



UNDERSTANDING **XC**|FRONTIER AND CLOUD COMPUTING

Table of Contents

Disclaimer & Copyright Notice	3
List of Abbreviations.....	3
Chapter 1 – About this Document.....	4
1.1 Document Introduction.....	4
1.2 Target Audience	4
1.3 Information Technology Background.....	4
Chapter 2 - Cloud Computing Landscape	6
2.1 Introduction to Cloud Computing	6
2.2 Virtualization and Cloud	7
2.3 Virtualization	7
2.4 Cloud Computing.....	8
2.5 Cloud Security	11
2.5.1 Introduction.....	11
2.5.2 Network Segmentation	12
2.5.3 Cloud-based Access Controls	12
2.5.4 Multi-tenancy in Cloud.....	12
2.5.5 Cloud Access.....	12
2.5.6 Cloud Computing Threats and Vulnerabilities	13
2.6 Public Cloud and Private Cloud	13
2.6.1 Private Cloud Concept.....	13
2.6.2 Public Cloud Concept	13
2.7 VDI vs. DaaS.....	14
2.7.1 DaaS and VDI Overview	14
2.7.2 DaaS – Desktop as a Service	15
2.8 Application Virtualisation	15
2.8.1 Application Virtualisation Overview.....	15
Chapter 3 – XC Frontier Technology	17
3.1 Overview	17
3.2 XC Frontier Architectural Overview	18
3.3 XC Frontier Centralisation Benefits.....	20
3.4 XC Frontier Microsoft Azure Data Centre Typical Deployment	21
3.5 XC Frontier STAR Wan Architecture Topology.....	22
3.6 XC Frontier Business Execution	23

3.7 XCFrontier Business Benefits	23
3.7.1 Enhanced Affordability	24
3.7.2 Reinforced Security	24
3.7.3 Improved Mobility	24
3.7.4 Increased Flexibility	24
Chapter 4 - XCFrontier Summation	25
4.1 Conclusion	25
4.2 Acknowledgements	25



Disclaimer & Copyright Notice

Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document contains information that is the property of XContent Business Solutions (Pty) Ltd. No Part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of XContent Business Solutions (Pty) Ltd.

XContent Business Solutions (Pty) Ltd assumes no responsibility for any direct, indirect, incidental, or consequential damages arising from the use of information in this document.

All diagrams, logos and information contained in this document are registered trademarks or trademarks of XContent Business Solutions (Pty) Ltd in South Africa and other countries.

This document remains the property of XContent Business Solutions (Pty) Ltd and no unauthorised replication of any information contained in this document may take place without the written authorisation of XContent Business Solutions (Pty) Ltd.

Other product and company names herein may be the trademarks of their respective owners.

List of Abbreviations

AD	-Active Directory	AaaS	-Application as a Service
Apps	-Applications	ByoD	- Bring your own device
CEO's	- Chief Executive Officer	CIO's	-Chief Information Officer
DaaS	- Desktop as a Service	EUD	-End User Devices
EUC	-End User Computing	IaaS	- Infrastructure as a Service
LaaS	-Logging as a Service	NaaS	- Network as a Service
NIST	-National Institute of Standards and Technology	OS	-Operating Systems
RACF	- Resource Access Control Framework	SaaS	- Software as a Service
SPLA	- Service Provider Access License	SPS	- SharePoint Portal Services
VDI	- Virtual Desktop Infrastructure	VPN	-Virtual Private Network
VM	-Virtual Machines	IT	-Information Technology
Capex	-Capital Expenditure	ITaaS	- IT as a Service

Chapter 1 | About this Document

1.1 Document Introduction

This “Understanding XCFrontier & Cloud Computing”, provides a high-level encapsulation of the current and existing cloud computing landscape including end user computing (EUC), desktop as a service (DaaS), virtualisation, cloud security, relevant methodologies and how XCFrontier is breaking new ground with its architecture and technical framework to deliver exceptional business value.

Using the context of the prevailing cloud technologies, this document goes on to explain the XCFrontier architecture, operations and business benefits for implementing a Centralised XCFrontier model.

Chapter 1 – About this Document: This short chapter introduces the document while setting out the intent and scope of the document.

Chapter 2 – Cloud Computing Landscape: A short Introduction to the current and existing cloud computing landscape.

Chapter 3 – XCFrontier Overview: A short Introduction as to how the XCFrontier solution fits into the existing cloud landscape as well as providing the benefits associated to implementing XCFrontier.

1.2 Target Audience

The reader of this document is expected to have some knowledge of the SaaS, VDI and Application Publishing and Microsoft Azure IaaS relevant products together with the environment in which it is intended to be used, be it as part of a corporate infrastructure or just for development as a proof of concept.

Readers of this document must have basic knowledge of IT management with an understanding of the workings of domain networks, Active Directory, web servers, cloud technologies, inherited domain security policies and IT terminologies.

1.3 Information Technology Background

Information Technology is not about technology. It is about building trust, exceptional service delivery, ease of use and solving problems for humans. Information Technology is about people,

and more specifically the ability to optimise the core competencies and capabilities of people and processes.

Even though service delivery underpinned by world class IT systems spark the promise of enhanced service levels, it always fails if there is no ease of use. In referring to the age old saying that “beauty and success is in the eye of the beholder”, the “beholder” in the case of IT is us, the end user. The biggest opportunities, threats, strong and weak points in our “IT World” are social and not technological by nature.

IT decisions for people investing in IT is therefore quite simple. The decision is cost vs. optimisation of core competencies and capabilities of problems to be solved.

In laymen’s terms this simply means “how much money must I spend on IT to enable me, and the people and processes that work for me, to make more money?” And from an IT vendor’s perspective “how do I ensure that the technology I’m developing and selling will ultimately put a smile on a person’s face”



Chapter 2 | Cloud Computing Landscape

2.1 Introduction to Cloud Computing

Cloud Computing is no longer new; however, it is still being adopted. The mind shifts for CEO's/CIO's to change from the Microsoft decentralised model (everything onsite and distributed) back to the concept of 80's centralised RACF Mainframe is still a concern. Probably, the biggest reason being fear of information no longer 'sitting under one roof' and the cost and risk of storing information offsite.

Microsoft's early on success can be contributed to the "windows based" Graphic User Interface (GUI) developed for end-user Desktops. Microsoft, through mouse driven point and click computing were the first, to successfully "make IT sexy" and bring 'eye candy' and ease of use to end-users. This was followed by competitors such as Apple, selling IT as "Social", "Sexy" and "Compulsory" artefacts.

Lessons should enable our future - and in this instance our future Cloud computing plans. Ultimately, Cloud must provide value to End Users and overcome issues of security, intellectual property, cost and complexity.

With End User Devices such as cell phones becoming more powerful, the goal is shifting towards usability and providing a "total" End User Experience to all users. The choice to choose between a Desktop, Laptop, Terminal or a Cell phone, as ones preferred end user computing (EUC) interface, will soon become a reality. Unfortunately, such a reality in a decentralised world, are stalled by issues of security, ownership and intellectual property, a decentralised computing model is immensely plagued by complexity. In many instances, such a reality seems problematic if not impossible.

It is crucial to understand that with a centralised model the focus is not on the desktop per say, but rather the applications and systems accessed from the "desktops"; previously it was dumb terminals accessing programs on a Mainframe, and today think "Apps" on a Smart Phone. Instead of just having the management and computing of Data and Information in mind, as per the decentralised model, Desktop as a Service (DaaS), Virtual Desktop Infrastructure (VDI) and Software as a Service (SaaS), focuses on providing end users with whole, and often much larger (centralised) Desktop experiences where the focus is on the applications being delivered, not the underlying operating system, application as a service, so to speak. The goal is to, irrespective of the EU device; control all Computing, Storage, Backups, Security, Access Control and auditing from a centralised system, which might be or not, in the Cloud. Thereby allowing no Documentation to be downloaded to the user's device unless authorised to do so.

By providing such an entry point for Application distribution, Cloud based End User Computing (EUC) can become the "Edge of the Spear" to Datacentre and Unified Communications.

The belief is Cloud EUC will change the way outsourcing is done. Moving from a Microsoft based decentralised computing model to a centralised RACF Mainframe computing Model, still utilising Microsoft technologies, among other, many of the traditional decentralised Desktop model's problems such as; Cost, Standardisation, Licencing, Security, Encryption, VPN, Authentication, Data Access, Load Balancing, Extreme Processing, Input / Output issues, Backup, Support and the need for Extended Datacentre required, will be solved.

Cloud EUC will change the way outsourcing is being done. Moving from a Microsoft based decentralised computing model to a centralised RACF Mainframe computing Model.

Since a centralised Computing model is far easier to manage than a decentralised model Cloud Application as a Service (AaaS) for EUC will be solving the traditional decentralised Desktop model with its short cummings and large Capex model.

2.2 Virtualization and Cloud

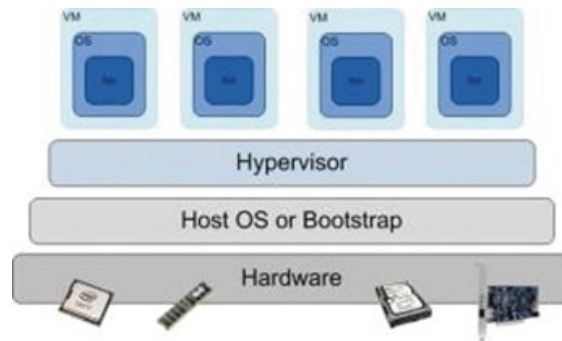
Virtualization simplifies the process of sharing computer resources. Cloud computing needs to be able to share resources to improve efficiency and reduce costs. This makes the two technologies a natural fit to work together. Virtualization increases the efficiency of hardware utilization, while cloud adds a layer of management so that VMs can be created, scaled and torn down as required. Therefore, most today's cloud solutions are built on virtualization technology.

However, virtualization is not a requirement of cloud computing. Look back at the NIST description of resource pooling. While it specifies that resources will be shared, it does not specify how. So, it is possible, and perfectly legal per the NIST specification, to build a cloud environment without using virtualization.

2.3 Virtualization

Virtualization, at its core, is the ability to emulate hardware via software. If we walk through the system initialization processes, some form of operating system still needs to be booted from the hardware. This may be a full blow OS such as Linux or Windows, or it may be a stripped-down OS specifically designed to provide virtualization, such as VMware's ESXi (which is a proprietary designed Linux operating system) or Microsoft comparable Hyper-V solution that runs on Windows Server. In either case an operating system is first booted, then an emulation software stack is loaded which is referred to as a "hypervisor".

The hypervisor is the component which is responsible for emulating specific hardware configurations to guest operating systems. When a guest is loaded into a virtual machine (VM), the hardware that gets detected is the simulated hardware via the hypervisor, not the actual hardware itself. The guest OS is abstracted from the true hardware, adding a component of versatility. The hypervisor can create multiple simulated environments, or multiple VMs, which permits us to run multiple operating systems that may have slightly different hardware requirements.



Benefits of Virtualization

Virtualization drivers in recent years have included:

- More powerful hardware, allowing each machine to run multiple applications simultaneously
- Pressure to lower IT costs and simplify IT administration
- Need to manage large-scale installations and clusters, such as server farms
- Improved security, reliability, scalability, and device independence
- Ability to mix multiple operating systems on same hardware.

2.4 Cloud Computing

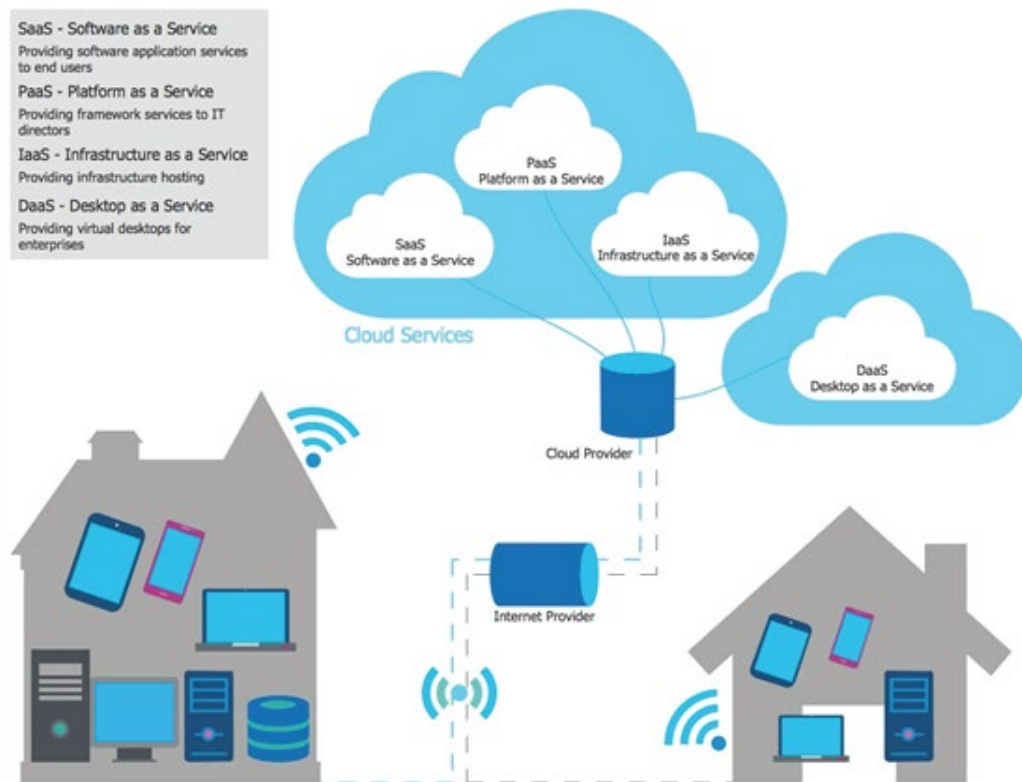
Cloud computing, as defined by [NIST 800-145](#), is:

“a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Note the reference to “shared pool of resources”. In fact, resource pooling is one of the specific characteristics NIST uses to define a cloud. The resource pooling section states:

“The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand.”

In Cloud computing, the word "Cloud" (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means a type of Internet-based computing, where different services —including servers, storage and applications — are delivered to an organization's computers and devices through the Internet.



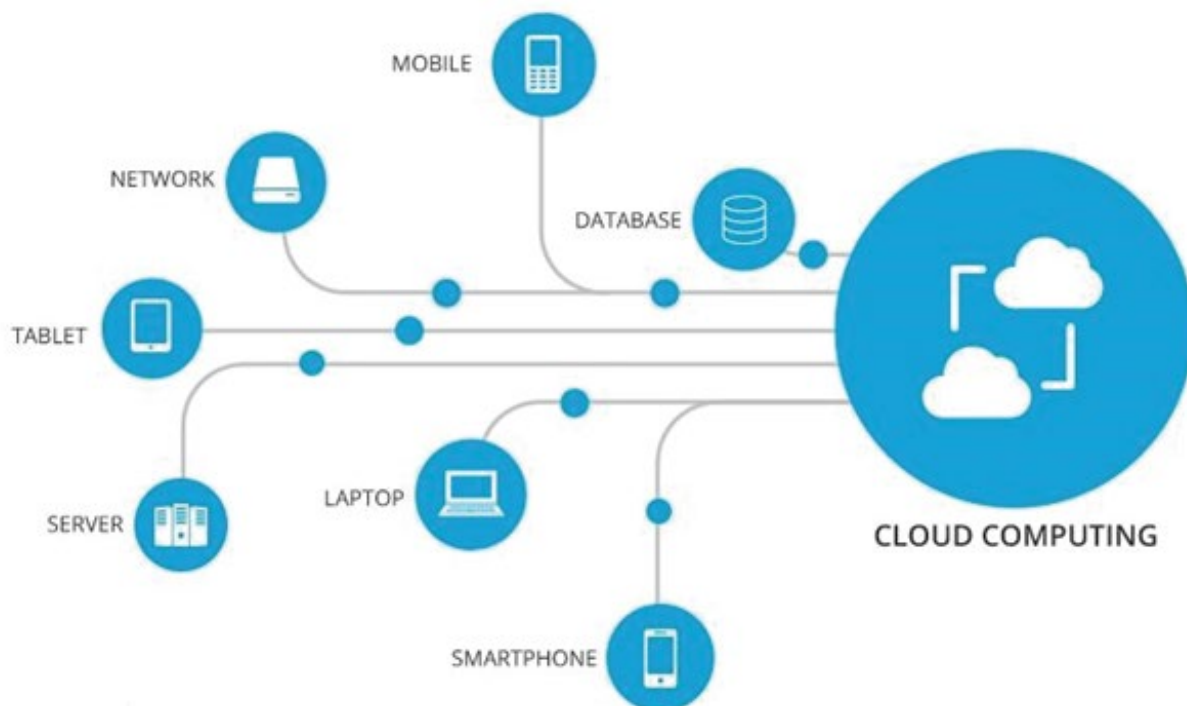
Cloud computing is an on-demand (automated) service that has obtained mass appeal in corporate data centres. The cloud enables the data centre to operate like the Internet and computing resources to be accessed and shared as virtual resources in a secure and scalable manner.

Most companies are not in the business of technology. Instead, they use technology to run their businesses. They might be in financial services, healthcare, retail, etc. Therefore, they may lack the technological savvy to manage and protect their data. Many firms have a false sense of security just because their data is on-site. However, having a data centre does not ensure that it is protected. Ironically, one of the inhibitors to early cloud adoption was around security concerns. Today, the cloud can often provide better data protection than having data reside on-site. This is due to the enhanced capabilities of IT staff whose one and only job is to protect your data. These IT professionals often have credentials, training, and experiences far superior to those roles at a firm's on-site facility.

In its most simple description, cloud computing is taking services ("cloud services") and moving them outside an organizations firewall on shared systems. Applications and services are accessed via the Web, instead of your hard drive. In cloud computing, the services are delivered and used over the Internet and are paid for by cloud customer (your business) -- typically on an "as-needed, pay-per-use" business model. The cloud infrastructure is maintained by the cloud provider, not the individual cloud customer.

Cloud computing networks are large groups of servers and cloud service providers that usually take advantage of low-cost computing technology, with specialized connections to spread data processing chores across them. This shared IT infrastructure contains large pools of systems that are linked together. Virtualization techniques are often used to maximize the power of cloud computing.

Currently, the standards for connecting the computer systems and the software needed to make cloud computing work are not fully defined at the present time, leaving many companies to define their own cloud computing technologies.



Cloud computing is the delivery of on-demand (automated) computing services -- from applications to storage and processing power -- typically over the internet and on a pay-as-you-go basis.

One benefit of using cloud computing services is that firms can avoid the upfront cost and complexity of owning and maintaining their own IT infrastructure including cooling, redundant power, uninterruptable power supplies and datacentre space, and instead simply pay for what they use, when they use it. Rather than owning their own computing infrastructure or data centres, companies can rent access to anything from applications to storage from a cloud service provider.

In turn, providers of cloud computing services can benefit from significant economies of scale by delivering the same services to a wide range of customers. Cloud computing services cover a vast range of options now, from the basics of storage, networking, and processing power through to natural language processing and artificial intelligence as well as standard office applications.

Pretty much any service that doesn't require you to be physically close to the computer hardware that you are using can now be delivered via the cloud.

2.5 Cloud Security

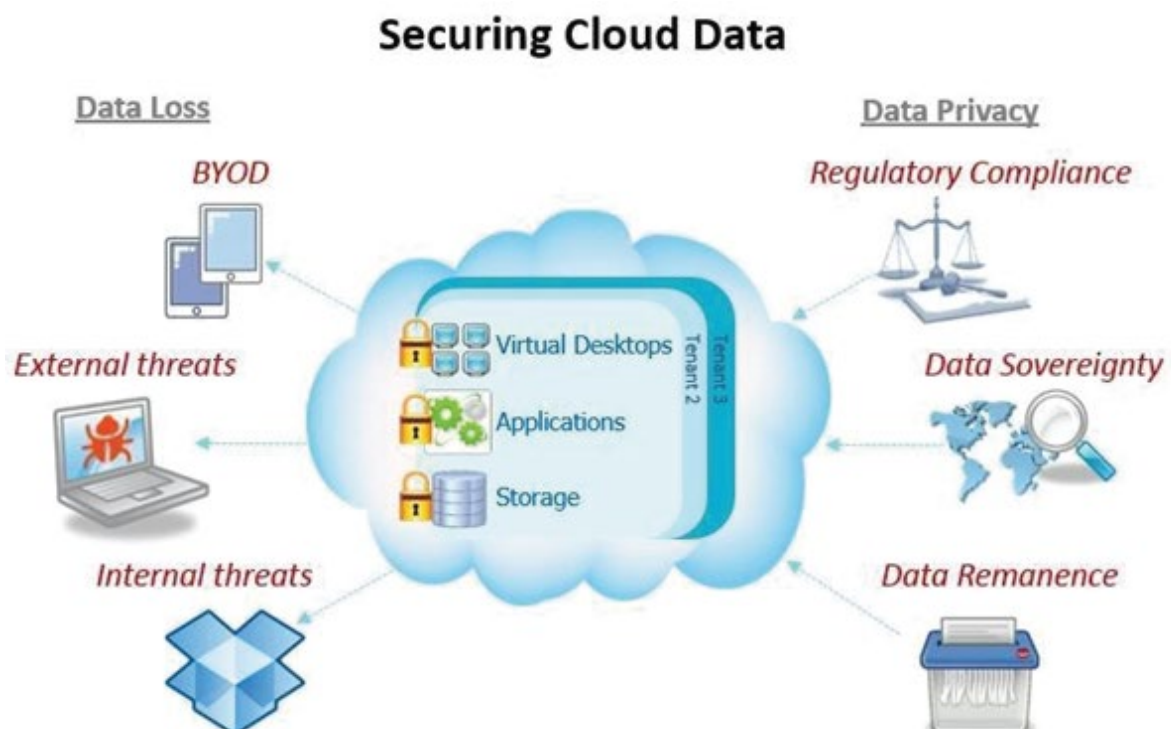
2.5.1 Introduction

Cloud Security have many benefits and are getting better by the day. The following benefits such as providing fast, high-capacity scaling, eliminating capital expenditures, and providing global reach with ease. There are also considerable benefits from a security perspective. Firstly, most of the cloud computing is implemented by highly skilled providers, utilizing data centres with uptime and security that small companies couldn't hope to replicate. The physical security mechanisms are considerable, including bio-metric access controls and other robust mechanisms. The infrastructure supporting the cloud services commonly abides by rigorous NIST standards for cybersecurity and undergoes continual evaluation by "red teams" of white-hat security experts. Small companies can't replicate this level of expertise for a reasonable price tag.

Secondly, the emergence of Software as a Service (SaaS) and Platform as a Services (PaaS) has been a boon for businesses because it eliminates the mundane administration and endless security patching (at the OS and application level) required to maintain the underlying infrastructure. Cloud providers are well equipped to provide this service continuously at a level of expertise that a small company couldn't match. Overall, this and other factors greatly increase the security of cloud-based systems when compared to non-cloud systems.

The takeaway is that your business and your data are considerably safer in the cloud than tethered to equipment under someone's desk. Any cloud provider worth its salt brings to the task a phalanx of time-tested tools, procedures and technologies that ensure continuous uptime, regular backups, data redundancy, data encryption, anti-virus/anti-malware deployment, multiple firewalls, intrusion prevention, and round-the-clock monitoring.

For information purposes, a typical high-level graphic on securing cloud data follows:



The following technologies and methodologies that apply to security also greatly benefit Cloud computing:

2.5.2 Network Segmentation

Consider a strong zone approach to keep instances, containers, applications, and full systems isolated from each other when possible. This will stop lateral movement in an attack and inappropriate access between systems by any threat actor.

2.5.3 Cloud-based Access Controls

All aspects of computing in the cloud should have access control lists. Since services like a database can be instantiated separately, it is more important than it is for on premise to define and implement proper access controls. This includes any virtual infrastructure, operating systems, applications, and even tools used to monitor the environment. A least privilege, or fully closed, security model is a preferred approach. In addition, just because it is in the cloud does not mean that it should be publicly addressable. Only expose the resources you need to the Internet (if any) and secure the rest.

2.5.4 Multi-tenancy in Cloud

While multi-tenancy provides scalability and segmentation benefits by design, there are also chances of data bleed and irregular boundaries (like reporting or data export) that might not be controllable in the cloud. Consider access controls in a multi-tenant environment and policy boundaries for any account that may have access across tenants.

2.5.5 Cloud Access

Remember, these are not your computers. Concepts like a crash cart do not necessarily apply. So, you need to manage privileged access to all cloud resources and consider disaster recovery and any failures in your privileged access scope. We manage privileges today on premise with password management solutions and administrator accounts. We need the same concepts in the cloud but do not want cloud administrator rights to be everywhere. This would negate the previous concepts of zones and access control lists. Privileges need to be role based, appropriately delegated, and monitored for usage to ensure the access is appropriate.



2.5.6 Cloud Computing Threats and Vulnerabilities

This concept translates one for one from on premise implementations but may use agents and other integration technologies to determine the premise of vulnerabilities. Once identified, they need to be prioritized using threat intelligence and remediated in a timely fashion. This is old school low hanging fruit that regardless of the computing environment must be done like clockwork to ensure good cybersecurity hygiene.

2.6 Public Cloud and Private Cloud

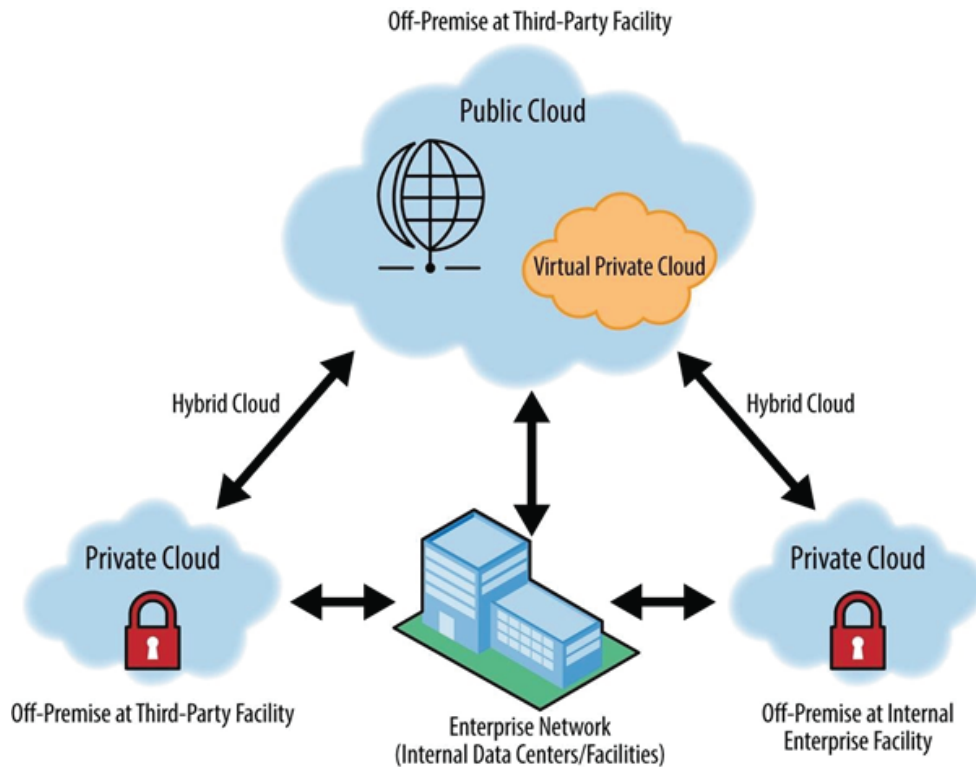
2.6.1 Private Cloud Concept

A private cloud hosting solution, also known as an internal or enterprise cloud, resides on company's intranet or hosted data centres where all your data is protected behind a firewall. This can be a great option for companies who already have expensive data centres because they can use their current infrastructure. However, the main drawback people see with a private cloud is that all management, maintenance and updating of data centres is the responsibility of the company. Over time, it's expected that your servers will need to be replaced, which can get very expensive. On the other hand, private clouds offer an increased level of security and they share very few, if any, resources with other organizations.

2.6.2 Public Cloud Concept

The main differentiator between public and private clouds is that you aren't responsible for any of the management of a public cloud hosting solution. Your data is stored in the provider's data centre and the provider is responsible for the management and maintenance of the data centre. This type of cloud environment is appealing to many companies because it reduces lead times in testing and deploying new products. However, the drawback is that many companies feel security could be lacking with a public cloud. Even though you don't control the security of a public cloud, all your data remains separate from others and security breaches of public clouds are rare.

A typical Off-Premise at Third-Party Facility graphic follows:



2.7 VDI vs. DaaS

2.7.1 DaaS and VDI Overview

DaaS offers companies the opportunity to have VDI capabilities, while maintaining a subscription-based price.

Virtual desktop infrastructure (VDI) virtualizes a host desktop operating system onto a central server that can display to a remote device. VDI allows users to access full desktop capabilities on thinner machines, as most of the processing and computing happens on the back end. This is cost effective for companies that have a large employee base. Since the technology is doing a lot of the heavy lifting, however, the sticker price is on the higher side.

VDI also requires a sturdy support system of IT professionals who are willing and able to develop and customize desktops, as well as maintain efficiency with deploying updates and managing data traffic. Network connectivity is also something to keep in mind with VDI. Without a strong connection, VDI goes to a crawl, cutting into valuable work time.

To mitigate that risk, there are excellent enterprise technologies out there designed for slow network connectivity, Citrix, VMWare Horizon and XCFrontier.

2.7.2 DaaS – Desktop as a Service

DaaS is like VDI, in that it also deploys an operating system from a hosted desktop to a remote device. DaaS differs from VDI because instead of hosting desktops in an on-premises data centre, DaaS uses a cloud-based back end from a third-party provider.

DaaS offers companies the opportunity to have VDI capabilities, while maintaining a subscription-based price. DaaS also has an easier method of deployment, as it is not necessary to build desktops in house. DaaS vendors handle connectivity and any issues, while IT can still maintain a role as the administrator over user accounts

A graphical representation of DaaS follows:

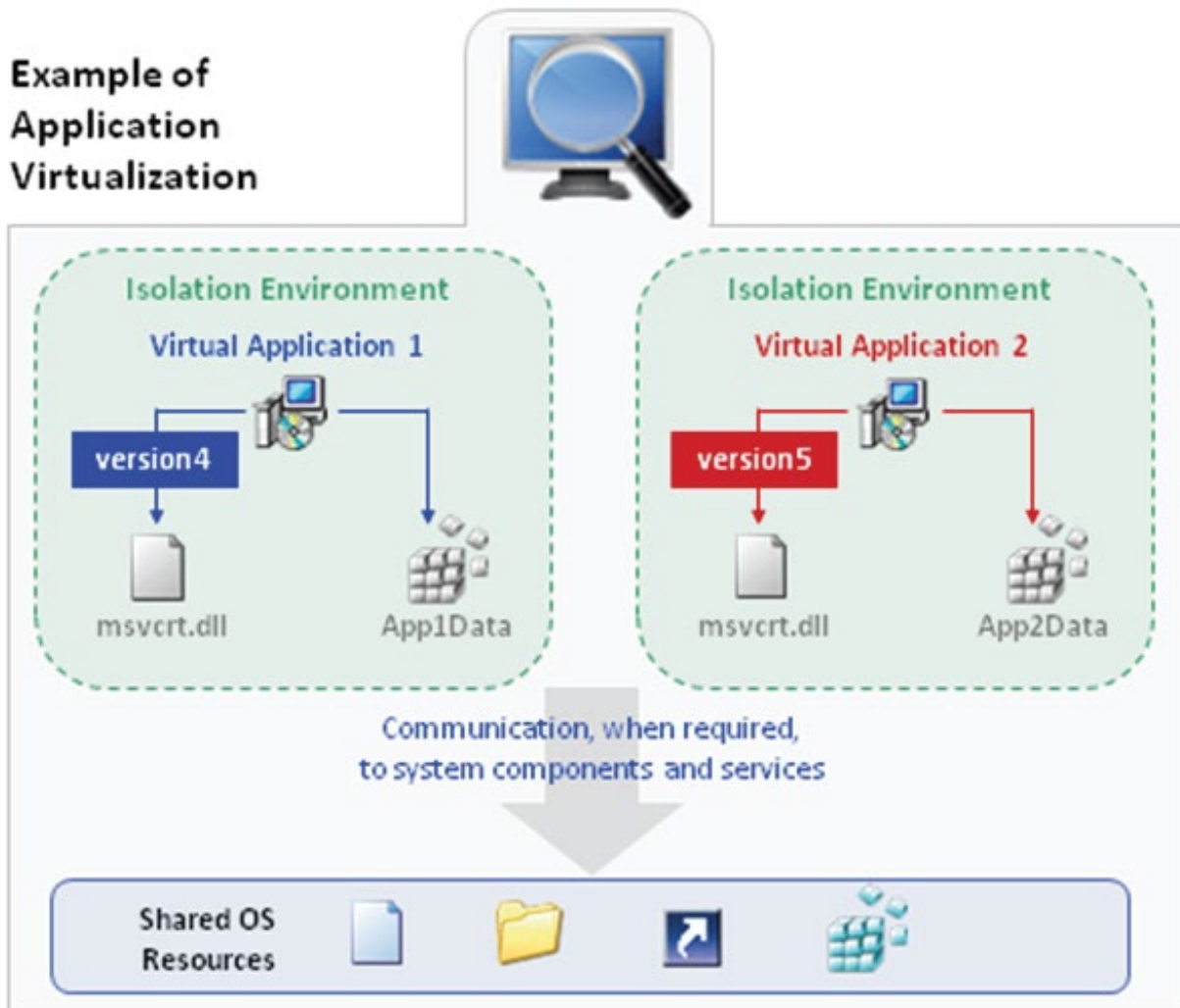


2.8 Application Virtualisation

2.8.1 Application Virtualisation Overview

Application Virtualization can make applications available to end user computers without having to install the applications directly on those computers. This is made possible through a process known as sequencing the application, which enables each application to run in its own self-contained virtual environment on the client computer. The sequenced applications are isolated from each other. This eliminates application conflicts, but the applications can still interact with the client computer.

App virtualization can be an effective way for organizations to implement and maintain their desktop applications. One of the benefits of application virtualization is that administrators only need to install an application once to a centralized server rather than to multiple desktops. This also makes it simpler to update applications and roll out patches. View the following example:



In addition, administrators have an easier time controlling application access. For example, if a user should no longer be able to access an application, the administrator can deny access permissions to the application without having to uninstall it from the user's desktop.

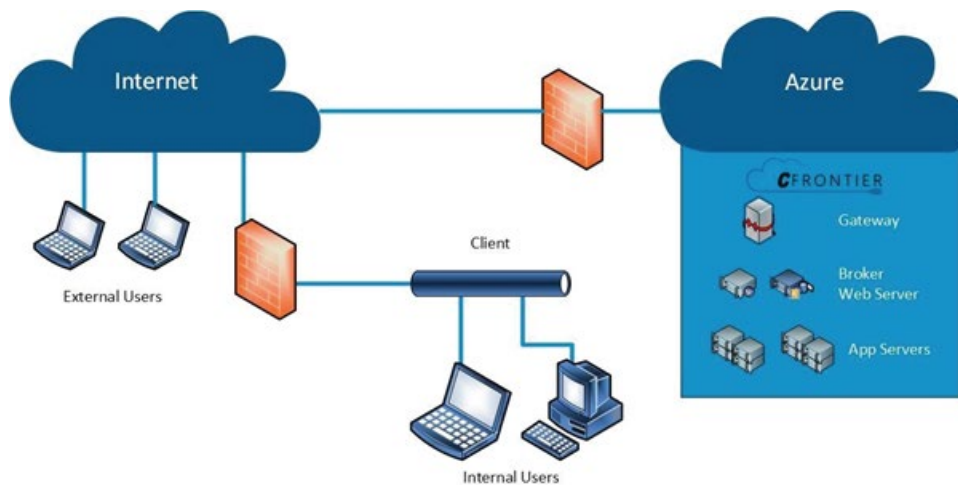
App virtualization makes it possible to run applications that might conflict with a user's desktop applications or with other virtualized applications. Users can also access virtualized applications from thin clients or non-Windows computers. The applications are immediately available, without having to wait for long install or load operations. If a computer is lost or stolen, sensitive application data stays on the server and does not get compromised. The centralised access of the app for all users now easily allows for the enforcement of centralised document management solution such as SharePoint Portal Services. Thereby enforcing documents management with revision control and centralised backups easily.

Chapter 3 | XCFrontier Technology

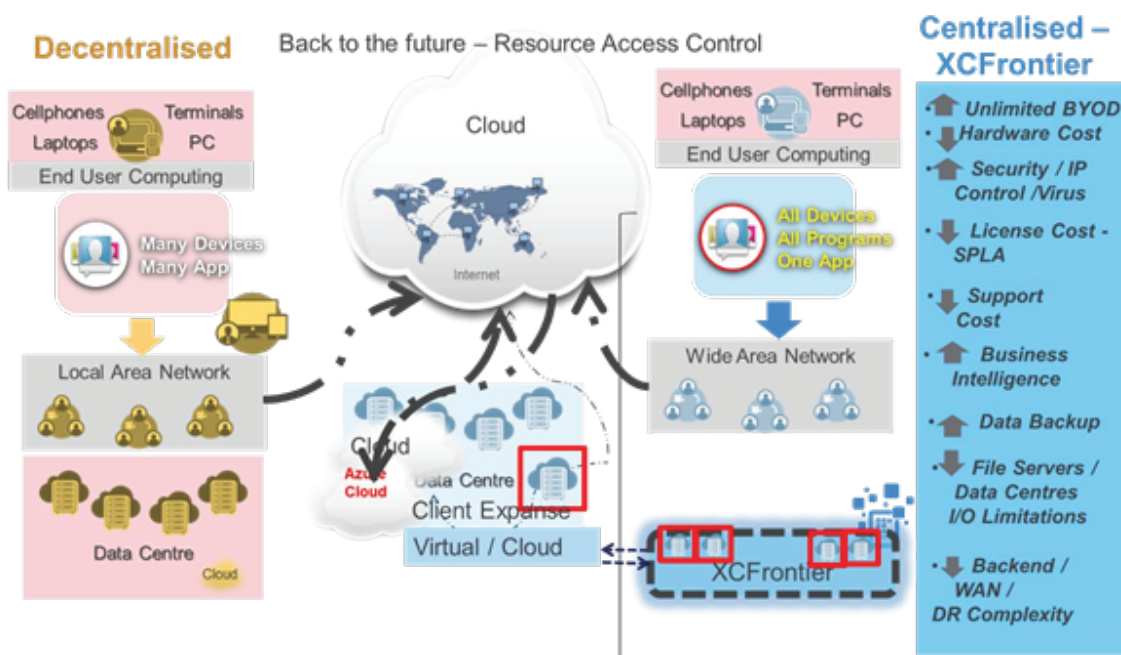
3.1 Overview

XCFrontier makes use of the Microsoft Azure platform as the framework on which it runs and was designed for safe long-distance Cloud computing with little or no latency. The technology can run either as Public Cloud, Private Cloud or Hybrid Cloud.

The following diagram shows a high level XCFrontier deployment

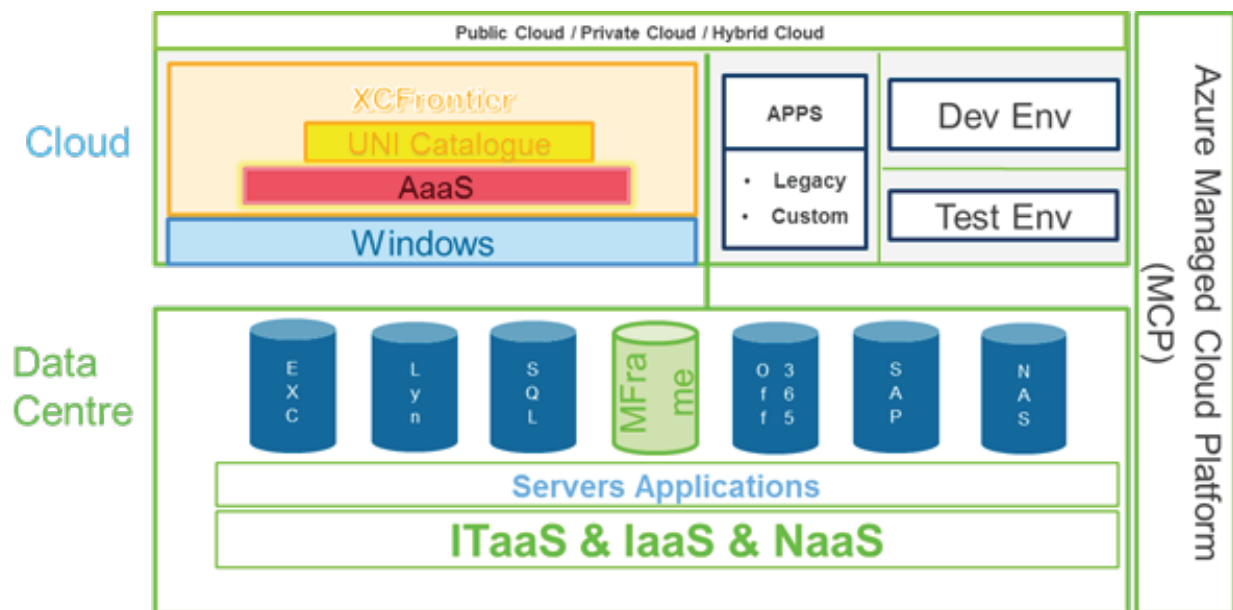


The following pictograph displays the XCFrontier relation in the Cloud and how the technology distinguish itself from the current decentralised computing model.



3.2 XCFrontier Architectural Overview

The following diagram shows the architecture components XCFrontier can support and successfully process on Azure Public Cloud / Private Cloud and Hybrid Cloud.



XCFrontier represents the frontend, End User Computing (EUC), side of the computing infrastructure. The Data Centre can either exist on Azure Public Cloud / Private Cloud and Hybrid Cloud configurations. Due to Microsoft heavy investment and strategic alliance toward Azure it is recommended that XCFrontier be deployed in an Azure Public Cloud to ensure optimal security and stability is achieved. The technologies of ITaaS, IaaS and NaaS can at this point only be provided for XCFrontier in the Azure Cloud Platform.

Data Centre Component can exist out of virtually any modern application, including the following more modern technologies:

- Microsoft Exchange
- Teams – Including the ○ Instant Messaging ○ Skype Voice
- SQL Databases
- SharePoint Portal Services
- OneDrive (Basic Requirement for XCFrontier)
- Proprietary Databases
- Entire Office 365
- SAP Client

Included in the list is:

- AS400 Mainframe (among other)
- NAS devices (Private Cloud)
- Call Centre Software (Private Cloud)
- CAD Design
- Artificial Intelligence Computing Systems

Linux Servers

The Cloud side of XCFrontier is a Virtualised Centralised computing environment that can be load balanced and a scaled both vertically and horizontally to both ensure high availability and load balancing.

From a high-level design point of view XCFrontier utilises the following concepts;

- The use of either Windows 2016 server or highly recommended the use of Windows 2019, is required for the base operating platform
- XCFrontier can function in the following modes or the hybrid execution of these modes:
 - Application as a Service (AaaS)
 - Full VDI

VDI with Application as a Services (AaaS) ○ DaaS with Application as a Services (AaaS) Since XCFrontier as a Technology is completely Role Based, scenarios where a specific user, like a developer or researcher both a full standardised computing platform as well as a development and/or Legacy environment can be simultaneously be published to the end user.

XCFrontier by inherited correction in design is the perfect solution for disaster recovery (DR) scenarios, due to XCFrontier centralised computing nature, it is possible to allow the end user to work from any place in the world, the only requirement is a stable internet connection. The use of VPN is not required since XCFrontier utilised 128bit RC4 with FIPS and NLA encryption, between Client and Server. Using dual layer encrypted authentication and RACF mainframe policies XCFrontier is always secure, and audit able.

Bring your own device (ByoD) is now a reality, even into the enterprise corporate environments. Companies no longer need to lock down their EUC devices on the corporate LAN and Wi-Fi networks. Allowing the opportunity for companies to no longer manage or buy any EUC devices for their staff, thereby introducing an allowance scheme into the workforce to supply and manage their own devices, Security best practice in the Data centre and network infrastructure is still required, since XCFrontier focus on the EUC devices. XCFrontier supports both latest Linux and Windows 10 operating systems.

XCFrontier is based on a centralized processing model, the audibility of all authenticated users can be tracked and monitored. Making the switch from a Microsoft Enterprise Agreement Licensing model to a Microsoft SPLA (Service Provider Access License) a very easy manageability process. Pay for what and when you use a certain reality! Similar model can be used for other licensed software vendors.

3.3 XCFrontier Centralisation Benefits

Since a centralized Computing model is far easier to manage than a decentralized model, the following benefits can be realized from this model:

- Cost effectiveness due to the centralized computing model (Mainframe)
- Far easier to standardize. (Centralization)
- Application Driven (Not Desktop OS) (Strict Modular Role Based execution)
- Concurrent Microsoft and Android Application/Linux/Unix (Not OS dependent)

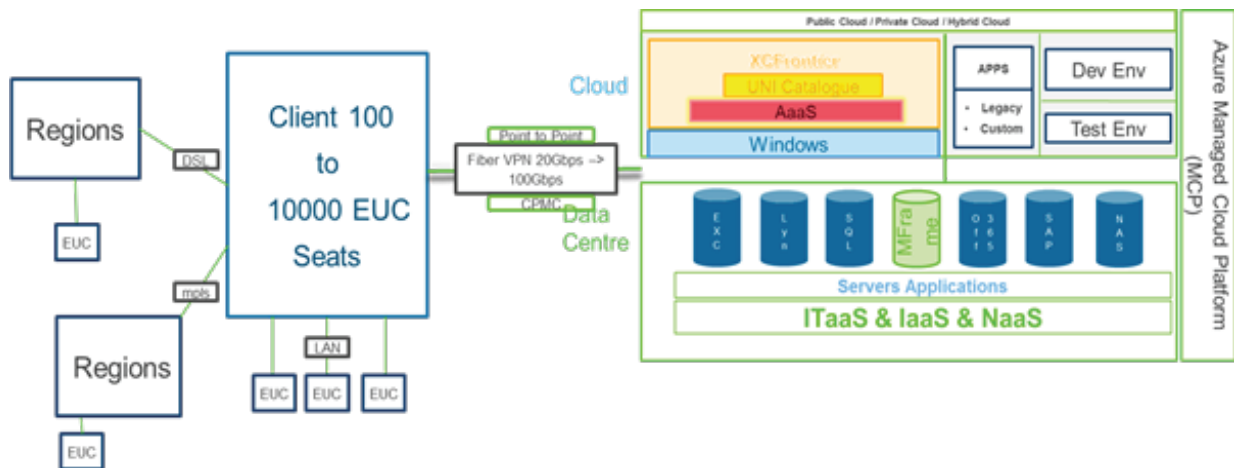
Simultaneous Licensed and Unlicensed Application Access determined by need, Since the solutions is Role Based, it allows for Open source and Closed source applications in one company depending on the role of user, with virtually no addition support. • High Security (RACF) policies can be implemented

- Further benefits can be realized:
 - a. True 128Bit key Encryption using the RC4 cipher between Client and Server
 - b. Forced High Security Connection – CredSSP (SSL with NLA) --(SSL-Secure Socket Layer with NLS – Network Level Authentication)
 - c. Full TLS (Transport Layer Security) – This is used by the server and client for authentication prior to a remote connection being established
 - d. FIPS Encryption (Federal Information Processing Standard) - This security level is FIPSCompliant, meaning that all communication between the server and client are encrypted and decrypted with the Federal Information Processing Standard (FIPS) encryption algorithms

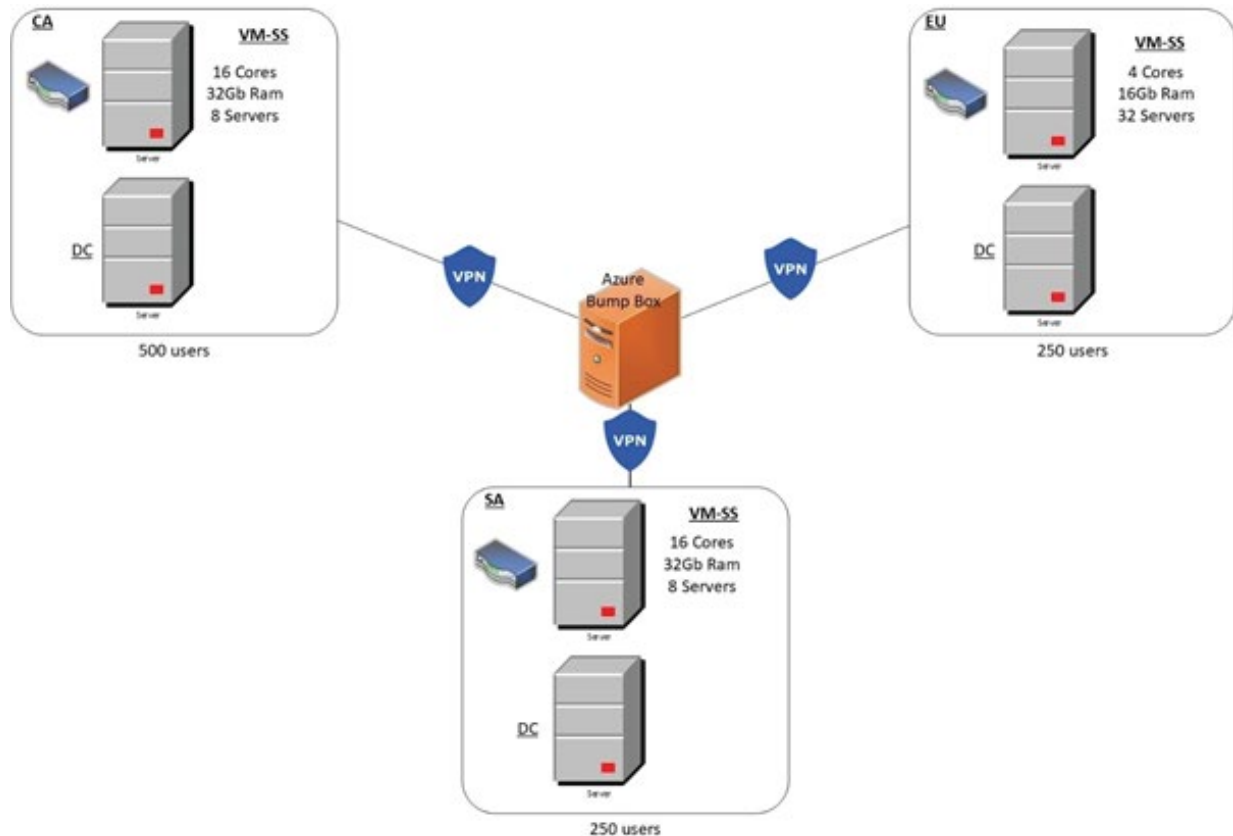
- e. All XCFrontier Servers no longer use the standard RDS port 3389, the new port is classified and will make it virtually impossible for a hacker to do RDS brute force port attacks
 - f. VPN are no longer required
 - g. Dual Layer Authentication can be forced from Azure if required
 - h. Centralized Data Access
 - i. Complete Audit Trail of Data Access (all registered/logged on users)
- High Availability & Load Balancing (centralized platform)
 - Centralized Access assist with better Disaster recovery benefits
 - Extreme Processing and I/O due to Data centre habitat
 - No further complex hardware expenses for EUC. (Laptops/PC) (ByoD - bring your own device becomes real)
 - No or little EUC support required (ByoD) ○ The ability to Shadow a user's session without 3dparty solutions
 - Low threat of Security vulnerabilities like document IP theft and ease of access from EUC device to back end servers. (Everything is centralized with proper document management and revision control)
 - Reduced treat from virus and worm infections (due to centralized access of EUC devices)
 - Guaranteed data backup & support due to centralized execution
 - Guaranteed Document management and structured Intellectual Property (Integrated document management)
 - No more File Servers Required, Huge Disk capacity reduction, all documents can be in centralized automated document management system - SPS
 - Simplified governance of Intellectual Property control
 - By leveraging on centralization and concurrent connection, software licensing can be reduced, pay for what you use
 - Full outsource costs greatly reduced due to simplified and locked down EUC capability
 - XCFrontier lives in the Data Center and can run complex software (include CAD) with virtually no reduction in performance! Whether accessed onsite or remotely.

3.4 XCFrontier Microsoft Azure Data Centre Typical Deployment

The below diagram pictograph shows how XCFrontier typically will connect to the Cloud Datacentre. As can be seen the Wan infrastructure play's a critical role in the accessibility of the Cloud infrastructure. The XCFrontier infrastructure deployed in the Microsoft Azure Datacentre is extremely scalable and can quickly scale either from 100 concurrent connections to 10 of thousands connection to the same backend infrastructure.

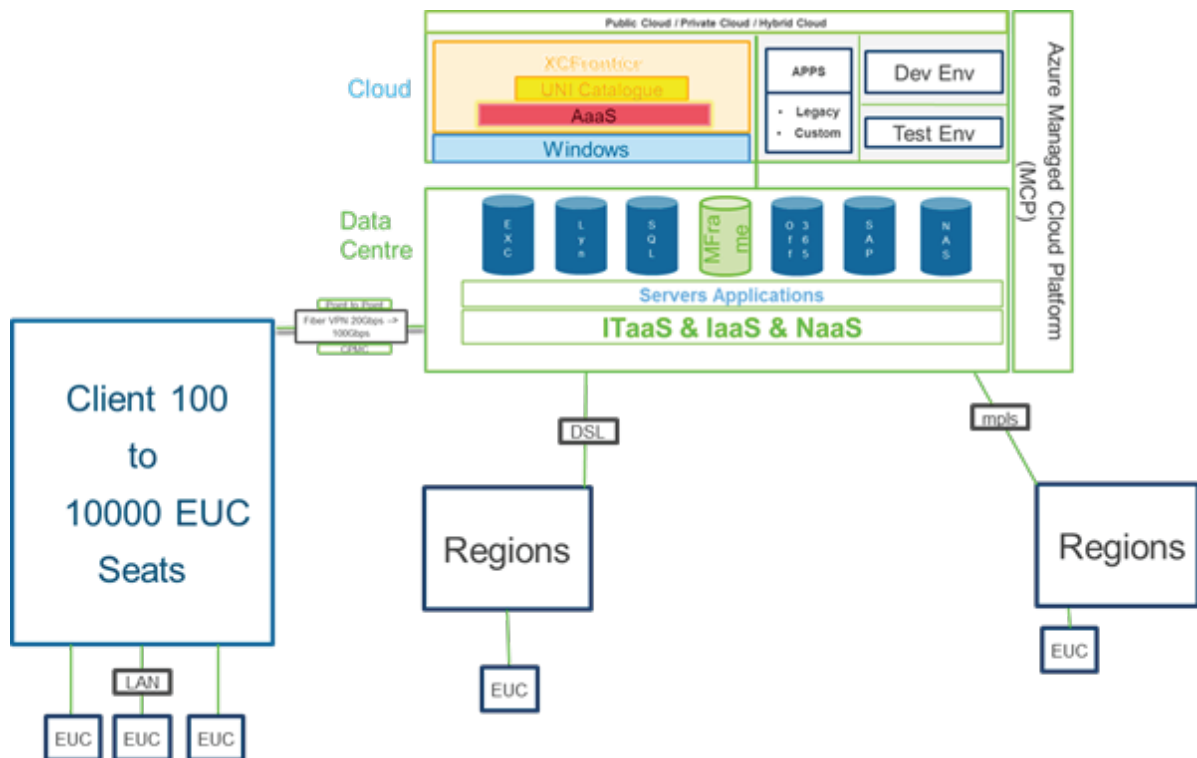


XCFrontier Azure High Availability Low Latency Global design for 1000 Concurrent Connections



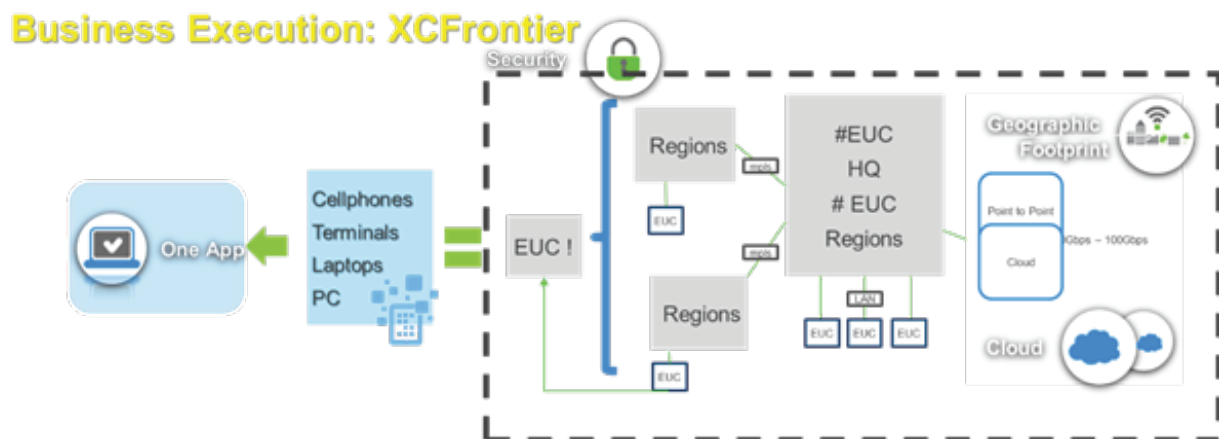
3.5 XCFrontier STAR Wan Architecture Topology

Although the diagram reflected under paragraph 3.4 is based on a typical BUS Wan Architecture, XCFrontier can easily and just as effectively function on a STAR Wan Architecture topology as can be seen from the below pictograph:



3.6 XCFrontier Business Execution

XCFrontier as a centralised end user computing technology, comes down to one application that will purposely deploy role-based applications to each user that requires the functionality of his or her application, the below diagram shows this scenario:



3.7 XCFrontier Business Benefits

Businesses looking to leave a mark in today's highly competitive market require efficient technology that goes beyond day-to-day operations and addresses organizational goals. But because business owners don't have much time, adopting innovative technology is often put in the back burner. And even if they did, they aren't necessarily experts who keep up with the latest tech trends.

Businesses can simplify their computing requirements by using a virtual desktop infrastructure (VDI), a service that allows users to access and use a desktop environment from a hosted data centre. And with Desktop-as-a-Service (DaaS), a subscription-based service wherein a cloud service provider manages the client's VDI, they'd have even lesser need to manage their own infrastructure. It is responsible for back-end tasks such as storing, securing, and backing up data while ensuring regular system upgrades. However, these aren't the only perks DaaS provides businesses with:

3.7.1 Enhanced affordability

According to an IDC white paper, desktop-as-a-service reduces hardware capital expenditure by 56% annually. When compared to traditional workstations, DaaS significantly reduces the total cost of ownership (TCO) due to its longer lifespan, the absence of a hard disk, and reduced power consumption. Virtual desktops also enable companies to reuse existing hardware and extending the lifespan of their tech resources, saving time spent searching for and installing replacements.

3.7.2 Reinforced security

Businesses with a bring-your-own-device (BYOD) policy need to realize that computers can be hacked into, lost, or stolen anytime. Allowing employees to store crucial business files on their own unsecured devices increases the risk of data breach. With Desktop-as-a-Service, you won't have to worry about loss because data is stored in the data centre, not the device.

Also, cloud desktops are unable to host malicious files and impede virus infiltration through remote displays. And since system updates are centralized, businesses benefit from a streamlined data backup and synchronization processes, and simplified compliance.

3.7.3 Improved mobility

With DaaS, working from home will no longer mean carrying around and possibly misplacing USBs containing critical business files. Just hibernate your virtual desktop at the office and access it from home. Virtual desktops ensure the same PC desktop experience from anywhere on any device, including iPads, MacBook's, tablets and laptops. You will have a choice of running either a Windows or Linux-based operating system.

3.7.4 Increased flexibility

Modern businesses are pressed for time, meaning new software, applications and updates must be completed in a few minutes, not days. DaaS can be quickly implemented, is scalable, and eliminates application compatibility issues.

Moreover, DaaS provides companies with a built-in disaster recovery strategy that gets desktops up and running in no time. With a DaaS, not only will you save money on IT management, but you'll also help your employees to be more mobile and responsive.

Chapter 4 | XCFrontier Summary

4.1 Conclusion

The core benefits of true cloud computing are flexibility and speed to deployment, while still offering a vast array of software features at the 'touch of a button.' However, for most companies, data security is increasingly also a key ingredient when deciding to opt for a Cloud platform over a traditional in-house solution. In the fight against cyber-crime, most enterprises simply cannot keep up with the 'security arms race' protecting data in traditional in-house systems. For many, the Cloud is the only realistic alternate at an achievable price point.

In the Cloud, an organization can store data and software in highly secure locations with massive ongoing security investments in ubiquitous threat monitoring, alerting, and data protection techniques. This is an ever-increasing key factor that makes the Cloud more desirable than the alternatives. Today all the leading Cloud platforms have a series of top security protocols, practices, and policies that protect company and customer data. Like many others, we already see Security as a key differentiator, and this will only grow as data security breaches across the globe become even more prevalent.

XCFrontier is the modern “gateway” between Cloud and the End user, with all the flexibility and mobility benefits that Cloud brings but without the large Capex expenditure of hardware and the complexity of support and security risks of current EUC.

4.2 Acknowledgements

XContent acknowledges the following information resources in the compilation of this document

1. <https://csrc.nist.gov/publications/detail/sp/800-145/final>
2. <https://digitalguardian.com/blog/cloud-computing-security-benefits>
3. <https://www.forbes.com/sites/joytan/2018/02/25/cloud-computing-is-the-foundationof-tomorrows-intelligent-world/#2bed9a7b4073>
4. <https://www.salesforce.com/uk/blog/2015/11/why-move-to-the-cloud-10-benefits-ofcloud-computing.html>
5. https://en.wikipedia.org/wiki/Cloud_computing
6. https://en.wikipedia.org/wiki/History_of_Microsoft