



# Unified Application Delivery Model

4<sup>th</sup> Software Engineering for Defense Applications Conference

David Cenciotti

System Engineer – Cloud Networking Group

Centro Alti Studi Difesa – Roma - 26 maggio 2015



# What's a Unified Application Delivery Model?

It's a model for the delivery of applications through a Cloud-like e Software defined infrastructure

- It's a framework whose aim is to set the baseline for standardised IT architectures capable to deliver new and legacy applications.
- It is based on three main tech trends:
  - Consolidation through virtualization
  - Cloud Networking
  - Enterprise Mobility Management
- It's vendor independent



# Why Citrix?

**CITRIX**<sup>®</sup>  
Market Leadership

#1 Desktop & App Virtualization

#2 Cloud Networking

#1 Public & Private Clouds

#2 Web Collaboration



# Why Citrix?

## **CITRIX**<sup>®</sup> By the Numbers

\$2.9B+ Revenue

9,000+ Employees

330,000+ Customers

10,000+ Partners in 100  
Countries



# Shifting paradigms

User devices have always been considered as a whole.

Monolithic units with their own:

- Form Factor
- Operating System
- Applications
- Network Interfaces

Most of today's systems were designed based on some core assumptions:

1. Mobile workers were an exception
2. Complex Web pages and apps were an exception
3. Personal devices were an exception
4. Wireless was an exception
5. Cloud-based services were an exception



# Current Tech Trends

## Mobility



- Extend the perimeter to include mobile devices
- Securely embrace BYOD initiatives but safeguard Private vs Corporate data

## Cloud & Cloud-based services



- Some companies want to build their own cloud
- Many others use or are about to use Cloud-based security services

## IT Consolidation



- Budget constraints impose the consolidation of both IT architectures and security countermeasures

← Visibility on Security, Performance, Apps, Network, Clients... →



# Best in class technologies to address requirements

Focus

Facing the “Mobility Threat”



Secure Cloud services



“Securely” consolidate



**Citrix approach**

- EMM with MDM and MAM
- Containerization
- Micro-VPNs for app specific L7 tunnels to the enterprise network
- Preserve User Experience

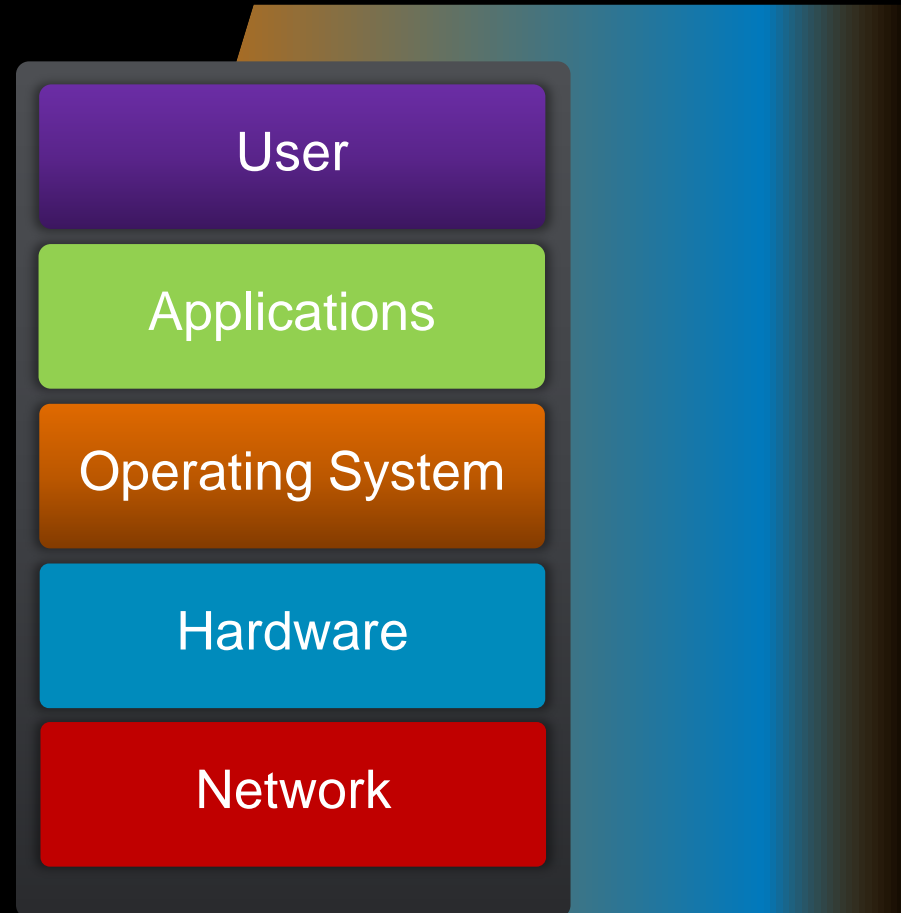
- Build, manage, orchestrate and securely interconnect datacenters
- AnythingaaS
- Cloud-based management control with on-premise data

- App virtualization
- Desktop virtualization
- Virtual ADCs for App Security and performance in multi-tenant environments

**Unified Visibility Plane**



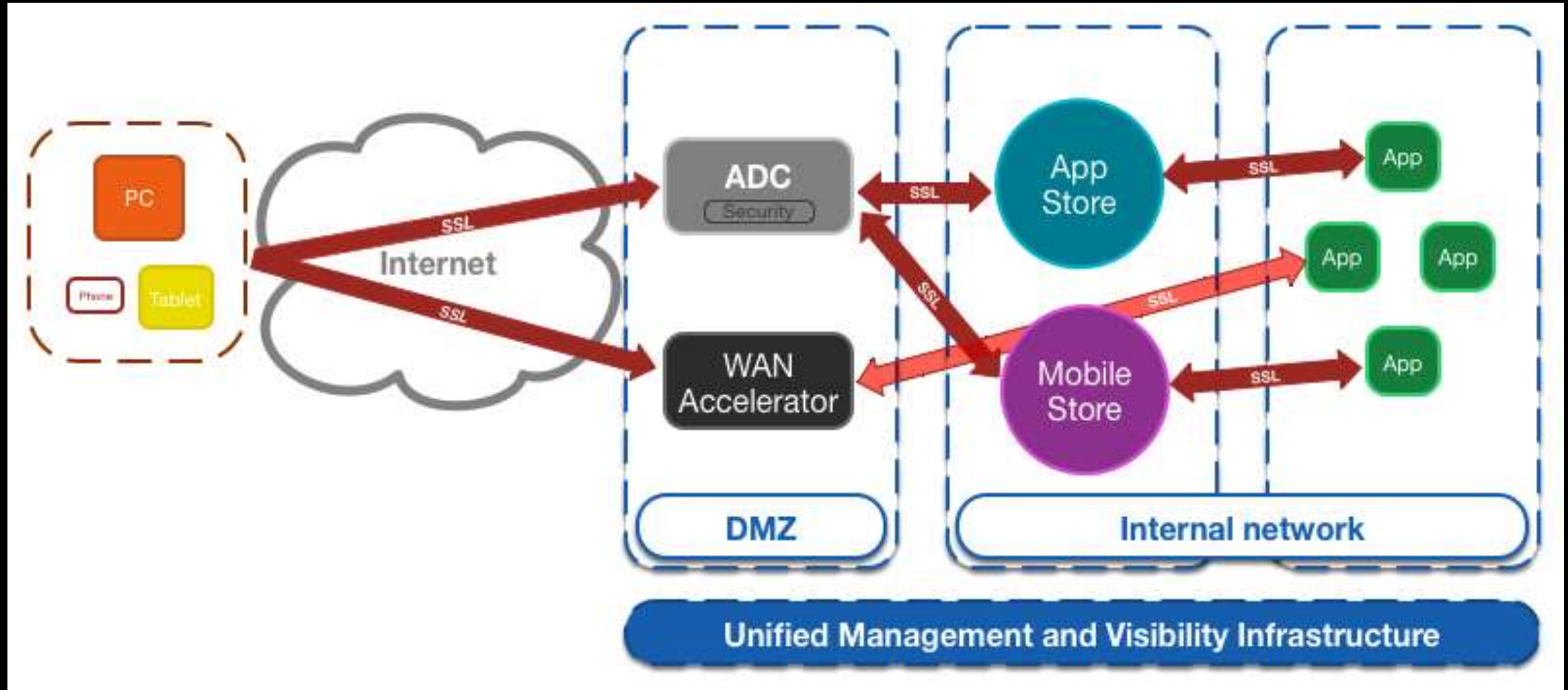
# UDM Layered Approach







# UDM – high level architecture





# UDM Building Blocks

- App Delivery
  - Mobile App distribution
  - Session virtualization
- Application Delivery Controller
- WAN Accelerator
- Unified Management and Visibility
- (SSL secured)



# Session virtualization

Centralized execution of any application made available to the users (regardless to their location, network or device) through a secure presentation protocol.

An App Store is used to provision, download and/or launch the desired app.

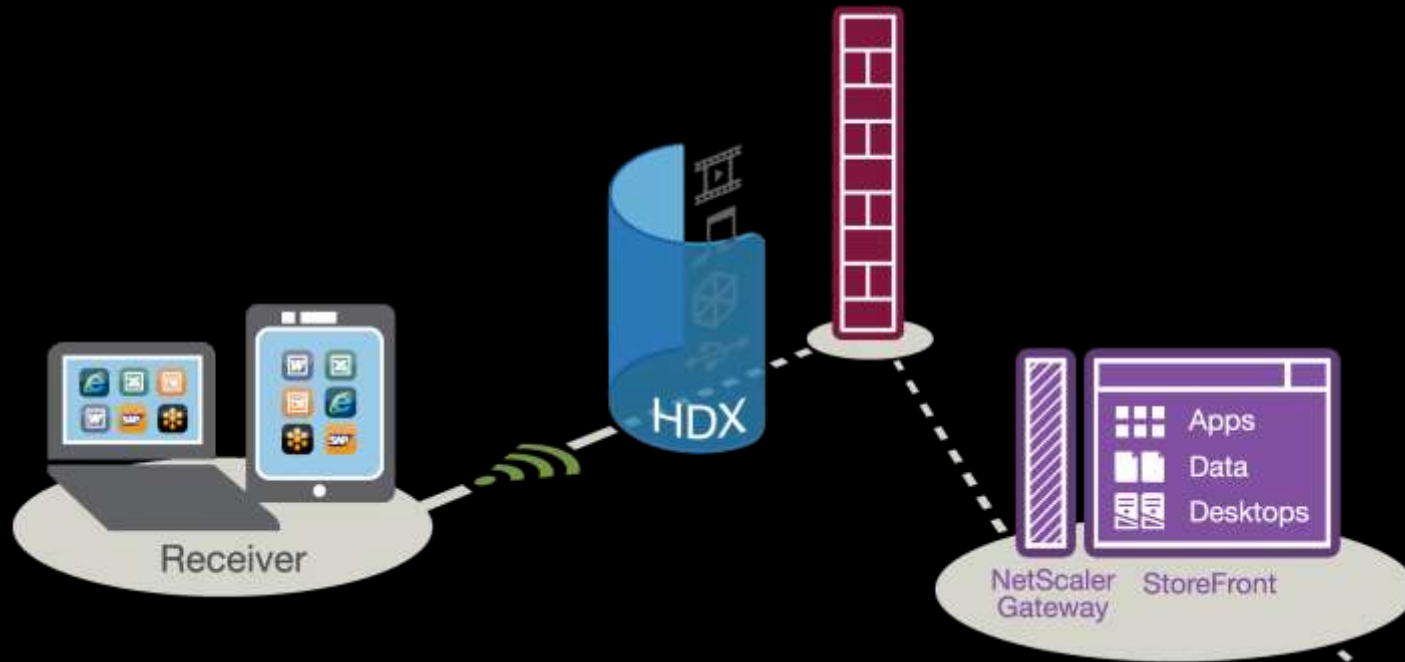
# Session Virtualization – Apps as a Service





# Secure by design

Keep data safe – keep it in the datacenter



No data on device

No data through the firewall

Unified Gateway

- Seamless remote access
- Granular access policies
- End point analysis



# Anywhere, anytime and from any device access

- **Simplify app compatibility** by delivering 5 generations of windows apps on-demand to any Windows or non-Windows device
- **Single point of management:** patching, upgrading, versioning
- **Improve business continuity** by enabling fast and secure restore
- **Eliminate/Reduce device support** while increasing manageability including patching
- **WAN optimized** networking with fine-grained QoS leveraging low-cost public network connections



## Centralized security to protect sensitive information

**Secure against data loss** of intellectual property and sensitive private information by *keeping data off the device*

**Reduce the risk of intrusion** through insecure devices or network connections leveraging granular access policy enforcement



# Simplify IT support of BYO devices

**Drive productivity**, employee retention and recruiting by supporting BYO demands

**Nearly eliminate costs** of employee onboarding, moves and exits

**Eliminate “best-efforts” support** for executives and top performers already using BYO

**Leverage new devices** without needing to support the hardware





# Application Delivery Controller

It's the Front End for the virtualized applications. It's where the policies (authentication, security, optimizations, etc.) are implemented. The ADC publishes an enterprise “App Store” from where the user can download or select the required App.

It is also used to balance sessions towards the backend servers ensuring availability of the services.

Since the ADC is the network element used to access the applications, it will provide security features (content filtering, anti-DDoS, Web Application Firewall, IPS controls, etc.).



# ADC vs Cyber Attacks: Application Security

## Block web-specific attacks

- Web Application Firewall
  - Protects HTTP(S), XML, SQL, for 0-day
- IPS
  - Signature-based protection
- HTTP DDoS Protection
  - Preserve User-Experience of legit users while discarding attackers

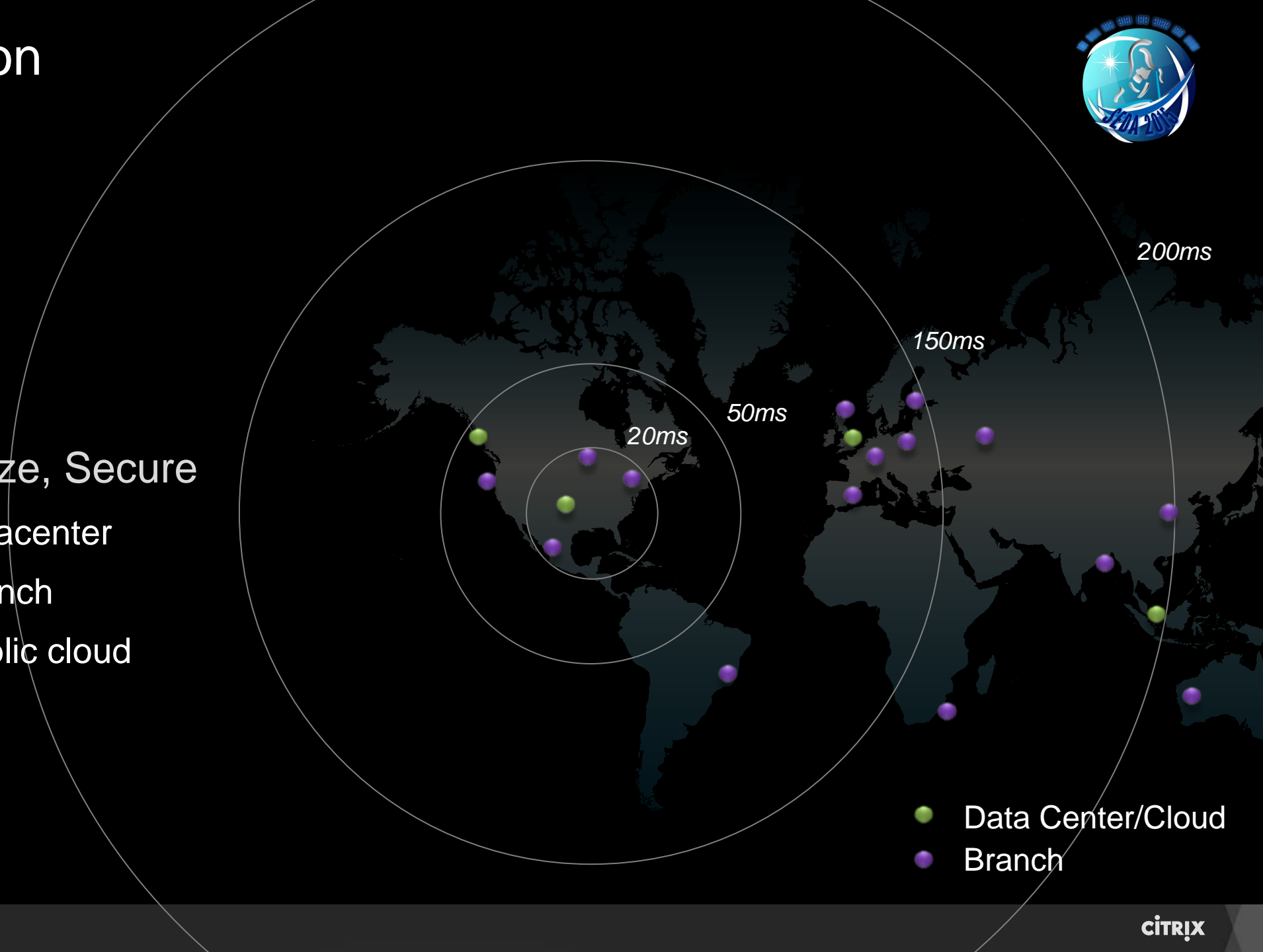


# WAN Acceleration



## Connect, Optimize, Secure

- Datacenter to datacenter
- Datacenter to branch
- Datacenter to public cloud





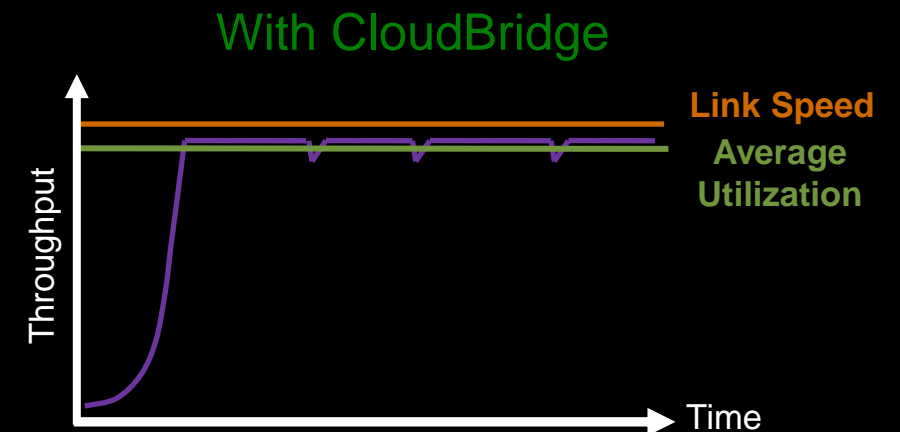
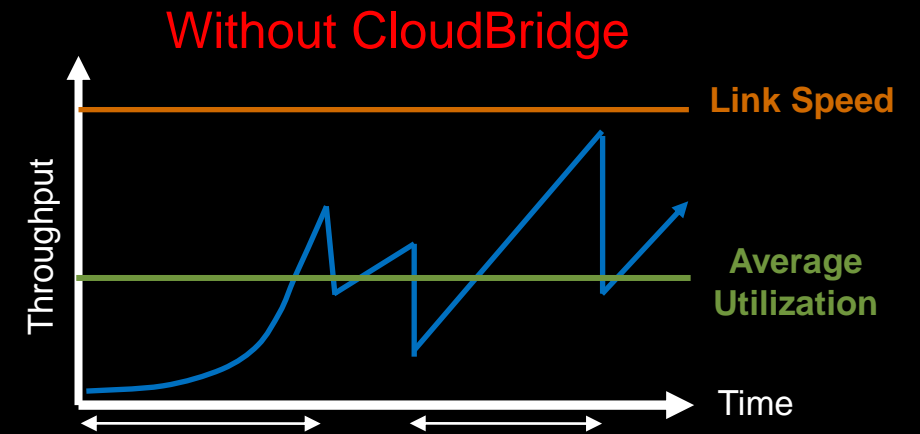
# Advanced TCP Flow Control

Network throughput impacted by TCP window size, latency and congestion

- Google “Mathis equation” or “TCP tuning”
- No packet loss:  $RWIN / RTT$
- Packet loss:  $MSS / (RTT * \text{SQRT}(\text{Packet Loss}))$

WAN Accelerators employ

- Window scaling of up to 16Kx of standard TCP
- SACK to minimize data that is resent
- Fast re-transmits to reduce delay before resend
- BIC TCP for faster recovery from packet loss





# Compression and De-Duplication,



**De-duplication: proprietary cross-stream pattern matching with byte caching**

- Disk-based – used for patterns larger than 1MB
- Memory-based – granularity as low as 6B for ICA / 64B for other



**Compression: single-ended, object-level compression**

- Zlib – Complex algorithm similar to WinZip that provides a 2 to 5x reduction (RFC1950)
- LZS – Used during high CPU/high memory conditions to provide up to 2x reduction (RFC2395)

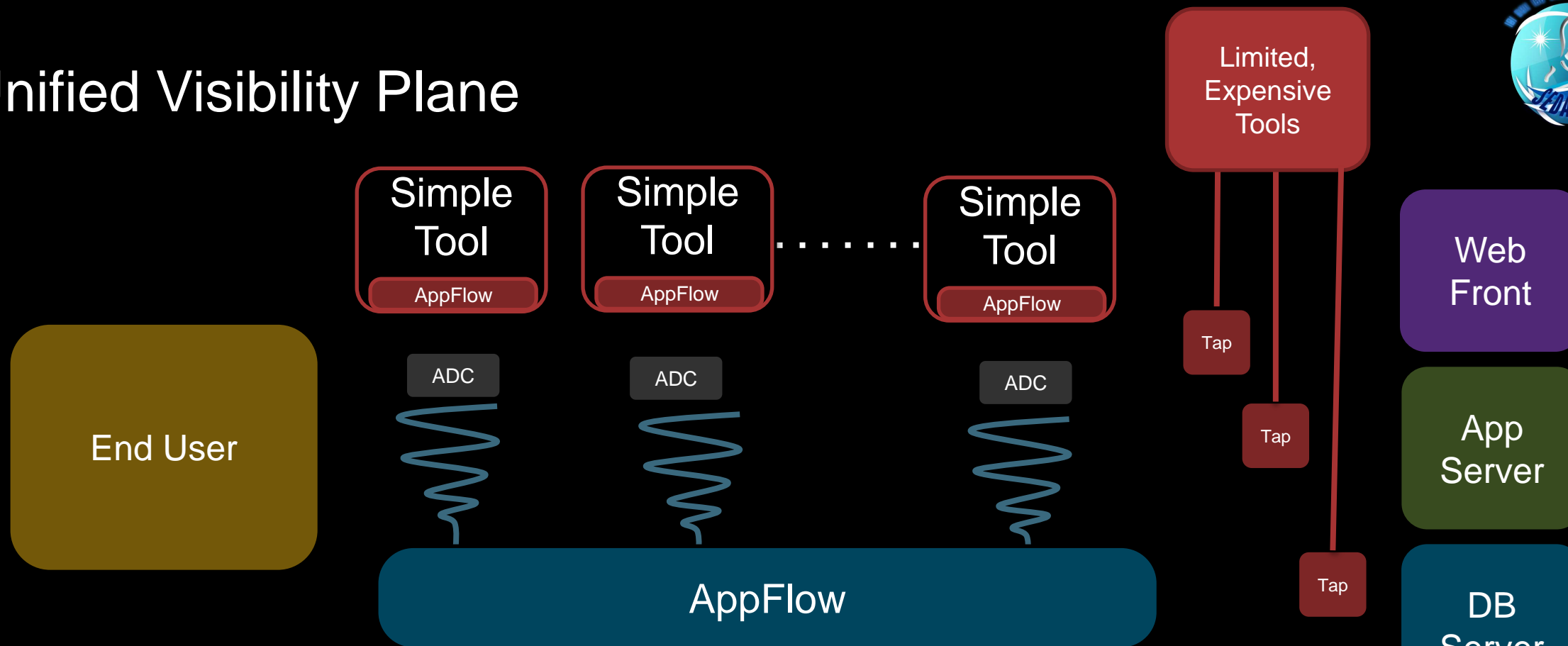


**De-duplication works on any TCP flow, except:**

- Encrypted flows may not be processed
- Compression of pre-compressed is minimal



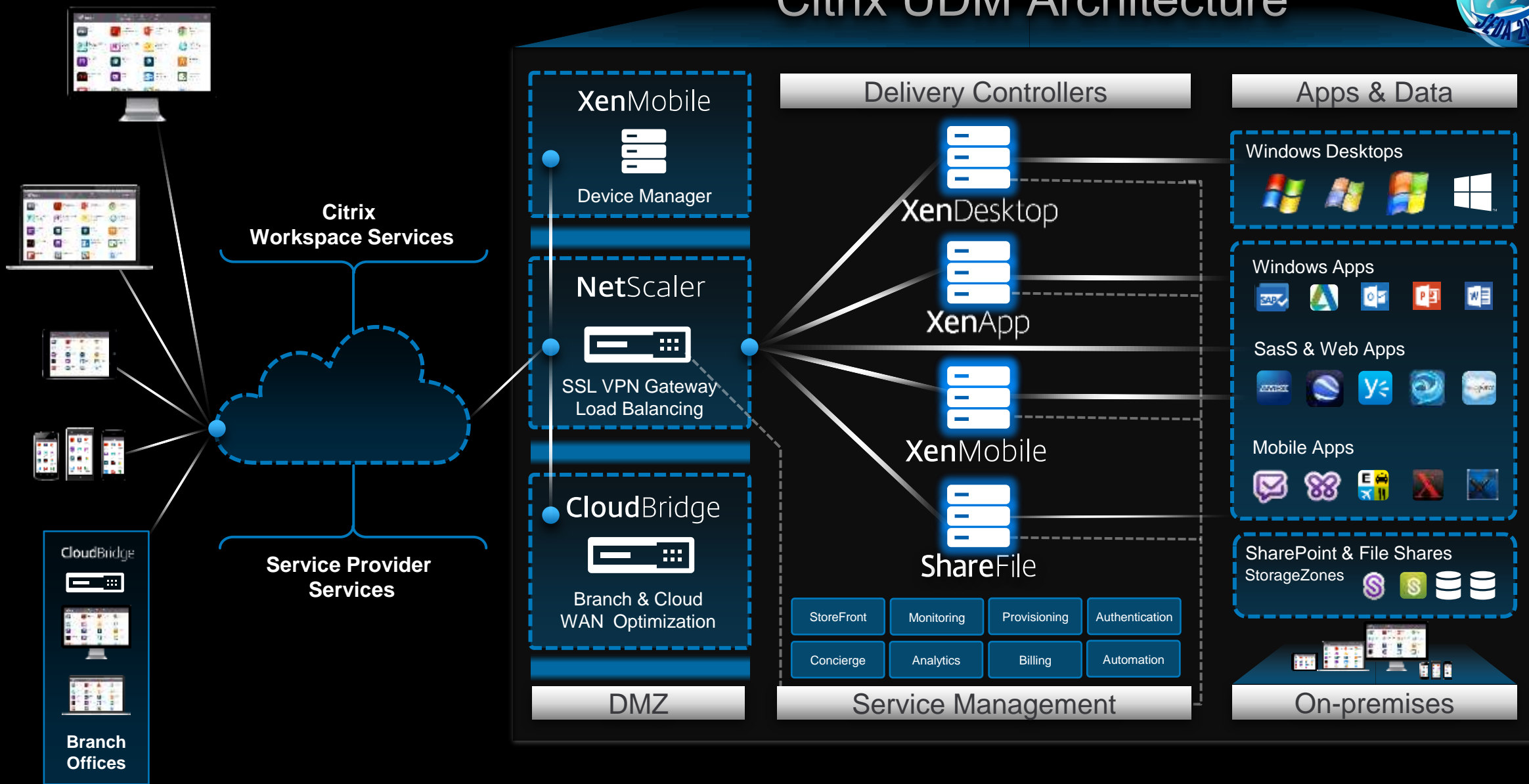
# Unified Visibility Plane



**In-Place Real Estate**  
Non-Intrusive | App Aware | Standardized



# Citrix UDM Architecture





# UDM Benefits/Goals

Optimized End-user experience

Interoperability of existing and new systems

Make resources and computational power available when needed, at runtime

Security and containerization

End-point independent

Cost-effective