Rocket

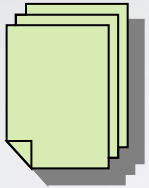
MFA for z/OS as viewed from Mainframe Myths:

Lessons Learned

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

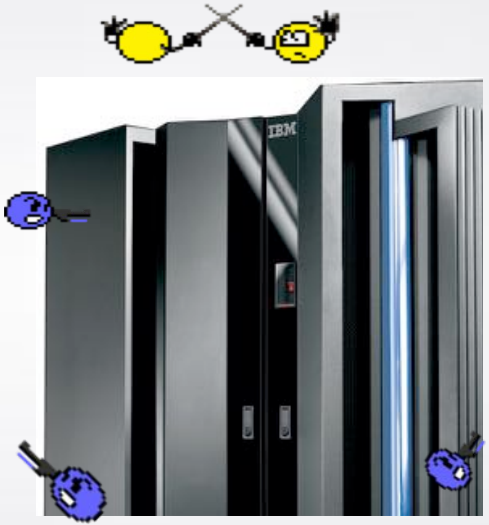
Compliance Reporting

Fraud Prevention, Forensics and Analytics

Rocket

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

Rocket

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

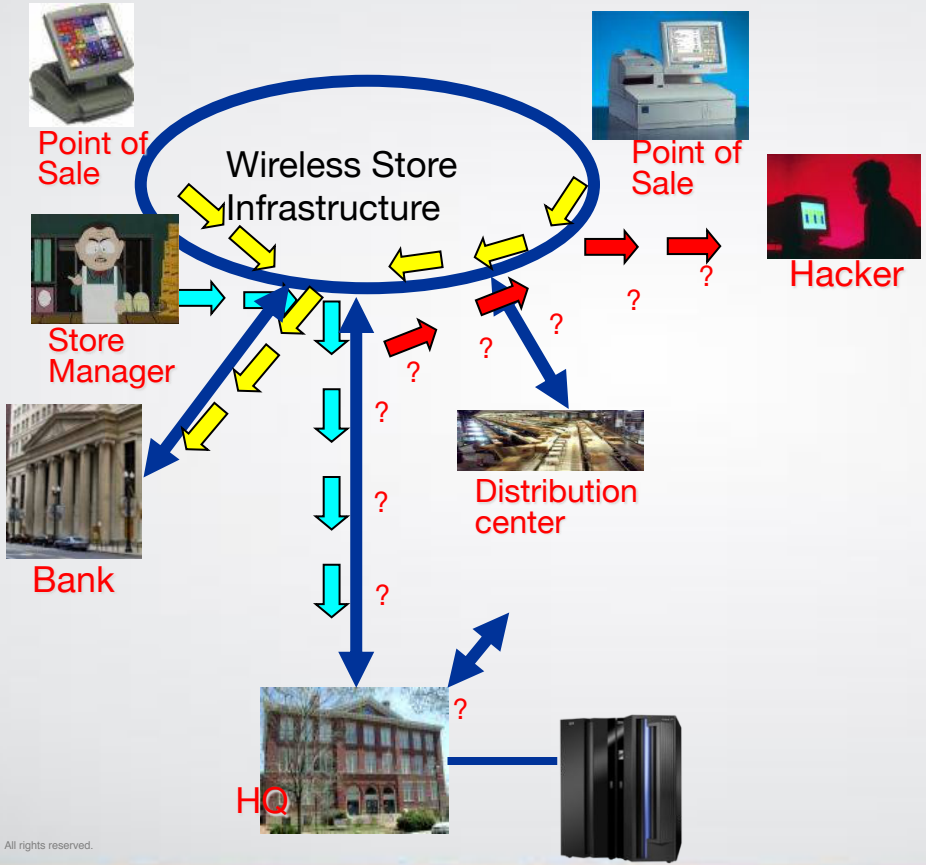
Breach cost?

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

$$ Damage to brand image

Rocket

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

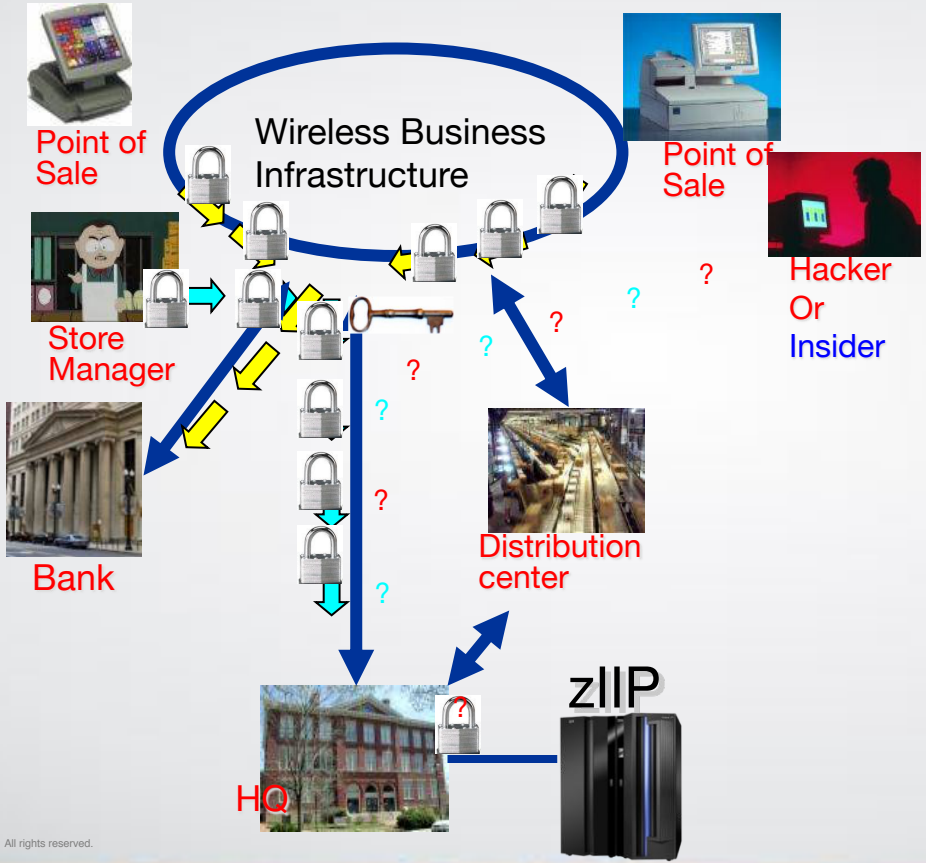
Rocket

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

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

Myths – try not to propagate them

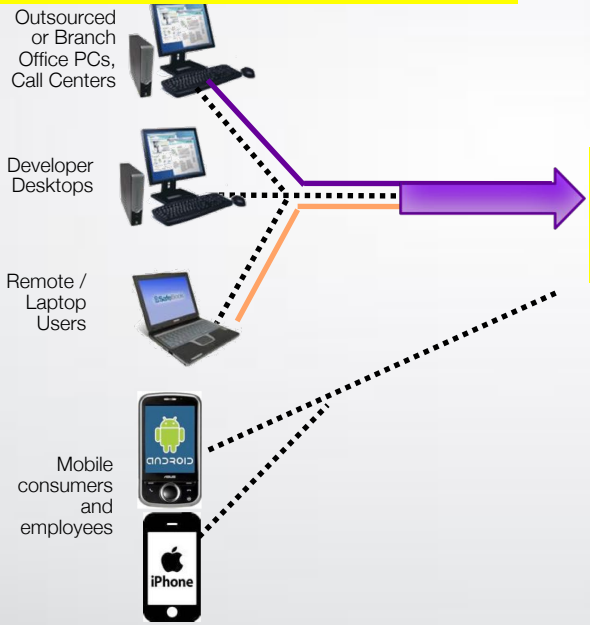
- Everything can be consolidated to run on System z
  - Not True: No Mobile or Desktop Systems run on the mainframe
  - The terms **Consolidation** and **Centralization** need to evolve:
    - Mainframe “advocates” would use them to direct physical consolidation of other architectures onto System z
      - 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

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

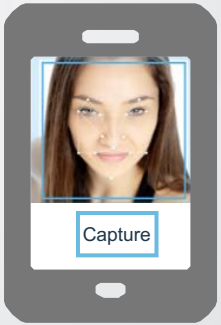
Systems of Engagement should share Insight with other Systems to reduce cost and risk

What is multi-factor authentication?

SOMETHING THAT YOU KNOW
- Usernames and passwords
- PIN Code

SOMETHING THAT YOU HAVE
- ID Badge
- One time passwords
  - Time-based

SOMETHING THAT YOU ARE
- Biometrics



Rocket

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?

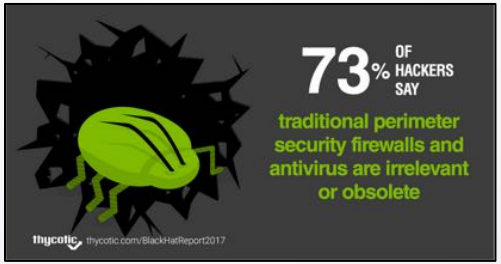
- Better policy: Replace Userid/PW with MFA
  - Sign on to PC / Mobile / VPN requires call out to MFA
  - Subsequent human sign on to System of Record requires call out to MFA
  - Screen saver time out requires call out to MFA
  - New *Insight:* Cross system audit log showing user sign on behaviors

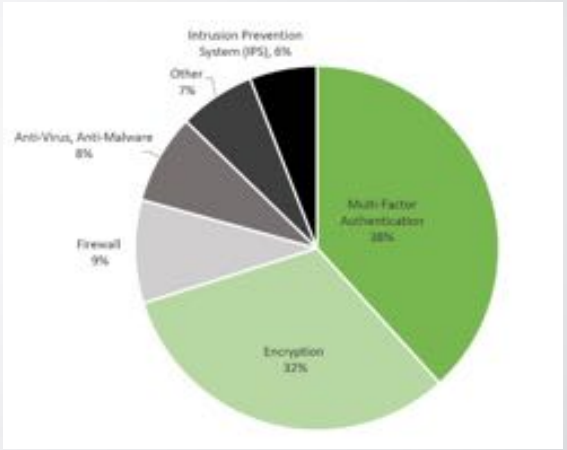
Consistency of Authentication across All systems is critical to driving end to end security

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/

Rocket

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

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!!

Example

- Callsign Virtual Appliance
-
- The Callsign Virtual Appliance should run on most hypervisors but only run our QA regressions tests on VMWare ESXi/vSphere for the moment. We do support RADIUS PAP out of the box.
-
- I have enabled your Callsign to access our developers' website which offers the VA documentation: https://developers.callsign.com/virtual-appliance-configuration/. We also have RADIUS guides here: https://developers.callsign.com/connect/radius/integration/ and here: https://developers.callsign.com/connect/radius/connector/.
-

What works with IBM MFA?

IBM MFA for z/OS supports a wide range of authentication systems!**

In-Band

Proprietary Protocol: RSA

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

TOTP Support: IBM, Google, FreeOTP, 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

Rocket

RACF Support

- RACF's MFA support introduces extensions to a variety of components of RACF
  - User related commands
    - Allow the provisioning and definition of the acceptable MFA tokens for a user
  - Extensions to authentication processing
    - Allows supported tokens to be used by any z/OS application
  - Extensions to SAF programming interfaces
    - Provides a new SAF service for IBM MFA allowing access to MFA data stored in the RACF database
  - Auditing extensions
    - Tracks that MFA was used during the authentication process for a given user
  - Utilities
    - RACF Database unload non-sensitive fields added to the RACF database used by MFA processing
    - SMF Unload – unloads additional relocate sections added to SMF records

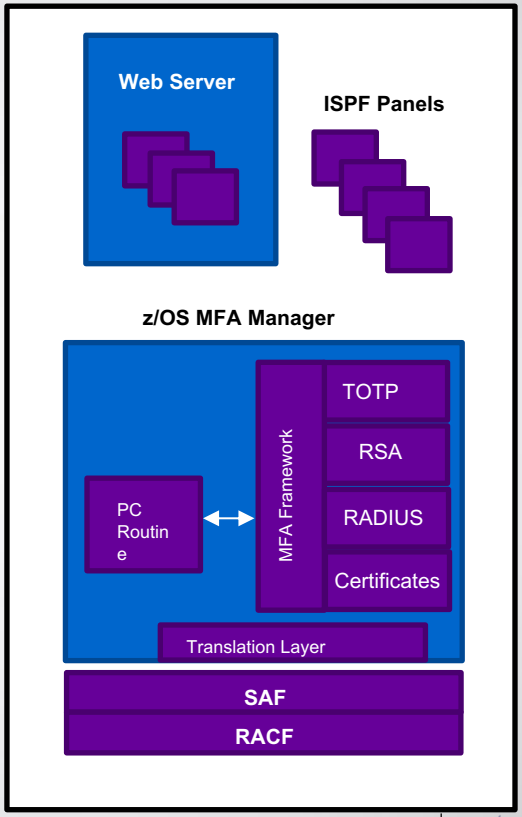
Rocket

22

IBM Multi-Factor Authentication for z/OS

- MFA ISPF panels for configuration and management of authentication tokens
- MFA Web Interface
  - User Interface supports factors such as Smart Cards and serves as web interface for registration – depending on factor type
- MFA Manager Services
  - Provides MFA main logic
  - Register MFA Factor Data for a z/OS user
  - Validates a user provided factor against RACF MFA Data
  - Accesses MFA Data via SAF/RACF via callable services

Runs completely on z/OS!!!



Rocket

What if something doesn't work?

Some applications have authentication properties which can prevent MFA from working properly:

- No phrase support – Some MFA credentials are longer than 8 characters
- Replay of passwords – Some MFA credentials are different at every logon and can't be replayed

IBM MFA for z/OS was architected with this in mind and provides a variety of accommodation mechanisms.

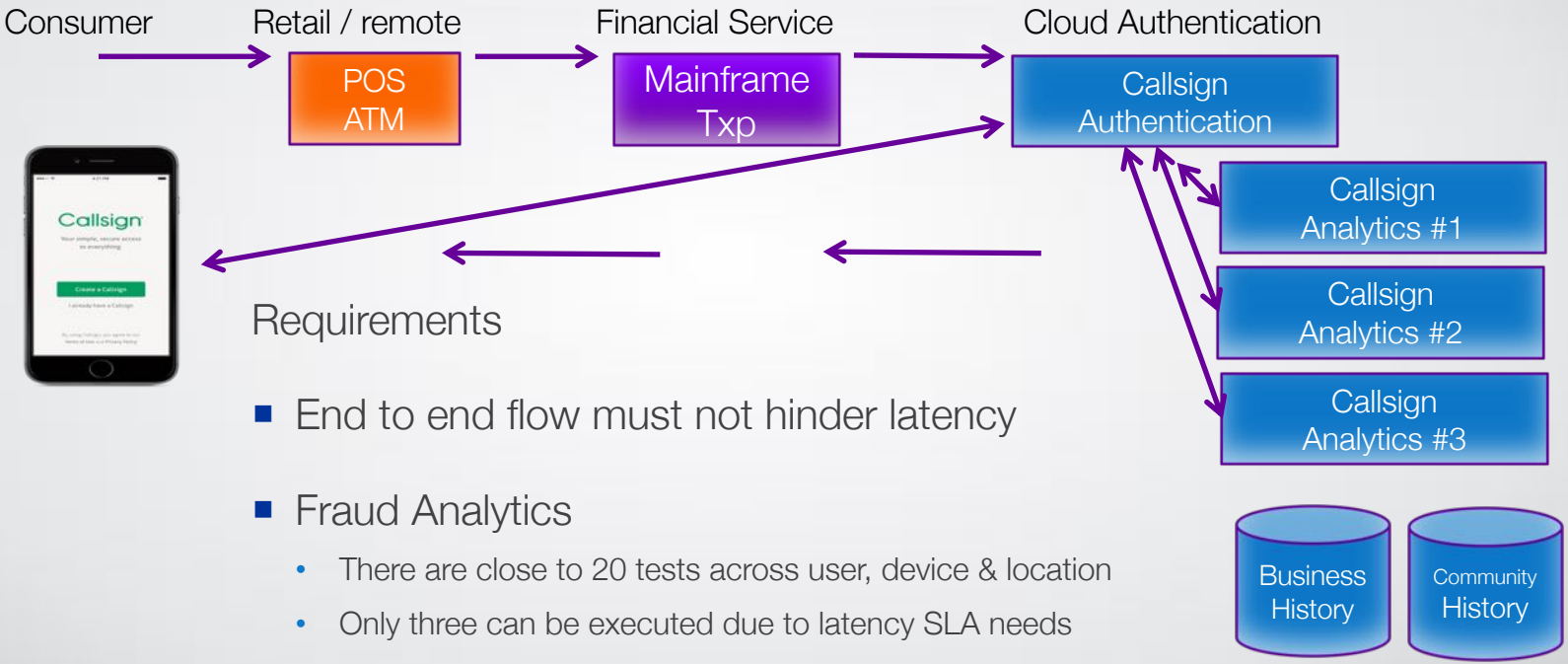
1. Selective Application Exclusion
   - Exempting MFA processing for certain applications:
     - Allows a Security Administrator to mark certain applications as excluded from MFA
     - Allows a user to logon to that application using their non-MFA credentials

2. PassTicket Support
   - Allows the Security Administrator to indicate that an MFA user can authenticate with a PassTicket instead of an ACTIVE MFA factor. New special MFA PassTicket Factor

3. Out-of-Band Support
   - Allows users to authenticate with multiple factors directly to IBM MFA and receive a logon token
   - The pre-authentication logon tokens behavior can be customized as needed
     - Controls to allow tokens to be single use or re-useable and how long a token is valid

Access **from** the Mainframe

Public or Private X86 Cloud Implementation



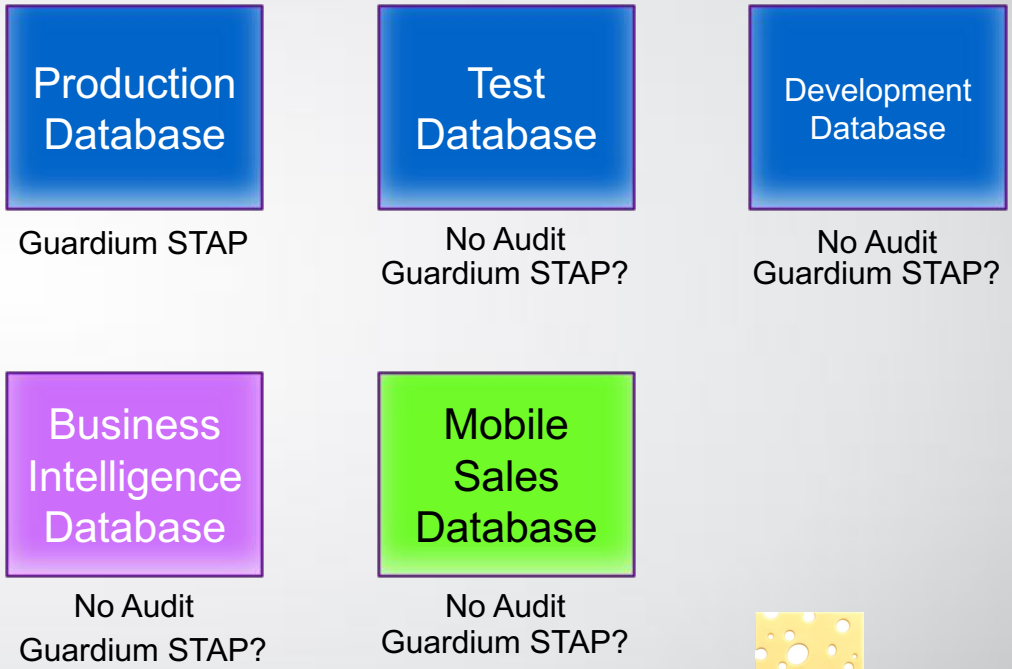
Requirements

- End to end flow must not hinder latency
- Fraud Analytics
  - There are close to 20 tests across user, device & location
  - Only three can be executed due to latency SLA needs

Rocket

How far will you go to protect data?

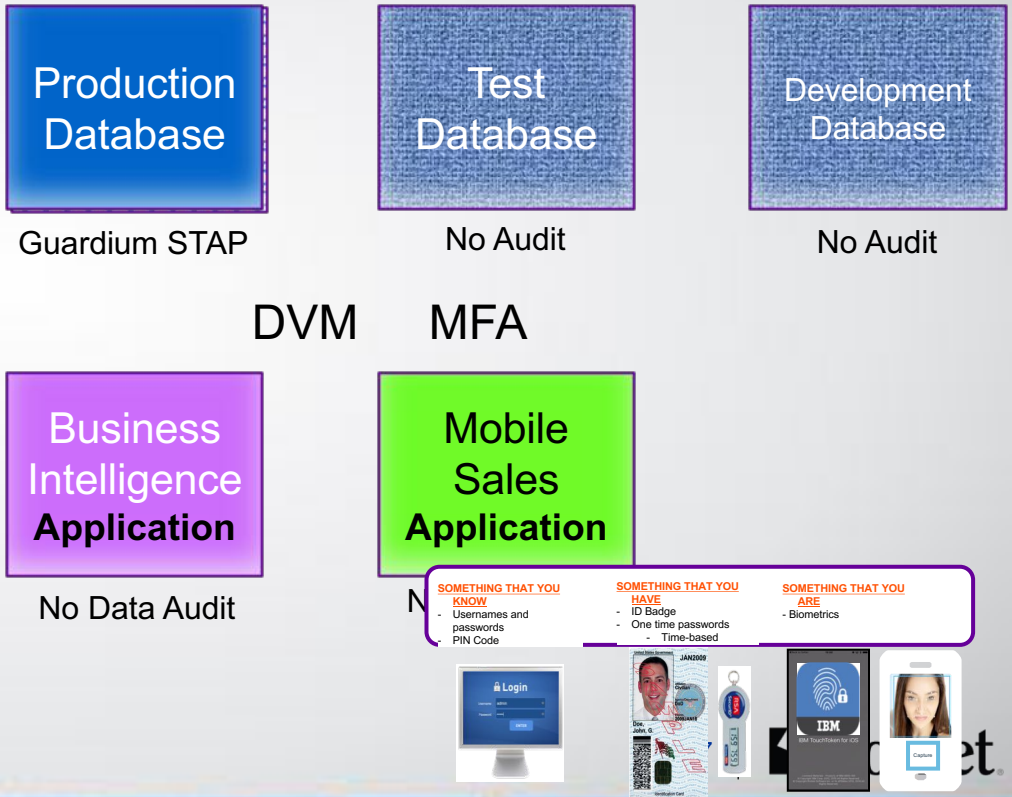
- Guardium STAP installed for audit
- Breach discovered, use the audit records
- Nothing conclusive found
- Were all records collected?
- What should be done for next time?



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

Executive Summary

- System z continues to provide the most secure technology in the industry
- Security is about People, Process and Technology
  - We are aware that businesses are not taking advantage of the best technologies
  - Desktops and Mobile devices, used to enter passwords are outside scope of z Technology and susceptible to key loggers, insider misuse and theft.
  - Detecting these types of issues results in a “black hole of cost” associated with investigations, mitigation and brand reputation
    - Bad guys aren’t telling you that they’ve stolen from a business. It’s the gift that keeps on giving.
- IBM believes many critical users are at risk when weak authentication is the accepted process
- Passphrase technology has been available for 17 years. MFA on z for 2.5 years
- All businesses should begin exploiting Passphrases and Multi Factor Authentication
  - Reduce the opportunity for hackers to compromise People and Processes toward getting your data.
  - It will require Process changes on the part of customers and users. We know these are time consuming
    - We can help guide those activities

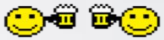
Additional Resources

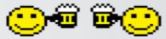
- Resources
  - Introduction to IBM MFA
  - IBM MFA Solution Brief
  - IBM Multi-Factor Authentication for z/OS V1.3 Announcement Letter
  - IBM Multi-Factor Authentication for z/OS Product Page

- Contacts
  - Michael Zagorski – Offering Manager (zagorski@us.ibm.com)

Rocket

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.