Rocket

Security in a Modern Mainframe Database

Jim Porell
Director, Solutions Advisors
Rocket Software
jporell@rocketsoftware.com

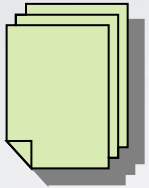
Goals for this presentation

- Really focuses on ideas more than products
- In particular, how the IT architecture is “strung together”, end to end, can dramatically change the operational characteristics.
- This presentation will give some examples of alternative deployment models.

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 mgt

Identity Management

Compliance Reporting

Fraud Prevention, Forensics and Analytics

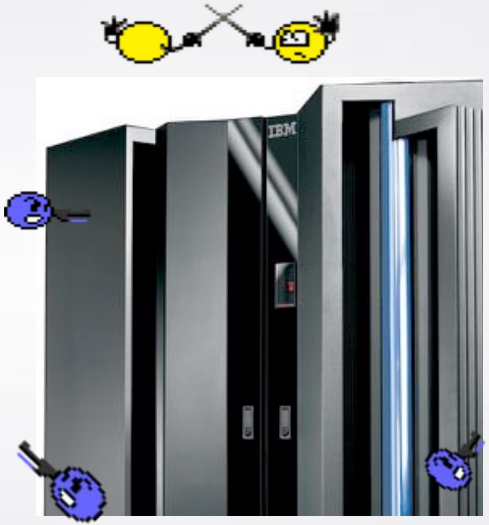
Rocket

- System z is the most secure platform in the world

- Why do we need to do anything extra for security?

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)

Rocket

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

Rocket

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

Rocket

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

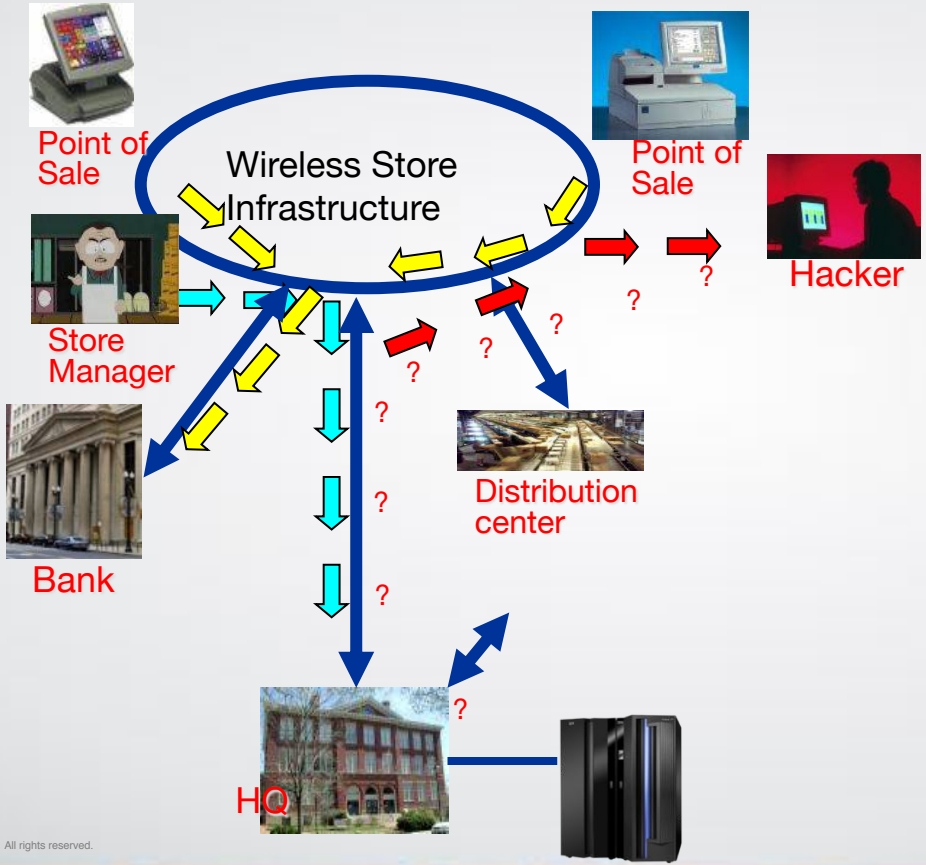
- Myth: 80% of mission critical data is on a mainframe
  - Reality – it's on x86/RISC too, because they made a copy.
    - We will never get to a single instance of data. However, z can be leveraged to reduce the number of instances of data and in doing so, assist to simplify governance and data protection.

- 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, 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

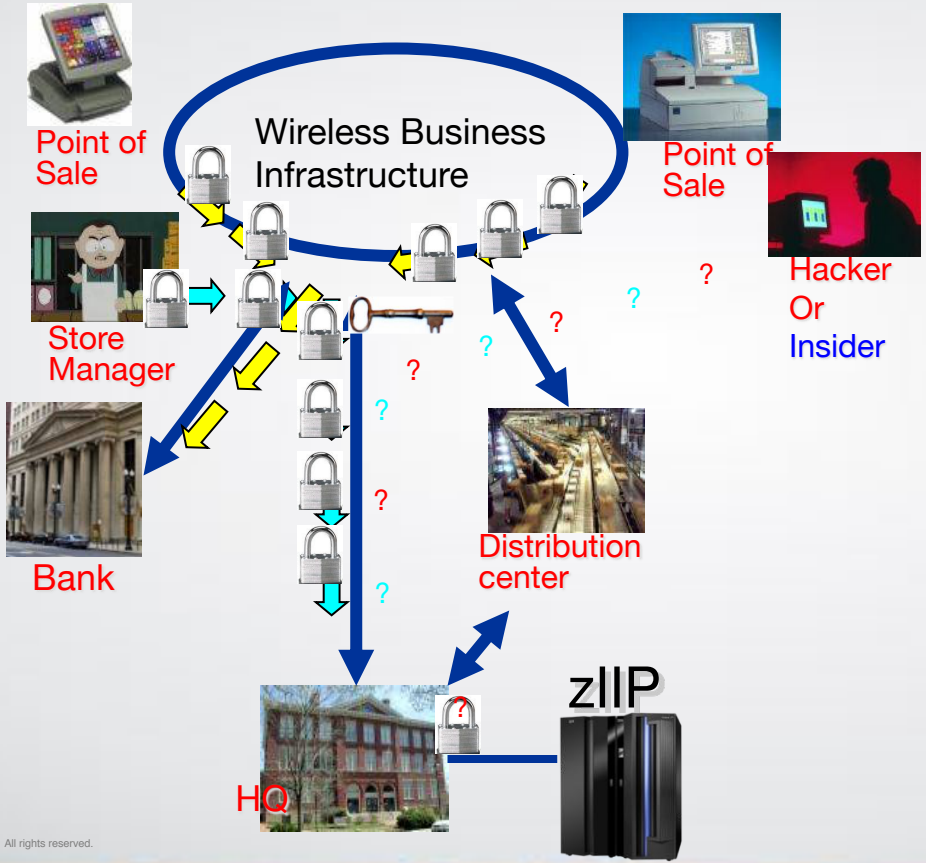
Rocket

Real World Customer Problems

- 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
  - Viruses, 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.
- Our Goal is to look at security management across these domains

Rocket

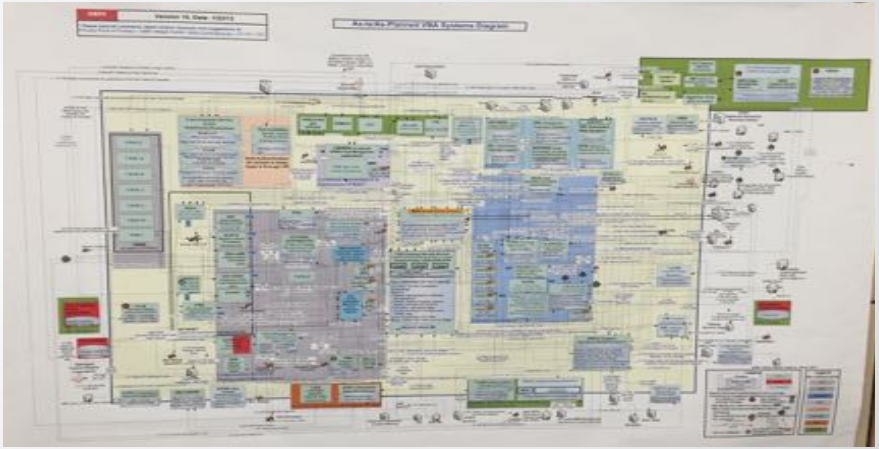
Examples of End to End Security



- 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

The Trust model requires Hybrid solutions

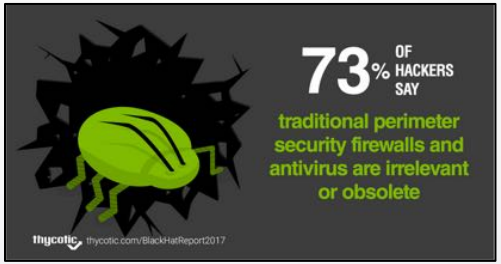
- Who initiates a transaction and where, has changed.
  - Employee → Agent → Consumer → Device → ??
- User Authentication must combat fraud
  - Userid/Password → Card Swipe → Chip/PIN → Two Factor Authentication with inanimate object → Multi Factor Authentication using biometrics and other Insight
- 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?

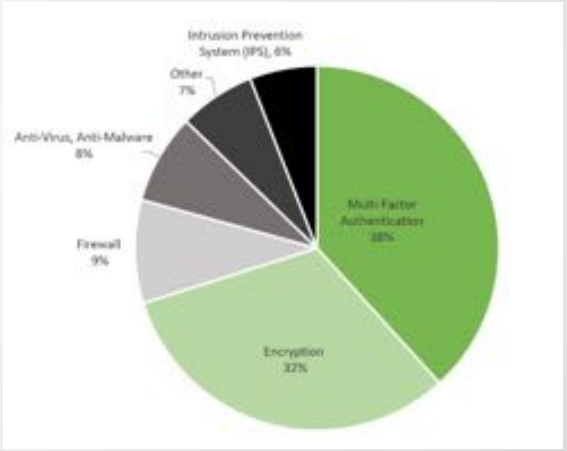
Consistency of Authentication across Engagement systems is critical to driving end to end security

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





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

17

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

IBM Multi-Factor Authentication for z/OS

Higher assurance authentication for IBM z/OS systems that use RACF

IBM Multi-Factor Authentication on z/OS provides a way to raise the assurance level of z/OS, applications, and hosting environments by extending RACF to authenticate users with multiple factors.

Fast, flexible, deeply integrated, easy to deploy, easy to manage, and easy to use
PCI-DSS *Achieve regulatory compliance, reduce risk to critical applications and data*
Architecture supports multiple third-party authentication systems at the same time

Rocket

Who should be protected with MFA?

- Work with Personally Identifiable Information
  - Human Resources
  - Healthcare workers
  - Law Clerks
  - DMV Clerks
- Authority over managing money
  - Brokers, Traders, Analysts
  - Tellers
  - Payroll
  - Credit Card Processing
- Knowledge of Corporate Intellectual Property
  - Executives
  - Engineers
- Business Partners – access YOUR data
  - Agents – Travel, Insurance
  - Contract organization - Outsourcers
- Those managing key IT assets
  - Systems Programmers
  - Security Administrators
  - Database Admins, Developers

Anyone with access to data that you don't want released to the public!!

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

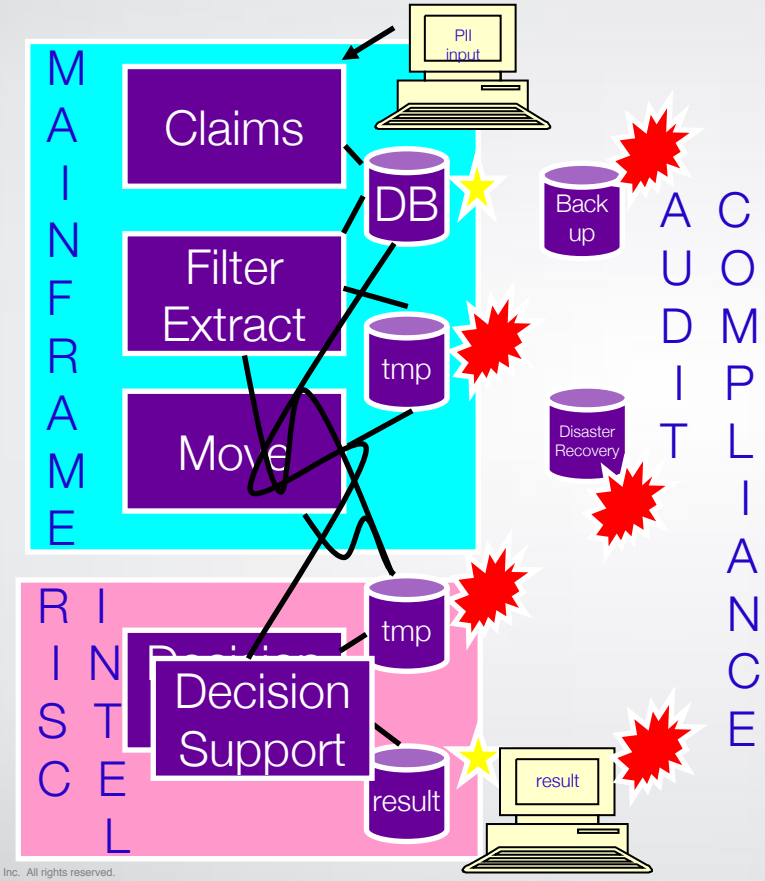
  - **Collaboration of IT operations across systems is critical** to driving end to end privacy and security policy management of data.

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



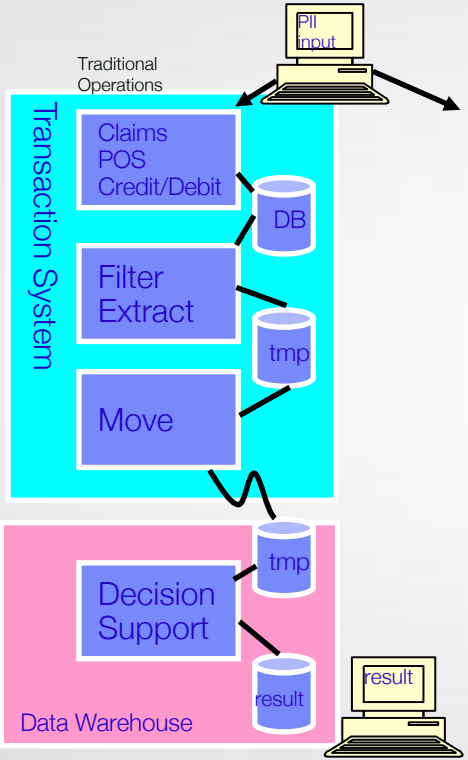
Typical Business Workflow

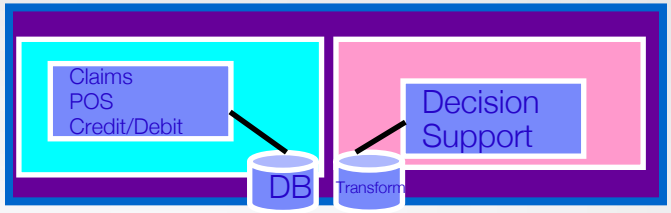
- Do you audit all places with Personally Identifiable Information?
  - Is the process automated?
- Data is easy to replicate
- Policies are not.
  - Reducing the copies will reduce compliance efforts and increase resiliency
    - Leverage a file server to delete copies and reduce data movement
    - 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

Rocket

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

Rocket

Optimizing access to all enterprise data

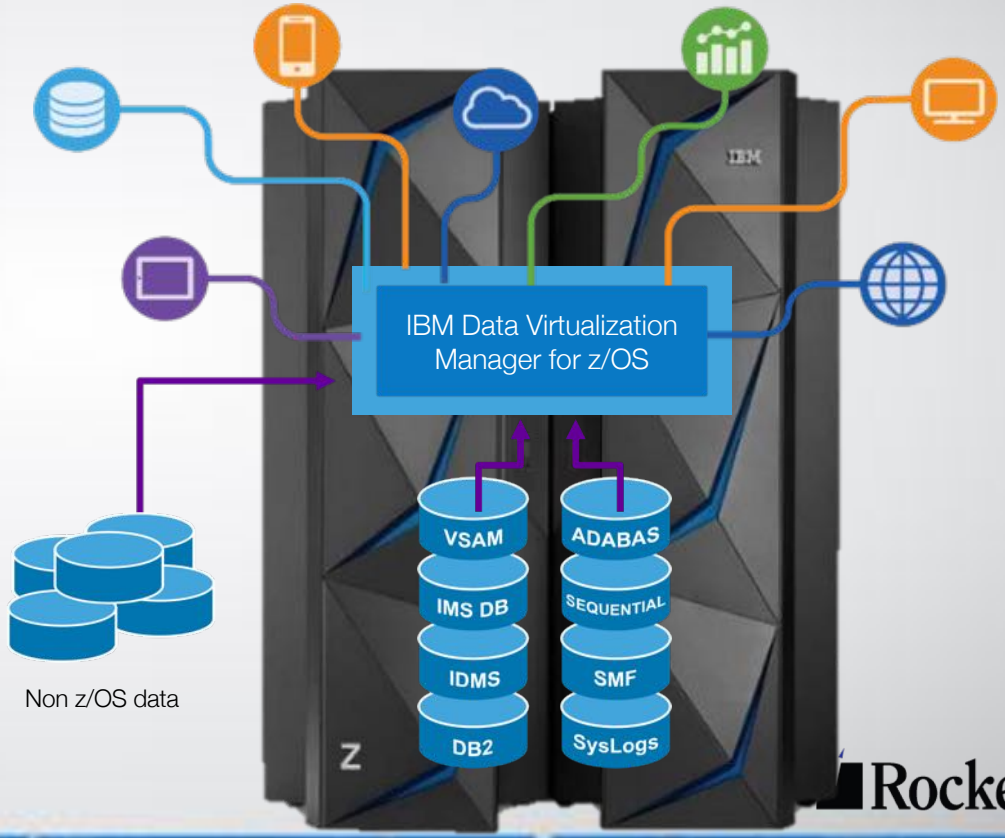
Simple
Get transactional access, no data movement

Open to all Apps
Modern APIs enable access

Secure
Avoid risk by reducing moving data off Z Systems

Fast
Exploits Z architecture, including parallelism and in-memory processing

Cost Effective
Keeps Z costs down with up to 99% zIIP offload



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?

Guardium STAP

No Audit
Guardium STAP?

No Audit
Guardium STAP?

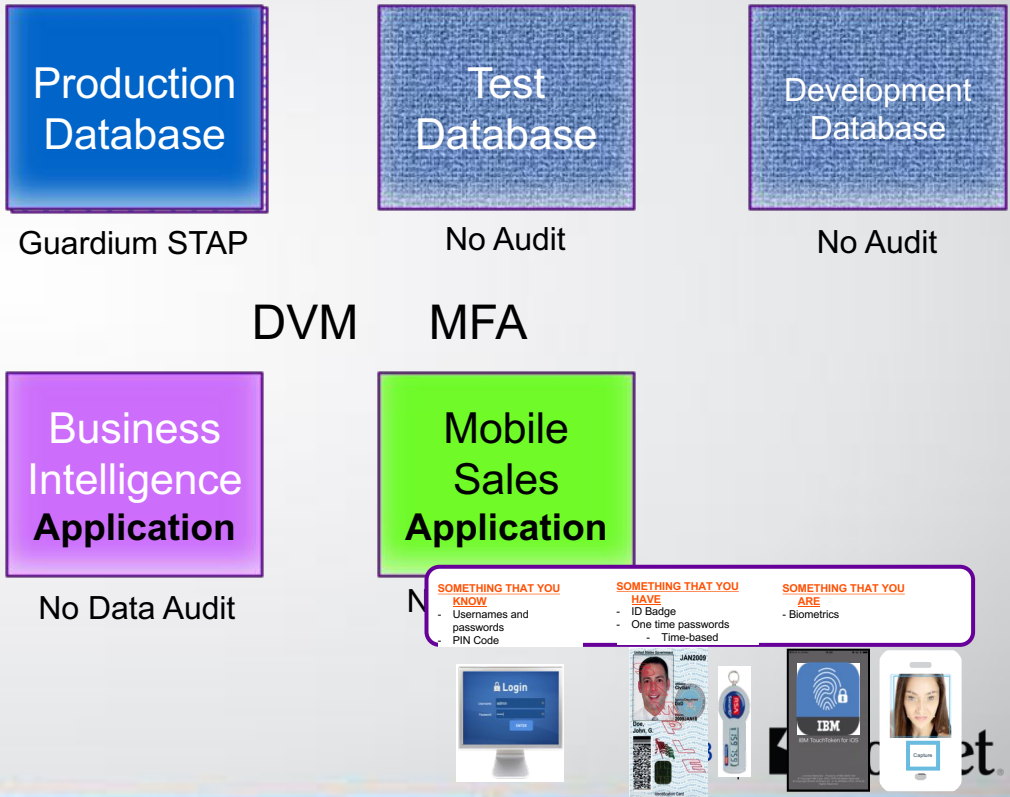
No Audit
Guardium STAP?

No Audit
Guardium STAP?

Rocket

A better approach to protect and manage data

- Use Cloning tools with anonymization or Optim 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



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

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

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?

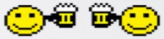
6) Consider MULTIPLE applications and databases being WORKLOAD managed in a server at reduced operational costs.

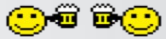
Rocket

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
  - 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

Data center of the future – Shared Hybrid Operations





Global Business Responsibilities

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

Rocket

IT'S NOT ROCKET SCIENCE.

IT'S ROCKET SOFTWARE.