Enterprise Security Myths: Lessons Learned

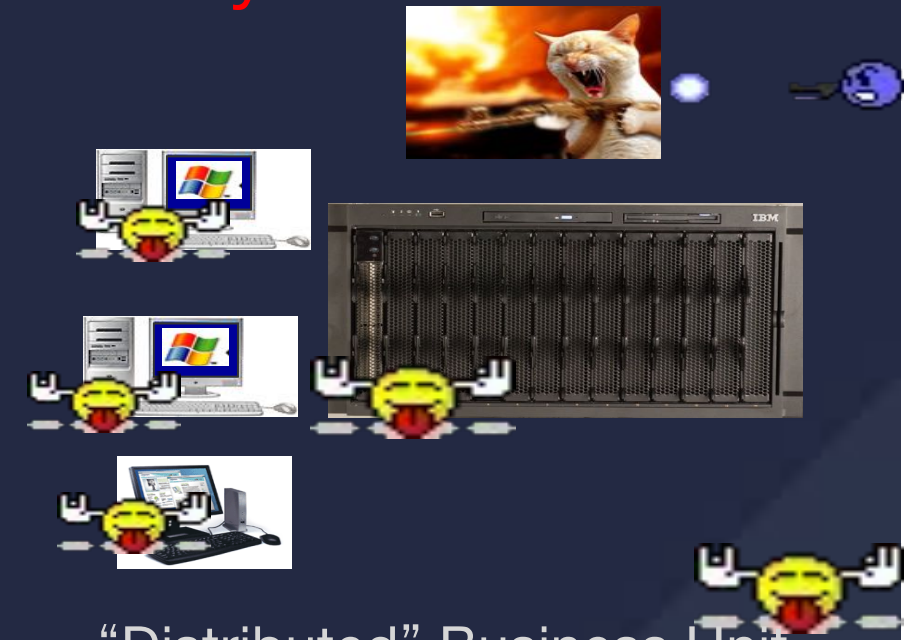
Jim Porell
Rocket Software

November 2019
Session FJ

IT Organization Wars – at a business near you?

"Distributed" Business Unit Architect and Operations

"Centralized" Glass House Operations



"Distributed" Business Unit Architects

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

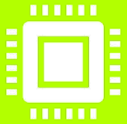
Myths – try not to propagate them

The mainframe has never been **hacked**

Not true. There has been a case where a poorly managed IT infrastructure was deployed that didn't keep software up to date for known system integrity issues and an outsider got in.

There are also cases where insiders have sabotaged the system. Is that a hack? Depends on the definition. It should be considered a **breach**

Could it have been prevented. Probably with some additional analytics deployed.



There have been several cases where PC's and mobile devices have been compromised.

From those devices, sign on to the mainframe was done and trusted.

That might not be a hack either, but results in data theft.

It can also be prevented.

Collaboration of IT operations across systems is critical to driving end to end security

What is Security from a customer view?

Security is not all about technology! ***It's really all about people.***

- Policy
- Corporate Directive
- Regulatory Compliance (e.g. HIPAA, Sarbanes-Oxley, GDPR)
- Technology (e.g. RACF, ACF2, TSS)
- Infrastructure (e.g. IBM, Vanguard, CA, 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)

Typically, it's not → a Solution

- **Leverage Security to make solutions better**

- Redundant
- Bureaucratic
- Too Sensitive
- Expensive
- Unresponsive
- Big Brother

- Many times implemented in silo's.
- Each server domain has its own security authority

Irrelevant facts – not myths, but not always helpful

The mainframe is hacker resistant with security built in.

That's true. However, security is about People, Process and Technology. The best technology can easily be circumvented by poor processes, human error and insider theft.

Security is also only as good as the weakest link. The weakest link is typically the end user device which is usually a PC or mobile device.

If that device is not secure or compromised, then all systems that the device accesses can be compromised as well.

Collaboration of IT operations across systems is critical to driving end to end security

Why should I care?

What's at risk?

- Disclosure of sensitive data
- Service interruption
- Corruption of operational data
- Fraud and ID Theft
- Theft of services

What's at stake?

- Customer trust
- Reputation and Brand
- Privacy
- Integrity of Information
- Legal and Regulatory Action
- Competitive Advantage

Breach cost?

- Research and recovery
- Notify customers
- Lost customer business
- Problem remediation
- Claims from trusted vendors and business partners

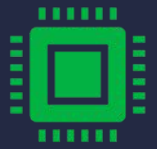
$$ Damage to brand image

The Facts – new era of computing: Digital Transformation

Myth: 80% of mission critical data is on a mainframe

Reality – it's on x86/RISC too, because they made a copy.

- We will never get to a single instance of data. However, z can be leveraged to reduce the number of instances of data and in doing so, assist to simplify governance and data protection.



Customers require "integrity" based computing

System z's can now host the same code as other platforms (e.g. Java, J2EE, C/C++)

However, z's architecture can greatly change the operational model

- Business Resilience, Security, Storage Mgt, Business Process Integration, Workload and Capacity Mgt
- System z delivers with it's holistic design and deployment of Middleware, Database, Operating Systems, Firmware, Hardware, Storage and Networks

Operational Risk is now a Real Time requirement, not a post processing exercise.

System z makes you safer by enabling real time access to SHARED mission critical data, while meeting service levels and reducing the complexity of data moves, data protection and regulatory governance.

- Where do those costs appear in a benchmark?

Throw away your traditional spreadsheets for benchmarking Nextgen costs

System z specialty engines and operational characteristics change an application's acquisition costs, upgrade costs and operations costs in ways that other server environments have yet to comprehend.

Real Customer Problem

- Store uses WEP wireless for Point of Sale devices
- POS processes cards with banks
- Common password on all store systems
- Security patches not applied to store systems
- Hacker plugs in and gets copies of all transactions
- Problem detected and store systems are getting fixed.
- Mainframe folks are happy they are bullet proof
- **Hypothesis: Mainframe could help secure stores if they use good procedures**
- Store managers run inventory transactions to mainframe
- No encryption on sign in
- No audit records analyzed

REAL WORLD CUSTOMER PROBLEMS

Our Goal is to look at security management across these domains

That problem could never happen at my business

- **Wrong** – this problem can occur anywhere there is a change in security administrative control

The weakest link in an enterprise is typically the end user interface

- Virus, worms, Trojan Horses enable someone to hijack the end user interface
- In turn, that hijacked desktop can be used to log into any other server
  - Is it "really the authorized end user"? Perhaps not.
    - That's a large risk to a business.

Outsourcers and mainframe IT operations have SLA's that protect the data they host on their systems.

Do their customers and end users have SLA's that specify minimum desktop security? Do they manage Desktops and mainframes together?

- Typically not – as a result, there is a major risk that a compromised end user interface can result in compromised mainframe access.

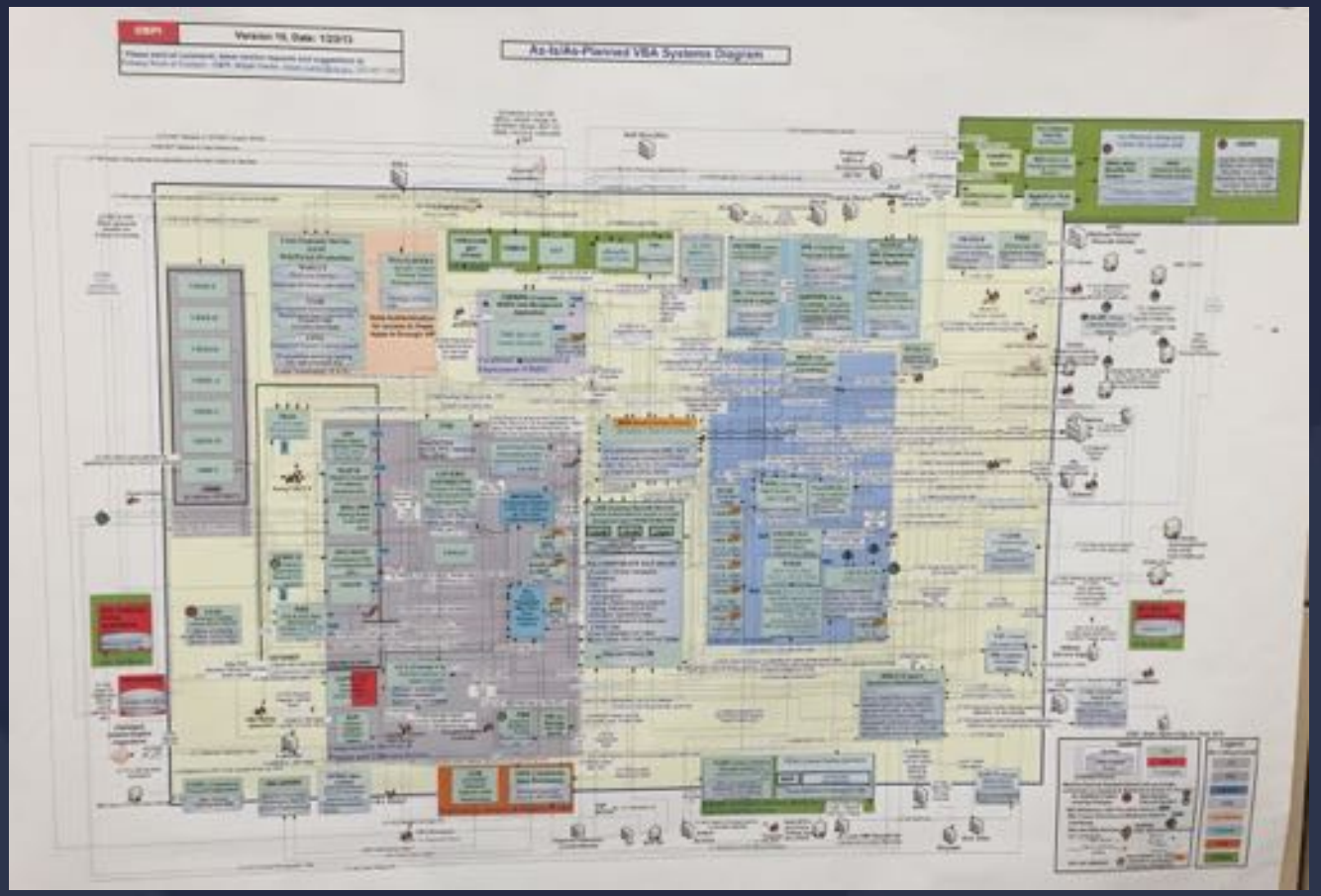
Examples of End to End Security

- Mainframe Userid and Password Encryption
- MultiFactor Authentication
- Virtual Private Network encryption (which exploits the zIIP)
- Audit and anomaly detection
- Fraud Forensics, Analysis and Prevention
- LAN encryption via WPA2 which exploits z/OS PKI
- z/OS PKI deployment
- PKI management
- Data encryption

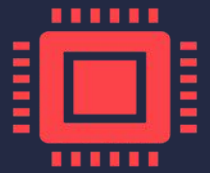
Typical mistakes companies make in protection…

- 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



Operational Models influence cost



Intrusion Prevention

Deploy IT architectures that inhibit viruses, malware and other attacks

It has a known cost of deployment and can be budgeted

It can be augmented with Forensics and Analytic Detection

Intrusion Detection

Let's you identify problems on your IT infrastructure

What you don't know can hurt you, for example:

- How long was the problem present?
- What was stolen or sabotaged?
- How many sales were lost or blocked?

Cost of a breach is unbounded. A business will spend to:

- "Fix" the problem, usually by adding more IT infrastructure
- Defend it's brand reputation

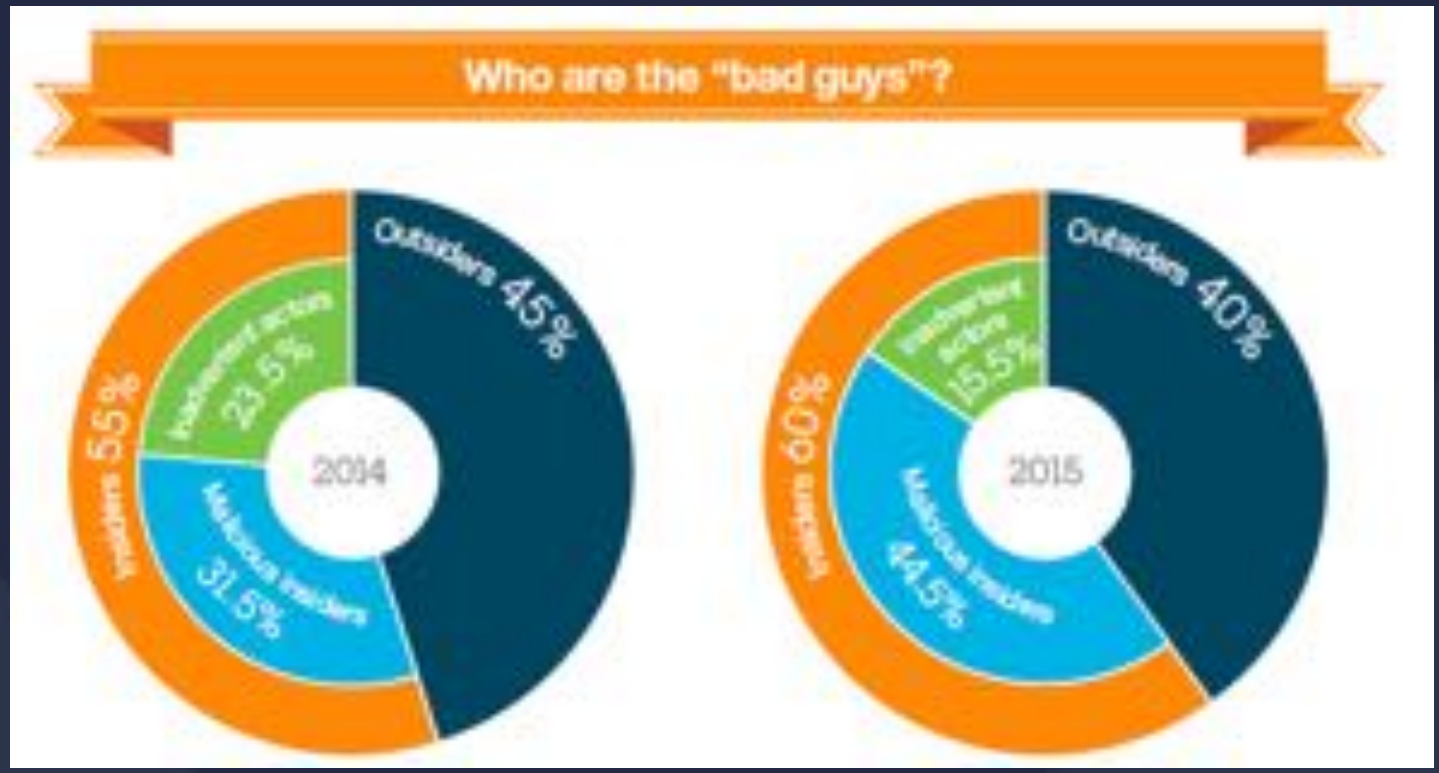
An ounce of Prevention is better than a pound of Detection

Not all insider threats are created equal

Who represents an insider threat?

- An inadvertent actor
- A malicious employee
- A 3rd party/partner with access to sensitive data

  (And falls into one of the categories above)



Employees with privileged access to sensitive data carry the greatest risks!

Image Source: IBM X-Force Research 2016 Cyber Security Intelligence Index

Target User Personas for MFA

- **Employees that work with personally identifiable info**
- Human Resources
- Healthcare workers
- Law Clerks
- DMV Clerks

- **Employees that have authority over managing money**
- Brokers, Traders, Analysts
- Tellers
- Payroll
- Credit Card Processing

- **Users that have knowledge of Corporate Intellectual Property**
- Executives
- Engineers

- **Business Partners that access YOUR data**
- Agents – Travel, Insurance
- Contract organization – Outsourcers

- **Users managing key IT assets**
- Systems Programmers
- Security Administrators
- Database Admins, Developers

Target personas for IBM MFA include anyone with access to data a client would *not want released to the public*

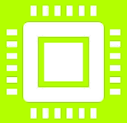
The Trust model requires Hybrid solutions

Who initiates a transaction and where, has changed.

Employee → Agent → Consumer → Device → ??

User Authentication must combat fraud

Userid/Password → Card Swipe → Chip/PIN → Two Factor Authentication with inanimate object → Multi Factor Authentication using biometrics and other Insight



Authentication call out from System of Record

Engagement: Point of Sale/ATM/VPN/Desktop/Mobile

Record: Calls out to MFA service for authentication

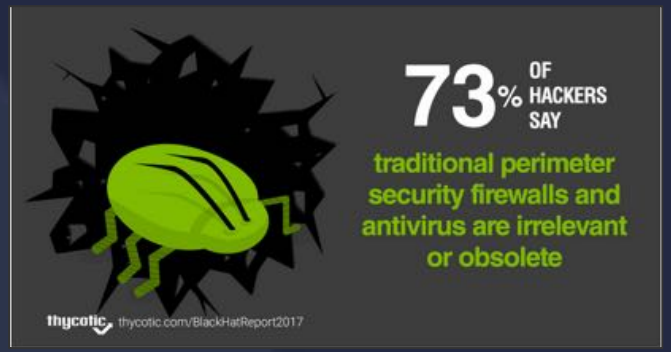
Insight: Is object/phone cloned? Is this really that person?

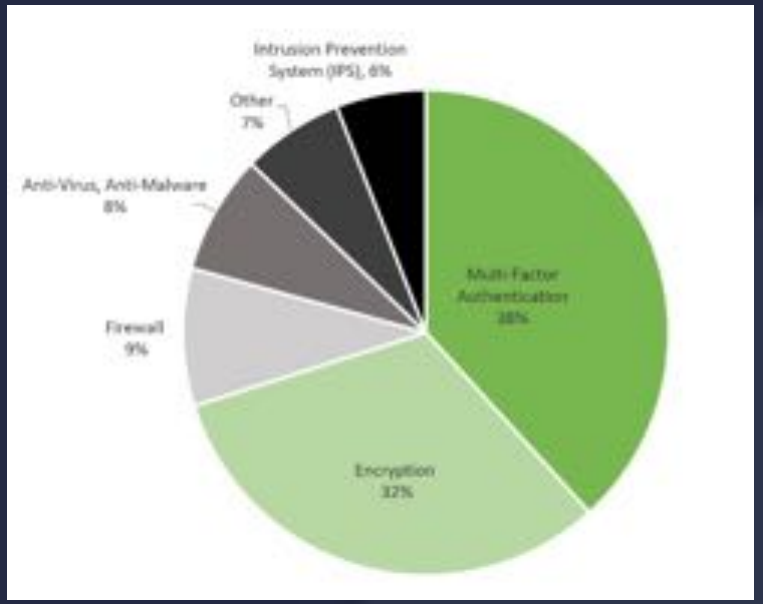
Consistency of Authentication across Engagement systems is critical to driving end to end security

Black Hat 2017 Hacker Survey Report[1]

QUESTION: What type of security is the hardest to get past?

68% say multi-factor authentication and encryption are biggest hacker obstacles





The majority of known data breaches on the mainframe are linked to a compromised password.

[1] thycotic Black Hat 2017 Hacker Survey Report
https://thycotic.com/resources/black-hat-2017-survey/

Trust model must be consistent across All Systems

Suppose a business adopts a new policy:

Multi Factor Authentication for mobile and/or desktop

Sign on to PC / Mobile / VPN requires call out to MFA

That user then goes to web page with malware

- A key logger gets installed prior to any "detection"

User signs on to "System of Record" with userid/password

- Those credentials are now stolen by key logger
- An insider theft occurs via unlocked device while user is out

What prevents the thief from signing on to the system of Record?

Better policy: Replace Userid/PW with MFA

Sign on to PC / Mobile / VPN requires call out to MFA

Subsequent human sign on to System of Record requires call out to MFA

Screen saver time out requires call out to MFA

New *Insight:* Cross system audit log showing user sign on behaviors

Consistency of Authentication across All systems is critical to driving end to end security

What works with IBM MFA?

IBM Z MFA supports a wide range of authentication systems!**

In-Band

Proprietary Protocol: RSA

RADIUS Based Factors: IBM, yubico, Microsoft Azure, gemalto security to be free, DUO, RSA, callsign, ONE IDENTITY, Symantec. VIP, okta, VASCO TRUST FOR THE DIGITAL WORLD

TOTP Support: IBM, IBM, Google, FreeOTP Open Authentication, DUO Mobile, AUTHY, RAPIDIDENTITY™ OTP with RapidIdentity Mobile App

Out-of-Band

Certificate Authentication:  , 


Password/Passphrase: RACF Password/Passphrase can be used in conjunction with all in-band authentication methods.

Disclaimer: Not everything above has been fully tested, but they *should* work, if not we will investigate.

**Not an all-inclusive list

Irrelevant facts – not myths, but not always helpful

All Data should be consolidated to a Master platform so there is a single version of truth

Fact: There will never be a single copy of data.

- There will be backup, read only and disaster recovery copies

Flow chart your data. The fewer copies of data, the better

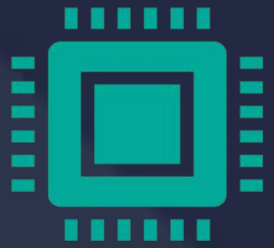
- Applications should be moved to data. Data shouldn't be moved to applications.

Each copy of data must be managed for privacy and access control at the same policy level, regardless of where the data is deployed. Policies need enforcement.

Test data and application data should never be the same as production data because their policies are not managed

Collaboration of IT operations across systems is critical to driving end to end privacy and security policy management of data.

Data Privacy Policy must be consistent across Systems



Data resides in many places

Systems of Record

- Transactional systems (memory, disk – local and network)
- Backups (tape, optical, disk, network)
- Cluster and DR copies
- Read only copies
- Test and Development

Systems of Insight and Engagement

- Physically on system or on Mobile or Laptop device (e.g. Spreadsheet)

Authentication, Access Control, Confidentiality and Audit should be consistent where ever it occurs

Physical security is not sufficient

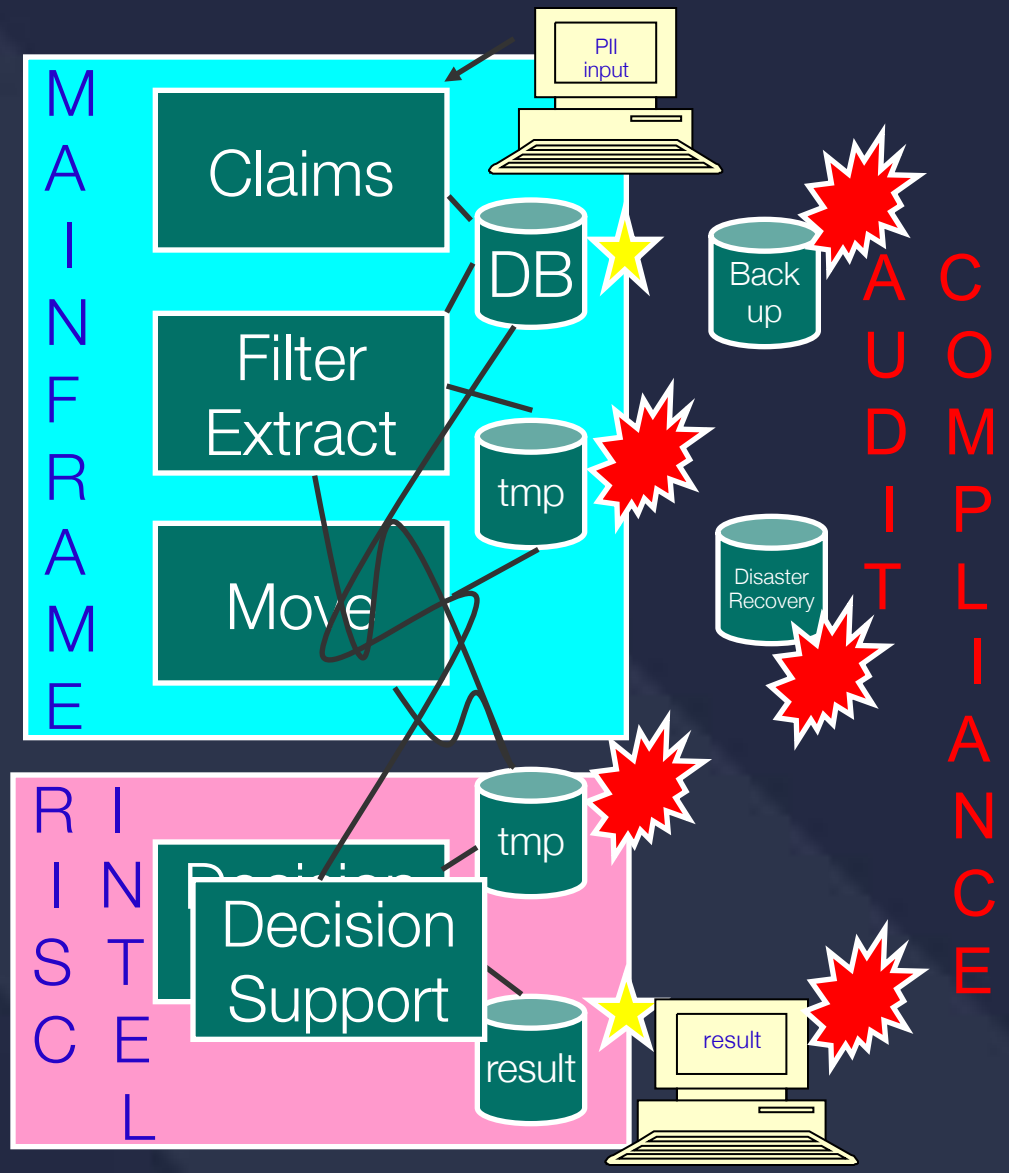
Reduce the number of copies by sharing across applications/systems

- New ***Insight***: logs identify how/when/where/who referenced data. Anomalies?

Leverage data masking tools to anonymize data for test & development

Consistency of Privacy Policy across systems is critical to driving end to end security

Why does Infrastructure simplification matter? HIPAA, Sarbanes-Oxley, GDPR

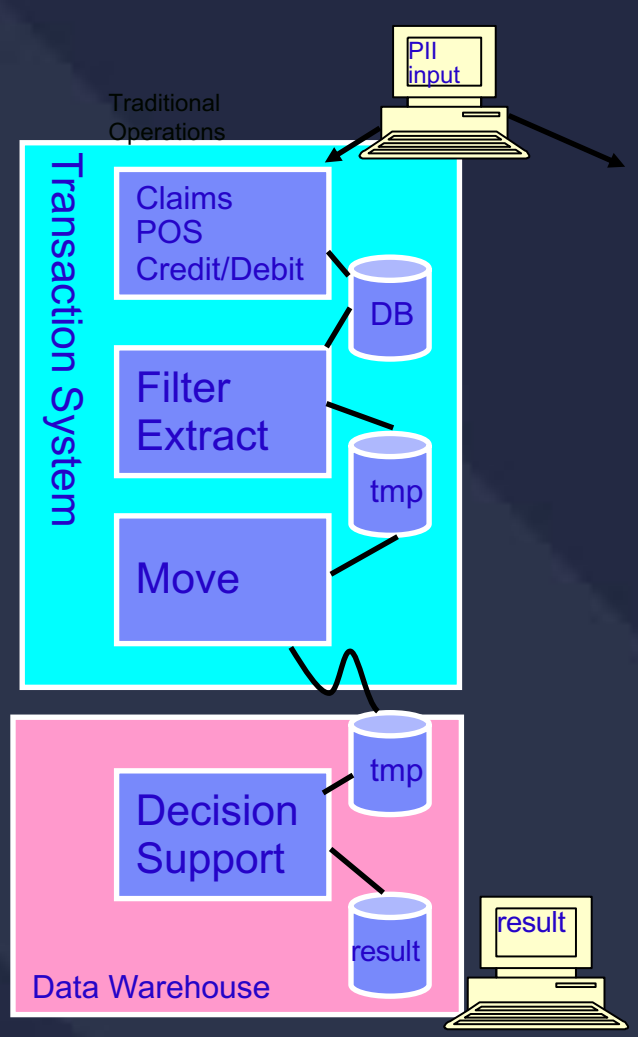


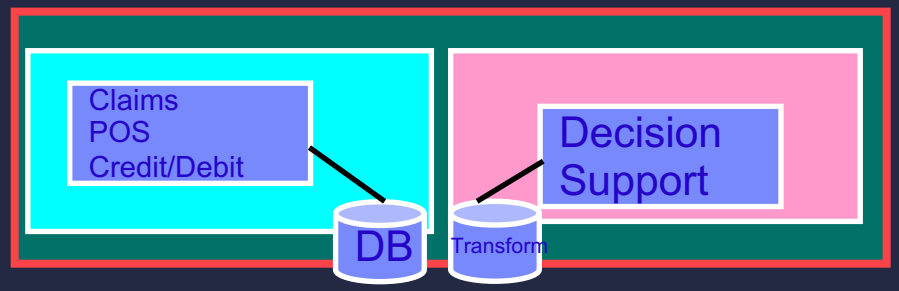
Typical Business Workflow

- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate
- Policies are not.
  - Reducing the copies will reduce compliance efforts and increase resiliency
    - Leverage a file server to delete copies and reduce data movement
    - Application data proximity
      - Move the applications back to the data source, where practical
      - Plus, able to use WebSphere SOA access facilities, where practical

System z: The Data Vault

Comparing shared data between Record and Insight





Business Problem

Data warehouse can detect trends, but not necessarily prevent fraud or upgrade transactions in real time because data is copied in bulk or batch mode

Direct sharing of data can foster **Insight instead of Hindsight**

- Data is copied in nanoseconds instead of hours or days
- Opens up opportunities for real time analytics
  - Preventing fraud
  - Making business analytic decisions faster
- Improves performance and lowers cost
  - If the ETL model is used for Fraud, the network call out for Insight will add latency and reduce the overall number of transactions that can be run.
- Boosts overall query performance n times
- Customers see a reduction in storage utilization
- Supports in-memory column store for parallel star schema queries
- Uses column-based compression to minimize storage needs
- Provides capability to perform both transactional (OLTP) and warehousing (OLAP) type of queries in the same database management system

Sharing Data can improve Insight

Unshared data assumes some form of Extract Transfer Load (ETL) to another system

There is typically a delay (window) between updates to the System of Record and ETL to the System of Engagement

- Tracking a package delivery may not require real time access
- Preventing a fraudulent transaction does require real time access

Using ETL likely results in additional copies of the data

- Temporary disk storage, network transfers, tape/optical (old school)
- These copies require the same Privacy Policy as the source

Time lags and non-managed backups are what criminals seek

Shared data has demonstrated improvements in the time to Insight

Up to 2000x faster

System of Record calls out to Insight for fraud analysis to Prevent theft/access

Significant cost and operational benefits as well

Sharing Data across systems is critical to reducing risks and costs

How far will you go to protect data?

- Guardium STAP installed for audit
- Breach discovered, use the audit records
- Nothing conclusive found
- Were all records collected?
- What should be done for next time?

Production Database

Guardium STAP

Test Database

No Audit
Guardium STAP?

Development Database

No Audit
Guardium STAP?

Business Intelligence Database

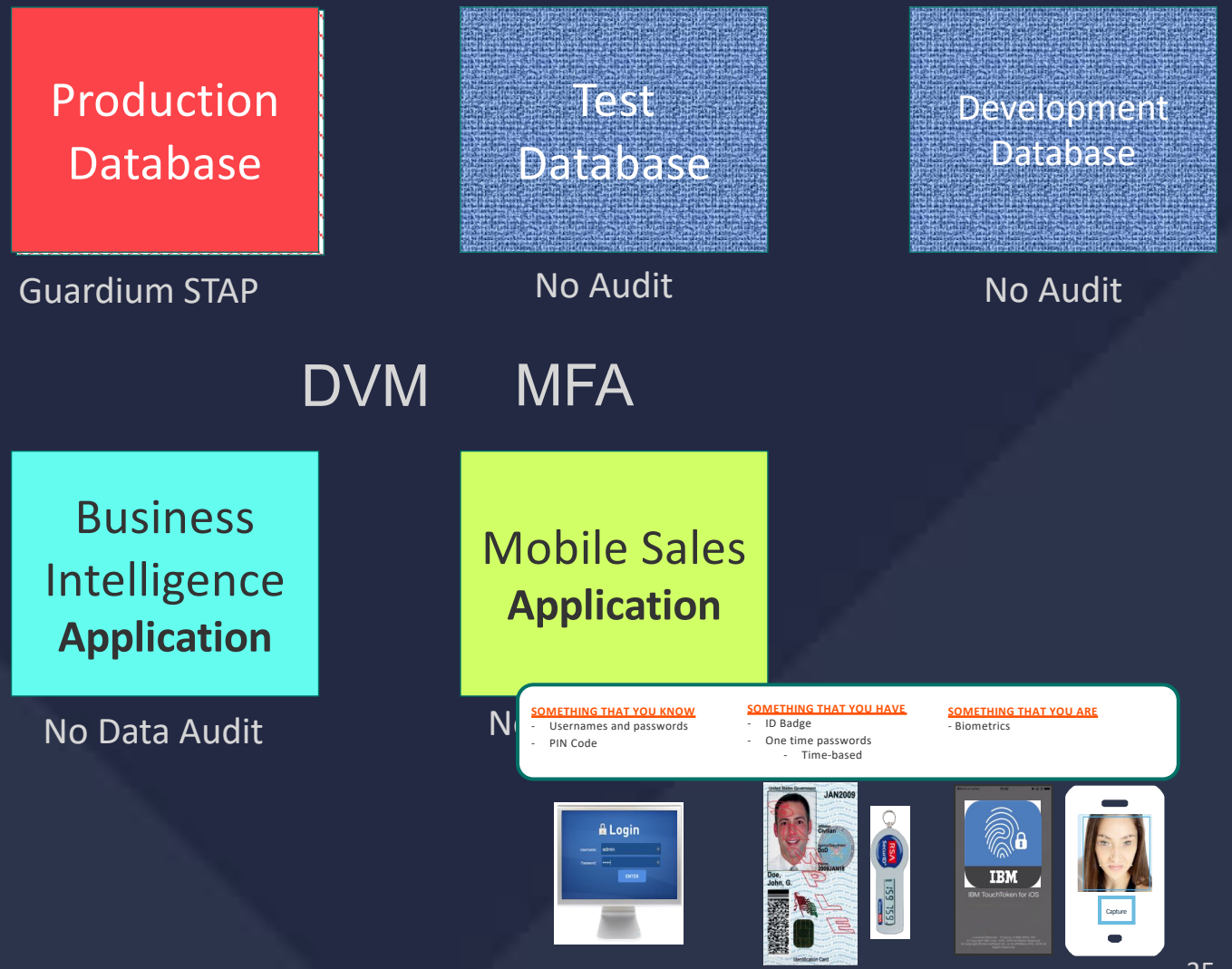
No Audit
Guardium STAP?

Mobile Sales Database

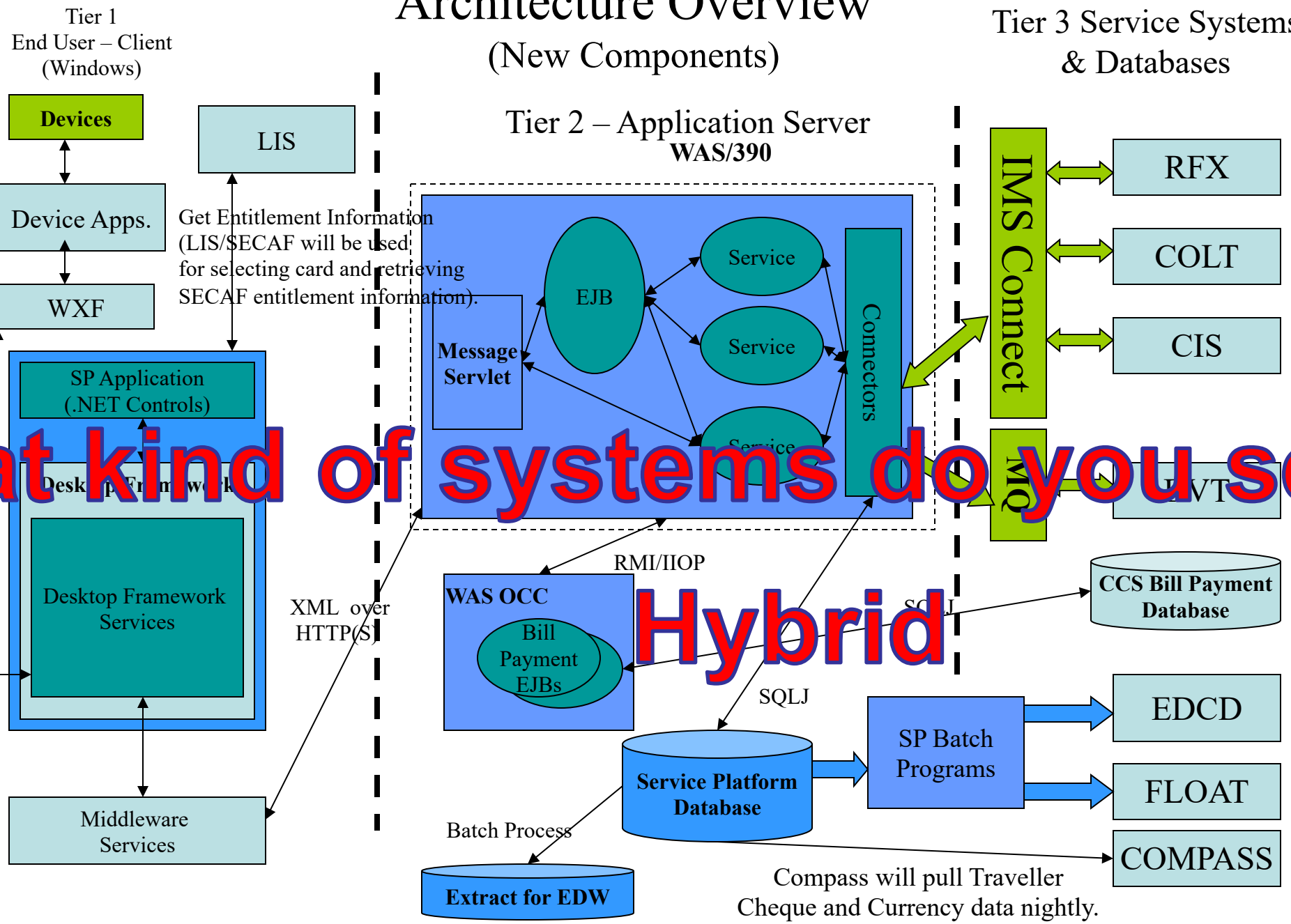
No Audit
Guardium STAP?

A better approach to protect and manage data

- Use Cloning tools with anonymization or Data Masking
  - Data modified. No need to audit
- Leverage DVM to access Data in real time
  - Applications access data now, not servers
  - Audit is done at base data
- Use MFA to authenticate to all systems
- Encrypt source data
- **Result: Fewer audit control points, improved security, lower operations cost**



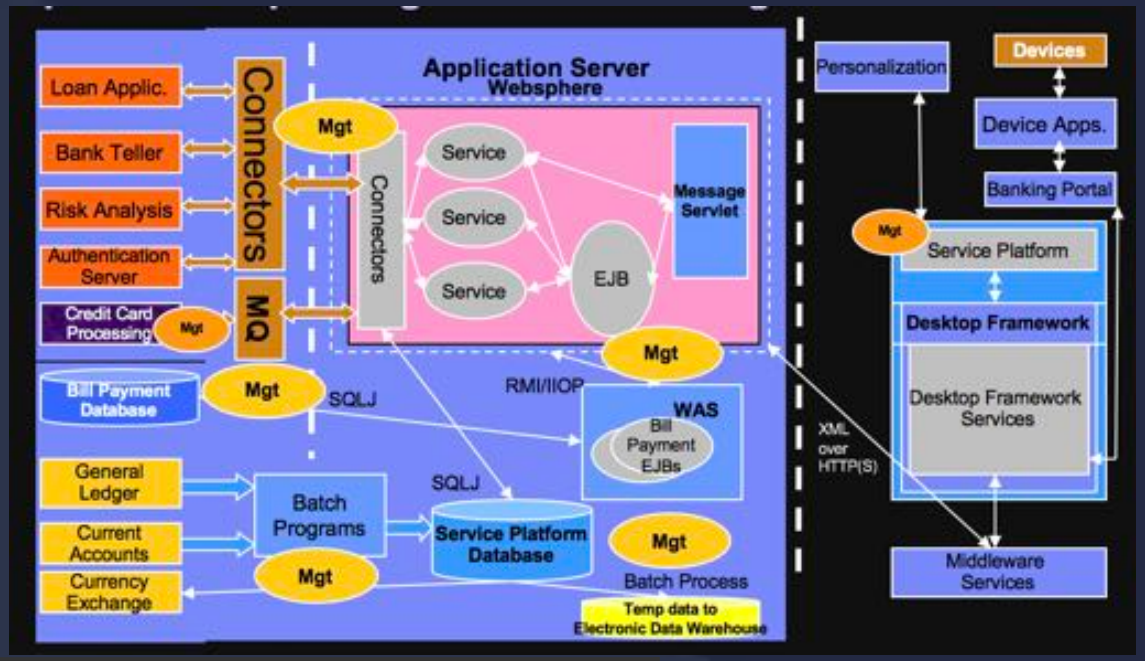
Architecture Overview
(New Components)



What kind of systems do you see?

Hybrid

MAINFRAME CO-LOCATION: AN OPERATIONAL ADVANTAGE OVER DISTRIBUTED



It's the very same programming model in a different container that provides a superior operations model

Washington Systems Center Benchmark

Processing Cycles

11.3 ms CPU for Distributed

3.64 ms CPU for System z (76% Fewer Cycles)

Data Movement

54.4 KB Data for Distributed

.5 KB Data for System z (99% Less Data Traffic)

Results Will Vary

Management Considerations for an enterprise	
Authentication	Network Bandwidth
Alert processing	Encryption of data
Firewalls	Audit Records/Reports
Virtual Private Networks	Provisioning Users/Work
Disaster Recovery plans	Data Transformations
Storage Management	Application Deployment
How does the Virtualization Manager improve these?	

Potential advantages of consolidating your application and data serving

Security	Fewer points of intrusion	With Linux
Resilience	Fewer Points of Failure	With Linux
Performance	Avoid Network Latency	With Linux
Operations	Fewer parts to manage	With Linux
Environmentals	Less Hardware	With Linux
Capacity Management	On Demand additions/deletions	With Linux
Utilization	Efficient use of resources	All z/OS
Scalability	Batch and Transaction Processing	All z/OS
Auditability	Consistent identity	All z/OS
Simplification	Problem Determination/diagnosis	All z/OS
Transaction Integrity	Automatic recovery/rollback	All z/OS

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

Highlighted in this color have built in security value

Z/OS ENCRYPTION READINESS TOOL (ZERT)

a core capability of **IBM Z pervasive encryption**, is an important feature of z/OS V2R3 Communications Server.

zERT provides intelligent network security **discovery** and **reporting** capabilities by monitoring TCP and Enterprise Extender traffic for TLS/SSL, IPsec and SSH protection, as well as cleartext. It also writes information about the state of that protection to new SMF 119 records. Moreover, **IBM zERT Network Analyzer**, a new **web-based interface** that IBM plans to make available in the future, will help you determine which z/OS TCP and Enterprise Extender traffic is or isn't protected according to specific query criteria.

Go run this tool…Find out what is clear text or encrypted on your networks!

https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.halg001/nfsrgvhzert23.htm

MYTHS – TRY NOT TO PROPAGATE THEM

Everything can be consolidated to run on System z

Not True: No Mobile or Desktop Systems run on the mainframe

The terms **Consolidation** and **Centralization** need to evolve:

Mainframe "advocates" would use them to direct physical consolidation of other architectures onto System z

- In some camps, this makes mainframe IT orgs the "enemy" of distributed organizations

Instead, the term should apply to **Operations**.

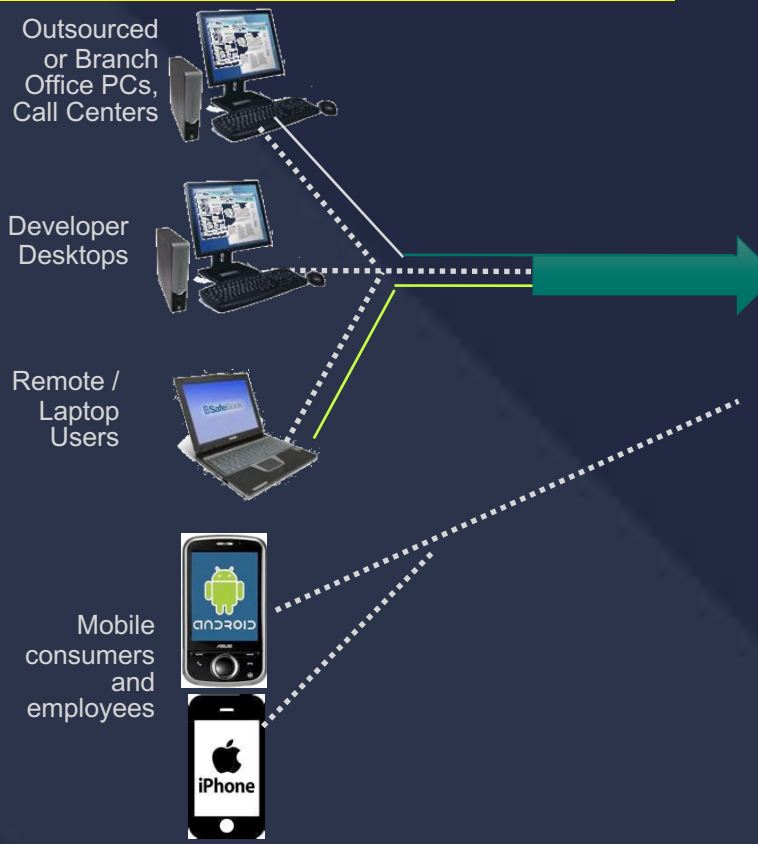
- A sharing of policies and IT resources for end to end solution value
- Leverage the best of each server technology
- The Integration of Systems of Engagement, Record and Insight

Collaboration of IT operations across systems is critical

Will the End to End solution be protected and resilient?

Systems of Engagement

Theft
Loss
Virus
Trojan Horse
Misuse



Systems of Record
Systems of Insight

Shared Storage

Data may be at risk.

Are you managing end to end?

Rocket IBM

Mobile and Desktop share operational characteristics

Security

Device

- BYOD, Secure e-mail, Document sharing

Content

- Secure sharing across devices and between employees

Application Deployment

- Instrument applications with security protection
- Identify vulnerabilities in new, existing and purchased apps

Transaction

- Provide secure hosting for consumers, partners and suppliers

Engagements

Differing users (consumer, partner, supplier), similar operations

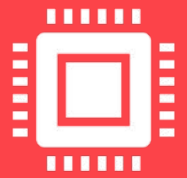
Insight

Correlate mobile and desktop events across broader end to end workload to identify vulnerabilities and anomalies

Systems of Engagement should share Insight with other Systems to reduce cost and risk

IRRELEVANT FACTS – NOT MYTHS, BUT NOT ALWAYS HELPFUL

The mainframe is 99.999% available and fault tolerant/fault avoidant.
The z = zero down time



That's true. However, if the web app front end, mobile, desktop or network are down and the mainframe can't be accessed, it doesn't matter.

As a result, availability of "solutions" should be measured and managed end to end. A business should deploy across IT architecture that will minimize down time and costs.

Collaboration of IT operations across systems is critical to driving end to end availability

SUMMARY OF IT ARCHITECTURE DISCUSSION

Different IT Deployments can have the same code with different operations models and costs

Centralizing/consolidation of operations has game changing value for IT solutions

Performance – reduce latency and improve scale
Security – Improve Trust and Fraud prevention
Business Resilience – end to end fault avoidance
Shared Skills – reduced labor, faster learning curve
Cost – lower Total Cost of Ownership, Cost of Acquisition, Cost of Upgrade

Integrating Systems of Engagement, Record and Insight can solve problems not possible before

Fraud prevention, location aware marketing, new channels

Share data – improves Privacy Policy, reduces costs

Virtualize Enterprise Mobile and Desktop operations

Simplifies BYOD

Protects against and prevents data leakage

Reduces help desk costs by 90%

Opportunities to reduce costs, risks & improve qualities of service

- Database Consolidation
- Data Virtualization
  - Move Applications to Data
- Deploy Firewall Appliance
- 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
- Multifactor Authentication
- Legacy Modernization – Simplify App Dev; Add Web services + mobile front ends

Many 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.

Security on System z: Reducing risk for the Enterprise

Basic Insurance Policy: $100,000 Liability

Rider: Excess replacement for valuable items

Rider: Excess medical coverage

Rider: Unlimited vehicle towing

Rider: Excess liability insurance $3,000,000

Basic Security: System z RACF

Data Encryption services
Enterprise Key Management

Identity Management

Compliance Reporting

Fraud Prevention, Forensics and Analytics

Executive Summary

- Provide a better understanding of the Shared Operations/Hybrid Cloud 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
  - Data Virtualization
  - Secure Authentication via Multifactor Authentication
- Identify Strategic opportunities
  - Legacy Conversion which includes modernization
- Address many Cyber security needs
- Identify and Evaluate risks of Silo-ed Operations going forward

- Hybrid means Collaboration
  - Customers across IT Server domains – Cloud and Non-cloud
  - Customers across disciplines
  - Sellers across brands
  - Sellers with IP Partners
- Consistency across organizations - skills, operations
- There are many opportunities available to provide customer value
  - Rocket can help IBM identify and assist in winning these opportunities

Data center of the future – Shared Hybrid Operations

Global Business Responsibilities

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

Please submit your session feedback!

- Do it online at http://conferences.gse.org.uk/2019/feedback/FJ

- This session is FJ