

Liquidware Labs ProfileUnity and its Role as a Disaster Recovery Solution

Executive Summary:

Many corporations around the globe leverage Virtual Desktop Infrastructure (VDI) as a strategic, cost-effective methodology to deliver business continuity for user applications and data. Virtualization renders a physical computer made of metal, plastic and silica as a portable file that can be moved through a network from a data center to a disaster recovery (DR) site. Although this may sound easy, transferring virtual machine files can be challenging for corporate networks in a number of ways. Moving large amounts of data is a time consuming process that may take days to complete. Moreover, once archival process is complete, the data is effectively out of date or out of context. As a response various strategies focus on leaving the bulk of the data transferred and only updating and replicating the changes in data. Desktop infrastructure is particularly sensitive to the issue of synchronization so applications run properly. The challenge is keeping desktops in sync because desktops, applications and data change often. This has given birth to a whole new set of strategies and software unique to desktops to accomplish backups safely and effectively. Liquidware Labs' **ProfileUnity™** is a best of breed solution that provides a seamless end user DR experience identical to the one at the home office.

Table of Contents

Why an Elegant Yet Simple Solution is Required.....	3
Setting the Stage: Current Data Systems Disaster Recovery Best Practices	3
ProfileUnity: Best Practices for Data Retention	4
Portability	5
Folder Redirection	5
What This Means for Your Environment	6
Scenario 1: Physical Desktops without ProfileUnity	7
Scenario 2: Physical Desktops with ProfileUnity	8
Scenario 3: Persistent Virtual Desktops without ProfileUnity	9
Scenario 4: Persistent Virtual Desktops with ProfileUnity	10
Scenario 5: Non-Persistent Virtual Desktops without ProfileUnity	11
Scenario 6: Non-Persistent Virtual Desktops with ProfileUnity	12
Conclusion	13
About ProfileUnity and Liquidware Labs	13
Summary Matrix	14

Copyright © 2011 Liquidware Labs, Inc.

All rights reserved. ProfileUnity is a trademark of Liquidware Labs. Other brand, product names and trademarks are the property of their respective owners.

Information in this document is subject to change without notice. No part of this publication may be reproduced in whole or part, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any external use by any person or entity without the express prior written consent of Liquidware Labs.

Liquidware Labs
3600 Mansell Road
Suite 200
Alpharetta, GA 30022
U.S.A.
866-914-9667
www.LiquidwareLabs.com

Why an Elegant Yet Simple Solution is Required

As desktop operating systems become more and more complex, the need for a proper disaster recovery methodology on the desktop is increasingly crucial. This is true of environments that operate in the physical space as well as the virtual space, including VMware View and Citrix XenDesktop environments. Many enterprise customers are leveraging additional desktop technologies including local hard drive encryption, persistent virtual images and non-persistent virtual images. As a result, the amount of work that goes into recovering a user's data from even a minor hard drive malfunction can be insurmountable. In order to combat long recovery times and complex procedures, the need for proper disaster recovery and backup techniques is paramount. However, in many environments, these cures are often worse than the disease. The amount of raw storage needed to house an entire operating system, as well as the data that resides upon it, quickly drives up the cost of storage systems beyond project budgets. This problem is compounded when disaster recovery plans call for off-site backups. This paper will attempt to address these issues and show how a disaster recovery (DR) plan, coupled with Liquidware Labs ProfileUnity™, reduces disaster recovery costs and recovery times.

Tip: Most organizations leverage a multi-tiered approach to data backup, and that approach includes a disaster recovery process. Using proper disaster recovery and backup techniques will simultaneously increase user productivity by reducing the amount of downtime a user will experience from an operating system crash, virus infections, hardware failures, or large scale systems loss.

Setting the Stage: Current Data Systems Disaster Recovery Best Practices

As a subset of a business' overall business continuity plan, customized disaster recovery plans are in place for most enterprise organizations. Most organizations have dealt with the need for local and off-site backups of crucial data, as well as the integration of some user data. However, a large portion of a corporation's intellectual property does not reside on a server or in a data center. Instead, it lives on the hard drives of the multitude of users that perform work on a day-to day basis. Let us first examine current disaster recovery best practices used in many organizations as we explore where corporate data lives.

First, we have the backbone of the data center—the data storage environments. Typically organizations deploy network-attached storage (NAS) and/or storage area network (SAN) technologies to house the lion's share of critical data from application servers, database servers, web servers, mainframe storage, and possibly some user data. Those following DR best practices will also house server, workstation and desktop images within the NAS and SAN infrastructure to facilitate a quick transition from disaster to production and meet the recovery time objective (RTO). The amount of user data stored on NAS and SAN systems is relative to the processes and limitations put forth by IT administration policies in an organization. It is important to point out that unless organizations desktops are either fully managed or fully locked down, data loss during a disaster scenario is inescapable.

Next, we have NAS and SAN backup environments. Backups that stay inside data centers are critical for the quick recovery of day-to-day data. They also offer users a more recent copy of their data, minimizing

the amount of work that is lost. However, onsite backups do not address major disaster recovery scenarios. It is possible with some disasters that the data center itself may be lost, which is a situation that some organizations have faced in the past.

This leads us to our final location—off-site archival backup environments. Traditionally, an off-site environment has been an actual structure housed by the corporation itself. More recently, enterprise customers have chosen to have off-site backups performed by third party vendors. This has two primary benefits. Foremost, it allows the data archive to be stored in geographically different physical location than the enterprise. This can be as distant as another state or another country. Secondly, it has been shown in many cases that a third party vendor can charge less for off-site archival services than it would cost the enterprise to operate its own off-site archival center.

While we have spent a great deal of time talking about the data housed within an enterprise, it is important that we do not overlook the many other disaster recovery plans that an organization may choose to implement. They can include contract retainers for alternative office locations, workstation supply companies, server supply companies, virtual infrastructure companies, and the myriad of other components necessary to rebuild the information technology infrastructure. These additional provisions and costs factor into the larger business continuity plan. However, your organization's actual data is its greatest asset. You can always purchase new equipment or a new building, but your data is priceless and unique. It is the lifeblood of your organization.

ProfileUnity: Best Practices for Data Retention

Now that we have covered the best practices of data systems disaster recovery, we can explore how ProfileUnity can be utilized to strengthen those practices. ProfileUnity is a software and virtual appliance product that integrates with your Active Directory environment. This integration automatically leverages the disaster recovery features of Active Directory. In the event that a replicated domain controller within your environment becomes inactive for any reason, Active Directory will automatically propagate to the next available domain controller. This makes the environment self-healing. Therefore, as long as any domain controller exists within your organization, ProfileUnity will continue to function even if the ProfileUnity appliance is no longer functioning. This hardened methodology is one of the many reasons that ProfileUnity can significantly add to your disaster recovery strategy. While ProfileUnity is an incredibly flexible product that can control many more aspects of your desktop solutions, for the purposes of this paper, we will focus only on the settings that are specific to your data retention strategy.

With this knowledge, we can now talk about the specific settings within ProfileUnity that you can leverage to ease your transition back to production mode during a disaster recovery scenario.

Portability Management

ProfileUnity allows the following portions of your physical desktop or virtual images to be migrated to your NAS or SAN environment:

Third Party Application Settings:

- Local Application Data
- Certificates
- Front Page Settings
- Internet Explorer Settings
- MAPI Profiles
- Custom Written Application Settings
- ODBC Settings
- Office Settings
- Password
- Local Printer Settings
- Remote Desktop Client Settings
- Screen Saver Settings
- Windows Appearance Settings
- Windows Explorer Settings
- Windows Themes

These settings are maintained on an individual basis. In the event of user corruption, they can be rolled back to a prior recovery point or removed entirely. ProfileUnity's granularity allows the default image settings to replicate in the event that a user corrupts their Internet Explorer settings, for example. Utilizing any combination of these settings, as well as custom settings that may pertain to an organization's explicit environment, allows for full replication and backup of these settings for a disaster recovery scenario.

Folder Redirection

ProfileUnity has a specific data migration feature to move user authored data to the users' soon to be redirected folders on the network. This feature can be set to run in the background prior to a migration or profile streamlining project. Built-in throttling lets administrators choose a data transfer speed that will not impact network performance so data can be trickled up to the new location over time. Once the migration is complete, the user then seamlessly accesses their user authored files in the redirected location.

Leveraging folder redirection of the host operating system into your NAS or SAN environment is the crux of ProfileUnity's ability to simplify your disaster recovery process. By instantaneously migrating any available user shell folder to your replicated storage, you guarantee that a user's data is available at any point in time. This can even be managed down to the application level. For example, Office Auto Recovery folders can be migrated to your NAS or SAN environment. Then if users have a number of new Office documents open at the time of a disaster, they can still be recovered later from the corporate data store. By default, ProfileUnity can instantly transition the following areas to your replicated storage environment:

- Start Menu
- Program Groups
- Startup Group
- Desktop
- Favorites
- My Documents
- My Pictures
- Cookies (Internet Explorer)
- History (Internet Explorer)
- Recent (Internet Explorer)
- Temporary Internet Files
- Send To
- My Music
- My Videos
- Application Data (Real-time Migration)

This comprehensive set of folders and areas means that even if you users choose to store data in different locations, you can always make sure that their data is safe in the event of a disaster. While your current IT policies may dictate that users must store their data on the home or network drives, without policies in place to enforce those rules, your data is at risk. ProfileUnity ensures local policy enforcement without encroaching on a user's need to store their pertinent data in places they deem necessary or causing application incompatibility.

Simplifying the Recovery Process

Using ProfileUnity to manage your environment simplifies recovering from a desktop disaster. Recovery points and recovery times are optimized because ProfileUnity replicates user settings and data to internal and external backup systems and then quickly restores the settings and data back to the user when needed. In the event of a disaster, a user needs to have another physical or virtual machine. Administrators should ensure that the user's operating system and applications are installed. Once the user logs back onto the network, ProfileUnity will automatically pull down the user's settings and data, in only seconds at login, fully recovering their workspace.

What This Means for Your Environment

Data disaster recovery plans include many diverse scenarios. The following use cases represent the most common situations a corporation might encounter. For the purpose of this paper, our simulated disaster is a large disaster that has deemed the main enterprise office and data center a total loss in terms of physical property and intellectual property recovery. In order to cover the full gamut of systems that you may have in your organization, we will discuss what will happen to your physical desktops (desktops and laptops), persistent virtual desktops, and non-persistent virtual desktops. We will leverage this into your disaster recovery storage costs, as well as NAS, SAN, and backup costs. Our discussion will also cover how much risk you will incur on the probability of singular device failure, as well as the amount of time lost in user productivity for any scenario. Finally, we will compare how implementing with or without ProfileUnity changes the probability for intellectual property loss in the event of a disaster.

Scenario 1: Physical Desktops without Profile Unity

Pros: Very well defined architecture and cost structure	
Cons: Very expensive due to deployment time and data loss probability	
DR Storage Costs	High
Probability of Device Failure	High
Time Lost in User Productivity	High
Probability for Intellectual Property Loss	High
Cost Considerations: High, due to cost of backup/restore process, possibility of data loss, and time to deploy or re-image machine	

The majority of enterprises in existence today still have physical desktops. Let's go through each of the points mentioned in the summarization of this configuration, and talk about how day-to-day work and disaster recovery will be affected without the use of ProfileUnity.

In terms of disaster recovery storage costs, this can mean the worst case scenario for your existing data. While you may be backing up your user's home drive, the local data that is present on their machines is highly susceptible to loss unless their entire hard drive is backed up to the NAS or SAN, and then again to the network storage backup mechanism in place, and then finally to the off-site backup site. This is a tremendously high cost to consider.

The probability of device failure, outside of a major disaster, is also quite high in this instance. With the introduction of local hard drive encryption, this probability simply gets worse. Data recovery for a failed encrypted hard drive is quite poor.

The time lost in user productivity for this scenario is also quite high. The amount of time to re-image a machine, install the applications, configure machine settings, and migrate user data back onto the unit can take up to one business day. This is, of course, in the event that the data on the old hard drive is available for extraction.

Finally, the probability for intellectual property loss in the event of a disaster or hardware failure is also quite high. Not all data can be recovered from a hard drive in the event of a crash. If a user was not backing that data up to their home drive after each business day, the delta between backups and data corruption is the equivalent lost time. For example, if a user did not back up their system data for two weeks, and then a system loss or hard drive loss occurred, it would logically take 11 business days for that employee to recover all that data. This is, of course, if they can remember everything they have done in this time. This time estimate includes the two weeks it would take to reconstruct the data along with one business day for re-imaging and restoring their data.

Scenario 2: Physical Desktops with ProfileUnity

Pros: Intellectual property is very safe, faster deployments and re-imaging	
Cons: Minimal cost of ProfileUnity, which can be recouped in the first deployment or loss of data	
DR Storage Costs	Low
Probability of Device Failure	High
Time Lost in User Productivity	Low
Probability for Intellectual Property Loss	Low
Cost Considerations: Moderate , due to lowered costs of deployment, re-imaging, and data loss	

Using the exact same organization in either a disaster recovery or system failure scenario, we can see that the landscape completely changes when pairing physical desktops with ProfileUnity.

First, the disaster recovery storage costs have been significantly reduced. Instead backing up an entire local image and managing the deltas between those images, we can instead focus just on the user's data. Because ProfileUnity is storing Portability Settings in a compressed, low footprint format, the amount of data to store is minimal. Folder redirection allows for native file and folder formats, so the data here can be de-duplicated for additional storage savings. Delta data on a user's system is no longer a concern, because ProfileUnity is updating these directories in real-time.

The probability of device failure with ProfileUnity has not changed, because we are not able to change the MTBF (Mean Time Before Failure) of any hardware device. What has changed, however, is the ability to immediately back up user data as they are working on it with no perceivable change to the user.

The amount of time lost in user productivity has changed drastically in this scenario. In the event of a complete disaster situation or a single user failure, the output is the same. The user would have their new machine re-imaged using the corporate image process. Then the applications for the user would be laid down on the machine. Finally, once the user logs in, all of their application settings, user settings, machine settings, and data are immediately available. If the machine was lost while the user was working on a new Office document, the Auto Recovery portion of Office would be able to recovery what the user was working on, down to the last few minutes of activity.

Adding ProfileUnity also has a tremendous impact on the amount of intellectual property lost for the company, which should be near-zero. This is due to the fact that ProfileUnity is cataloging all user data in almost every area of the operating system and can couple that with advanced application recovery features, securing the intellectual property of the organization and ensuring its integrity.

Scenario 3: Persistent Virtual Desktops without Profile Unity

Pros: Very well defined architecture and cost structure	
Cons: Very expensive, susceptible to data loss between backups	
DR Storage Costs	High
Probability of Device Failure	Low
Time Lost in User Productivity	High
Probability for Intellectual Property Loss	High
Cost Considerations: High, due to cost of backup/restore process, storage costs, possibility of data loss, and time to deploy or re-image virtual machine	

Many organizations choose to implement virtual desktops in a persistent format, or a one-to-one desktop to user ratio. Deploying persistent desktops is one of the easier ways to implement a VDI environment, because it does not require a majority of the user applications to be provided by a streaming service. While the probability for device failure is greatly reduced in this scenario, DR storage costs, time lost in user productivity, and probability for intellectual property loss are still very high.

Actually, disaster recovery storage costs here are exorbitantly high due to the fact that the one-to-one mapping requires more NAS and SAN storage to maintain each user's image. When backups run, the entire image needs to be backed up to both the internal backup environment and the off-site backup. Data de-duplication can reduce data storage requirements, but this generally has little impact when considering the costs for off-site backup.

In the event that the user corrupts their system or the disaster scenario is applied, we still find that the user has lost a tremendous amount of productivity. The amount of data lost includes anything created or modified since the last backup. Since weekly backups are optimal for this environment due to their size, the worst case is that a week's worth of data would be lost. Coupling the data loss with the time that it would take to create a new user image, install the applications and migrate the user data, further increases each user's loss in productivity. While this scenario is not nearly as difficult to accept as the physical example, it is still quite high.

The probability for intellectual property loss here is again quite high. The impact of the loss depends on the amount of work done between the last complete backup and the actual loss of the system. Any new work generated in this time will have to rely solely on the user's memory to re-create those documents.

Scenario 4: Persistent Virtual Desktops with ProfileUnity

Pros: Intellectual property is very safe, faster virtual deployments and re-imaging	
Cons: Minimal cost of Profile Unity, which can be recouped in the first deployment or loss of data	
DR Storage Costs	Low
Probability of Device Failure	Low
Time Lost in User Productivity	Low
Probability for Intellectual Property Loss	Low
Cost Considerations: Moderate , due to lowered costs of virtual deployment, re-images, and data loss	

ProfileUnity immensely changes the landscape for all types of costs and losses when deployed in a persistent virtual desktop environment. ProfileUnity eliminates the need to keep backups of entire images both internally and off-site.

Disaster recovery storage costs for multiple or single users exponentially decrease. Instead of keeping full image captures of a user's system, we can simply backup the master image once and then incrementally backup all of the user's data. The user data can then be deduplicated, further reducing the storage costs. When transitioning this data to an off-site backup, the gains can be realized yet again, as we are only interested in capturing a master image, application installation packages, and user generated data.

Time lost in productivity is also completely changed. Because ProfileUnity automatically migrates user documents the network storage share in real time and then replicates the updates to both internal and off-site backup environments, a user doesn't risk losing any work between backups. Administrators can simply generated a new user image, and have the user logon the system to install whatever applications they need to perform their work. All of their data and application settings will automatically follow them to the new image including any data they may have been working on in any application that stores Auto Recovery data.

The probability for intellectual property loss here is also very low, due to the reasons stated above. If all user data is immediately accounted for and backed up in multiple locations, then any intellectual property created by the user is considered safe.

Scenario 5: Non-Persistent Virtual Desktops without ProfileUnity

Pros: Very inexpensive to implement	
Cons: No user retained settings for programs, data is only as safe as the last backup	
DR Storage Costs	Moderate
Probability of Device Failure	Moderate
Time Lost in User Productivity	High
Probability for Intellectual Property Loss	High
Cost Considerations: Moderate , due to cost of backup/restore process, possibility of data loss, time to deploy or re-image virtual machine, and lack of persistence, which can cause users to change settings and data multiple times	

Non-persistent virtual desktops are a fairly new way to employ virtual desktop infrastructure within your enterprise at a much lower cost. With non-persistent virtual desktops there is one master image that is separated from a user's settings and data. Eliminating the one-to-one mapping requirement significantly reduces the amount of data that needs to be stored. Lower storage requirements and concurrent licensing models primarily account for the cost reductions associated with this model. In order to realize the benefits of non-persistent virtual desktops, all non-image included software must be streamed to the desktop. However, along with the cost savings and simplification comes an additional challenge. Utilizing non-persistent virtual images without a profile management solution is fruitless. Settings and documents will only follow a user until the system has been recomposed, which may happen several times a year or as often as once a week. This depends on how often you choose to install newer security updates and software updates into the system. Despite the fact that very few companies choose to employ a method such as this, we will still discuss the issues involved in such a scenario.

Many companies choose to also employ a method known as destructive linked clones, where no local data is stored after the client logs off. Instead, the delta data is destroyed. This forces users to save all data to a network location, or they will lose it. Needless to say, this is not a perfect solution, as users may forget to save data at many points during their work day.

Disaster recovery storage costs here are considered moderate because only the master image and image deltas need to be backed up. Unfortunately, as soon as a master image is recomposed, all delta data is lost, and cannot be moved to a newly composed image. This is a fairly useless endeavor, as any data you back up will only be as good as the last image that you released.

The probability for device failure here is moderate, mostly due to the disposable nature of non-persistent desktops. Because most applications are streamed, most IT help desks will simply reissue a new desktop to a user in the event of image or data corruption. Any data created since that point will be lost.

The time lost in user productivity is also high. If system corruption causes a reboot or causes the system to be unresponsive, any data the user has been working on is now lost.

Finally, the probability of losing intellectual property data is also very high in this case, because you are relying on your users to constantly save their data to a network location. This also assumes that the system is going to be responsive at all times and will never require a recomposition, which is an unrealistic expectation.

Scenario 6: Non-Persistent Virtual Desktops with ProfileUnity

Pros: Intellectual property is very safe, fastest virtual deployments	
Cons: Minimal cost of Profile Unity, which can be recouped in the first deployment or loss of data	
DR Storage Costs	Low
Probability of Device Failure	Moderate
Time Lost in User Productivity	Low
Probability for Intellectual Property Loss	Low
Cost Considerations: Lowest possible cost of any configuration	

The final scenario that we will cover in this paper uses ProfileUnity to manage the user data in a non-persistent environment. Pairing ProfileUnity with non-persistent desktop deployments offers the greatest positive impact to disaster recovery methodologies and storage costs for an enterprise.

First, disaster recovery storage costs are the lowest of any of our scenarios. Only the master image needs to be stored. Any user delta data is simply treated as temporary and does not have to be backed up. Only the ProfileUnity data will need to be backed up, and that data again can be subject to de-duplication. This fractional amount of data will also need to be backed up using the off-site backup method. Because the amount of data being backed up in all environments is fractional, costs associated with this method are fractional as well.

Second, the probability of device failure has not changed from the previous scenario. Non-persistent desktops are still considered a “throw away” operating system in this case. In the event that a user has a problem, they simply reboot, and are generated a new operating system. In the event of a major disaster, IT simply has to generate the required amount of concurrent images, and all user installed programs and data are instantaneously migrated over.

The amount of time lost in user productivity is the lowest possible amount. A reimage is as simple as rebooting a machine. Essentially, the user is reimaged every time they log into a fresh non-persistent machine, and there is never any user downtime for reimages. The idea of spending time to rebuild an image is now a thing of the past. Gone are the days of full business day losses provisioning a new machine. In the event of a major catastrophe, images and NAS or SAN systems simply have to be restored on any compatible virtual hardware. The actual location of the new data center is also more flexible with today’s available network infrastructure. An organization simply needs to be aware of the network traffic required by the total number of systems to support. As long as that bandwidth is available, the data center can be nearly anywhere in the world.

Finally, the probability of intellectual property loss during a major disaster or single user loss event becomes completely mitigated. Due to the previously stated reasons, we now have all user backed up in duplicate, both on-site and off-site. Auto Recovery technologies mean that getting a fresh image is as simple as a re-boot. A new system is available in seconds, and the user can resume working in as little as a minute. The amount of possible intellectual property loss is negligible.

Conclusion

Implementing ProfileUnity significantly decreases the risk of data loss to a client in the event of any catastrophic failure. Coupling this with disaster recovery best practices can result in:

- ✓ Drastic decreases in the amount of storage necessary to carry DR data
- ✓ Reduced storage costs for both local storage and off-site storage
- ✓ Instantaneous availability to current user data
- ✓ Faster re-image and restore processes in physical environments
- ✓ Faster restore process in virtual environments
- ✓ The ability to fully leverage linked clones and linked clones DR
- ✓ Immediate data availability for persistent virtual images
- ✓ No proprietary databases to recover when just one file is needed
- ✓ No need to worry about encrypted hard drive failure.

The examples set forth in this document have demonstrated the strengths and weaknesses of deploy physical and virtual machines with and without ProfileUnity. In all cases, ProfileUnity reduces the costs involved in desktop deployment and ongoing maintenance. As a very low cost user environment management solution, ProfileUnity immediately increases the return on investment (ROI) of your infrastructure. These gains are further realized the first time that a user has a corrupted physical or virtual machine immediately recovered with no data loss. ProfileUnity also enhances the user experience by reducing to near zero the amount of time that a user spends reconfiguring their application and machine every time the master image is either reimaged or recomposed whether due to software updates or new deployments.

The end result is that ProfileUnity will pay for itself within the first few machine deployments, and will continue to pay for itself many times over with the amount of intellectual property retained in the event of a disaster.

About ProfileUnity and Liquidware Labs

Liquidware Labs ProfileUnity™ is a complete migration and environment management solution for virtual and physical desktops. The solution enables users to seamlessly experience any Windows OS (XP/2000/Vista/7) from any desktop – a Citrix XenDesktop, VMware View session, or a physical PC. ProfileUnity delivers each user's personal workspace in Windows own native format, regardless of where the user logs on to the network.

Liquidware Labs™ is the leader in desktop transformation solutions for next-generation physical and virtual desktops, including VMware View, Citrix XenDesktop, and Microsoft Windows 7. The company's Stratusphere™ and ProfileUnity™ solutions have been described by analysts as the industry's first "On-Ramp to VDI", providing a complete methodology and software that enables organizations to cost-effectively plan, migrate, and manage their next generation desktop infrastructure. LWL's comprehensive solutions provide Assessment, Personalization Management, User Configuration, and Service Level Assurance. Liquidware Labs products are VMware and Citrix certified, and are available through a global network of certified partners. Visit www.liquidwarelabs.com for further information, and follow us on Twitter @LiquidwareLabs.

Liquidware Labs ProfileUnity Disaster Recovery Summary Matrix

Scenario	Description	Storage Costs	Probability of Device Failure	Time Lost in User Productivity	Probability for Intellectual Property Loss	Cost Considerations	Pros	Cons
1	Physical Desktops without ProfileUnity	High	High	High	High	High, due to cost of backup/restore process, possibility of data loss, and time to deploy or re-image machine	Very well defined architecture and cost structure	Very expensive due to deployment time and data loss probability
2	Physical Desktops with ProfileUnity	Low	High	Low	Low	Moderate, due to lowered costs of deployment, re-imaging, and data loss	Intellectual property is very safe, faster deployments and re-imaging	Minimal cost of ProfileUnity, which can be recouped in the first deployment or loss of data
3	Persistent Virtual Desktops without ProfileUnity	High	Low	High	High	High, due to cost of backup/restore process, storage costs, possibility of data loss, and time to deploy or re-image virtual machine	Very well defined architecture and cost structure	Very expensive, susceptible to data loss between backups
4	Persistent Virtual Desktops with ProfileUnity	Low	Low	Low	Low	Moderate, due to lowered costs of virtual deployment, re-images, and data loss	Intellectual property is very safe, faster virtual deployments and re-imaging	Minimal cost of ProfileUnity, which can be recouped in the first deployment or loss of data
5	Non-Persistent Virtual Desktops without ProfileUnity	Moderate	Moderate	High	High	Moderate, due to cost of backup/restore process, possibility of data loss, time to deploy or re-image virtual machine, and lack of persistence, which can cause users to change settings and data multiple times	Very inexpensive to implement	No user retained settings for programs, data is only as safe as the last backup
6	Non-Persistent Virtual Desktops with ProfileUnity	Low	Moderate	Low	Low	Lowest possible cost of any configuration	Intellectual property is very safe, fastest virtual deployments	Minimal cost of ProfileUnity, which can be recouped in the first deployment or loss of data