Executive Insight
Business Fit Assessment

FREEFORM DYNAMICS

Digital workspace disasters and how to beat them

New roles for user management and app deployment in the digital workspace

in association with

liquidware™

Windows is still vital to the desktop

Mobile technology has found its place in business, as have PC alternatives such as Macs and Chromebooks. Look around the average enterprise, though, and Windows PCs or virtual machines (VMs) sitting on the corporate network will still represent the primary end user computing platform for many, if not most, employees.

If this applies to your organization, you will know how essential it is to keep these connected Windows desktops up and running. In many cases, if an employee can't get to their familiar Windows workspace, they can't do their job effectively. If a whole department or even the entire organization is denied access, the results can be catastrophic. Ransomware attacks in recent years have given a stark demonstration of how critical Windows systems are in both the private and public sectors.

Against this background, this paper looks at risk management as it relates to the Windows desktops that are permanently connected to a campus, head office or branch network. In particular, we will look at how 'digital workspace' solutions designed to streamline desktop delivery and provide greater user flexibility can also be leveraged to enable a more effective and efficient approach to desktop disaster recovery (DR).

Along the way, we will use offerings from Liquidware, the sponsor of this paper, to illustrate the role of modern digital workspace management technology in desktop DR. While this shouldn't be taken as an endorsement of any particular vendor or product, talking through a specific solution allows us to illustrate how key principles translate to practical reality.

Desktop 'disaster' scenarios

The term 'disaster recovery' might sound old fashioned, which is why nowadays most people prefer to speak of 'business continuity'. But whatever term you use, it's about recovering from incidents that lead to significant disruption. In the context of end user computing, however, we also need to consider smaller-scale 'disasters' (Figure 1).

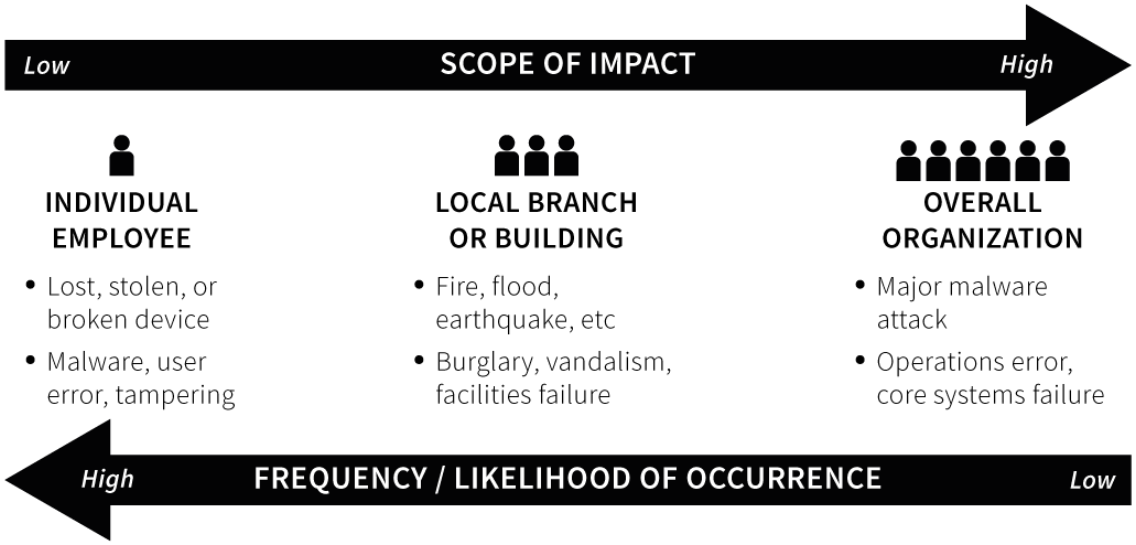

Figure 1

The above graphic is not exhaustive, e.g. when listing potential desktop-related disasters we could add VDI infrastructure failures, software upgrades causing accidental system corruption, deliberate sabotage, rogue applications, and so on.

The key point, though, is that we must think about much more than just those relatively-rare organization-wide catastrophes. Incidents affecting single locations or even individual users on a day-to-day basis can in aggregate be just as costly, disruptive and damaging to the business, and consume a lot of IT time. Anyone in desktop support will corroborate this. Dealing with frightened, frustrated or angry users who have suffered some kind of personal computing disaster can be a big part of the job.

Current practices and their limitations

When it comes to maximizing desktop availability, the first step is to minimize the likelihood of a problem occurring in the first place. Security and management tools and processes are important here, as are user policies and training. Unfortunately, given that none of this can be made foolproof, and that some disasters are beyond your control anyway, there will always be occasions when desktops need to be recovered.

When recovery is necessary, the aim is to recreate the user's pre-disaster desktop environment as quickly, accurately and efficiently as possible. Traditional approaches to achieving this, however, all fall short in various ways.

TRADITIONAL WINDOWS DESKTOP DR APPROACHES	
Approach	*Limitation*
AD HOC / MANUAL APPROACH Each machine is essentially considered unique, so you install the operating system and all of the necessary applications, then recover the user's data from a recent backup (assuming this exists), or re-synchronize via the relevant 'sync and share' solution.	This approach is very labor-intensive for IT, as well as being prone to errors. Simply knowing the software versions to install can be a challenge. It's also inconvenient for the user as the process takes a long time, and then they have to reapply much if not all of the personalization that was previously in place.
INDIVIDUAL IMAGE BACKUP/RECOVERY Each machine is again considered unique, but disk imaging is used to take complete backups of the operating system, installed applications, user settings, and locally stored data. Recovery is achieved by restoring the most recent image of the user's machine.	This is the sledgehammer approach to backup and recovery. It is very resource-intensive and cumbersome when implemented on more than a few machines, though. The process can also be intrusive, tempting users to postpone backups, which means the recovered machine is unlikely to be up to date.
USE OF STANDARD IMAGES Each machine is provisioned using one of a small selection of standard images that include the operating system and company standard applications. Recovery is achieved by reinstating the relevant standard image, and restoring or resyncing the user's data.	This approach is somewhere between the above two. Getting the machine back to a standard state is relatively quick, but the user (or IT) still has to reinstall any additional applications, and the user's personalization and configuration settings may still need to be manually recreated.

The approaches we listed here are not mutually exclusive, and it's not unusual for an IT team to use more than one of them. If you use a modern VDI environment, there may be various other options and approaches in place too. The likes of Microsoft, Citrix and VMware all include some kind of backup and recovery functionality, though this often only works within the proprietary environment concerned.

Pull all this together and the upshot is complexity and overhead - multiple mechanisms and processes to deal with different delivery platforms and/or user requirements. This, in turn, makes it hard to manage user expectations and achieve service level standardization.

Time to think and act differently

If you recognize any of the above approaches, limitations and challenges, then you will find the remainder of this paper particularly relevant. The same goes if, like many organizations, you have little or nothing in place at the moment to manage desktop DR in a structured way. In either case, however, there is an important opportunity to think differently and reframe the traditional DR discussion.

Reprovisioning rather than recovery

A useful trick when looking to drive improvements in desktop DR is to start thinking in terms of reprovisioning the environment or workspace, rather than recovering from backup in the more traditional sense. The principle then becomes one of optimizing recovery by streamlining and automating the initial provisioning process.

In order to make this adjustment, we need to remind ourselves that the core elements of a Windows desktop are not specific to each individual user, or at least they needn't be, with a little care and planning:

- **The physical device:** Most users' Windows environments could in reality operate on any physical or virtual machine capable of handling the application mix. It doesn't have to be a specific machine, or even a strict specification.
- **Operating system:** Dependencies between applications and operating system versions sometimes exist, but on the whole, from Windows 7 onwards most software will run quite happily on most releases of Windows.
- **Applications:** The mix might vary between users, but the applications themselves are usually the same. Even if you support multiple application editions or versions, the number of variants will be minimal in a well-managed environment.

If you thought the above was too simplistic, maybe because your organization seems to be running every operating system and application version under the sun, then you have highlighted an important related issue. Just as with a migration exercise, it's much easier to move forward safely, efficiently and effectively if you first rationalize your desktop estate and application portfolio as much as possible. That said, we would never advocate a one-size-fits-all policy, but as we will discuss, there are ways to minimize dependencies. That way, you can maintain a reasonable level of variation, while

minimizing internal political conflict and still boosting service levels and operational efficiency.

Before getting into these, let's complete our analysis of desktop anatomy by considering the elements that really are user-specific:

- **Settings and preferences:** Whether it's color schemes, menu items, notification preferences, application layouts or other settings, users will personalize their desktops, and that personalization data will be held somewhere.

- **User data:** No matter how much you provide space on the network or in the cloud for users to store files, human nature being what it is, most will store at least some material locally. The infamous Documents folder is the usual destination.

So what's all this got to do with the core aim of rapid, accurate and efficient recovery?

Desktop DR becomes just another provisioning event

Having defined the elements of a Windows desktop in this way, then at a high level we can envisage the provisioning process as the way everything is pulled together into a working desktop. In the broader scheme of things, recovering a desktop following a disaster becomes just one of several types of provisioning event (Figure 2).

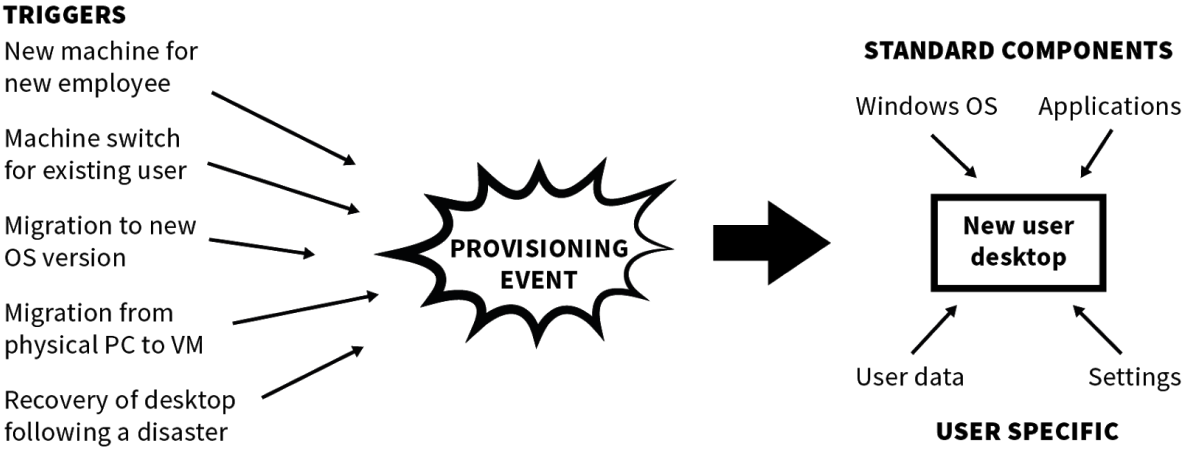

Figure 2

If we enable rapid and automated provisioning, even on-the-fly, the benefits are huge for both business users and the IT team. Beyond desktop DR, we also gain significant user flexibility. This could include improving the user experience around hot-desking, roaming between corporate locations, and the use of multiple devices more generally.

Recover physical to virtual

Of course you don't have to recover to the same device. If we can reprovision rapidly and flexibly, then in the event of a major disaster or other service interruption we could, for example, recover desktop PCs to cloud-hosted PCs or VDI, either on a temporary or permanent basis.

User workspace management

The steps required to implement rapid and automated provisioning of the desktops that live on your corporate network - including reprovisioning them for desktop DR - are part of an overall process. Different developers have given this process different names, which we will paraphrase here as 'user workspace management' or UWM. The key steps or elements required to enable an effective UWM process are:

- Effective user segmentation based on business needs.
- Smart and efficient use of standardized base images.
- Rapid (preferably just-in-time) application deployment.
- Device-independent personalization and data redirection.
- Effective central management of user-authored data.
- Overall workspace monitoring and management.

Let's walk through some of these steps and consider the practicalities.

User segmentation

The aim here is to analyze users' desktop computing requirements so you can group them together. This allows you to define a limited number of configurations to use as starting points for provisioning (Figure 3). Each should include the most appropriate release of Windows, and the set of applications relevant to everyone in that segment.

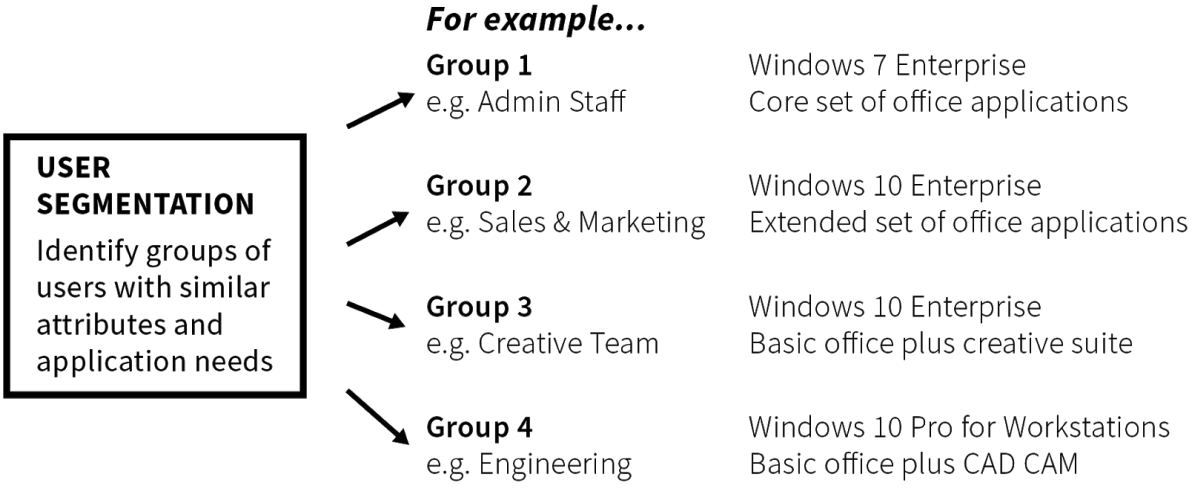

Figure 3

When segmenting users, it makes sense to take an 80:20 approach. If only a small percentage of admin staff need a specific piece of scanning and character recognition software, for example, it's perfectly legitimate to treat this as an exception that will be added on top of a base configuration on a case-by-case basis. The significance of this becomes clear when we look at adopting an image-based approach.

Image-based deployment

An image in this context is either a disk image of a system drive for deployment on a physical machine or a full VM image for deployment via VDI. Either way, the base image for a particular user segment will have the operating system, associated system

software, and the segment's standard set of applications pre-installed. This approach means that a machine can be brought to a standard state, regardless of its starting point, simply by deploying (or re-deploying) the relevant image.

Provisioning via standard images is obviously much faster than manually installing the operating system and each individual required application. It also ensures that each machine in a group is essentially the same from a core system perspective, which will be important later, when it comes to reuse, support and diagnostics.

In practical terms, you will have one image or set of images for each user segment. The reason you might have more than one image per segment is to deal with different deployment options, for example, physical versus virtual machines.

A big consideration when provisioning from standard images is that each image needs to be stored, managed and maintained. This is why it is a good idea to minimize the number of user segments and associated images (plus their contents), although this only works if you can quickly and easily deploy any additional applications needed.

Application deployment options

It is almost inevitable that users will need to add applications that are not in the standard image for their user segment, and there are several ways to achieve this (Figure 4). Typically these will be applications with just a handful of users, but there may also be ones that are problematic to image, perhaps because of how they are packaged or updated.

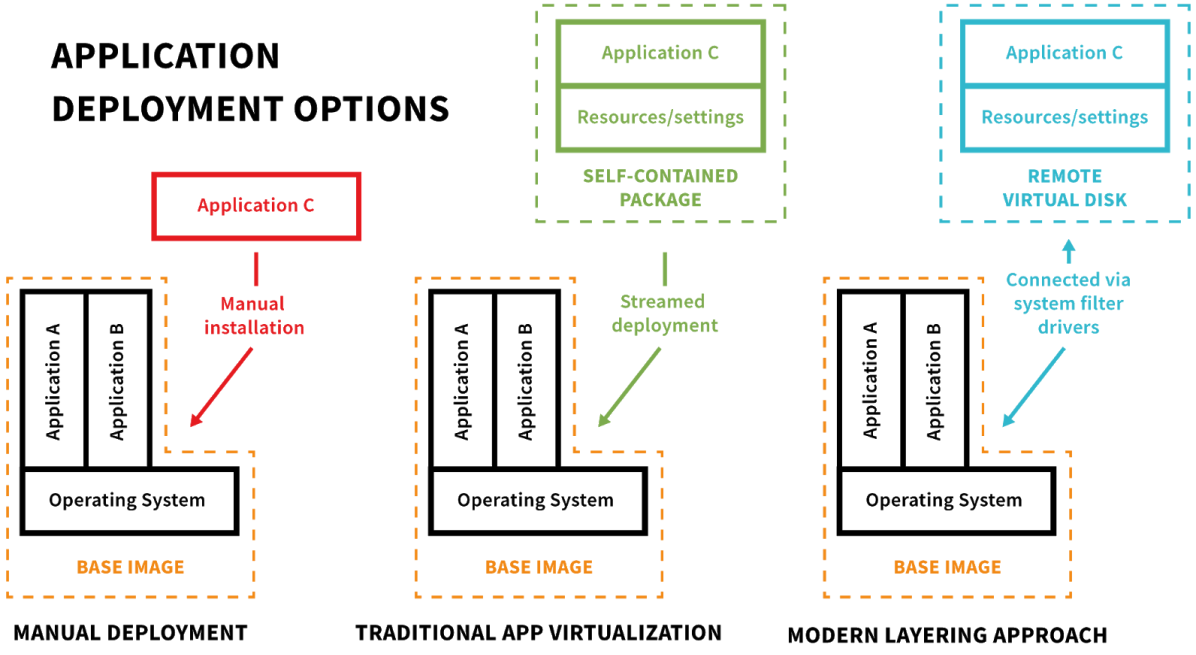

Figure 4

While **manual deployment** is feasible in low volumes, it brings speed, scalability and management challenges. A more practical option at scale is **application virtualization**, where the application is repackaged to run without formally being locally installed. Several technical routes exist to do this, including examples from the mainstream VDI

vendors such as Microsoft App-V, VMware ThinApp and Citrix Virtual Apps (previously known as XenApp).

This technique is useful if you want to implement a full sandbox ('application in a bubble') approach. It tends to go hand-in-hand with **application streaming** to get the software package onto the target machine incrementally, so the user can start working with the application before it has completely downloaded.

Much has been written about application virtualization, and if you run large desktop estates you may already be exploiting it in one form or another. We therefore won't say much more about it here, but if you need more background, please see our paper entitled "Desktop virtualization as an accelerator of digital transformation" (https://bit.ly/306pYpT).

Application layering

More pertinent to our rapid provisioning and DR discussion is a deployment option known as application layering or application volumes. This more lightweight and agile approach is not new but has recently gathered momentum as the enabling technology has matured and become more capable.

In the layering approach, the application never becomes fully resident on the target desktop, either in native or repackaged form, except for caching to enhance performance. It lives on the network along with application-specific resources and settings, and is connected into the desktop environment either at login or on demand, in a way that mimics a natively-installed application.

One of the big advantages of application layering is that deployment can be near instantaneous. In conceptual terms, you are simply pointing the Windows operating system at a virtual disk on the network, where the application resides. It's for this reason that some refer to this approach as just-in-time application deployment.

Application cloaking

One other delivery method to mention is cloaking. This includes one or several applications in the base image but in a concealed form - they are deployed but not made visible or active. This increases the image size and adds to the management workload because it is another element to keep up to date, but on the other hand, it can reduce the total number of images required, because the same image can now serve more than one user segment.

Because the cloaked application is part of the image, its integration with the system once uncloaked is almost guaranteed. You will need to ensure however that the cloaked application does not count against your total of licensed copies, for example by having strong auditing and monitoring tools in place as well as a legal agreement with the ISV.

What about the user-specific elements?

Key software developers, such as Citrix, Microsoft and VMware, all offer tools that provide various degrees of user and application portability. However, each vendor's

tools have their own limitations, in particular they typically focus on that vendor's software infrastructure. This has opened the door for other companies to develop more broadly-compatible profile virtualization and synchronization tools. The caveat is that most of these solve only the user profile part of the puzzle, so additional integration and administrative work may be needed to cover the other provisioning elements.

Visibility and control

The final step required for a complete UWM solution is the ability to keep track of what's installed and in use, where user-created data is located, its access controls and so on. This takes in some of the capabilities of traditional licensing and inventory/asset management systems.

Let's explore all this further, and consider some other potential advantages of having a complete workspace management environment, by looking at an example of a real-world solution to the challenges of UWM and desktop DR. As mentioned above, this should not be taken as an endorsement of this or any other vendor or product; however, talking through a specific solution allows us to illustrate how key principles translate into practical reality.

Real-world desktop DR: The Essentials

Liquidware packages its user workspace management solutions together as a suite under the Essentials label. As we have discussed, such a UWM suite needs to provide rapid provisioning and migration, and of course effective desktop DR.

Earlier in this paper, we outlined some key steps or elements required for an effective UWM process. In order to translate those process elements into a practical example, let's first rearrange them into logical functional groupings:

- Overall workspace monitoring and management, plus user segmentation and management.
- Creation and maintenance of standard images, etc.
- User-specific elements, including both device-independent profiles and user-created data.
- Rapid application deployment.

Overall management: Stratusphere UX

The overall 'management console' elements of the UWM process are many and varied, and Liquidware's Stratusphere UX is correspondingly broad. As well as obvious tasks such as endpoint monitoring, it handles user segmentation and categorization. Other tasks such as the design, creation and management of images also fall within its remit, plus of course remediation and DR planning.

From a day-to-day perspective, an important aspect is the way that the diagnostics and performance management capabilities of Stratusphere UX are user-centric. Application and infrastructure monitoring are still present to assist with root cause analysis and

remediation, of course, but in UWM, the monitoring priorities are the user, the workspace and the relevant desktop system.

Personalization: ProfileUnity

Liquidware's ProfileUnity software delivers what it refers to as 'universal profiles', enabling a user's entire environment or workspace to be migrated, restored or even delivered as a service.

Running via an agent on the desktop, ProfileUnity periodically harvests the user's profile details (whether stored locally or in a remote profile disk/container) including application settings, Windows preferences and so on. As well as local user profiles, it is also compatible with profile disks and profile containers from other vendors - these redirect the user profile to a network or cloud location. Regardless of its original location, ProfileUnity then packages the user profile up to make it portable, whether for DR, to repair a corrupted profile or for system migration.

By default, profile settings are updated on logout, but they can also be set to save at a specific time interval or when an application is closed, and they also can be saved to cloud storage and made cross-OS compatible, for example, to support DR to a cloud-based desktop. This kind of profile portability and versatility is important because it allows you to build more flexible desktop DR plans which are able to respond to the gamut of threats from individual to organization-level disasters.

One other notable feature of ProfileUnity is the ability to copy and redirect a user's local Documents directory. Nothing is deleted, but user-created files are replicated to a safe location on the network, thereby assisting in data protection processes. The original local directory remains in place but is hidden from the user, though it can optionally be left active for offline use in the case of laptops - support for mobile users can be a weak spot in UWM solutions, and will need careful evaluation if you have many such users.

Application deployment: FlexApp layering

FlexApp is the name under which Liquidware delivers its application layering software. It is not the only offering in this space, but as a proven product that first came to market in 2011, it represents a mature and tested solution. It's therefore a good example that can illustrate the concepts of application layering in action.

One of Liquidware's main objectives with FlexApp is to add a degree of platform independence to application layering. It has therefore been designed to operate with any release of Windows from version 7 onwards, whether the machine is physical or virtual. In the case of the latter, FlexApp is similarly agnostic to the virtualization platform employed. It can, for example, layer applications into a Citrix, VMware or Microsoft environment.

In summary: the strategic view

Desktop DR - the recovery of individual desktop systems from a disaster or system failure - has long been a challenge. Part of the problem is that there are so many desktops, storing so much valuable data and - unlike servers - with so many different end user configurations and too little central control. Imaging everyone would be a huge task, generating huge amounts of backup data. And even if those problems could be overcome with the use of software agents, plus de-deduplication to take common files such as the operating system out of the backup window, restoring damaged systems could still mean days of software reinstallation and reconfiguration.

Yet at the same time, most organizations have a strategic need to deploy and provision new desktop systems, and to be able to migrate existing ones to new platforms. Again, these are tasks that benefit from reducing both duplication and the need to reconfigure the resulting installation. The parallels with desktop DR should be clear.

We often write about the importance of an integrated approach to investing in backup and recovery. By bringing together business needs that have a shared technical foundation, we can, for example, gain incremental benefits from backup, such as improved data visibility and governance, or we can gain DR capabilities from an investment in systems and data management.

So it is with desktop DR and user workspace management. Both of these are growing in importance as organizations' desktop estates grow more complex. Not only are we adding more ways to work online, such as virtual PCs, more applications, and more layers of middleware, but the resulting systems face more risks and threats and are subject to higher regulatory and legal requirements.

Increasingly then, both desktop DR and UWM will be not just valuable, but essential. Getting one as an incremental bonus from the other therefore not only strengthens the business case for that investment proposal, it is a win-win scenario in its own right.

Resources and further reading

Desktop virtualization as an accelerator of digital transformation
Fast-track creation of a modern digital workspace

The stuff they don't tell you about workplace transformation
Tips and tricks for getting past those 'people problems'

Rethinking desktop delivery
Time to break out of the Windows upgrade spiral?

About Freeform Dynamics

Freeform Dynamics is an IT industry analyst firm. Through our research and insights, we help busy IT and business professionals get up to speed on the latest technology developments and make better-informed investment decisions.

For more information and access to our library of free research, please visit www.freeformdynamics.com or follow us on Twitter @FreeformCentral.

About Liquidware

Liquidware is a leader in adaptive workspace management solutions for Windows desktops. The company's products encompass all facets of management to ensure the ultimate user experience across all workspaces – physical, virtual, DaaS or in the cloud. Enterprises across the globe utilize Liquidware solutions to dramatically decrease time spent managing desktops, while delivering increased security, flexibility and scalability. Supported platforms include Microsoft physical, WVD (Windows Virtual Desktop), and RDS desktops, Citrix Desktops, VMware Horizon View, Amazon WorkSpaces (AWS), and Nutanix Xi Frame.

Learn more at www.liquidware.com.