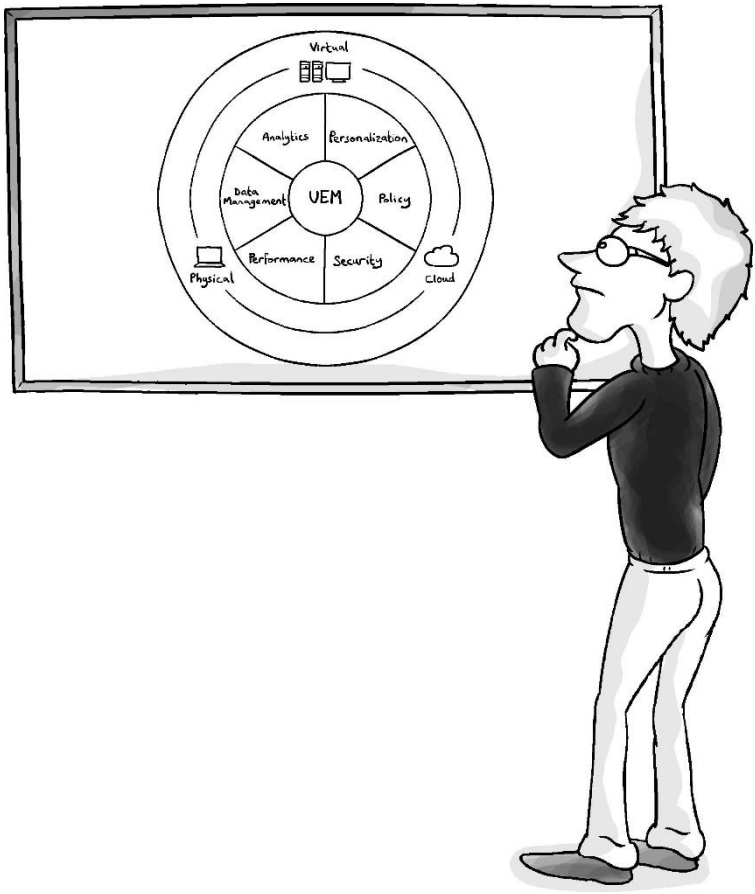
These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.

Greetings. Within these boxes, I can share just about anything on the subject at hand. Read ’em!

User Environment Management (UEM)



Although often overlooked, user environment management (UEM) is one of the most important concepts to address within an environment. The reason for this is extraordinarily simple. End-users and IT professionals have completely different goals from one another.

Users generally want one thing, and one thing only - full, unrestricted access to their desktop environment. In other words, users want to be able to customize and configure their

desktop (physical or virtual) in a way that makes sense to them. They want to be able to personalize their workspace as they see fit, and they want to be able to use their desktop without the underlying technology getting in the way, and they want it fast, real snappy… seconds count!

IT pros tend to have completely different needs when it comes to desktop environments. First and foremost, IT pros are responsible for making sure that the physical/virtual desktop environment performs well and remains healthy. As a general rule, IT professionals have a tendency to want to lock down desktops to the maximum extent they can get away with in an effort to prevent the end-users from accidentally (or deliberately) doing anything that might compromise integrity or performance.

As such, IT pros need a lot of tools. They want to be able to set policies and privileges, and they need to be able to measure performance and analyze the resulting metrics. For an IT professional, the end user's needs might even be something of an afterthought.

Remember, IT staff and the end-users have completely different goals from one another. Users want complete freedom to do what they perceive they need to get work done. It pros often want to lock everything down to the point that the user can't possibly mess anything up. Of course this raises the question of whether these two goals have to be in complete opposition to one another.

Believe it or not, it is possible to give the users what they want, while also keeping the people in IT happy, all without breaking the bank in the process. Doing so means delving into something called User Environment Management.

The term User Environment Management gets tossed around a lot, and it seems to mean different things to different people. For the purposes of this book, you can think of User Environment Management as a process by which IT is able to fully control the physical/VDI environment while still allowing users to personalize their own desktops. (You'll hear it referred to as Persona Management, User Experience Management, User Experience Virtualization, User Profile Management and more…)

This of course raises another question… Can't I already do that? Well, maybe… It really depends on what software you're using. For example, from a VDI perspective, Microsoft, VMware, and Citrix natively include features in their VDI products that allow these goals to be achieved to at least some degree. All three vendors allow users to perform at least some degree of personalization (assuming the administrator allows them to do so). Likewise, each of the previously mentioned vendors provides its VDI customers with tools for managing and maintaining their VDI environments. The problem is however, that just as the native tools probably aren't going to allow the users to have quite the level of personalization they want, the tools might not be an ideal fit for the folks in IT either. And not only that but in the real world IT has to manage users across physical, VDI, RDSH, and their virtual applications, across many different devices – and the users expect a consistent experience; not all native tools work seamlessly across all environments for all users.

In some ways, this is to be expected. After all, a VDI vendor's job is to sell VDI software, not to build tools. The VDI vendors give you the tools to handle basic management tasks, but if you want to go beyond the basics you are probably going to need to use a third party tool.

There are numerous third party VDI management and monitoring tools available on the market, and most of them are pretty good. If you really stop and think about it, no third party

vendor would be able to sell their VDI management or monitoring tools unless those tools were significantly better than what is natively available from the VDI vendors.

User Environment Management in Windows 10

User environment management presents a special challenge to organizations that have adopted Windows 10. These challenges go beyond those that have already been discussed. There are two main challenges that Windows 10 organizations must overcome:

The first of these challenges has to do with Windows 10 support. To put it simply, Windows 10 really hasn't been out all that long, and a lot of the vendors who make user environment management products have not yet updated their wares to support Windows 10. Granted, some of the products that were designed to run on Windows 8.1 may very well work in Windows 10 environments, but as a best practice, administrators should always try to use software in a way that is fully supported by the vendor that created it.

The other challenge that organizations face with regard to Windows 10 stems from Microsoft's introduction of universal apps. For those who might not be familiar with the concept of universal apps, they are applications that can be downloaded from the Windows store and run on any Windows 10 device including PCs, tablets, phones, and anything else that runs Windows 10.

6 Key UEM Features

So with that said, let's get back to talking about user environment management. User environment management seems to be one of those things that's easy to do, but tough to do well. There are plenty of tools that can perform user environment management to various degrees. Some of these tools are naturally better than others. In order for such a tool

to be able to perform comprehensive user experience management, it has to be able to do six different things:

- Allow for Personalization – The end users want to be able to personalize their environments, so the tool needs to be able to allow them to do so, but in a safe manner.

- Policy Based Management – The IT department has to be able to set limits around what users can and cannot do and therefore needs to be able to implement policies.

- Ensure Security – Users must be prevented from running malicious or unauthorized executables (although there is a little bit more to it than that. I will talk about this in more detail later on).

- Maintain Performance – If a user launches an application, it should arrive fast… oh and just in case you're accessing shared resources it shouldn't negatively impacts other users' experiences.

- Provide Data Access – Today's users work from a variety of devices, so a good user experience management solution should be able to make data seamlessly available to users regardless of what type of device they are using.

- Perform Deep Analytics – An administrator needs to know how well virtual desktops are performing and what resources are being consumed in order to deliver that performance. Hence, a good User Environment Management product needs to have good analytic capabilities.

User Environment Management (UEM) allows for both the user goal of being productive and IT's goal of maintaining control.

Personalization

So the first aspect of user environment management I want to talk about is personalization. As previously mentioned, users want the ability to personalize their own experience. Although this sounds really simple and straightforward, IT shops can't just give users the so-called keys to the kingdom. There's nothing wrong with enabling personalization. If anything, personalization helps users work more efficiently. Even so, we have to think about the underlying mechanisms that will allow for user personalization, while still allowing the IT department to maintain some degree of control.

There are a lot of different products on the market that support user experience personalization. Generally speaking, these products fall into one of two categories with regard to the way they handle personalization. Regardless of which method is used, a user's personalization settings have to be portable. After all, there is no guarantee the user is going to log on from the same device every time, or access the same virtual desktop during every session.

The first approach involves capturing a user's personalization settings, and storing those settings within a file share. In some ways, this approach is similar to the one natively used by the Windows operating system when roaming profiles are enabled. Typically, an administrator will redirect a user's home directory to a centrally located file share, and the various elements that make up the user's profile will be stored in that location.

The other approach involves capturing personalization settings and storing them in a database. On the surface, the difference

between these approaches may seem trivial. After all, both methods capture the elements that make up a user's personalized experience, and they centrally store those elements. As such, it would initially appear that the only real difference is the use of a file share versus the use of a database.

Windows 10 is seeing a strong adoption. By having the profile centralized and served in real-time, users' settings are easily brought over to Windows 10

UEM Personalization is the concept of capturing all of the user's desktop settings, both Windows and applications customizations, and managing the settings centrally.

It is worth noting however, that not all forms of personalization are created equal. There is basic personalization (which is sometimes called simple personalization), and then there is advanced personalization. Basic personalization usually refers to desktop personalization. For example, a utility that allows for basic personalization would probably capture a user's desktop wallpaper, the way icons are arranged on the user's desktop, and maybe even which applications the user has installed on their virtual desktop.

Advanced personalization is different. Yes, advanced personalization can handle desktop personalization, but it also captures application level personalization settings. So what is application level personalization? Well, consider Microsoft Word. There are a number of different user specific settings that can be configured within Word.

For example, each user has their own custom dictionary containing words they have added to the default dictionary. Similarly, a user might customize the toolbar layout or configure Word to use a specific template, or to save

documents in a certain location. The point is that Word contains a number of different personalization settings that are configurable at the user level.

Of course Microsoft Word is only one example of an application that supports user level personalization. It's also common for a user to personalize their browser. For example, the user may wish for the browser to go to a specific website anytime it's opened. Most applications support at least some level of personalization.

Virtualization vendors provide basic UEM personalization, whereas UEM dedicated vendors provide more advanced personalization.

From a software level, there are two main things needed in order to adequately support application level personalization. First of all, the personalization software needs to have a solid understanding of the various applications. Consider my earlier example of Microsoft Word. In order for a solution to capture personalization data for Word, the application will need to know what settings are configurable to the user, and where those settings are stored. Some user environment management products on the market accomplish this through the use of application templates that make the product aware of each individual application's unique nuances.

The other thing needed is a helpdesk interface. There's no harm in allowing a user to perform personalization, but as we all know, users do occasionally make mistakes. What happens if a user accidentally rearranges a toolbar or deletes an application shortcut?

In such situations, the helpdesk needs a way of rolling back these types of changes in order to get the user back on track. This is different from resetting the user's virtual desktop to its

default configuration. A rollback would only reverse the change that had been made accidentally while leaving all of the other personalizations in place.

Policy

When IT professionals think of user environment management, policies may very well be the first thing to come to mind. That's probably because the concept of policies is fairly open-ended. A policy can mean almost anything.

When it comes to managing and securing Windows environments, the policies that are most commonly used are probably group policies. Group policies were first introduced in Windows 2000 Server over fifteen years ago and have been evolving ever since. As such, group policies are well documented, reliable, and fully supported by Microsoft, so it isn't exactly a surprise that so many organizations use them. Even so, group policies have their limits. And although Windows has evolved (with Windows 10 being the latest end-user OS) the same issues and solutions carry down to today.

Group policies are great for controlling access to the desktop operating system. Each new version of Windows Server introduces brand-new group policy settings designed for the latest Windows desktop operating system. This ensures that all of the latest OS features can be configured or controlled by a group policy. However, group policy doesn't really work all that well when it comes to application personalization.

Out-of-the-box, group policy doesn't really provide controls for any applications aside from the web browser that comes with Windows. Even Microsoft Office, which is made by Microsoft and is one of the most popular business applications in the world is not natively configurable by a group policy. This isn't to say that you can't use group policies to configure Microsoft Office, but rather that the ability to do so isn't available out-of-the-box.

Administrators who want to use group policies to control Microsoft Office must download administrative templates from Microsoft in order to add the necessary policy settings to the existing group policies. The problem with using this approach is that most vendors do not provide administrative templates that allow their applications to be managed through group policies. As such, organizations that are looking for a way to manage personalization on a per application basis through the use of policies will have to turn to third party solutions.

Another issue with using group policies is that they are somewhat limited when it comes to triggered actions. When a user logs on, Windows gathers the applicable policies for the user and for the device from which the user logged on, and then combines those policies in a specific order to create the resultant policy. This policy remains in effect for the duration of the user's session, or until the policy is manually refreshed.

This isn't to say that group policies cannot perform any type of triggered actions. It's possible to configure Windows to run a script at logon or at log off. However, it is sometimes useful to be able to run scripts at other times as well. For example, it might be useful to run a script when a user launches an application. Such a script might map a network drive that's used by the application, or it might clean up temporary files left behind the last time the application was run. There are countless reasons why an administrator might want to run a script in response to a user launching or closing an application.

Similarly, an administrator might find it useful to run a script after the desktop appears. Since the desktop appears almost immediately after a user logs on, it might seem that such a capability would be unnecessary because logon scripts can handle any required actions. However, automated events often need to occur in sequence. It's very possible that certain automated events are unable to run until the desktop appears. Consider a script that checks to see if the user's firewall is turned on. Such a script probably would not be able to function

correctly until the user has progressed far enough into the logon process for the desktop to be displayed.

Another good example is mapping a printer or a drive that no longer exists; the IT guy that wrote that script 3 years ago left the company, and the printer broke and was never replaced. The logon script will hang until the mapping action times out, but a parallelized script will run the rest of the logon script.

If an organization only needs to run scripts at logon or log off, then the capabilities that are natively built into Windows are probably fine. However, if it wants to take advantage of other triggers such as application launches or specific connective states (such as a Citrix connected laptop versus a laptop that is working off-line) then a third-party solution is needed.

Default scripting technology is limited. Advanced UEM will allow you to launch scripts based on a wide variety of triggers, and allows the scripts to fork and run in a parallel fashion.

Another way third-party solutions may be able to help with scripted policy actions is in the way that instructions are processed. The Windows logon and logoff processes are linear. In other words, the operating system has to perform various tasks in a specific sequence. If any of the items in the sequence take a while to complete, then that long-running item will delay the entire logon or logoff process. In contrast, some of the third-party solutions that are available can perform parallel processing so that multiple tasks can be run simultaneously, thereby potentially speeding up the logon or logoff process.

Endpoint Security

When it comes to user environment management, security is one of those things an entire book could be written about. Let's face it, security is a big topic.

Consider the example of privilege management. Most employees are running around with admin rights which opens up the enterprise to attacks. Every security expert and security audit strongly recommends least privilege principle. Removing admin rights severely restricts what the user can do on their desktops and damages user's experience. The answer is in a) finding out who is using what privileges (not in theory but in practice, using UEM Analytics) and b) implementing granular privilege management where people can feel like they're still in control, but the risk to the enterprise is drastically reduced.

It's easy to think of security as being the same thing as policies. But there are distinctions. As previously discussed, in the world of user environment management, policies tend to focus on controlling personalizations within the operating system and within individual applications. Security on the other hand, often refers to a user's ability to either install or run an application. If a user were to attempt to run an application, security features within the user environment management software would first check to see if the user is allowed to run the application, and policies dictating personalization controls would only become applicable once the user has received permission to run the application.

There are two main approaches to application execution security - white listing and blacklisting. White listing allows

specific applications to be run, but forbids all others from running. Conversely, blacklisting prohibits specific applications from being run, but allows everything else to run. Unfortunately, neither of these methods are perfect.

The problem with application blacklisting is that it is nearly impossible to create and maintain a list of every application that should be prohibited from running. Not only would such a list need to block unauthorized software, but also malware (and new malware is created every day).

Application white listing has its problems as well. For one thing, the operating system itself contains a number of executable files that must be allowed to run. If an administrator fails to white list any of these applications, problems will eventually occur.

The larger issue with application white listing is that application identification can sometimes be problematic. Consider for example, simple application white listing in which applications are white listed based on their filename. Such a security mechanism could easily be circumvented by a user simply by renaming the executable file associated with a prohibited application.

Some of the more sophisticated application white listing products hash executable files and use the hash as a way of uniquely identifying the file. The nice thing about this method is that it will continue to work even if the user renames a file. Unfortunately however, identifying executable files by their hash is somewhat impractical. Think about how often applications and even the Windows operating system itself are updated. Every time an update occurs, files are replaced with new versions. These new file versions will have a different hash than the original version and will therefore not appear on the white list. As such, a white list can be very difficult to maintain.

It is also worth noting that there are vendors who have attempted to solve this problem by creating a cloud-based, universal list of every conceivable executable file and its hash. Unfortunately, these types of global cloud databases can be hacked, which would completely undermine the value of the data within the database.

Perhaps a better approach to application identification involves looking at application metadata. In this day and age, many vendors digitally sign their executables as a way of proving the executable file has not been tampered with. This digital signature can be used to positively identify the application.

Of course there are plenty of older applications that are unsigned. For such applications, trusted ownership makes a good alternative to examining digital signatures. The basic idea behind trusted ownership is that an application is trusted if its owner is trusted.

As I'm sure you know, the NTFS file system allows for permissions to be assigned to individual files and folders. NTFS also makes it possible to assign an owner to individual files. Therefore, it's possible for user environment management software to take action when a user tries to launch an application, and compare the owner of the executable file against a list of authorized owners. The software might, for instance, allow a file owned by the Domain Administrator to be executed, whereas it might block access to a file owned by the end user. This would effectively prevent the user from downloading a file from the Internet and executing it.

Any user environment management application must also take elevation of permissions into account when dealing with application security. The basic idea is that in Windows Vista and newer Windows operating systems the end user no longer has full blown administrative permissions over their desktop OS. Instead, the user has limited permissions, and there are

certain tasks that can only be performed by someone who has elevated (administrative) permissions.

In some cases, a user can claim administrative permissions for themselves when performing certain tasks. The operating system might pop up and say something like “This task requires administrative permissions. Do you want to perform the task?”. This prevents malware from exploiting certain functionality within the operating system.

When it comes to user environment management, the administrator must be able to control when a user is and is not allowed to use administrative privileges. An administrator might, for instance, set a policy that allows a user to claim administrative privileges on an as needed basis with the understanding that the user’s actions will be audited. On the other hand, a policy might stop the user from ever performing any administrative function. This would keep the user from being able to do things like uninstalling software or stopping system services.

We mentioned earlier the challenges presented by universal applications with Windows 10. These are very similar to the challenges brought about by Windows Store applications in Windows 8. Specifically, personalization of these applications is tied to a Microsoft account. Because Microsoft accounts exist outside of the IT department’s control, almost nobody uses Windows Store apps in an enterprise environment. For right now, the same basic concept also applies to universal apps. Microsoft is eventually going to give enterprise organizations a way to set up their own App Store and maintain control over universal app deployment. Until then, administrators who want to take advantage of universal apps are going to have to look to third party solutions to control those apps.

Done correctly, UEM not only secures, but also improves the user experience. These two have been at odds more so in the security space than anywhere else.

Performance

One of the most important issues that must be taken into account in any VDI environment is performance. To put it bluntly, users don't really care that they are working from virtual desktops. They expect those virtual desktops to perform just as well as their physical desktops did.

With this being the case, VDI administrators tend to spend a lot of time using performance monitors and other tools to fine tune VDI performance. Although such actions are necessary, performance monitoring tools often focus on the hardware level and may sometimes overlook the root cause of performance problems.

To give you a more concrete example of this, imagine for a moment that a particular application contained a memory leak. A server level performance monitoring tool would simply report that excessive memory consumption is occurring, and it would be up to the administrator to either find a way to reduce memory consumption or to add additional memory to the server.

Most de facto performance optimization tools look at low level metrics and don't identify the root cause of performance issues.

A better approach to this problem would be to monitor individual processes within each user session and look for

excessive memory and CPU consumption. This is important not only for ensuring a good end user experience, but resource consumption also controls the number of sessions a particular server can host. A server only has so much memory, and once all of that memory is used up there is no more room for additional user sessions.

So with that in mind, a good user environment management application should be able to keep track of memory and CPU usage within user sessions and make adjustments if necessary.

To give you another example, imagine that a particular user is browsing the web using Google Chrome. Chrome is a multithreaded application. If the user opens up five browser tabs, they are effectively launching five separate processes. Now suppose the user goes to a buggy website that runs flash or some other code that causes the browser to go nuts.

In this type of situation, it's not enough to say that Chrome is having a problem. In this case, Chrome has four tabs (and four processes) that are working fine. It's only one specific process that is suddenly consuming too many resources. A good user environment management application should be able to identify the process and throttle it so that it does not consume enough resources to disrupt other processes that are running within the user's session. Likewise, the process should not disrupt other sessions being hosted on the server.

By taking control over the resources consumed by each individual process, the user environment management software is allowing hardware resources to be used in a much more efficient manner. The side effect to this is that it potentially allows the host server to handle more concurrent VDI sessions than would otherwise be possible, and that of course translates into lower overall cost for the IT department (which makes the bean counters in Finance happy).

One other “side effect” of improving server resource allocation is the potential for an increased number of users on the same hardware. IT often sees an instant boost - up to 30-40% increase in server capacity without any other software or hardware changes.

Data Access

Data access has been a problem for IT shops for roughly about the last twenty years, but over the last three or four years it has become a much bigger problem. Let me explain.

In the most literal sense of the word, data access refers to users’ ability to get to the data they need. In the past, data access problems were largely attributed to users who would create and store data on their laptops. Because the data resided on a laptop hard drive, it was not accessible to other users who needed access to the data. Furthermore, storing data on laptop hard drives sometimes resulted in data loss because as we all know, laptops are often lost, stolen, or broken, but are seldom backed up. Of course any time data is stored on a laptop hard drive, there is also the possibility of unwanted data disclosure in the event the laptop falls into the wrong hands.

These and other data access problems have been compounded over the last few years by the so-called Bring Your Own Device trend. Bring Your Own Device refers to the ongoing trend in which users want to bring in their own laptops, tablets, and smart phones and work from those devices rather than using a corporate issued laptop.

So how has Bring Your Own Device resulted in new data access problems? Well, for one thing users now expect to be able to access their data from anywhere and from any device. That’s a

tall order. And needless to say, the issues associated with storing data locally on a device have never really gone away.

Some users have attempted to make their data more readily accessible by using consumer grade file sharing solutions such as Drop Box, OneDrive, or Google Drive. The problem with these solutions is that they are outside of the IT department's control, and if not properly secured could result in unwanted data exposure.

The key to getting a handle on these types of problems is to implement enterprise file sync and share as a part of an organization's user environment management initiatives. In other words, the organization can do the same basic thing Dropbox and OneDrive are doing, but they can bring that functionality in house where it can be centrally managed, rather than having user data exist on public file shares that extend beyond the control of the IT department.

The key to getting a handle on these types of problems is to implement enterprise file sync and share as a part of an organization's user environment management initiatives.

Analytics

The last aspect of user environment management is analytics. By providing actual metrics from your users' desktops, analytics in effect becomes both the gradebook and guidebook for the five other components.

Effective analytics will report what your users are experiencing: slow or fast logons, policies that are being enforced and ones that aren't, privileges they're using or not using, drives they're mapping and files they're accessing, and so on.

From IT's perspective, analytics will identify the root cause(s) of slow logons, help streamline policies and privileges, show users' individual and aggregate storage needs, etc.

There are many tools on the market that provide monitoring or endpoint data reporting. The challenge in UEM analytics is around a) knowing which data to collect and which 99% to throw away, and b) knowing how to interpret the data that is collected. Doing this requires deep, kernel-level Windows knowledge and translating that knowledge to useful, actionable information.

For example, let's look a simple metric like how long did it take John's PC to log in, which is defined as the time he entered his password to the time he is ready to launch his application. There are literally hundreds of individual data points generated during that time period. Some are easily identifiable, like begin drive mapping and drive is mapped. Some are much harder to decipher, like Windows Service Logon or Windows Run Key. Some events have start and corresponding stop events, others don't.

The Big Takeaways

User Environment Management (UEM), while traditionally an IT vs. End-User monster movie, can be mitigated and managed in a physical and virtual desktop environment using third-party tools to assist in this regard.

With more users moving to Windows 10 we will see a continued need for UEM tools, especially with migrations to assist in a smoother and less IT-intensive migration process.

Notes

Whether you're dealing with Windows 10, P2V, PC refresh or Murphy's Law, AppSense can help.

AppSense®

Learn more: www.appsense.com/migrations

Easily “converse” about user environment management in any setting.

User environment management has always been challenging, but has become more complex in recent years due to trends such as VDI and Bring Your Own Device. The goal of this book is to help folks who manage VDI environments to allow users to personalize their own environments without giving up control in the process. Even if you have never worked in a virtual desktop environment before, this book will allow you to talk about user environment management as if you have been working with VDI for years.

About Brien M. Posey

Brien Posey is a 14 time Microsoft MVP and an internationally published author and conference speaker with over two decades of IT experience. In addition to his technology work, Posey is also working toward earning his civilian astronaut wings. Follow him on Twitter @BrienPosey