The Myth of Mainframe Security

Glinda Cummings
IBM
Sr. Security Product Manager
glinda@us.ibm.com

Session: 16144

The mainframe is the most **SECURABLE** environment

Agenda

- Where did it all start?
- Aren't Mainframes dead?
- Where are we today?
- What do we need to do?
- Summary
- Questions

Where did it all start?

Where did it all start?

- Well that depends
  - Was it the start of the Share project looking at data security which started way back in 1972
  - Was it when IBM gave us the The IBM Statement of Integrity
    - In 1973, IBM announced its Statement of Integrity for its new Operating System, OS/VS2. OS/VS2 was the predecessor to MVS and z/OS. In its current form, the IBM Statement of Integrity states…..

IBM Statement of Integrity

- IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation. Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF®), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized. In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.

The IBM MVS Authorized Assembler Services Guide

- goes on to say that…

- "… to ensure that system integrity is effective and to avoid compromising any integrity controls provided in the system, the installation must assume responsibility … that its own modifications and additions to the system do not introduce any integrity exposures. That is, all installation-written authorized code (for example, an installation SVC) must perform the same or equivalent type of validity checking and control that the system uses to maintain its integrity."

IBM Statement of Integrity

- It is important to note in the first statement that IBM does not state that z/OS will have no system integrity problems, but rather that if one is reported, they will always take action to resolve it. And, the second reference clearly states that it is the installation's responsibility that any authorized code they add, and this would include products from Independent Software Vendors and any installation developed code, also performs the same validity checking that z/OS uses to maintain its integrity

- http://www-03.ibm.com/systems/z/os/zos/features/racf/zos_integrity_statement.html

- z/OS MVS Programming: Authorized Assembler Services Guide – SA22-7608-15, page 423

Aren't mainframes dead?

Aren't mainframes dead?

- OK, some twenty plus years after InfoWorld editor Stewart Alsop announced the death of the mainframe, it's time to put the poor thing out of its misery. I declare the mainframe finally.... DEAD…….
  RIP……..really ☺

- Of course, if you want a server that is highly available (well, one where 5 minutes downtime a year, including "planned downtime", is worrying); one which can handle multi-tenanting with no possibility of one tenant affecting another's service; which can run several programs at the same time with no risk of something low priority stopping something higher priority working; and one that is capable of running, say, an ATM business for the whole of Europe or North America; then you might still get a zEnterprise as an alternative to other technologies

Aren't mainframes dead?

- But stories of the mainframes demise have led to poor investment in system z infrastructure and security tools and processes
- Mainframes are very-much-alive and as Mark Twain famously commented that reports of his death were greatly exaggerated
- Recent Share News Flash: The Mainframe (Still) Isn't Dead
  - http://www.share.org/p/bl/et/blogaid=256

Have you talked to a ‘mainframe’ today?

- Did you withdraw cash out of a bank’s ATM?
- Did you make a purchase at a major retail store?
- Did you make a bank to bank transfer locally or internationally?
- Did you make an airline ticket reservation?
- Did you apply for a credit card?

… at some point in these daily transactions, you likely touched a mainframe.

The Mainframe (System z) is The Platform Choice Of …

- 25 of the Top 25 Global Banks
- 110 of the Top WW 120 banks ranked by asset size
- 23 of the Top 25 U.S. Retailers
- 21 out of the Top 25 Insurance Organizations
- 9 Of The Top 10 Global Life/Health Insurance Providers

Workloads that run on the Mainframe (System z)

What is a workload?

*The relationship between a **group** of applications and/or systems that are related across several business functions to satisfy one or more business processes, typically running on 'virtual servers'.*

Banking	Insurance	Retail	Healthcare	Public Sector
Core Banking	*Internet Rate Quotes*	*On-line Catalog*	*Patient Care Systems*	*Electronic IRS*
Wholesale Banking – Payments	*Policy Sales & Management (e.g. Life, Annuity, Auto)*	*Supply Chain Management*	*On– line Claims Submission & Payments*	*Web based Social Security*
Customer Care & Insight	*Claims Processing*	*Customer Analysis*		*Tax processing*

Where are we today?

Where are we today?

- Some may say Old Dog, New Tricks…..Just look at the uptake of Linux on system z on a worldwide basis
- The mainframe is still one of the IT industry's most enduring inventions
- Growing sales abroad have allowed IBM to invest heavily in the new mainframe, dubbed zEnterprise EC12
- The mainframe has stayed relevant by adapting, whereas the PC, its supposed slayer, has stayed pretty much the same and is now being pushed aside
- A recent quote stated: "PCs are considered a mature platform"
- A don't forget the mainframe is 50 years old on the 7th April 2014!
- But….so are many of the security professionals looking after them!

Where are we today….

- We are faced with ever increasing compliance challenges at the Enterprise Level
- Auditors are becoming increasingly Knowledgeable about Mainframes, zOS, RACF, ACF2 & TSS

- The biggest threat is still the Insider one
- There have been several recent breaches at organisations such as Barclays & Nordea Bank….BUT these are only the ones that get found out or reported…

- Don't ever forget the Mainframe IS the most secur**able** server on the planet……*BUT* …

Common z/OS Security Challenges

- Security architecture extensions for cloud, mobile, big data
- Too many users with the ability to circumvent controls
- Inadequate attention to Monitoring, Alerting, Reporting
- Mainframe Unix System Services managed less securely then distributed UNIX/LINUX servers
- Excessive access to utilities that allow bypassing of security policies
- Shared data between environments: development, test & production
- Lax access controls allowing users elevated privileges
- Poor data management practices for data access, copying & reuse
- System z isolation – siloed –from enterprise security monitoring
- Outdated security monitoring – does not meet compliance standards

Where are we today….

- Security Wise?
  - Well its not all doom and gloom
  - There are solutions to the issues we face…but…..
  - We are faced with serious security issues on the mainframe and an ever growing list of compliance and audit issues

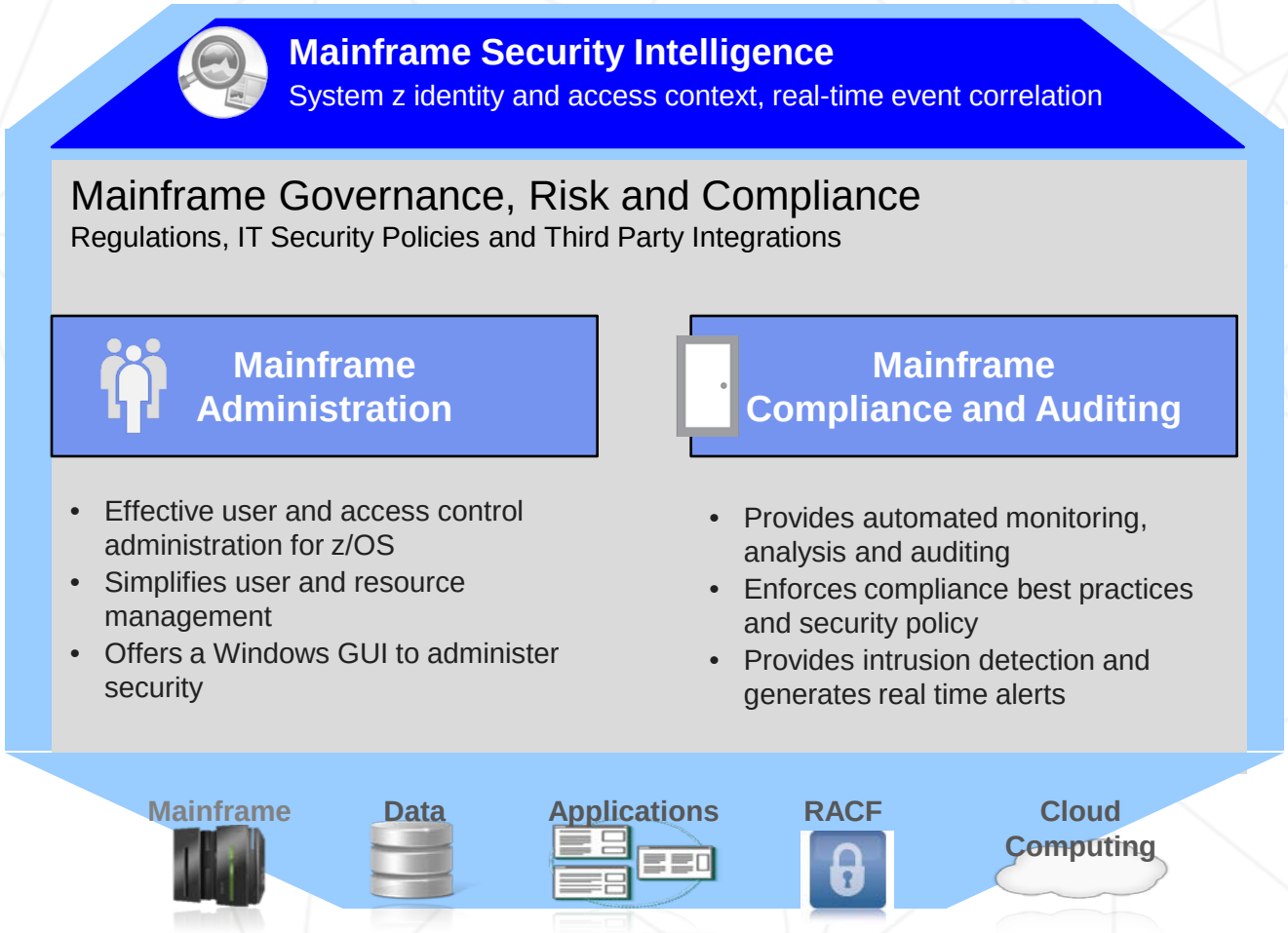
Gartner Comment

- *"The IBM z/OS mainframe continues to be an important platform for many enterprises, hosting about 90% of their mission critical applications.* ***Enterprises may not take the same steps*** *to address configuration errors and poor identity and entitlements administration on the mainframe as they do on other OS's.*

- *Thus,* ***the incidence of high-risk vulnerabilities is astonishingly high****, and enterprises often lack formal programs to identify and remediate these."*

- Gartner Research Note G00172909

Mainframe Security Management Vision



Ok, great job folks .. so we think all of our sensitive data is now identified and protected .....

How do we continue to ensure this? What about Cloud and Mobile on our mainframe

New Mainframe Trends We Need to Secure

Securing the Cloud

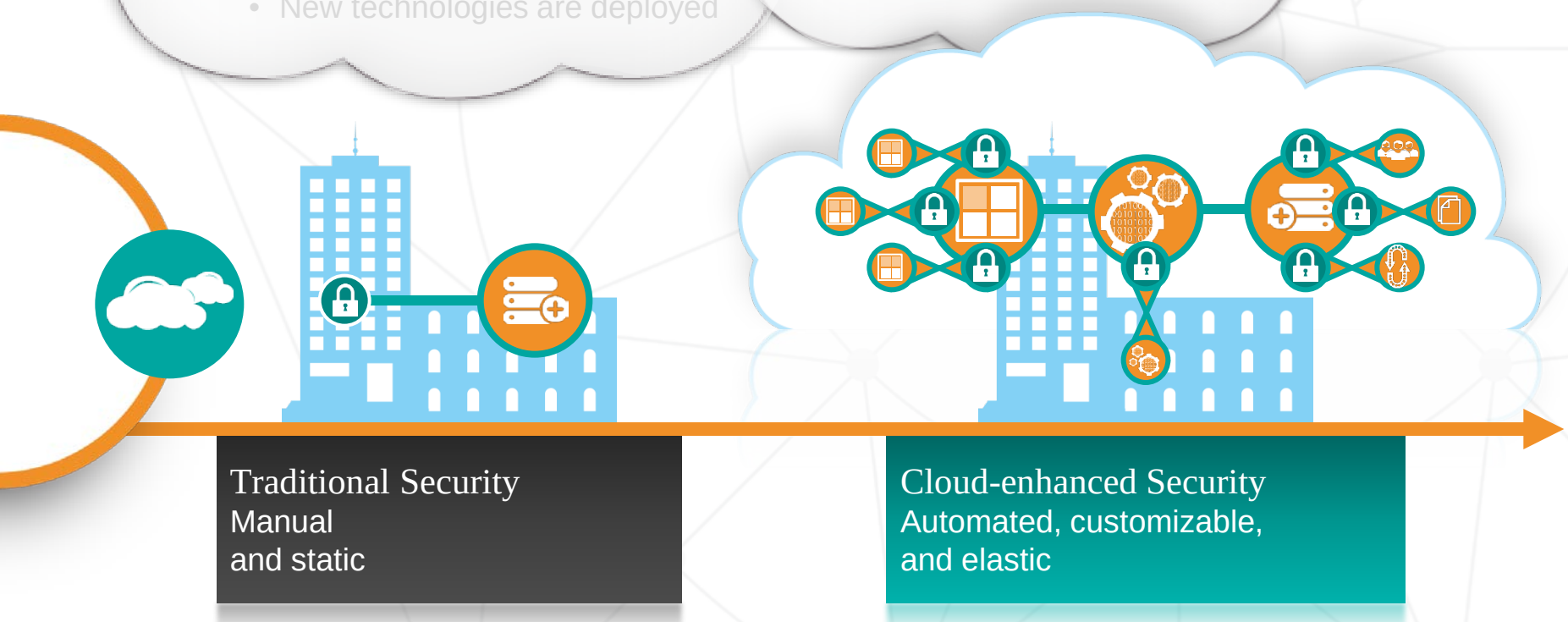
Securing the Mobilized Mainframe

Cloud is an opportunity for enhanced security

In the Cloud

- Access expands
- Responsibilities change
- Control shifts
- Speed of provisioning increases
- New technologies are deployed

Affecting all aspects of IT security



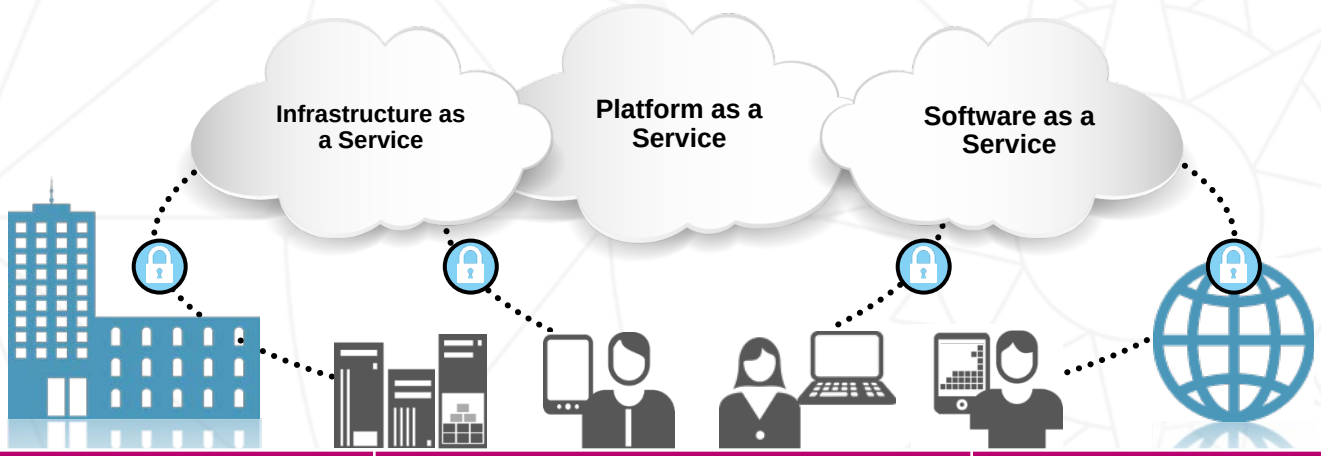
Traditional Security
Manual
and static

Cloud-enhanced Security
Automated, customizable,
and elastic

Supporting innovation, building security in at the start

Secure cloud interactions and infrastructure with Security Intelligence

Protecting the cloud data center, and next-gen business and application platforms



Interactions	Infrastructure	Intelligence
Securely federate Identity **Manage access controls**	**Monitor activity & state of all resources** **Provide network isolation**	**Auditable intelligence on cloud activities** **Identify vulnerabilities proactively**
• Privileged Identity Manager • Federated Identity Manager • Identity as a Service	• Appscan • Guardium • Network Intrusion Protection	• QRadar Security Intelligence Platform • zSecure suite

Where is the mobile business data located? Where are the commerce engines that drive business?

60-70% of operational business data resides on System z

85%

of business transactions are processed on a mainframe

70%

of top 500 System z customers run CICS

23 of top **25**

US retailers use System z

70 of top **75**

world's banks use System z

Source IBM and IBM Systems Magazine

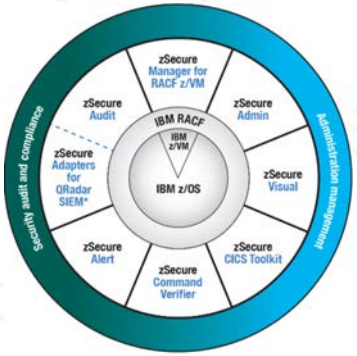
What do we need to do?

What do we need to do?

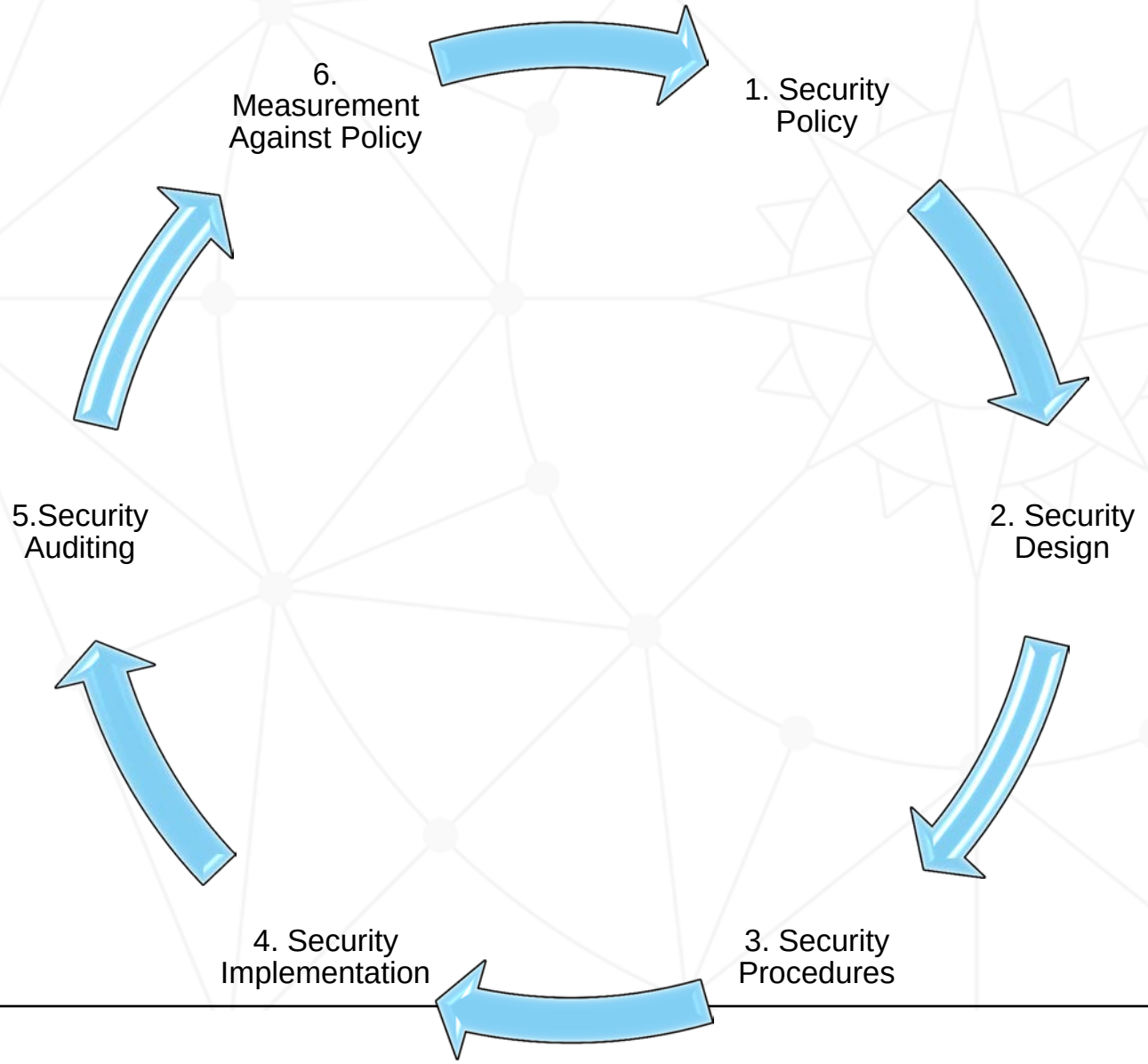
- We need to include mainframe security in all enterprise wide security discussions and plans – Make the mainframe KNOWN
- We need to avoid comments from our Risk & Compliance colleges such as:
  - Didn't realise we still had a mainframe
  - Do we still have one of those
  - Thought we had got rid of those years ago
- We need to work closely with the Risk, Compliance & Audit teams, Educating them on the unique values that the mainframe has
- We need to recruit and train the next wave of mainframe security professionals…. YES THAT MEANS AUDITORS as well
- Wonder what the average age is in this room?

What do we need to do?

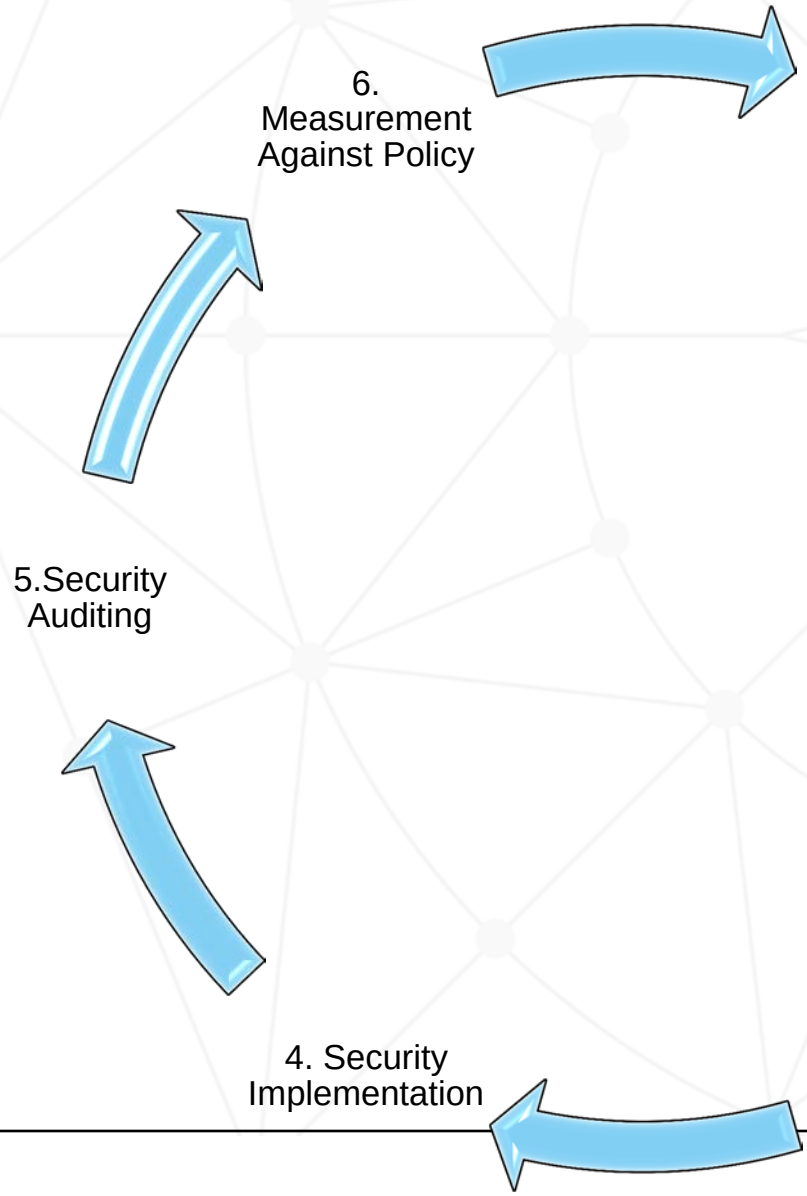
- We need more real time; proactive monitoring of our mainframe systems
- We need to equip the security teams with the correct tooling to meet the security requirements effectively



What do we need to do?



What do we need to do?



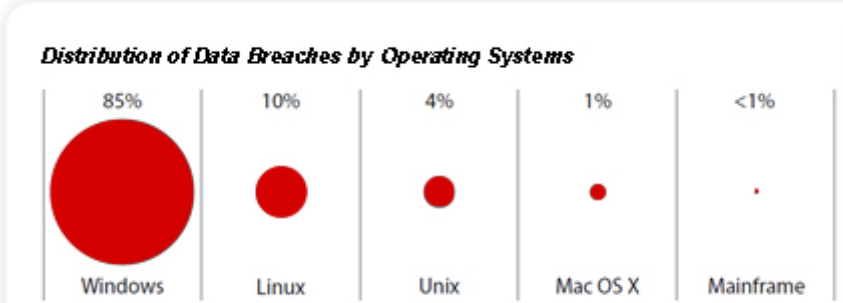
Security Tooling Provides:

2) ***Assistance with security design***
3) ***Greater flexibility in Security procedures***
4) ***More methods in security implementation***
5) ***Powerful auditing***
6) ***Powerful reporting***

Fortunately IBM's System z is Highly Secure

- Highly secure platform for virtual environments and workloads
  - **80%** of all active code runs on the Mainframe[1]
  - **80%** of enterprise business data is housed on the Mainframe[1]
  - ***This makes the Mainframe a desirable target for hackers***

- Security is built into every level of the System z structure
  - Processor
  - Hypervisor
  - Operating system
  - Communications
  - Storage
  - Applications
- System z security features address compliance
  - Identity and access management
  - Hardware and software encryption
  - Communication security capabilities
  - Extensive logging and reporting of security events
- Extensive security certifications (e.g., Common Criteria and FIPS 140) including EAL5+
- But today's mainframe must interoperate in a complex environment including cloud, mobile, big data and social networking and is susceptible to multiple vulnerabilities
  - [1]Source: 2013 IBM zEnterprise Technology Summit



Summary

- Mainframes are **SECURABLE**
- Insider threats are a concern
- There are processes that can help
- The correct tooling makes life significantly easier – Automate the manual tasks for compliance and auditing to reduce human error
- We need to act fast as recent breaches show just how costly these issues can be

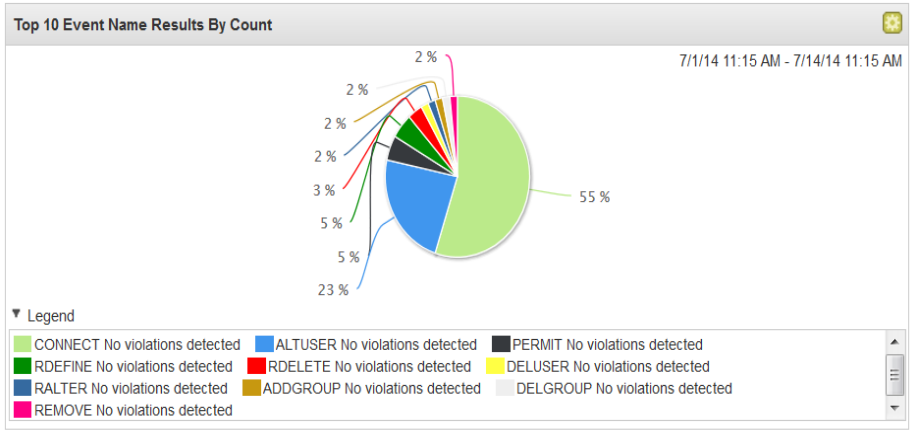
Questions?

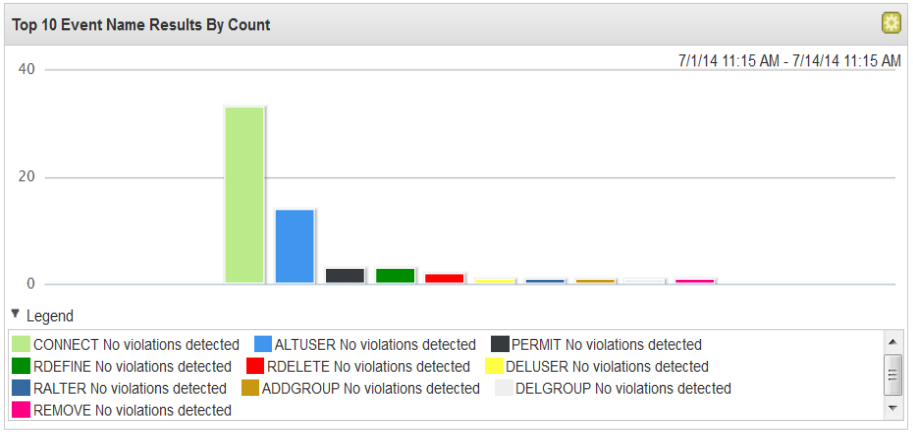
How about if you could transform this . . .

```
Audit Reporting Suite  30Jun14 09:30 to 13Jul14 16:30
RACF Command Activity

User      Count    Date  Time  RACF cmd
PEASEJ        69
                30Jun 09:30 ALTUSER PEASEJ SPECIAL
                30Jun 09:39 ALTUSER PEASEJ SPECIAL
                30Jun 12:32 ALTUSER PEASEJ SPECIAL
                 1Jul 10:35 ADDUSER DEMOUSER AUTHORITY(USE) DFLTGRP(SYSPROG) N
                 1Jul 10:35 ALTUSER DEMOUSER NOOIDCARD NOPASSWORD RESUME
                 1Jul 10:35 CONNECT DEMOUSER AUTHORITY(USE) GROUP(SYSPROC) NOA
                 1Jul 10:35 ADDSD 'DEMOUSER.WORK.*' NOSET OWNER(SYSPROG)
                 1Jul 10:35 PERMIT 'DEMOUSER.WORK.*' ACCESS(NONE) CLASS(DATASE
                 1Jul 10:35 ALTDSD 'DEMOUSER.WORK.*' UACC(NONE)
                 1Jul 10:35 RDEFINE SURROGAT (DEMOUSER.SUBMIT) LEVEL(0)
                 1Jul 10:35 RALTER SURROGAT (DEMOUSER.SUBMIT) OWNER(DEMOUSER)
                 1Jul 10:35 PERMIT DEMOUSER.SUBMIT ACCESS(READ) CLASS(SURROGAT
```

Into this . . .





(Hide Charts)

Event Name	Command (Unique Count)	Log Source Time (Minimum)	Username (Unique Count)	Log Source (Unique Count)	RACF profile (Unique Count)	Descriptor (Unique Count)	Low Level Category (Unique Count)	Count
CONNECT No violations det…	Multiple (33)	7/1/14, 11:35:28 AM	PEASEJ	JAZZ03 RACF	Multiple (32)	Success	User Account Changed	33
ALTUSER No violations det…	Multiple (6)	7/1/14, 11:35:28 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	User Account Changed	14
PERMIT No violations detec…	Multiple (3)	7/1/14, 11:35:29 AM	PEASEJ	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDEFINE No violations dete…	Multiple (3)	7/1/14, 11:35:30 AM	Multiple (2)	JAZZ03 RACF	Multiple (3)	Success	Policy Change	3
RDELETE No violations det…	Multiple (2)	7/1/14, 11:35:31 AM	Multiple (2)	JAZZ03 RACF	Multiple (2)	Success	Policy Change	2
DELUSER No violations det…	DELUSER DEMOUSER	7/1/14, 11:35:32 AM	PEASEJ	JAZZ03 RACF	DEMOUSER	Success	User Account Removed	1

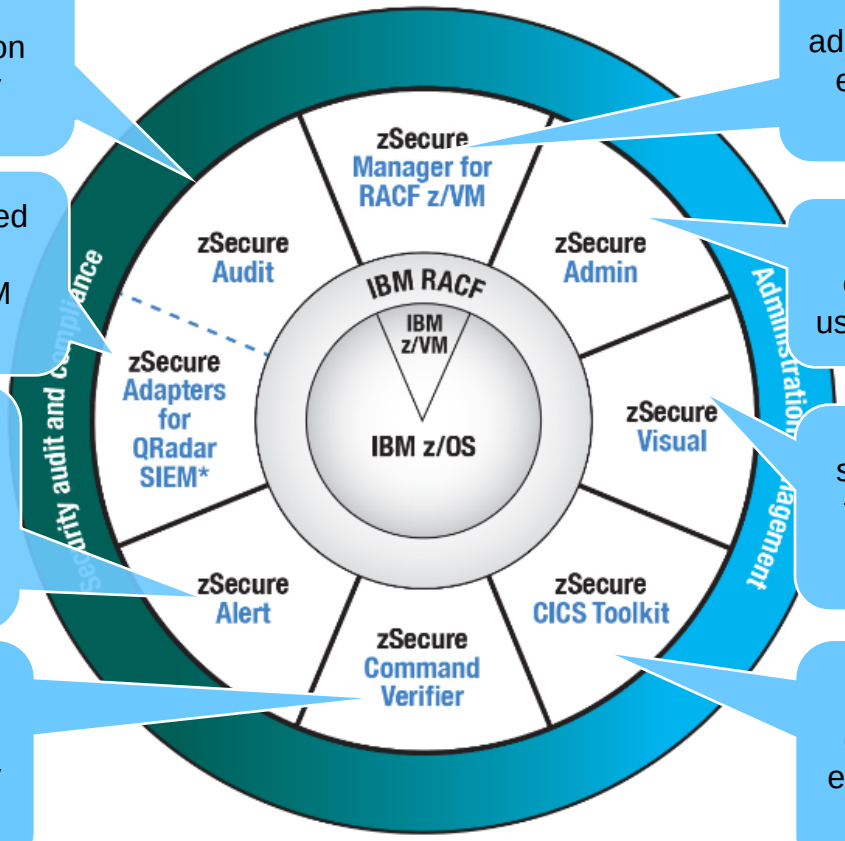
IBM Security zSecure helps address mainframe security challenges

Vulnerability analysis for the mainframe infrastructure. Automatically analyze and report on security events & detect security exposures

Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to IBM Security QRadar SIEM

Real-time mainframe threat monitoring permits you to monitor intruders and identify misconfigurations that could hamper your compliance efforts

Policy enforcement solution that helps enforce compliance to company and regulatory policies by preventing erroneous commands



Combined audit and administration for RACF in the VM environment including auditing Linux on System z

Enables more efficient and effective RACF administration, using significantly fewer resources

Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Provides access RACF command & APIs from a CICS environment, allowing additional administrative flexibility

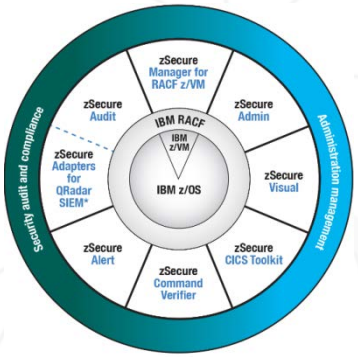
* Product offers a subset of the capabilities provided by zSecure Audit

* Supports RACF, CA ACF2 and CA Top Secret
****** Supports RACFand CA ACF2
ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Compliance Testing Framework

- Support newer external standards
  - DISA STIG for z/OS RACF
  - DISA STIG for z/OS ACF2
  - IBM outsourcing GSD331/iSec
  - PCI DSS
- Eliminate need for 2-pass queries
- Show positive compliance, not just non-compliance
- Allow showing progress in compliance efforts %
- Support in-standard customization
  - Members with authorized IDs (using STIG naming)
  - Allow rule override (suppression) with reason – visible in reporting
  - Allow creation and seamless integration of site standards
- Extend data collection CICS, IMS, MQ, DB2, IP, FTP, TELNET

Enhanced compliance reporting



- Features
  - Extend automation and coverage for PCI-DSS*, STIG**, GSD331*** and other regulatory requirements
    - New reports specific to PCI-DSS, STIG
    - More flexible reporting
    - Ability to combine report types
    - Allow for exceptions
    - Target percentage reporting
    - Improved UI
    - Enhanced zoom in UI reporting
- Benefits
  - Helps customers comply with latest iterations of regulations
  - Helps customers identify, document, and remediate security breaches

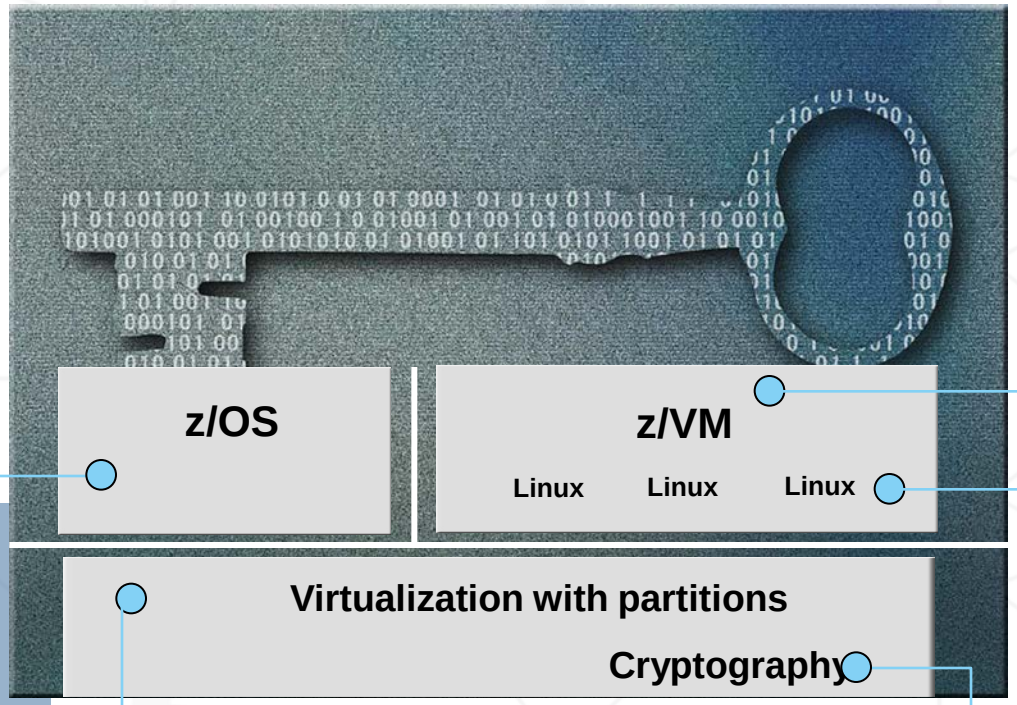
* PCI DSS: Payment Card Industry Data Security Standard for retail payments

** STIG: Security Technical Implementation Guide; Guidelines from US Defense Information Systems Agency (DISA)

*** GSD331: IBM's primary information security controls documentation for Strategic Outsourcing customers

System z Certifications

The Common Criteria program establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles



z/VM

- Common Criteria
  - z/VM 6.1 is EAL 4+ for OSPP
  - z/VM 6.1 System SSL is FIPS 140-2 certified.
- System Integrity Statement

z/OS

- Common Criteria EAL4+
  - with CAPP and LSPP
  - z/OS 1.7 → 1.10 + RACF
  - z/OS 1.11 + RACF (OSPP)
  - z/OS 1.12 , z/OS 1.13 (OSPP)
- Common Criteria EAL5+

RACF V1R12 (OSPP)

RACF V1R13 (OSPP)

- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services
- FIPS 140-2
  - System SSL z/OS 1.10 →1.13
  - z/OS ICSF PKCS#11 Services – z/OS 1.11 → z/OS 1.13
- Statement of Integrity

- zEnterprise 196 & zEnterprise 114
  - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions
- System zEC12
  - Common Criteria EAL5+ with specific target of evaluation -- LPAR: Logical partitions
- Crypto Express2 Coprocessor, Crypto Express3 & Crypto Express4s
  - FIPS 140-2 level 4 Hardware Evaluation
  - Approved by German ZKA
- CP Assist
  - FIPS 197 (AES)
  - FIPS 46-3 (TDES)
  - FIPS 180-3 (Secure Hash)

Linux on System z

- Common Criteria
  - SUSE SLES11 SP2 certified at EAL4+ with OSPP
  - Red Hat EL6.2 EAL4+ with CAPP and LSPP
- OpenSSL - FIPS 140-2 Level 1 Validated
- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

ibm.com/security