A Practical Guide to VDI Change Management

How VDI testing will help to protect the business continuity of large organizations

November 2018 – v1.17

Frans Wauters, Marketing Director

Mark Plettenberg, Senior Product Manager

Disclosure and Warranty

Table of contents

Executive summary

IT has transformed into a core competency for every modern organization, and CIOs have become the most important drivers of business innovation today. Tasks and responsibilities of IT executives have grown past hardware, software and networks, towards much larger goals such as business innovation, business continuity, and corporate governance.

The more complex infrastructures become, the greater the chance for something to fail. It is not only the number of different parts that increase the chances of failure, but also the exponential number of interdependencies between these parts that can fail. VDI is basically a big stack of interrelated components with a very high utilization. VDI environments therefore have a high chance for failure.

The main advantages of a centralized Windows user environment, such as VDI, are flexibility and security. Also, the more efficient management of desktop images and servers is often mentioned. But the more consolidated infrastructures become, the bigger the business impact if something fails.

As change is inevitable and accelerating, change management has become an essential IT service management (ITSM) discipline. The objective of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to the IT infrastructure, to minimize the number and impact of disruptions to IT services.

The introduction of Windows 10 accelerates the rate of software change dramatically. In addition vulnerabilities such as Meltdown, Spectre and L1TF require patches which must be implemented. To make things even worse, application vendors are moving towards Software as a Service (SaaS) models, where change and maintenance are becoming a constant fact of life. On average in 2010 a typical core business application would receive 4 updates per year. In the new SaaS models, it is expected for that number to grow to 120 by 2020: a 30-fold increase.

Service continuity management is about making sure IT services can continue to deliver as expected, despite a growing and accelerating flow of (planned) changes or possible incidents. The focus of this discipline is not only on recovery measures, but more and more about pro-active activities, because preventing interruptions is clearly the most effective way to contribute to better business continuity.

The combination of these factors makes it absolutely necessary to implement a comprehensive change impact analysis process that covers every type of change that may hurt IT operations and as a result damage the organization's Business as Usual. A comprehensive change management structure needs a complete set of pro-active solutions for change impact validation to prevent problems caused by planned changes, unplanned changes, gradual deterioration and disasters.

Login VSI offers enterprises and vendors a complete software solution to build and safeguard the optimal performance, scalability, availability and compatibility of desktops and applications running in virtual desktop environments, based on proven industry standard virtual (synthetic) user technology.

Change Management maintains the proper balance between the need for change and the potential detrimental impact of changes (ITIL©).

1. IT Change Management in general

1.1 IT is a business function, not a back-end function anymore

In the early days the information technology (IT) department was mainly a back-end function in most organizations. IT and finance, for example, were the departments that were quite remote from the business. Sales and marketing roles were front and center in the day to day optics of the company. The main task of IT in front-end activities was to facilitate the productivity of sales and marketing. Today all this has changed!

After joining Gartner and other strategic analyst conferences for many years, one major change has become very clear. IT has transformed into a core competency for every modern organization, and CIO's have become the most important drivers of business innovation today. Tasks and responsibilities of IT executives have grown past hardware, software and networks, towards much larger goals such as business innovation, business continuity, and corporate governance.

1.2 Change Management is an essential part of modern IT management

As IT infrastructures become more embedded into every function of a company, they start to form the essential fabric of the entire organization and all its processes. The optimal and uninterrupted working of systems becomes a critical success factor for every organization, and failure is always very costly in loss of time, money and possibly even image. For this reason, many large organizations turn to very structured approaches in managing their IT projects and operations, such as ITIL* and ITSM*.

As change is inevitable and accelerating, change management has become an essential IT service management (ITSM) discipline. The objective of change management is to ensure that standardized methods and procedures are used for efficient and prompt handling of all changes to the IT infrastructure, thereby minimizing the number and impact of any disruptions to IT services.

The primary objectives of change management include:

1. Minimal disruption of IT services
2. Reduction in back-out (roll-back) activities**
3. Economic use of resources involved in the change

In the description of its 'IT Change Management Policy Documentation Guidelines of 2017', Gartner also recognizes the role of change management in reducing risks after change: "effective IT change management processes balance the ability to enable change, with the need to mitigate the risks resulting from releasing changes to the computing environment."

Change Management is the process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made, with minimum disruption to IT services (ITIL©).

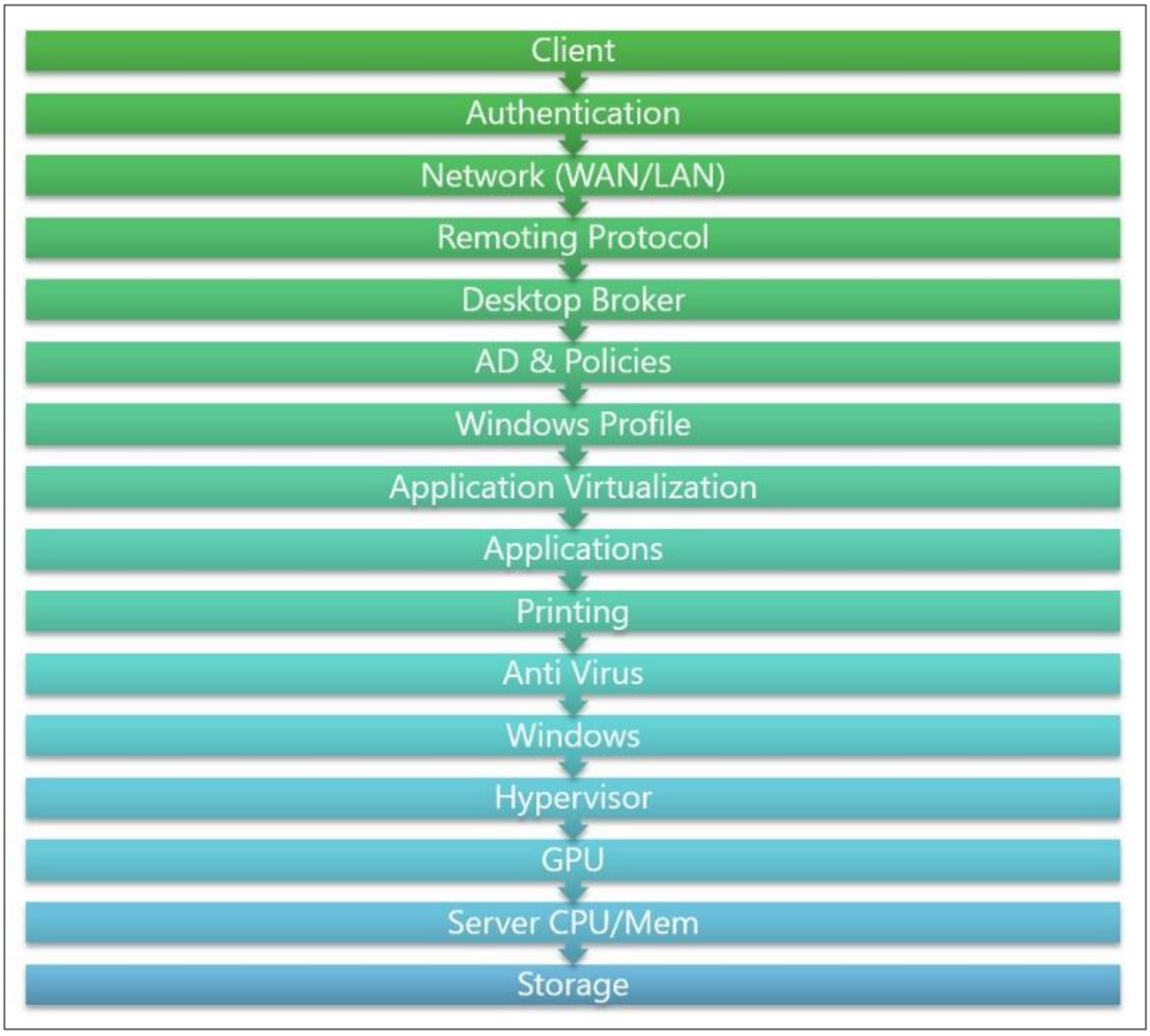
** ITIL (formerly an acronym for Information Technology Infrastructure Library) is a set of detailed practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. Source Wikipedia.*

**Back-out (roll-back) activities are activities you need to perform to restore an IT service to the previous state.

2. Why VDI is very sensitive to change

2.2 VDI chance of failure is higher due to infrastructure complexity

Centralized desktop and application environments such as Virtual Desktop Infrastructures (VMware Horizon View and Citrix XenDesktop), but also Server Based Computing (Citrix XenApp and Microsoft RDSH), typically use a complex and elaborate combination of many hardware and software parts, including CPUs and GPUs, storage, memory, hypervisors, publication layers, clients and more.



Picture 1: Different components of a VDI environment

The more complex infrastructures become, the bigger the chance for something to fail. It is not only the number of different parts that increase the chances of failure, but also the exponential number of interdependencies between these parts that can fail. VDI is basically a big stack of interrelated components with a very high utilization. VDI environments therefore have a high risk of failure.

Conclusion: The more complex environments are, the more critical change management becomes.

2.2 Impact of VDI failure is high due to centralization

The most mentioned advantages of a centralized Windows user environment such as VDI, are flexibility and security. Also, the more efficient management of desktop images and servers is often mentioned. But the more consolidated infrastructures become, the bigger the business impact if something fails.

VDI introduces a single point of failure for all end-users of an organization as a group. In organizations with 10,000s of end-users, the size of the impact is obvious. Also in SME companies, with 100s of users, the impact is relatively the same if all users are unable to work efficiently, or not able to work at all.

Conclusion: The centralization of VDI dramatically increases the business impact of failure.

2.3 Different ways to quantify the impact of VDI failure

With IT transforming into a core competency for every modern organization, IT downtime causes an immediate and sizeable negative impact on basically every aspect of the business. In our white paper "The real costs of VDI downtime and how to mitigate" we look at what industry analysts say on this.

There are many estimates of what downtime costs a company, and they vary based on the size of the company and what systems are down. Here are some of the different estimates we found:

1. Ponemon Institute Research did a study of multiple datacenters and estimated the average cost of datacenter downtime at approximately $7,900 per minute, and the average incident length at 86 minutes (Ponemon.org, Cost of Data Center Outages 2013).
2. CIO Insight found that when systems are down, employees are only able to work at 63% efficiency (cioinsight.com, IT Downtime Carries a High Price tag).
3. Gartner makes a very conservative estimate at the hourly cost of downtime at $42,000 (networkworld.com, How to Quantify Downtime).
4. Enterprise Management Associates puts the cost of application downtime at $45,000 per hour, averaged across low mid-tier to large enterprises (zdnet.com, Real Cost of Application Outages).

Based on these reports, we can see that there's little consensus on what downtime costs, but we can use this to come up with some conservative estimates. The Ponemon numbers are the most referenced and have the most backing data, so we'll work with these, and we'll use the CIO Insight research to assume users can still work at 63% efficiency while systems are down (good employees will find ways to do their job), so this conservative result bakes in some user ingenuity into the equation.

Conclusion: a VDI outage may cost a large company, on average, $5,000 per minute of downtime.

Picture 2: Different dimensions affected by downtime

In the same white paper, we also explored, in-depth, the three key dimensions of the business that downtime affects and should be considered: productivity, lost opportunity, and reputation. Calculating these for your own organization will help to better materialize the impact of downtime.

Now just imagine this.

That all your desktops and applications are not available, or just too slow to be used, for 1 hour.

- Then imagine the total number of users in your organization that will be affected
- Calculate the total out-of-pocket cost of lost hours (in dollars/euros)
- Add any other out-of-pocket costs (in dollars/euros)
- Then add the lost-opportunity costs (in dollars/euros)
- Now you have a feel for the tangible damage such an occurrence brings to your organization
- Then add the angry customers, damaged company image, and you own position (priceless).

If you have ever experienced this, we need to say no more. If you haven't we hope you get the picture.

It has become clear that the chances of IT failure are relatively high in an VDI environment, due to the complexity of the infrastructure stack. It has also become clear that the impact on the business can be high, considering lost productivity, lost opportunity, and damaged reputation. With change being the most important cause of potential problems, change management becomes key.

Conclusion: The more consolidated environments are, the more critical change management becomes.

3. Change accelerates with Windows 10

Adopting Windows 10 forces you to significantly change your deployment and update processes to ensure you stay current with all expected feature and quality updates. Falling behind on updates will result in the loss of service and support by Microsoft and is therefore not an option anymore.

Windows 10 updates will not only be released more often than before, they are also bigger in size as they will be cumulative, and therefore have a bigger potential impact. Typically, larger Windows migration projects required 12 to 18 months of work and occurred every 3 to 5 years. With Windows 10 we must get used to a more continuous process of implementing bigger and smaller changes.

3.1 Windows 10 introduces two major feature updates a year

Windows 10 feature updates will be released twice a year, one in springtime (March) and one in the fall (September). As the update cycle is shorter now the changes will be bite-sized chunks compared to the big updates that where released every 3 to 5 years. Microsoft still recommends a preview and pilot period before moving to full production (and some time to phase-out after production). This means that in large organizations 2 or 3 different builds could be in use at the same time (see picture 3).

In September 2018 Microsoft announced that:

- All *currently supported* feature updates of Windows 10 Enterprise and Education editions (versions 1607, 1703, 1709, and 1803) will be supported for 30 months after their original release date.
- All *future* feature updates of Windows 10 Enterprise and Education editions with a targeted release month of September (starting with 1809) will be supported for 30 months after release.
- All *future* feature updates of Windows 10 Enterprise and Education editions with a targeted release month of March (starting with 1903) will continue to be supported for 18 months after release. This maintains the semi-annual update cycle and allows customers to update twice a year.

3.2 Windows 10 also introduces 3 to 4 new builds a year

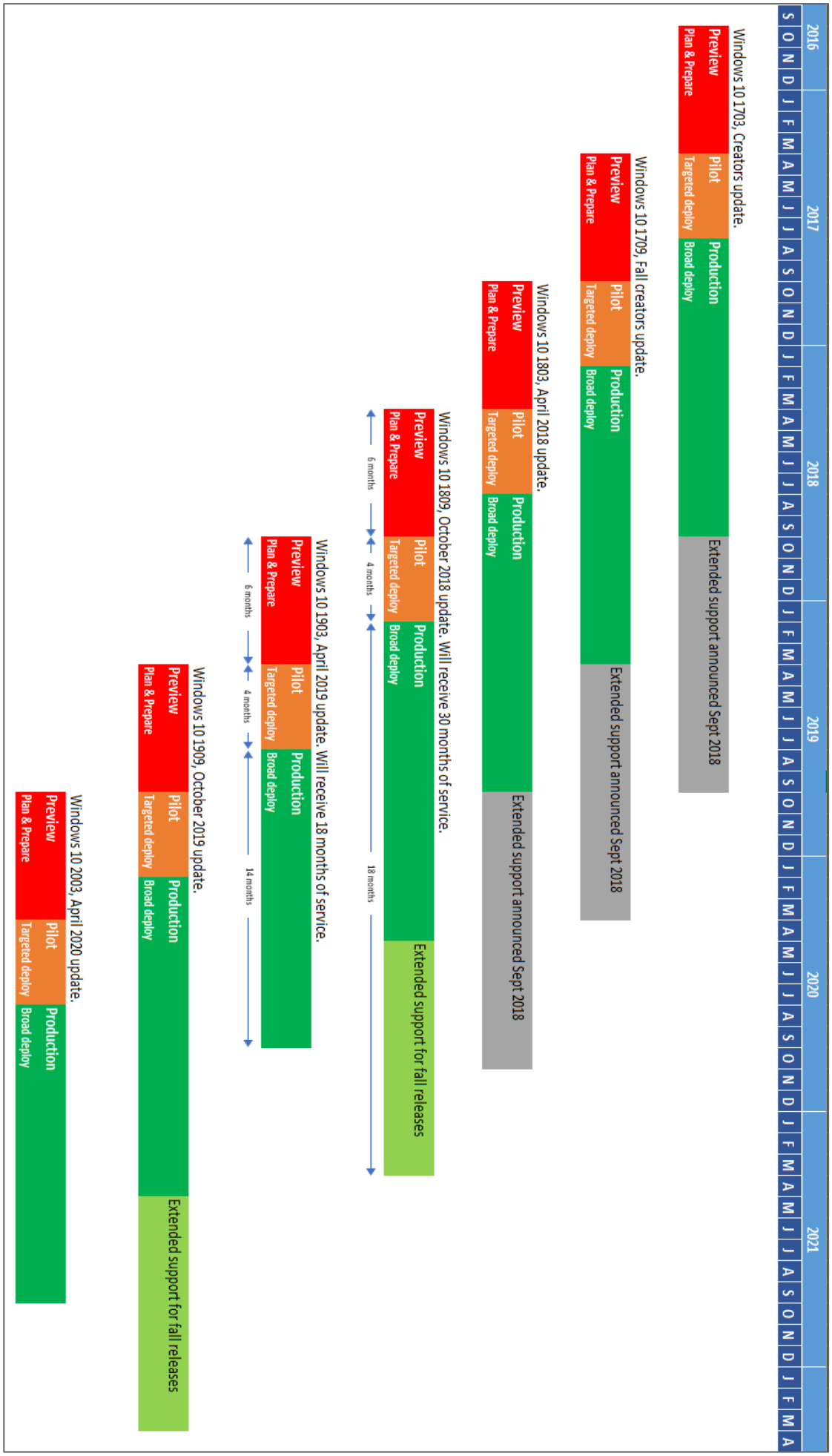
Microsoft is now making new builds available during their development phase. This new practice enables IT administrators at customer organizations to plan and prepare compatibility tests with their existing applications and infrastructure, to validate new features and to provide early feedback on any issues encountered (to relevant ISV's and to Microsoft).

Microsoft is collecting telemetry (when enabled) on these builds to spot application compatibility and other problems. This helps but is not effective for in-house applications as there simply isn't enough telemetry reported back. Testing early preview builds also does not guarantee the perfect workings of the final build due to further changes and updates in the builds before production.

3.3 Windows 10 quality updates are cumulative and therefore bigger

Small updates are typically released on the second Tuesday of each month ("Patch Tuesday"), but when required can be released at any time. These regular updates can consist of security updates, bugfixes, driver updates and more. Windows 10 quality updates are cumulative, which means that installing the latest quality update is sufficient to get all changes to date. As a result, quality updates will become bigger in size every month, unless techniques like express updates are implemented.

Conclusion: The introduction of Windows 10 accelerates the rate of software change dramatically.



Picture 3: Multiple Windows builds may be in use at the same time

4. IT change accelerates in general

In the previous chapters we stated that “the more complex infrastructures become, the bigger the chance for something to fail”. We can easily expand this into a logically related conclusion when we state that “the more complex infrastructures become, the bigger the chance for something to change”.

An average VDI environment is subject to many changes, upgrades, updates, and patches, such as:

- New / updated Operating System / Patch releases (accelerated with the introduction of Windows 10, see previous chapter)
- VDI related software infrastructure changes (EU layer and hypervisor)
- Core business application updates and upgrades
- Security patches such as for Meltdown, Spectre, and L1TF
- Hardware changes / Configuration changes / Firmware revisions
- Memory upgrades / Storage upgrades / GPU’s

The flow of changes that can affect a smooth running VDI environment is already significant due to its complexity and many parts. In addition, this flow of changes is growing and accelerating as vendors are more and more moving towards Software as a Service models, where maintenance is a constant fact of life. On average in 2010 a typical core business application would receive 4 updates per year. In the new models it is expected for that number to grow to 120 by 2020: a 30-fold increase.

Looking at a few large corporations we found some impressive numbers in this respect:

- A major US retailer went from 1 update per month to 80 per week
- A major US online retailer pushes 300 changes per day

Like Microsoft, most other major software vendors are switching to a release schedule based on Software as a Service. Sending out many small updates with a short interval e.g. two to four weeks. While this eases troubleshooting as the changes are smaller, it does force IT departments to push a lot more changes to production, to keep up to date and to stay within support.

4.1 Microsoft

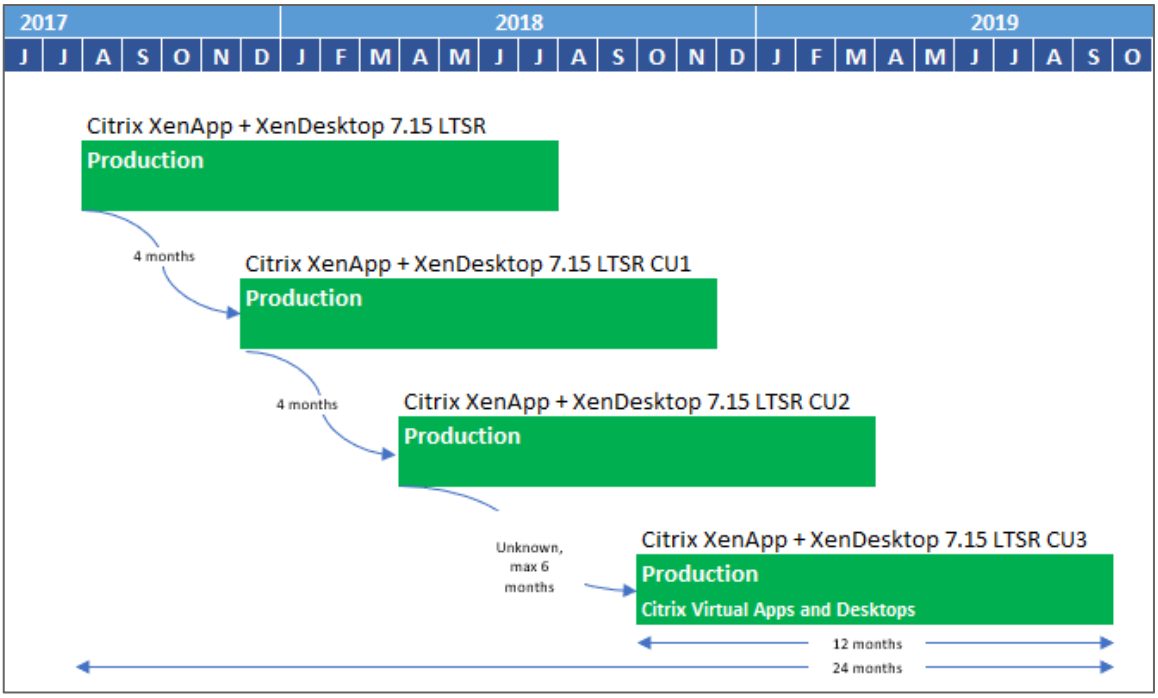
We mentioned the Windows 10 update cycles but there are two other Microsoft products that also must be maintained in nearly every enterprise environment: Microsoft SCCM and Microsoft Office.

Many organizations rely on Microsoft SCCM to orchestrate Windows desktop deployments, application installs and even mobile devices. To be able to deliver two feature updates per year for Windows 10, three SCCM feature updates must be done per year, to make sure the systems are compatible.

Tests executed by the EUC initiative, VDI Like a Pro, show that every Microsoft Office update has a tangible impact on the End User Experience (in some cases decreasing application performance and/or server density with more than 20%!). The Microsoft Office suite is also notorious when it comes to macros and other in-house or third-party built plugins, as updated security features often block applications that contain these additions.

4.2 Citrix

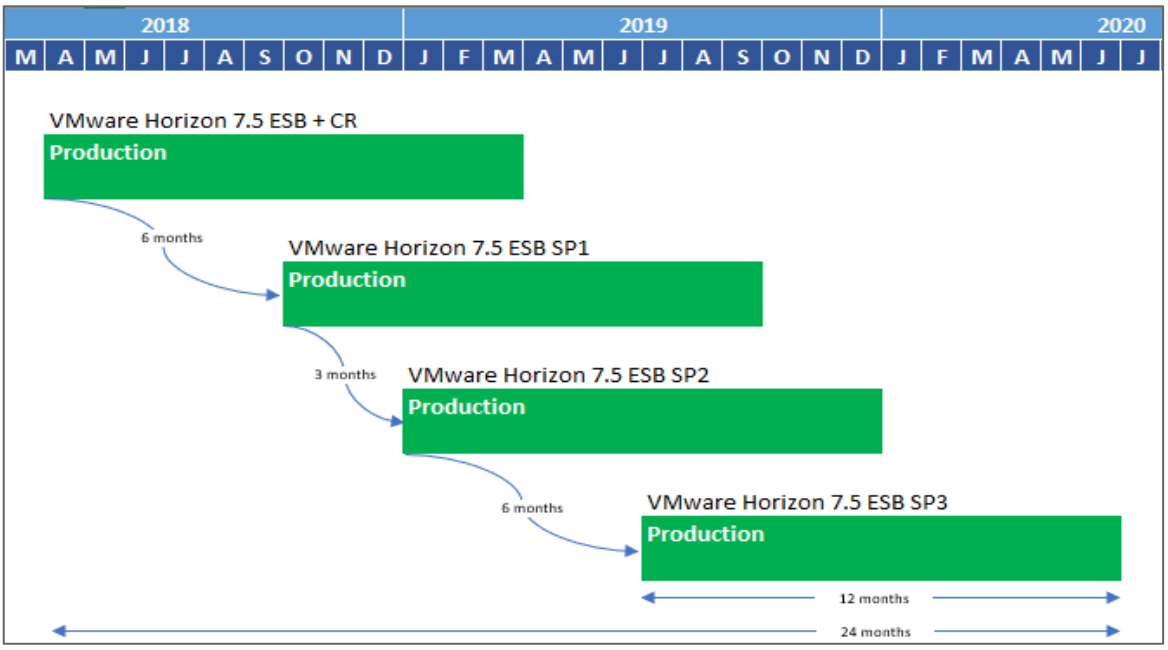
This infrastructure company now offers three service plans to keep XenApp/XenDesktop environments up to date ranging from their Citrix Cloud offering that's automatically brought to the latest version, a Current Release (CR) version every 3-9 months and (since January 2018) a Long-Term Service Release (LTSR) version being released every 12-24 months with cumulative updates every half year.



Picture 4: Citrix XenApp/XenDesktop – Virtual Apps and Desktops LTSR update cycles

4.3 VMware

Starting with VMware Horizon 7.5 in Q2 of 2018, VMware now introduces updates in two speeds, a Current Release (CR) regularly and an Extended Service Branch (ESB) every 3 to 6 months.



Picture 5: VMware Horizon View ESB update cycles

4.4 Core business applications

Core business application upgrades can have big impacts. Starting early 2018 one of the leading US based EHR-vendors plans to roll-out one major release per year, complemented by one Special Update (SU) per quarter. Rumors are that a performance loss (read extra hardware) should be budgeted for, with additional resource needs of approximately 20% for the major releases and 9% for the Special Updates (results may vary), when a SBC platform is used to deliver the application. This adds up to about 50% (when quarterly compounded) in incremental hardware capacity being required each year.

Whatever the real numbers will be, it is clear that new releases and updates of your core applications need to be taken very seriously. As every environment will react differently, testing with a full user load in your organizations' own specific production environment is the only way to predict the exact impact, and the only way to be able to react pro-actively in the most appropriate way possible.

An IT manager at a large American healthcare enterprise using Epic as EHR, mentioned that Login VSI will save them millions of dollars each year, and ensures they stay ahead of performance problems.

4.5 Security patches

Meltdown & Spectre

Recent malware releases and security flaws (sometimes even in hardware) force IT departments to be very careful. At the beginning of 2018, when news about Meltdown and Spectre became public, more than 100 affected vendors started pushing mitigations, followed by more permanent workarounds and fixes. The hasty job of putting together these patches resulted in many outages and application failures as well as degraded performance in many enterprises.

L1 Terminal Fault (L1TF)

Security patches for the latest Intel focused danger, L1TF, are predicted to damage scalability and performance in VMware environments with 20 to 30%! Even though the L1TF security problems are not as prominent in the news as Meltdown & Spectre this is not a patch to be taken lightly.

And this is not the end

Following these vulnerabilities emerging in the first months of 2018, we can be quite sure the chances are high that more new vulnerabilities will follow. Making preparing for the impact of security patches, something that needs to be embedded in any well-structured change management program.

4.6 Hardware renewal in datacenters

Major hardware vendors recommend a hardware refresh every 3 to 5 years depending on warranty and workload. Newer generations of hardware are significantly faster (e.g. Intel promised a 17x better performance in hardware from 2007 to 2013) and more efficient when it comes to power usage and space requirements. Less hardware can also considerably lower licensing costs, but centralizing more services also means more single points of failure that can bring down the whole environment.

In addition to complete servers, smaller portions of the infrastructure may be upgraded due to the availability of new technologies in storage or GPUs.

Conclusion: The more complex environments are, the more (often) changes will occur.

5. Building resilient VDI infrastructures

5.1 IT service management emphasizes reliability and resilience

As discussed in chapter 1, ITIL provides a comprehensive description of practices that are part of the IT service management (ITSM) function. This function is crucial in every large organization as it aligns the IT service operation with the business needs of an organization. ITIL covers 5 phases: Strategy, Design, Transition, Operation, and Continuous Improvement.

In the Design phase the following service management processes are discussed (source: Wikipedia):

1. Design coordination
2. Service catalogue management
3. Service-level management
4. **Availability management**
5. **Capacity management**
6. **IT service continuity management**
7. Security management
8. Supplier management

When we seek to design and build resilient VDI infrastructures that will provide and guarantee an optimal end-user experience and application performance to the organization, ITIL gives useful recommendations for managing availability, capacity, and service continuity.

Availability management

Availability management covers the ability of an IT function to perform at an agreed level over time. This is often documented as a Service Level Agreement (SLA). Aspects such as reliability (does it work as required) and resilience (can it weather changes/failures) are key components of availability management.

Capacity management

Capacity management covers the optimal balance between business needs and IT services. This includes activities such as IT capacity planning and IT infrastructure sizing.

Service continuity management

Service continuity management is about making sure IT services can continue to deliver as expected, despite a growing and accelerating flow of (planned) changes or possible incidents. The focus of this discipline is not only on recovery measures, but more and more about pro-active activities, because preventing interruptions is clearly the most effective way to contribute to better business continuity.

5.2 How testing helps to design and build better VDI environments

Compare VDI performance to fat-client performance

When trying to decide if a virtual desktop solution is an option to augment or replace your fat-client desktop environment, the ‘same or better’ end-user experience will most often be the decision-making factor. Objective load testing of the old and new environment is the preferred way for vendors, system integrators and enterprises, and must be a part of every well-executed proof of concept.

A large organization in Europe used performance testing to establish a baseline measurement for their VDI environment. When benchmarking different hardware options, the one that came closest to the fat-client baseline was chosen, which not only helped user acceptance but also helped to prevent subjective discussions about the performance of the new system.

Benchmarking different virtual desktop infrastructure options

When moving to a virtual desktop solution, enterprises must choose between different infrastructure options including the solutions of Citrix, VMware or Microsoft, as well as different hardware options like hyperconverged infrastructure, server, storage and GPUs. Objective load testing is the best way to benchmark the different infrastructure options under consideration and to make fact-based decisions.

A large hospital organization in Europe challenged the vendor requirements of two separate server environments for their XenDesktop VDIs and their Electronic Patient Record application on XenApp. Login VSI was used to verify this option against the all-in-1 system option. With a just-as-good load test result on both performance and scalability, the hospital saved 1.3 million$ on hardware while providing their users with the same user-experience and application performance.

Sizing, scaling and tuning the new virtual desktop infrastructure

The correct scaling and sizing of the virtual desktop infrastructure is important in every VDI project. Too little infrastructure will obviously cause problems with performance when systems are heavily used. Too much infrastructure will cause unnecessary spending in hardware purchase and maintenance, as well as wasting energy cost and datacenter space. Objective load testing is used by vendors, system integrators and especially enterprise organizations to correctly size and scale Citrix XenDesktop, Citrix XenApp, VMware Horizon View and Microsoft RDS infrastructures.

A large healthcare organization in the USA migrated to a new version of Epic using Citrix software on a new Nutanix hardware environment. After installation, based on vendors best practices, the environment could support 2,900 users. After some initial doubts about the performance, Login VSI was used to tune and optimize the entire environment, which increased the density to 4,000 users on the same environment with the same performance. Using standard TCO numbers this represents a monetary value of $3,000,000.

Pre-production (stress) testing

To safely move a new virtual desktop environment into production, it is advised to perform a (virtual) full-scale load test of the production system. Any risk of failure may be unacceptable, especially when business critical applications are involved. Objective load testing is used by smart vendors, smart system integrators and prudent enterprises to load and stress-test virtual desktop infrastructures before they go into production. These tests also indicate the resilience of the system to weather logon storms and other usage peaks.

A large organization in the USA pre-tested their new application in a VDI environment before going into production. During the tests serious failures occurred that were not detected with the original extrapolated tests with smaller loads. Testing prevented a significant loss of business in this case.

6. Handling change in VDI production

6.1 In a healthy VDI production environment, the main enemy is change

In chapter 2 we concluded that the chance of failure in VDI is relatively high due to infrastructure complexity. We also concluded that a failure in VDI carries a heavy negative impact on organizations due to centralization. In chapters 3 and 4 we see that the amount and speed of changes that need to be digested is growing fast.

The combination of these factors makes it critical to implement a comprehensive change impact process that covers every type of change (see picture 5) that may hurt your IT operations, and as a result may damage the organization's Business as Usual (BAU).

Chance of Occurence	Impact on Organization *Low / Medium*	Impact on Organization *High*
Facts of Life	• Planned Changes • Unplanned Changes • Gradual Deterioration	
Very Rare		• Major Incidents/Disasters

Picture 5: Different types of change can disturb IT operations and therefore business continuity

The changes discussed in chapter 3 and 4 are examples of **planned changes**. These types of changes are known, anticipated, and explicitly implemented and processed by the responsible IT staff. Changes of this type include new builds of Windows 10, new versions of business applications (like SAP or Epic), regular weekly or monthly updates (e.g. "Patch Tuesday") and all significant security patches.
The impact on performance and density of systems can vary in the range of 0% to 30% (L1TF) to 50% (EHR vendor) but the impact can be predicted and therefore be anticipated (if properly tested!!!).

More and more applications and infrastructure software are automatically updated (examples include AWS and security software). Most of these updates will not have a performance impact but some may. This type of automatically processed change falls in the category of **unplanned changes**. Unplanned changes may also be caused by someone else in the organization that altered a switch or added or deleted something.

Next to the planned and unplanned changes the regular daily use of IT environments can also cause a slowdown of desktop and application performance called **gradual deterioration**, which may be caused by the pollution or saturation of registries, storage and/or other devices.

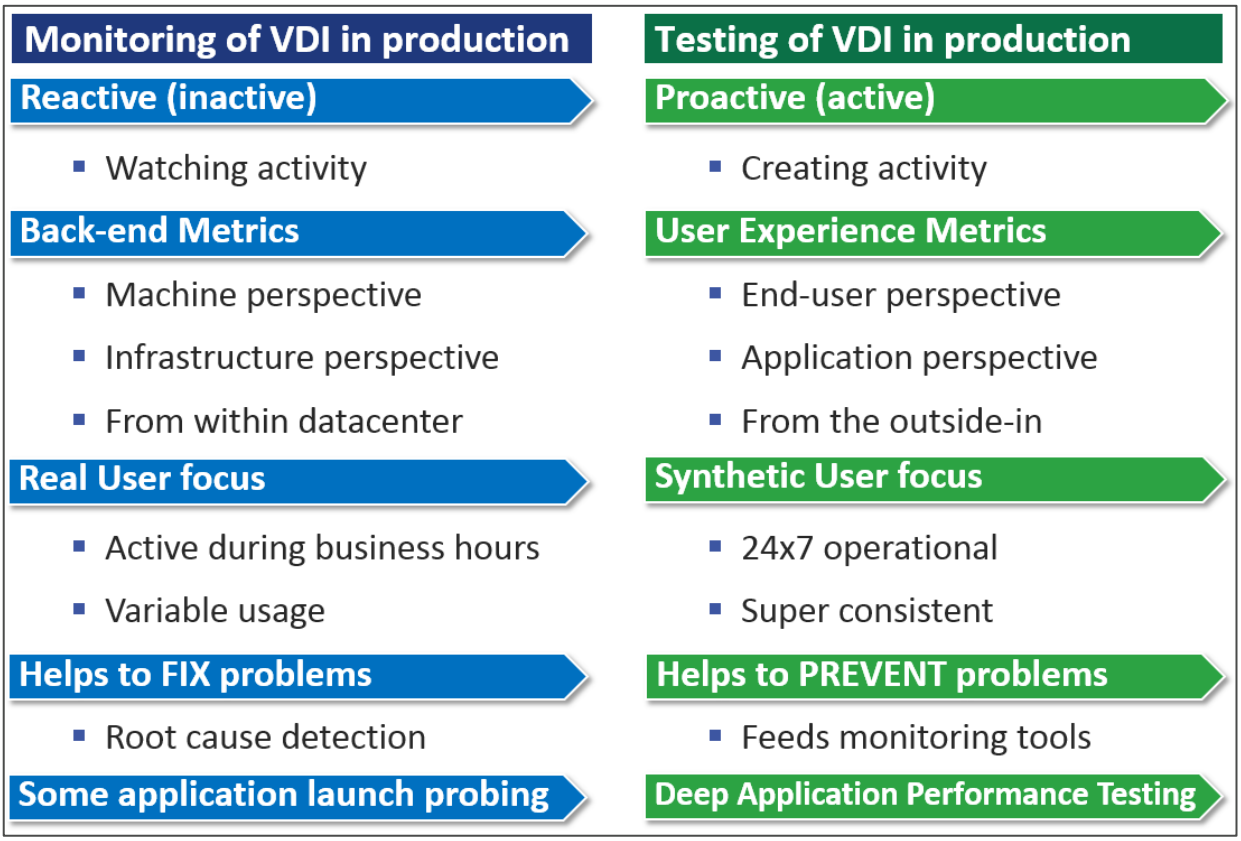
The last type of change we need to plan for are those rare occasions that come with a very big impact such as **disasters or other major incidents** that can be caused by nature or have human causes.

"The only constant in life is change" **- Heraclitus of Ephesus (535 BC – 475 BC)**

6.2 Why stack monitoring solutions are not enough

Traditional stack monitoring, or End User Monitoring (EUM), solutions are infrastructure focused by nature and will tell you all about CPU, I/O and memory health. With their strength in measuring and analyzing real user activity they are reactive by nature, offering effective solutions for root cause analysis. This way they help organizations locate and fix IT problems that occur during production.

Some vendors in the End User Monitoring space also use predictions based on the extrapolation of historical data. In environments where professional testing solutions are not available this can add value but this is certainly insufficient when a comprehensive change management process is needed, such as in health care, finance and other verticals where the cost of failure is high and very tangible.



Picture 6: Stack monitoring solutions are effective for problem fixing but not for problem prevention

Some EUM vendors recently introduced light versions of the virtual user concept to add a pro-active concept to their monitoring solutions. These solutions do start applications to test availability but lack real-life simulation of in-depth application user experience as is needed for key business applications.

Modern organizations looking for effective ways to safeguard business continuity (often after serious outages) must complement their infrastructure-oriented monitoring solutions with 100% pro-active, strict end-user experience perspective focused, test solutions, designed to 100% prevent problems.

To safeguard a delicate, complex, and business critical centralized Windows environment, prudent organizations must leverage a comprehensive pro-active testing environment to handle and prevent possible negative impacts of all the four types of change as described above. Combining best of breed monitoring solutions with a best of breed testing solution will significantly reduce business outages.

Conclusion: Monitoring solutions are good for fixing problems, testing is best for preventing problems.

7. Change impact management for VDI

Enterprises looking to provide the best possible user-experience for the business-critical applications that are running in VDI, SBC or DaaS, need a clever combination of pro-active testing solutions to create a comprehensive change impact validation environment.

A comprehensive change impact management structure needs a complete set of pro-active solutions for change impact validation to prevent problems caused by planned changes, unplanned changes, gradual deterioration and disasters.

7.1 Planned changes: load testing to predict the impact

VDI load testing solutions simulate the behavior of many users on your test, or better, VDI production environment. To predict the impact of every planned change load testing is used to first establish a clean performance baseline by executing a pre-change load test, simulating the intended number of real concurrent users expected on the system.

After every planned change, the same test is then repeated to determine if there is a performance and/or density impact. If an unacceptable impact is detected, the changes can be rolled back before real users are affected, or the infrastructure can be scaled up as much as needed.

Load testing should also be used to post-test every regular patch implementation using realistic production user loads during maintenance windows, to detect problems before your real users do.

7.2 Unplanned changes: 24/7 continuity testing to detect potential impact

Continuity testing 24/7 lets a virtual user walk through the system and test all the relevant actions of its most important applications every 10 minutes, all day, every day. This type of testing allows operations staff to see performance metrics from the end-user's perspective and enables a type of pro-active monitoring that will detect the potentially negative impact of unplanned changes caused by automatic software updates or human error, before real users will be affected.

This type of testing is also used to check the logon quality, desktop user experience, and application performance from remote locations which is crucial for geographically distributed organizations.

24/7 continuity testing of remote locations is used by hotel chains to check the health of central reservation systems at each hotel location, by airlines to check the health of their temporary kiosks at each airport, and by shipping companies where ships are the remote locations.

7.3 Gradual deterioration: 24/7 continuity testing to detect/predict slowdown

Virtual (synthetic) user technology is very precise and therefore very reliable as it detects and predicts gradual deterioration of application performance which could be the result of a slowly progressing pollution of disks and other infrastructure resources.

With this type of testing a complete end-user workflow is repeated every 10 minutes, where each step of the workflow is measured in milliseconds. This way every change, no matter how small, is detected and analyzed. By setting thresholds, the extrapolation of the measurements will allow predicting the exact moment where real users will start to be affected. This way gradual deteriorations are detected before they will slow down end-user productivity and disturb business continuity.

7.4 Disaster Recovery (DR) planning: load testing for different scenarios

Next to handling changes, which are a fact of life in any IT environment, organizations must also prepare for the unexpected. For this reason, large organizations spend much time and money to ensure that their IT infrastructure will survive any natural or human-caused disaster. This activity is most commonly referred to as Disaster Recovery (DR) planning.

A large organization in the USA uses load testing to verify that their core applications will work when during a complete HQ failover 20,000 employees connect to their applications from remote locations. Another scenario tested is if after a power failure, 10,000 users can reconnect in a few minutes time. In addition they wanted to know if their 2nd data center is capable to support the extra user numbers if all users from the 1st data center must be moved, due to an unexpected total stand-still.

The ability to simulate large numbers of users (read load testing) is very well-suited to test scenarios that are not very typical, but nonetheless are very valid and make planning and preparation critical. Login VSI supports large organizations, looking to safeguard business continuity through DR planning.

A large healthcare organization in the USA uses load testing to regularly test the health of their "cold site" environment as this is maintained for DR scenarios. These regular DR tests are required by regulations and must be documented on audit forms. Load testing is used in regular (quarterly) tests to put genuine stress on the DR environment. At the same time, the end-user experience is pro-actively monitored in all their remote locations using 24/7 continuity testing solutions.

7.5 Application Compatibility: test large numbers of applications after change

Large organizations typically have large numbers of applications running on their Microsoft Windows platform. Prudent organizations require a compatibility test for every application after every upgrade or other change in the relevant hardware and software infrastructure components.

With the flow of software changes growing constantly, the need for automated application compatibility verification grows accordingly. To cope with the challenge of keeping all applications working after every change, organizations rely on costly and inconsistent "testing armies" or on traditional software tools such as AppDNA, that are considered hard to use and often unreliable.

Automated application compatibility testing replaces the traditional and labor-intensive checking of applications after planned changes, such as the Spring & Fall releases of Windows 10, the monthly builds of Windows 10 ("Patch Tuesdays") or any other potentially compatibility disturbing update.

8. A complete solution for VDI change management

8.1 Login VSI is the industry standard in VDI testing

Login VSI offers enterprises and vendors a complete software solution to build and safeguard the optimal performance, scalability, availability and compatibility of desktops and applications running in virtual desktop environments, based on our industry standard virtual (synthetic) user technology.

"Login VSI adds confidence to our VDI change management process"- a large enterprise customer

Login VSI offers 3 industry leading solutions for enterprise level VDI testing:

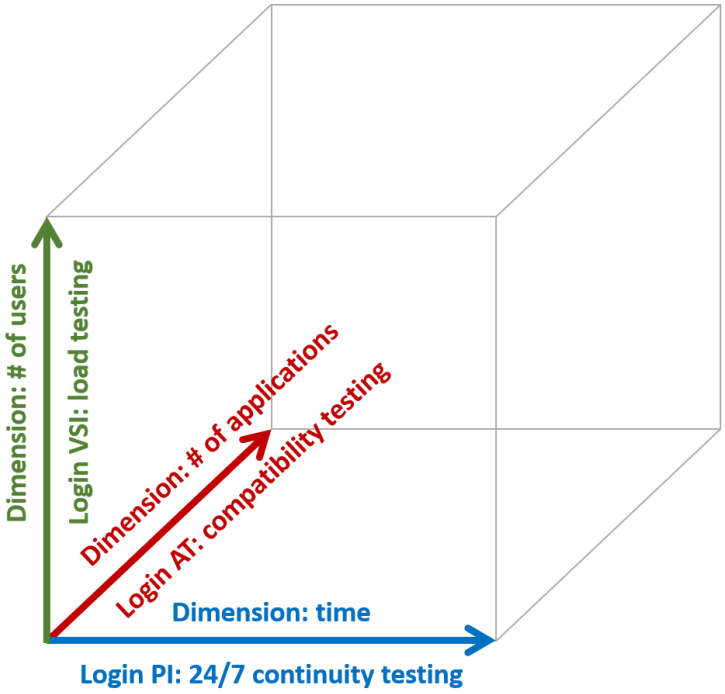
- Login VSI – Industry Standard Load Testing
- Login PI – Pro-active 24/7 Continuity Testing
- Login AT– Application Compatibility Testing

8.2 Login VSI Enterprise Edition (EE)

The Login VSI Enterprise Edition uses the smart combination of Login VSI for load testing, and Login PI for 24/7 continuity testing, to optimize and protect the performance of business-critical applications running in VMware Horizon View, Citrix XenDesktop, Citrix XenApp, and Microsoft Remote Services.

8.3 Login VSI Enterprise Edition XL (EEXL)

For organizations using centralized virtual desktop environments to provide very large numbers of applications to their end-users, we offer Login VSI Enterprise Edition XL, our extended solution suite that in addition to Login VSI and Login PI, also includes Login AT for Application Compatibility Testing.



Picture 7: Login VSI: a complete solution suite for VDI change management

"The adoption of Login VSI EE introduced predictability in change" – a large enterprise customer