

NY and Tampa RACF Users Groups Oct 2016

Shared Operations Models across System z
and other systems and what it means for
Security

Jim Porell

Principal, Consultant

James Porell Consulting LLC

jim@jimporell.com

914-474-1864



Agenda

- Executive Summary
- Mainframe Attributes and Myths
- Customer pain points
- Large Government agency that doesn't collaborate across IT today
- Examples of Collaboration across platforms
- Changing the “face of the mainframe”
 - Secure front end device – Trusted Thin Client from Forcepoint
 - Multi-factor biometric access to and from the mainframe – Callsign
- Executive summary

Goal: Explain the Architecture, Capabilities and Economic possibilities of a Shared, Hybrid Operations Model

Executive Summary

- Provide a better understanding of the Shared Operations/Hybrid Model
- Have the Shared architecture direction pay for itself via savings achieved
 - Perform better
 - More secure, resilient and meeting all SLA's
 - Provide Investment protection for the future
- Identify tactical opportunities for Shared Ops
 - Stop the Proliferation of Data
 - Database Consolidation
 - Data Virtualization via Rocket Data Virtualization Server
- Identify Strategic opportunities
 - Legacy Conversion which includes modernization
- Address many Cyber security needs
- Identify and Evaluate risks of Silo-ed Operations going forward

IBM LinuxONE



A single platform for all business workloads

- Exceptional service delivery
 - Multi-dimensional growth
 - Non-disruptive scalability
- Leadership performance
- Unparalleled qualities of service
 - Highest availability
 - Absolute security
- Economic advantage

System z Differentiators (some of them)

- Kernel Architecture
 - Storage Protection/Isolation keys
 - SMP constraint relief (memory, CPU, I/O, operations)
 - Fault avoidance & service infrastructure (ESTAE, FRR, FLIH)
 - Dynamic change management
 - Workload balancing across disparate workloads
- Middleware Architecture
 - Resource Recovery Services (heterogen. 2 phased commit)
 - Application Isolation – fault avoidance/recovery
 - Parallel Sysplex RAS and Scale Out
 - Applications and Data co-resident
 - Local and Remote access to resources via open api/fap
 - Batch and Real time sharing of R/W access to data (24x7)
- Security
 - Shared system access facility (SAF → RACF, ACF2, TSS)
 - HW cryptography
 - System SSL and PKI
 - Multi level Security – government → commercial
 - Partitioning/Isolation – EAL5
 - CERT “participation” & service philosophy
- Virtualization
 - Shared I/O, storage, memory, CPU
 - Resource balanced processor granularity
 - Offload processors
 - Batch and Real-time R/W to single DB
- Storage
 - Heritage I/O FICON and UNIX/Intel I/O SAN/NAS
 - Enables cross system application integration with shared data

- Kernel Architecture
 - Integrity Guarantee
 - Scalable Growth
 - System based RAS
 - Continuous Availability
 - Flexible deployment
- Middleware Architecture
 - Business Process Integration
 - Integrity Guarantee
 - Continuous Availability
 - Business Process Integration/TCO
 - Rapid Application Deployment
 - BPI, TCO
- Security
 - BPI, Simplification, TCO, Compliance
 - TCO
 - Collaboration, TCO
 - Privacy
 - BPI, TCO
 - Privacy, Compliance
- Virtualization
 - BPI, TCO
 - Flexibility
 - TCO
 - BPI, TCO, Privacy, Compliance
- Storage
 - Storage Vault – Privacy, Compliance, TCO

These are TRANSPARENT to application developers

z Systems security is superior to other platforms, and augmentation costs less

Security Natively Covered by Platform

Security Level Description	IBM System z	x86	Competative UNIX
Normal corporate	100.00%	18.16%	30.26%
Credit card processing involved	99.00%	11.04%	18.28%
Banking	94.00%	5.26%	10.22%
Healthcare	100.00%	3.24%	8.51%
Research	92.50%	2.86%	4.16%
Defense	85.54%	0.26%	1.86%

Major security deficiencies exist on distributed platforms

Distributed platforms require *considerable additional expense*

On z Systems, most security requirements are standard

Little additional augmentation is required on z Systems

















Incremental Cost to Achieve Required Security

Security Level Description	IBM System z	x86	Competative UNIX
Normal corporate	0.00%	32.54%	12.37%
Credit card processing involved	2.32%	16.27%	29.53%
Banking	2.07%	51.31%	26.58%
Healthcare	0.00%	57.26%	35.89%
Research	4.28%	91.26%	64.28%
Defense	11.36%	125.41%	102.26%

Source: "Tracked, Hacked and Attacked?"

© 2013, Solitaire Interglobal Ltd. https://www.ibm.com/services/forms/signup.do?source=stg-web&S_PKG=ov14292

Comparing options about concurrent operations during maintenance, limiting downtime

Capability	IBM z	Today's distributed servers
ECC on Memory Control Circuitry	 Transparent While Running	 Can recognize/repair soft errors while running; limited ability with hard errors
Oscillator Failure	 Transparent While Running	 Must bring server down to replace
Core Failure	 Transparent While Running	 Must bring server down to replace
Microcode Driver Updates	 While Running	 Some OS-level drivers can update while running, not firmware drivers; reboot often required
Memory Replacement	 While Running	 Must bring server down
Memory Bus Adaptor Replacement	 While Running	 Must bring server down
I/O Upgrades	 While Running	 Must bring server down to replace (limited ability to replace I/O in some servers)
Concurrent Driver Maintenance	 While Running	 Limited – some drivers replaceable while running

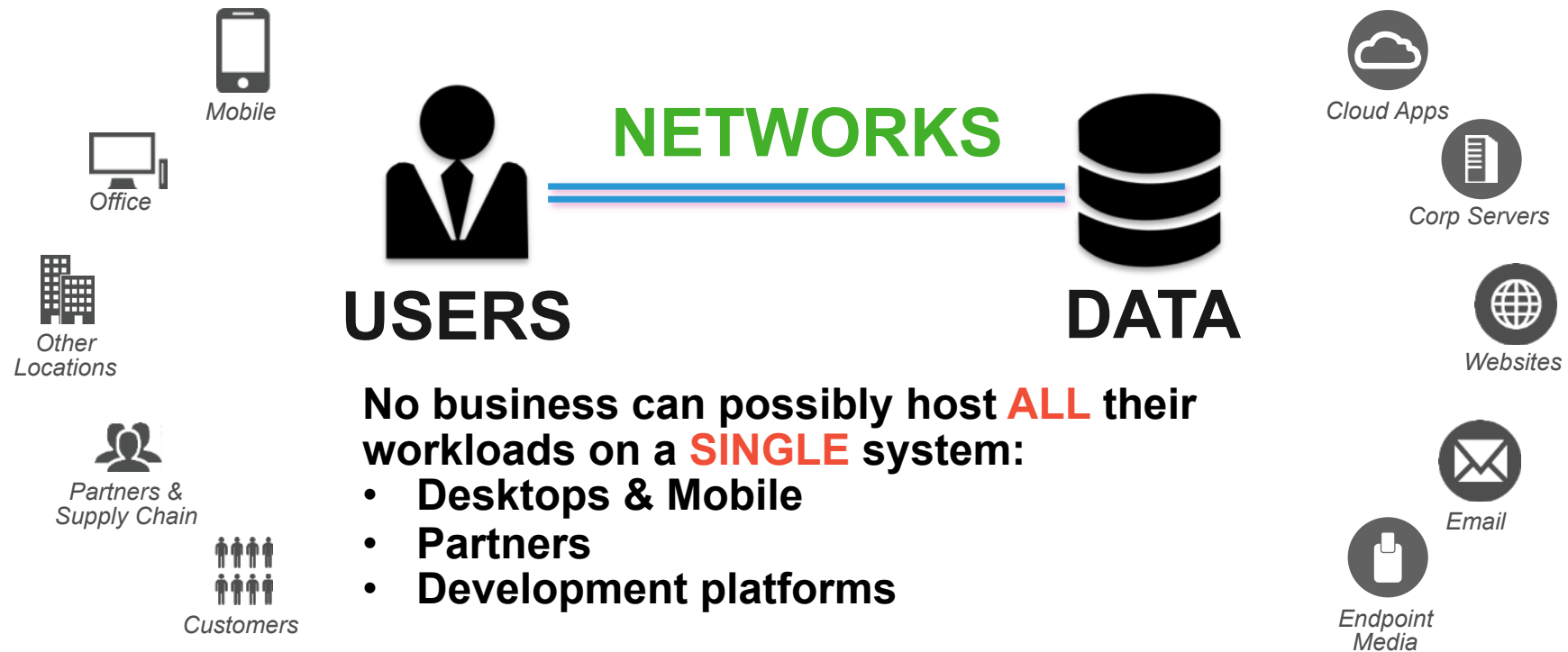
Consider the alternative – IBM LinuxONE



A ~~single~~ platform
for ~~all~~ business workloads

- Exceptional service delivery
 - Multi-dimensional growth
 - Non-disruptive scalability
- Leadership performance
- Unparalleled qualities of service
 - Highest availability
 - Absolute security
- Economic advantage

Modern Business is all about safely connecting users to data

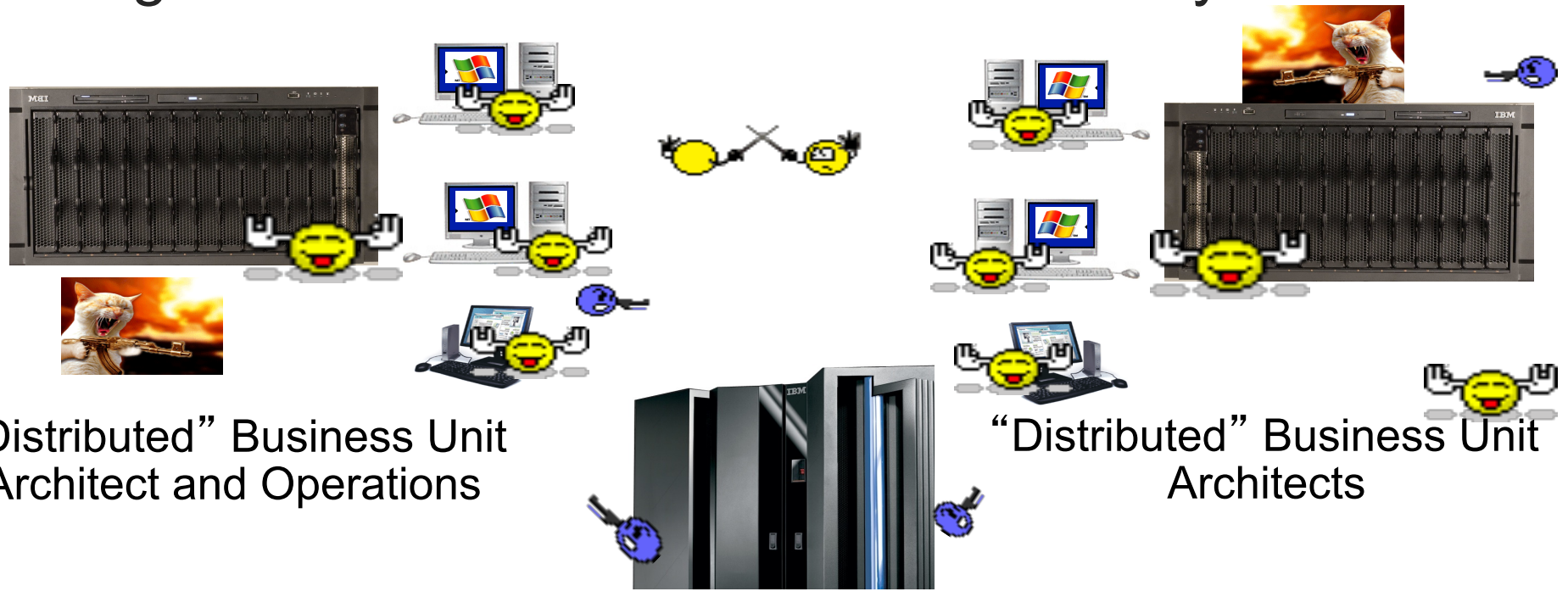


No business can possibly host **ALL** their workloads on a **SINGLE** system:

- **Desktops & Mobile**
- **Partners**
- **Development platforms**

Collaboration/Sharing Operations is critical

IT Organization Wars – at a business near you?



“Distributed” Business Unit Architect and Operations

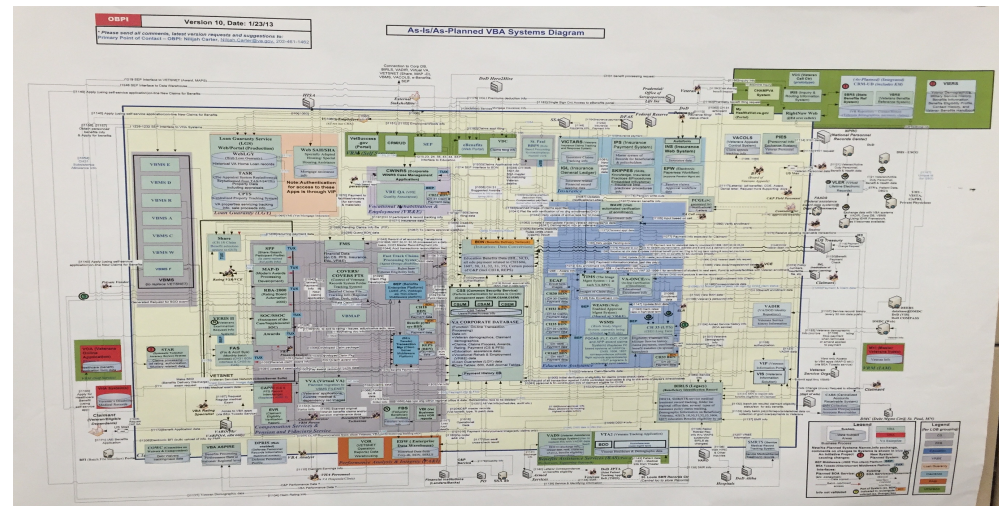
“Distributed” Business Unit Architects

“Centralized” Glass House Operations

10 **Silos of computing are the worse thing for security (and resilience)**

Typical mistakes companies make in protection...

- Lack of knowledge where confidential data is (PII, Trade Secrets, etc.)
- Lack of logic and data flow- the source and destination of data
- Failure to encrypt data
- Reliance on weak passwords
- Lack of segregation of duties
- Lack of adequate access controls
- Bad firewall rules
- Failure to maintain systems
- Changes in configurations
- **Lack of consistency in deploying security across systems**
 - E.g. Audit one platform for data, but not another one, where the data was copied



Growing number of losses occur from within

What is Security from a customer view?

- Policy
- Corporate Directive
- Regulatory Compliance (e.g. HIPAA, Sarbanes-Oxley)
- Technology (e.g. RACF, ACF2, Tivoli Access Manager)
- Infrastructure (e.g. Tivoli, Vanguard, Consul, Beta)
- Components (e.g. firewalls)
- Preventative (e.g. anti-virus, intrusion defense)
- Business workflow (e.g. Analytics, audit)
- Physical (e.g. Badge Access, Biometrics)
- Multi-media (e.g. Video cameras, voice analysis)
- Executive Position (e.g. CISO, CPO)
- Skill specialty (e.g. CISSP)
- Department (e.g. Info Assurance, IT Security)
- Redundant
- Bureaucratic
- Too Sensitive
- Expensive
- Unresponsive
- Big Brother
- Many times implemented in silo's.
- Each server domain has its own security authority
- Typically, it's not → a Solution
 - Leverage Security to make solutions better

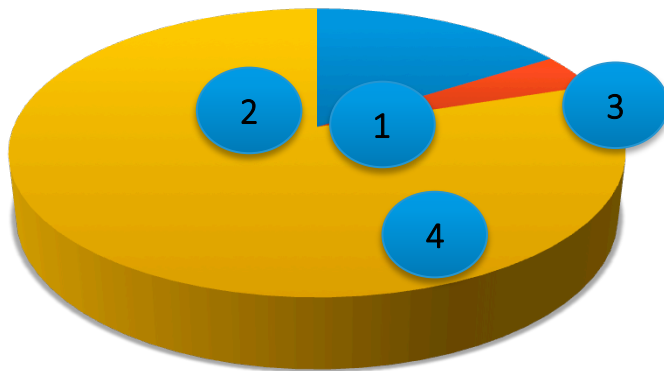
Shared Operations Model, needs to work end to end

- Even though security on Mainframe may be great, the weakest link must be secured as well
- Leveraging an end to end approach to security is critical
- System of Record must be secured, regardless of where resident
 - Need to be consistently managed and auditable, regardless of location
- System of Engagement must provide secure access to Systems of Record and Insight
- System of Insight should be leveraged to prevent loss(real-time) vs. detect risk (batch)

Finding new IT opportunities

Drive Datacenter Shared Operations

Silo-ed Operations



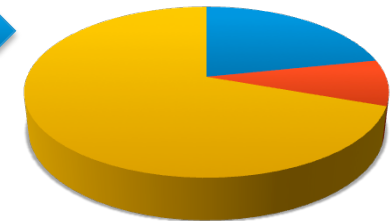
1. Open communications across IT Programs
 - development, test and operations
2. Stop the proliferation of data
3. Modernize IT
4. Migrate some distributed to z

Save \$xxMM in IT



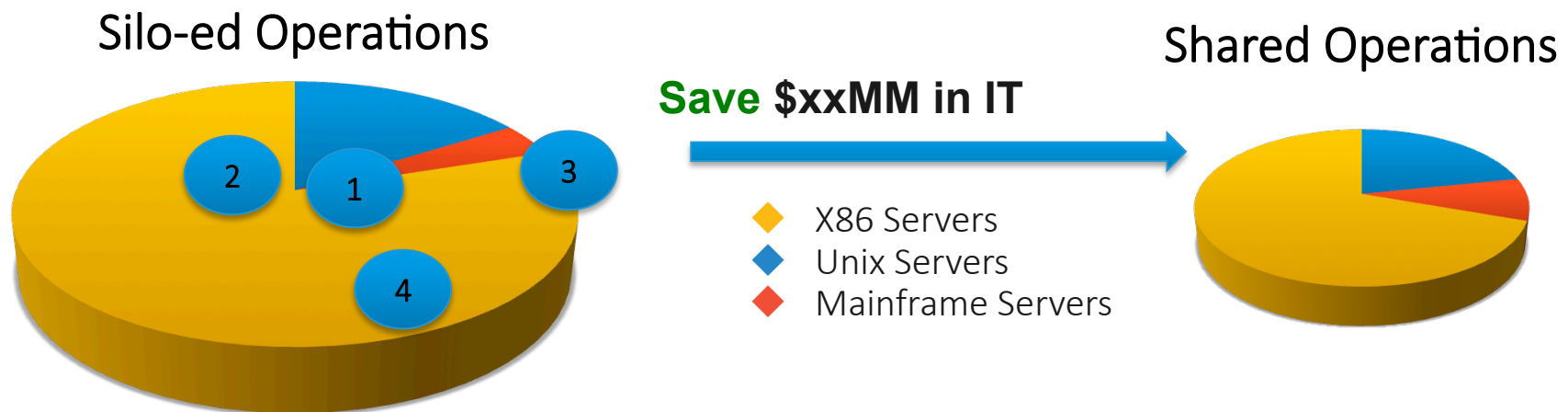
- ◆ X86 Servers
- ◆ Unix Servers
- ◆ Mainframe Servers

Shared Operations



- Reduce acquisition costs by taking some costs out
- Reduce operational costs
- Reduce operational and deployment risks
- Improve the security and resilience
- Provide investment protection and continued cost benefits through future technology deployment
- **Aid in Mitigation, Migration and Modernization business goals**

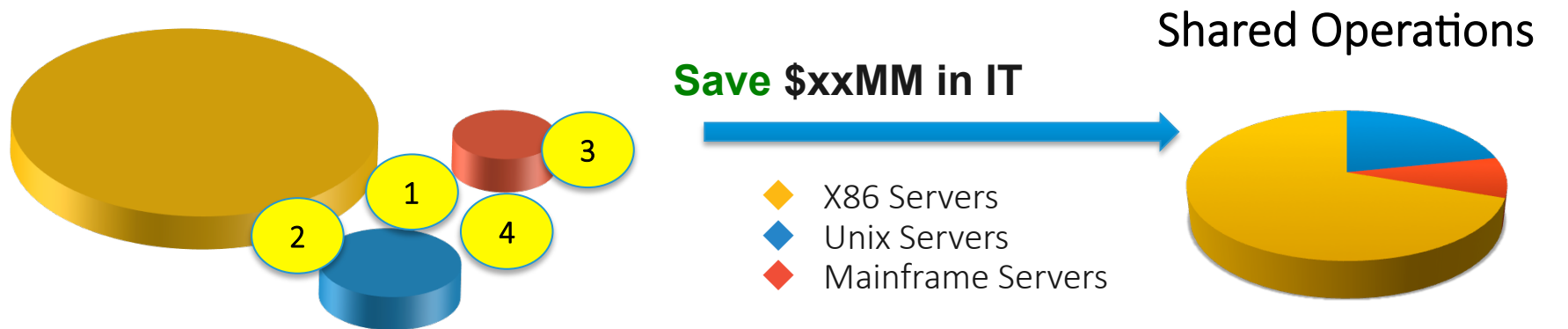
Customer Reaction to this slide



- This is a good representation of what we want to achieve.
- The accuracy of the amounts in the individual slices of pie is irrelevant.
- However, going from a large pie to a smaller pie is absolutely relevant.
 - Note: We had IBMers arguing to not show chart without raw data. It's a model. Customers get it.
- If System z can take us there and improve our security and resilience in the process, we'd like go do it.
 - They could see a larger spend in z, but less spend, overall.
- We know we will still have a lot of x86, but our environment will be more manageable.
 - Reinforcing that not ALL business workloads will run on a SINGLE system.

Finding new IT opportunities

Drive Datacenter Shared Operations



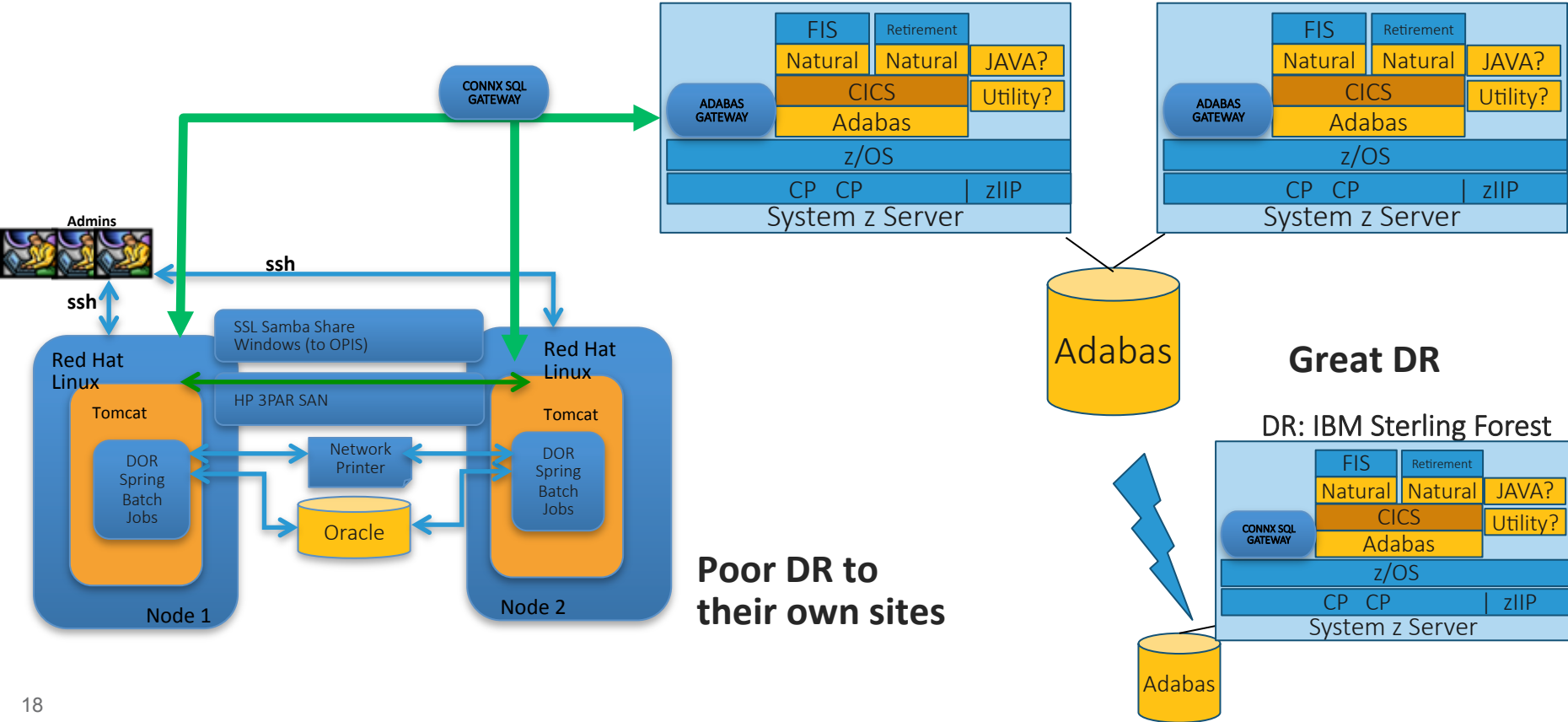
1. Open communications across IT Programs
 - development, test and operations
2. Stop the proliferation of data
3. Modernize IT
4. Migrate some distributed to z

- Reduce acquisition costs by taking some costs out
- Reduce operational costs
- Reduce operational and deployment risks
- Improve the security and resilience
- Provide investment protection and continued cost benefits through future technology deployment
- **Aid in Mitigation, Migration and Modernization business goals**

Mainframe as a Security Hub

- z/OS is known for running mission-critical workloads for your Enterprise
- Ensuring your applications run and run securely is a business requirement
- z/OS offers highly available, secure, and scalable database hosting
- z/OS has well-honed security processing with very granular permissions capabilities
- z/OS offers superb auditing of operations performed
- control of user/group definitions in multiple registries, including RACF, from z/OS, is now available
- services-based security capabilities, hosted on z/OS and Linux for System z, are now available
- **Using a combination of Linux for System z and z/OS systems, the mainframe can host many of the security functions for the Enterprise**

Customer Example Mainframe Environment

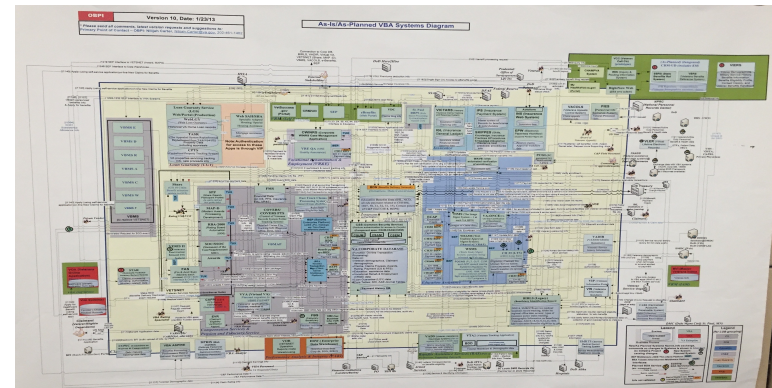


Identifying Customer Pain Points

- Proliferation of Data
 - Inhibits Real time analytics –
 - windows for Fraud
 - Inaccurate decisions made
 - Burns up CPU, storage and Network making copies
 - more costs
 - More complexity
 - Increases Security Audit burden and complexity
- Complain about cost of mainframe software
 - Identify MLC usage – vendor and IBM
 - Look at where they've "offloaded" applications to alternative platforms
 - Look at where they've copied data to alternative platforms
 - Look at the user interface of the applications on the mainframe
 - Are they graphically challenged?
 - Are they exporting data/applications to alternative platforms to enable a mobile interface?
- Operationally manage mainframe independent of other systems
 - Fosters aggregate IT cost growth
 - Fosters major security and resilience vulnerabilities
 - Fosters growth in application deployment on alternative platforms

Customer – Their Current State

- System and middleware
 - Legacy COBOL, TEX, JCL, and GMAP languages and IDS-II database,
 - Legacy online TP monitor requiring proprietary gateway systems at user sites for unique screen handling
 - Bull GCOS operating system is no longer widely deployed
- Application code
 - Decades of software entropy have accumulated significant technical debt,
 - Too difficult, time consuming, and expensive to maintain/modify,
 - E.g. Two years to add Electronic Funds Transfer – Route Codes and account numbers are “tucked” into empty spaces in existing db
 - Poor knowledge of database elements and usage,
 - No Application Development Environment, no Modern Development Tooling nor understanding tools
 - No code management nor generation
 - Source may not match production code
 - Aging work force
 - Skills acquisition/training is difficult
 - Use of retirees as contractors to modify code
- Operations
 - Lacks automation
 - Labor intensive



Our view of “commodity” deployment alternatives

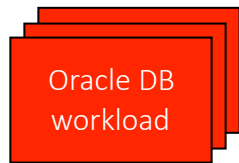
- Will take the same amount of time and cost to deliver
- Result will be less resilient and less secure
- Result will have much larger operational cost of ownership
 - Many more cores and System images
 - Much more network overhead between applications and databases
 - More copies of data to address System of Record (OLTP) and System of Insight (analytic) needs
 - This diminishes capabilities to address real time analytics

Deployment Platform

- We've chosen IBM Mainframe in a shared operations with commodity servers
 - Customer already operates and inter-operates with IBM mainframes
 - Continues Security and Resilience value over commodity servers
 - Provides an open development environment
 - It's ability to automate work easily and maintain service level agreements
- Both the mainframe and commodity servers can leverage a cloud deployment model if desirable in the future.
- Analytics – COTS products deliver these capabilities when linked to Transformed code
 - Fraud/Audit, for example:
 - Excessive/inaccurate billing by schools
 - Benefit usage attempts by unauthorized individuals
 - Location discrepancies between residence and location of service providers for brick and mortar schools
 - Resource usage/Performance
 - Capacity Planning
 - Workload balancing
 - Functionality
 - Monitor time necessary to approve benefits
 - Monitor time necessary to process a claim
 - Ad hoc queries of any content without special programs to join disjoint data fields
 - Executive Insight
 - Dashboard to look into Operational Efficiency
- Transformation goal is to preserve end user interfaces to minimize online changes.
 - This will speed deployment from Bull to new state
 - New state is enabled to easily support a modernized front end, but that can be delayed, based on business need.

Database workloads with high I/O bandwidth requirements benefit from Linux on z architecture

Which platform provides the lowest TCA over 3 years?



Customer Database Workloads
each supporting 18.3K tps
Oracle Enterprise Edition
Oracle Real Application Cluster



3 Oracle RAC clusters
4 server nodes per cluster
12 total HP DL380 servers E5-2699v3 2.3GHz
2ch/36co
(432 cores)

\$29.3M (3 yr. TCA)



3 Oracle RAC clusters
4 nodes per cluster
Each node is a Linux guest
LinuxONE with 61 cores

\$13.5M (3 yr. TCA)

54% Lower cost

TCA includes hardware, software, maintenance, support and subscription.
Workload Equivalence derived from a proof-of-concept study conducted at a large Cooperative Bank.

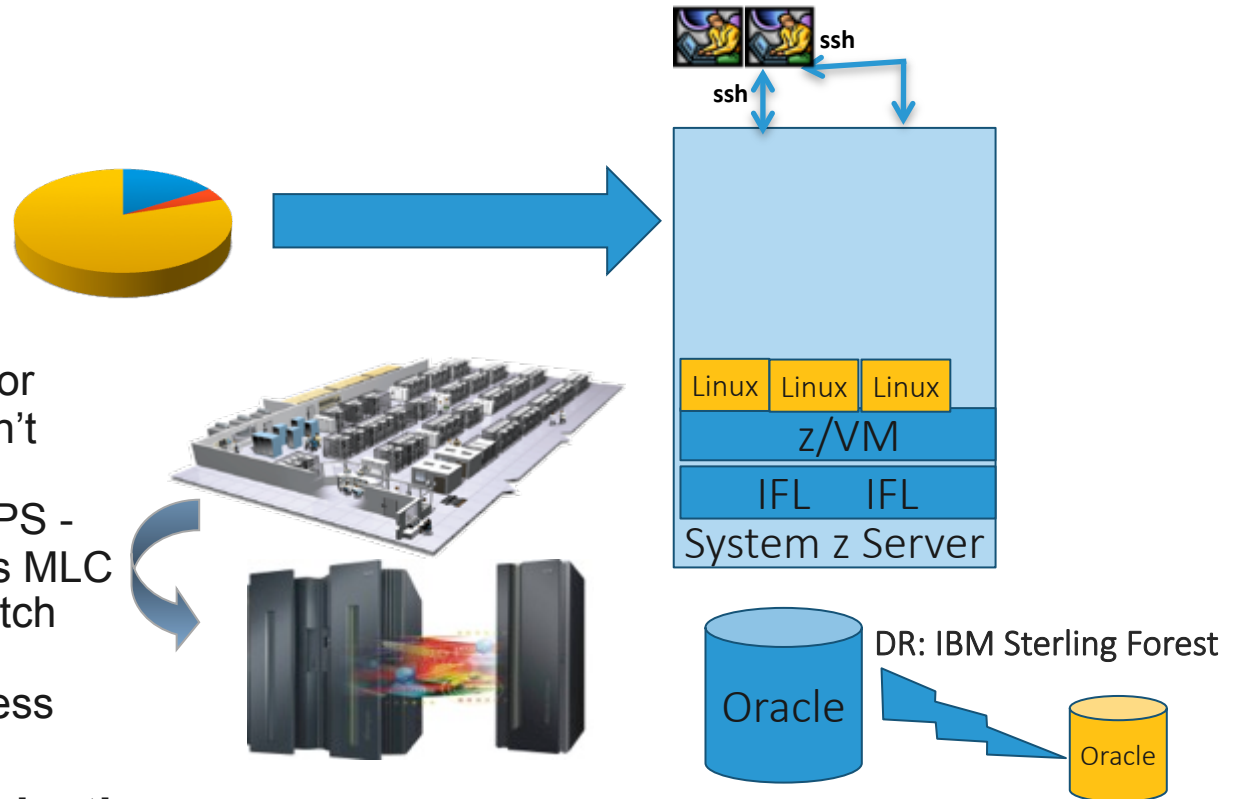
x86 Server Consolidation to Linux on z Pilot

- Move other x86 work to z
 - Oracle Consolidation
 - Data Warehouse
 - Applications

Value:

1. **Migrates** x86 footprints with associated TCO: licenses, floor space, cooling, energy. Doesn't eliminate x86
2. Reduces ETL MLC based MIPS - reducing all other sw products MLC
3. Enables near real-time vs. batch analytics
4. Improves Security and Business resilience. **Mitigates risk**

Goal: Facilitate Migration objectives

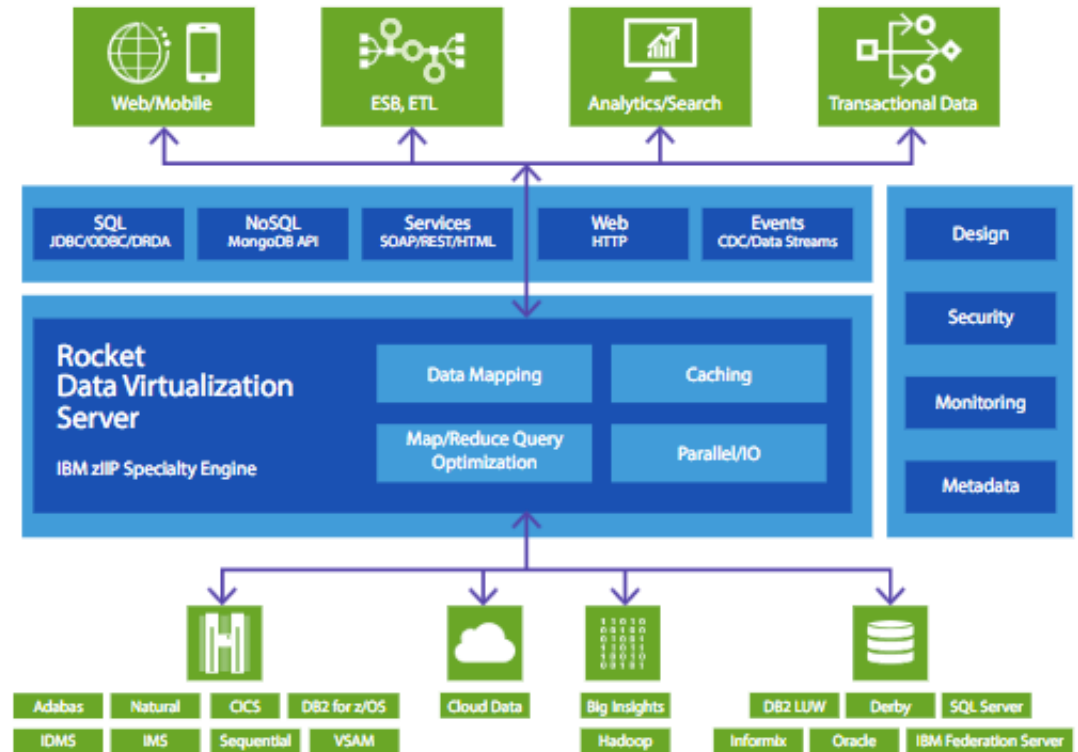


Rocket Data Virtualization

The industry's only mainframe-resident data virtualization solution for real-time data access from any application, Rocket® Data Virtualization software helps the IBM® z Systems® platform reach its full potential for high-performance data processing.

It provides a virtual representation of data while eliminating the cost and complexity of data movement technologies, including ETL operations.

Puts remote data requests under mainframe security authority

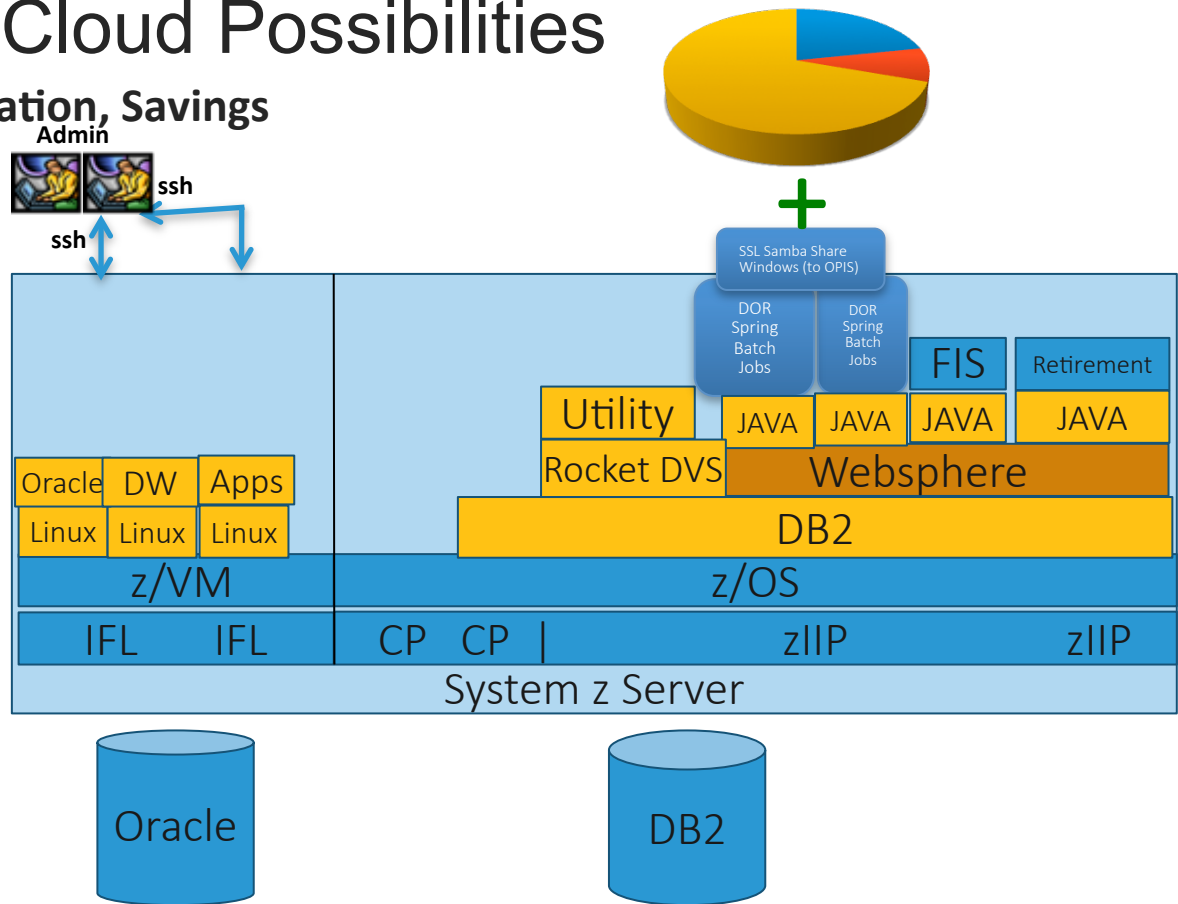


Shared Ops/Hybrid Cloud Possibilities

Mitigation, Migration, Modernization, Savings

- Exceptional performance and superior virtualization
- Infinite scalability and elasticity
- More secure platform, effective disaster recovery
- Resiliency and qualities of services
- Economic benefits

Fit for Purpose Operations



Management Considerations for an enterprise	
<ul style="list-style-type: none"> • Authentication • Alert processing • Firewalls • Virtual Private Networks • Disaster Recovery plans • Storage Management • Owned, Private or Hybrid Cloud 	<ul style="list-style-type: none"> • Network Bandwidth • Encryption of data • Audit Records/Reports • Provisioning Users/Work • Data Transformations • Application Deployment • Fraud prevention
How does the Virtualization Manager improve these?	

Why is IBM working with Forcepoint?

“Fast and secure transaction processing is core to the IBM mainframe, helping clients grow their digital business in a hybrid cloud environment,” said Tom Rosamilia, senior vice president, IBM Systems. “With the new IBM z13s, clients no longer have to choose between security and performance.”

Total system security requires deep knowledge of specific industries and threats. That is why IBM is working with other leaders in the field to augment its own solutions. IBM’s strategic partnership program for security, “Ready for IBM Security Intelligence,” now includes more software applications from key ISVs integrating their solutions for z Systems.

Source: <http://www-03.ibm.com/press/us/en/pressrelease/49021.wss>

TRUSTED THIN CLIENT® for Mainframe

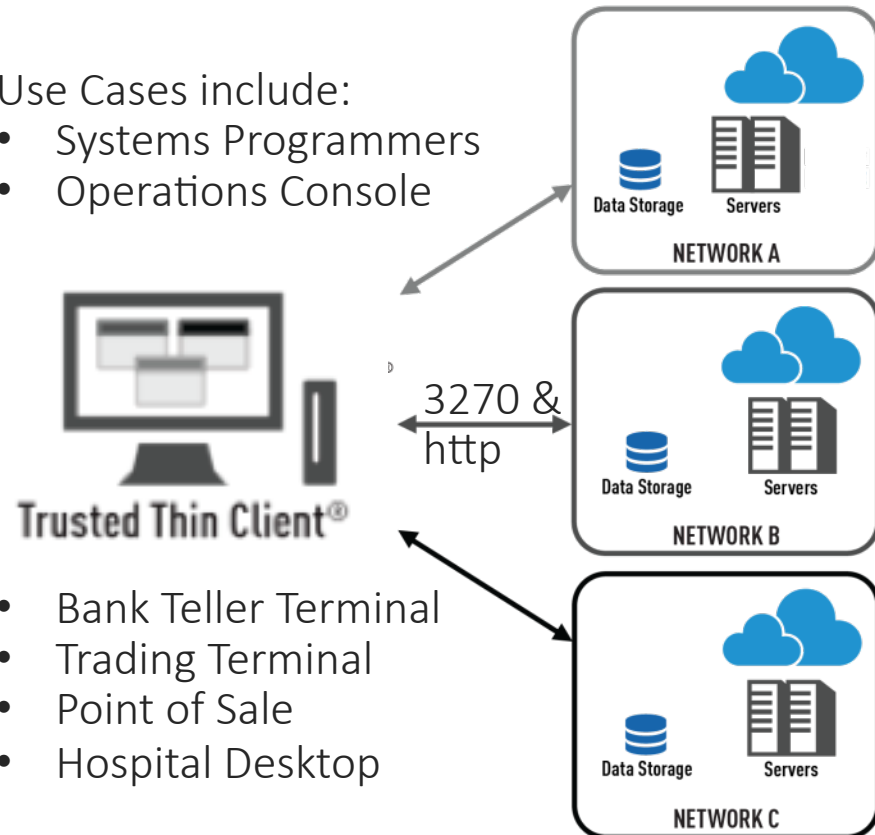
FEATURES & BENEFITS

Secure access to critical business resources from a single endpoint

- Centralized management and monitoring
- Streamlines administration while increasing enterprise data security
- Increased productivity, lowers costs, high security posture, prevention of data spills and leakage
- No VDI infrastructure required – standalone state-less Device
- Inhibits introduction of viruses & malware to corporate networks
- Reduces desktop hardware and allows for space reclamation
- Reduces infrastructure for cabling and cooling
- Supports accessories including webcams, smart-cards, multi-media redirection & unified communications
- Remote access capability and extension to mobile devices

Use Cases include:

- Systems Programmers
- Operations Console



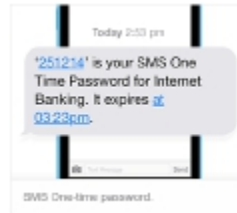
- Bank Teller Terminal
- Trading Terminal
- Point of Sale
- Hospital Desktop

Towards Intelligent Access

1st
Generation



2nd
Generation



Callsign™




Offline

Offline + Online

Offline + Online + Cyber + Context

Callsign introduces a new approach that eliminates the need for passwords and security tokens, delivering intelligent access based upon a combination of biometrics as well as cyber & contextual

Copyright © 2015 Callsign Inc. All Rights Reserved.



Any application that
requires passwords or
security questions can be
enhanced by Callsign

Key Use Cases

VPN Access, e.g. Cisco, Juniper, Citrix

SaaS, e.g. Salesforce, Workday, Google

PAM, e.g. CyberArk, Palantir

Websites, e.g. e-commerce

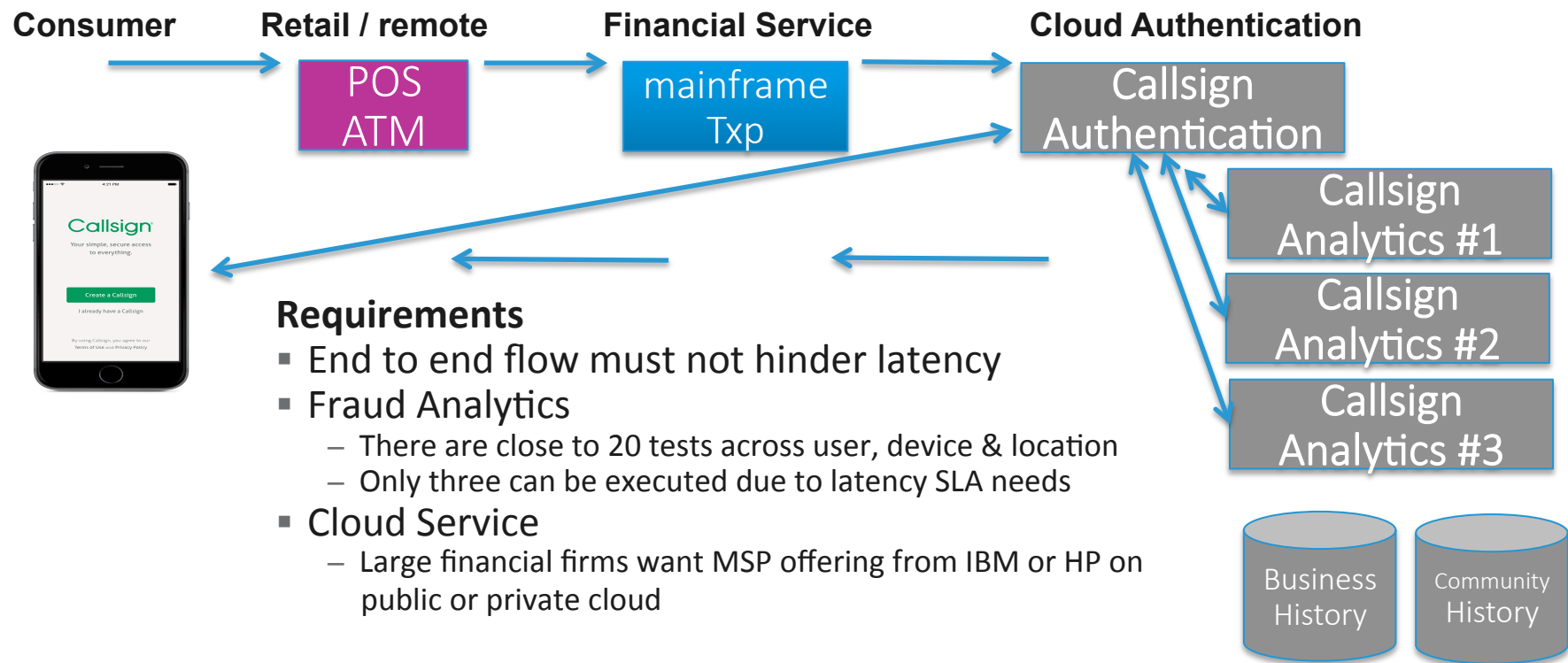
Enterprise Apps, e.g. Finance, CRM

Contact Centre, inbound and outbound

IoT, e.g. ATMs, Smart Meters, Inventory

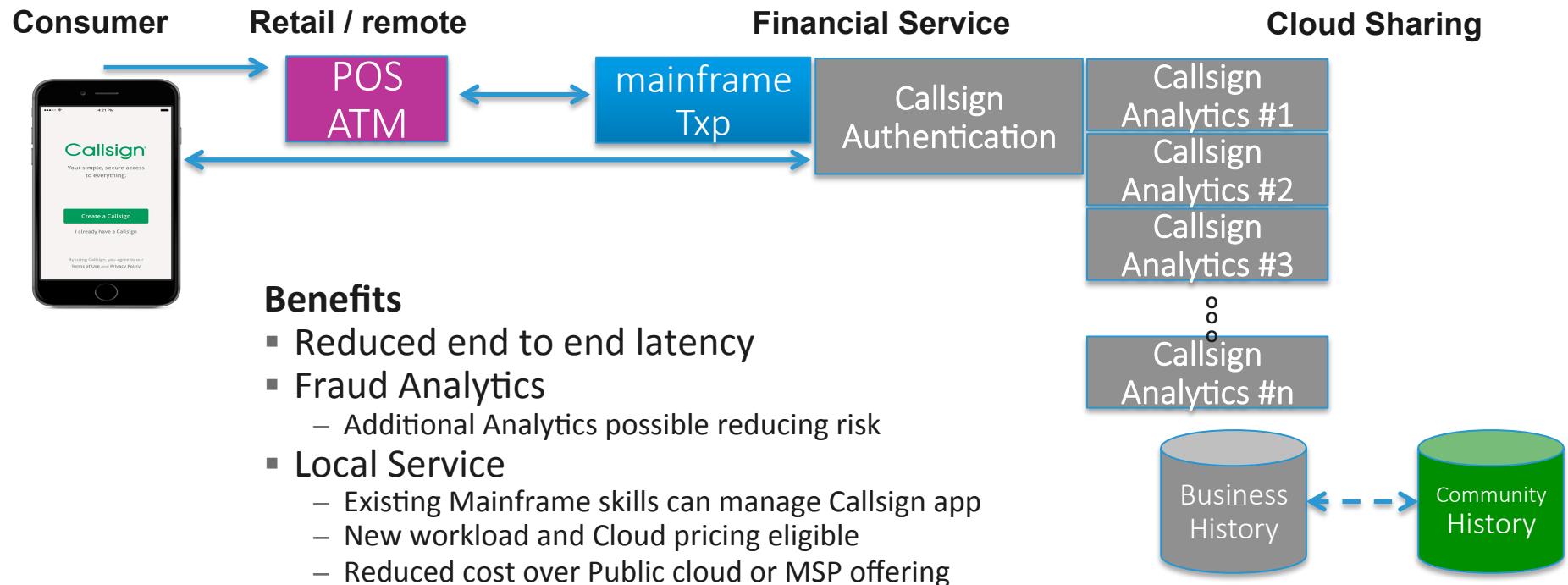
Access from the Mainframe

Public or Private X86 Cloud Implementation



Access from the Mainframe

Local z/OS or Linux on z Callsign implementation

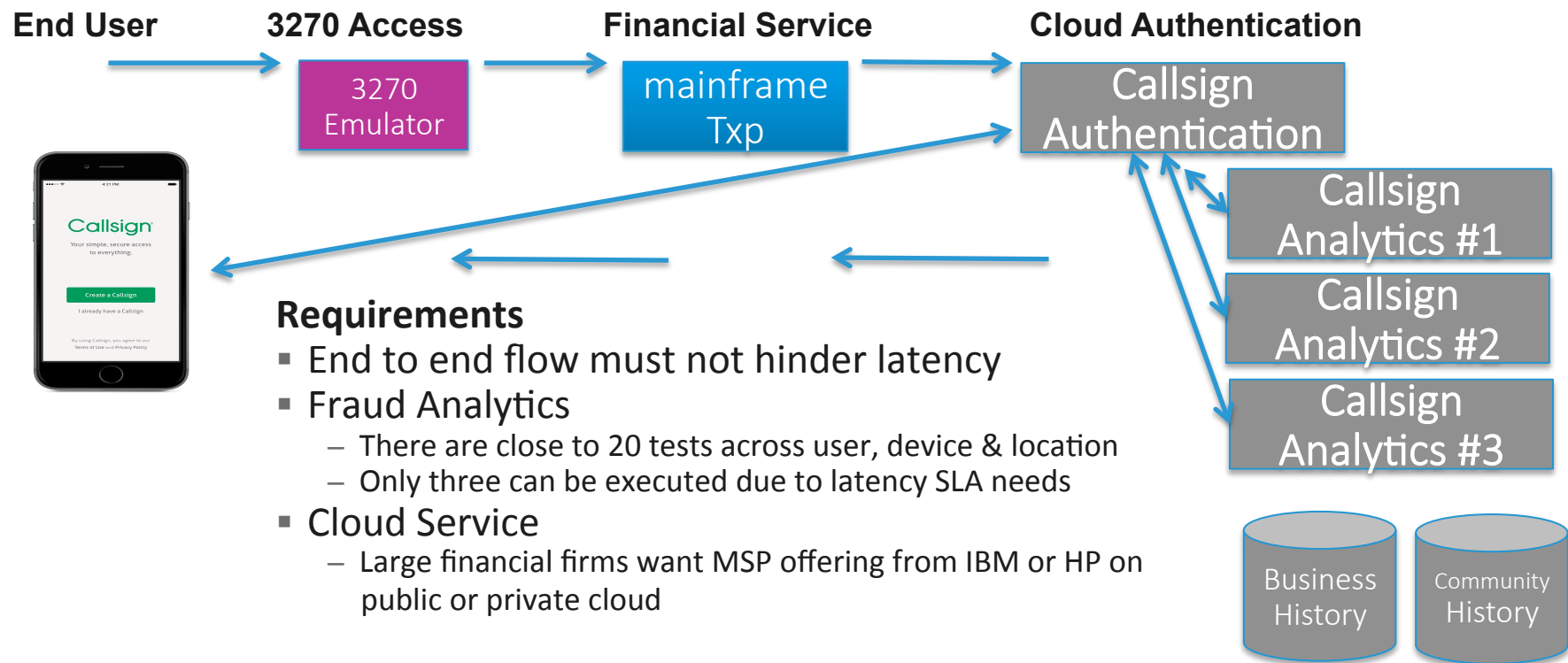


Benefits

- Reduced end to end latency
- Fraud Analytics
 - Additional Analytics possible reducing risk
- Local Service
 - Existing Mainframe skills can manage Callsign app
 - New workload and Cloud pricing eligible
 - Reduced cost over Public cloud or MSP offering

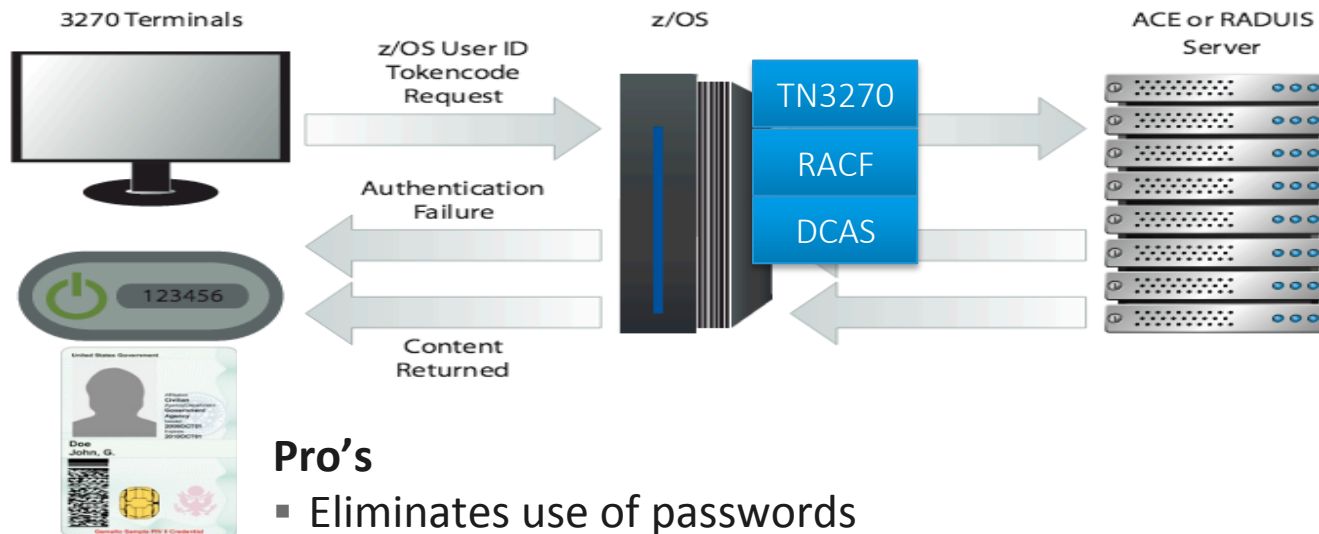
Access to the Mainframe

Public or Private X86 Cloud Implementation



Access to the Mainframe

Use of Inanimate object for Multi-Factor Auth



Pro's

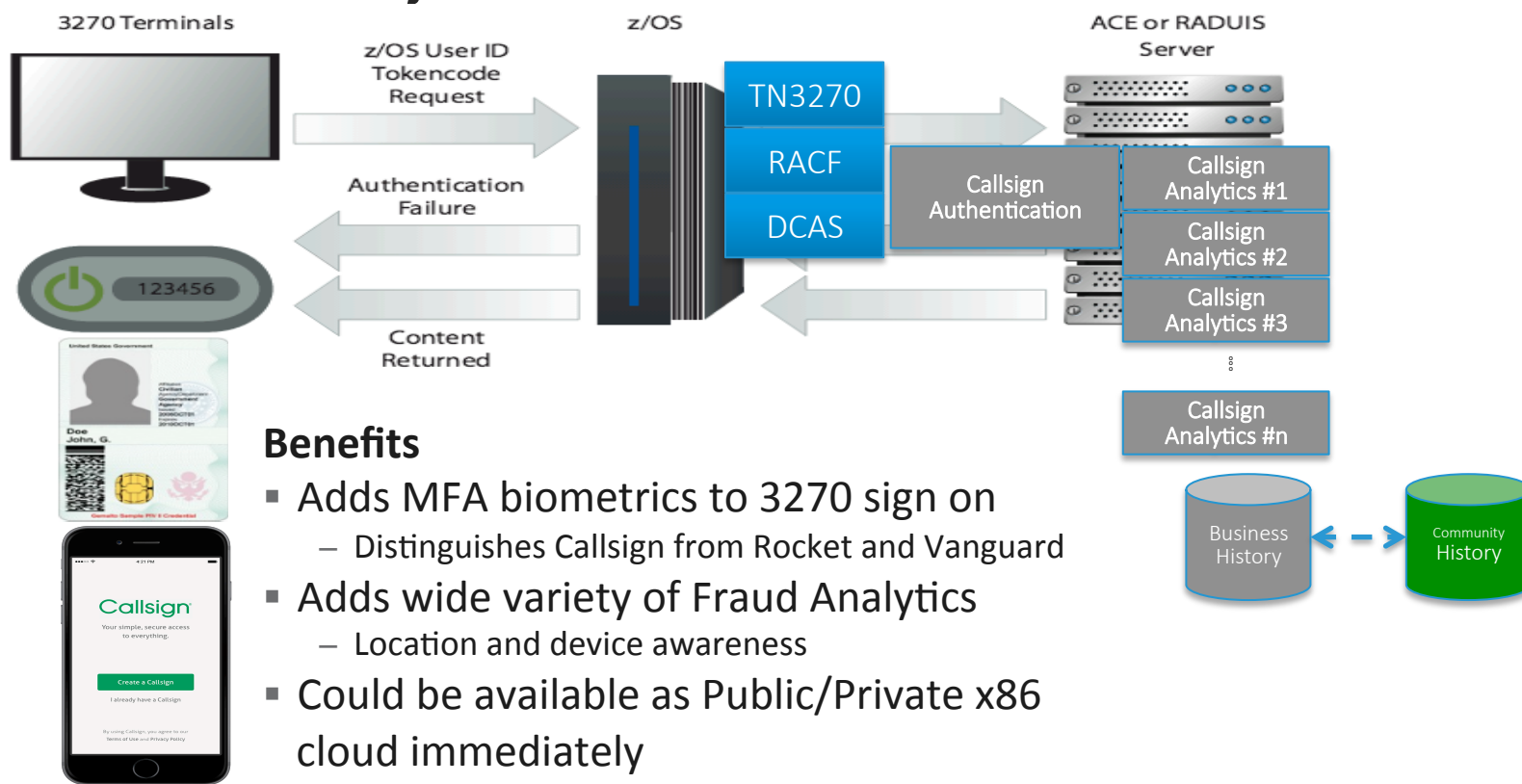
- Eliminates use of passwords

Con's

- Uses inanimate object for authentication
 - No proof it hasn't been stolen nor compromised
- Advanced Fraud analytics require additional products

Access to the Mainframe

Use of Inanimate object for Multi-Factor Auth



Callsign Operations

- **Analytics**, i.e. multiple factors in one solution.

There are about 20 potential “tests” across:

- **Line** – derive trustworthiness of telephone line
- **Location** – derive trustworthiness of location
- **User** – derive trustworthiness of user
 - **PIN** – crypto architecture means NOT stored anywhere
 - **Finger** – works on iPhone 5s+ and Galaxy S5+
 - **Retina** – works across any smartphone device
 - **Facial** – works across any smartphone device
- **Device** – derive trustworthiness of device

- **Elapsed Time** – Should be less than 21 seconds to complete analytic tests

- **Deployment Types:**

Cloud Type	Solution	Analytic Tests per tran	Status
Public	Amazon Web Service	3	Production
Private	X86 servers	4	Prototype
Private	Linux on System z	8	Under Development
Private	IBM z/OS	10	Hypothesis

Why leverage the IBM Mainframe for Callsign?

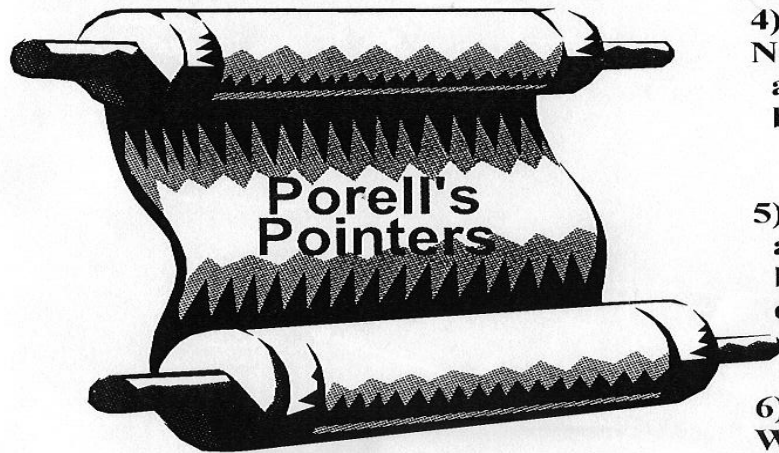
- **Cloud:** Each of the analytic functions occur as virtual image within same server
- **Latency:** Hardware memory used rather than network to dispatch functions, saving time
- **Scale:** CPU utilization enables 10,000's of simultaneous transactions
- Disaster Recovery and hot standby servers: part of mainframe architecture and reduced pricing terms and conditions
- **Transaction Programs:** When called from z/OS, proximity to Callsign will reduce latency and allow additional analytics
- **Improved Analytics:** Mainframe architecture enables near real-time analytics while sharing transactional data
- **Security:** The mainframes built in HSM, Digital Certificate processing and encryption on each core reduces overall operational risk
- **TCO:** Cloud deployment on System z will be less expensive compared to Public Cloud

Opportunities to reduce costs, risks & improve qualities of service

- Database Consolidation
- Move Applications to Data
- Deploy Firewall Appliance
- Enterprise Service Bus
- Application dev and test sandbox – z/OS, Linux , Windows
- Application consolidation
- Hybrid Cloud
- Distributed Tech refresh to “the cloud”
 - Application Migration offerings
- More Analytic Services
- Web services
- Key management (certs, application, CAC cards, biometric authentication)
- Case Management
- Content Management – find, tag and share your data
- Virtual Machine Management
- Secure VDI and BYOD support
- Mobile Device Management/Content Mgt
- Multi-level security
- Legacy Modernization – Simplify App Dev; Add Web services + mobile front ends

Most of these could be applied as a Virtual Appliance Model

*Yea, Verily, Although I
walk in a data center full
of servers, I shall know
no fear - for I have
Porell's Pointers to guide
and comfort me. . .*



- 1) Look for **TORTURED** data flows.
Reduce the number of data moves, copies, and transforms.
- 2) **CO - LOCATE** applications and data. Avoid distributed data.
 - a. Distributed data may be faster to prototype, but
 - b. Distributed applications will be cheaper to operate
 - Avoiding redundant security for data and applications
 - Reducing network bandwidth to move data
 - Reducing points of failure
 - Reducing two-phased commit complexity
- 3) Measure **END-TO-END**, not just one technology slice. Include performance, capital and **OPERATIONS** costs in measurement.
- 4) Understand benchmarks measure **CAPITAL** costs/tran of **NEW** systems.
 - a. They assume **NEW** system/ server **FOR EACH** application.
 - b. They don't include **LEGACY** costs used moving, copying or transforming data to **NEW** servers.
- 5) Consider **INCREMENTAL** growth opportunities.
 - a. How many servers is enough, day 1 to year 5?
 - b. How is growth satisfied, upgrade, replacement or migration?
 - c. What are the hardware, software and operations growth costs?
- 6) Consider **MULTIPLE** applications and databases being **WORKLOAD** managed in a server at reduced operational costs.

Executive Summary

- Provide a better understanding of the Shared Operations/Hybrid Model
- Have the Shared architecture direction pay for itself via savings achieved
 - Perform better
 - More secure, resilient and meeting all SLA's
 - Provide Investment protection for the future
- Identify tactical opportunities for Shared Ops
 - Stop the Proliferation of Data
 - Database Consolidation
 - Data Virtualization via Rocket Data Virtualization Server
- Identify Strategic opportunities
 - Legacy Conversion which includes modernization
- Address many Cyber security needs
- Identify and Evaluate risks of Silo-ed Operations going forward

Data center of the future – Shared Hybrid Operations



Global Business Responsibilities

- Governance
- Risk and Compliance
- Business Continuity
- Privacy
- Agility
- Lean and Green

Acknowledgements

- Gary Peskin - garyp@firstech.com - Extraordinary Java consultant
- George Thompson – IBM SWITA – fellow bounty hunter
- SWG Competitive Project Office – they produce Gold on System z
- Bryan Smith – CTO and VP of Rocket Software
bsmith@rocketsoftware.com
- Jeremy Wilson – Director, Forcepoint LLC
jeremy.wilson@forcepoint.com
- Zia Hayat – CEO, Callsign zia.hayat@callsign.com

