Security Innovations in a World going Mobile

Jose Castano
Director, z Systems Worldwide Software Technical Sales
castano@us.ibm.com

Agenda

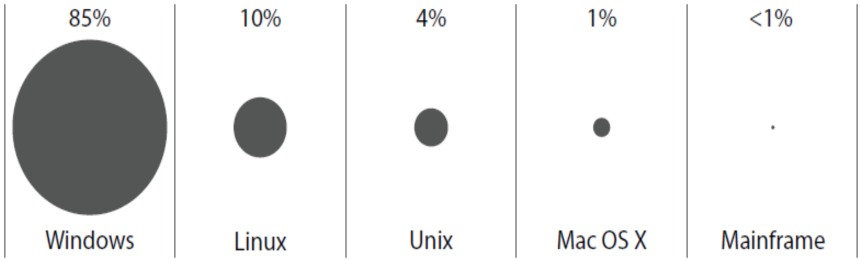
- **Changing Mainframe Threat Landscape**
- Enterprise Security Intelligence
- Protecting Data
- Protecting Applications
- Managing the Changing Threat Landscape

You know? you can do this online now.
P.C.VEY

IBM’s Fort Knox: IBM z Systems

- A strong heritage of being an extremely secure platform for virtual environments and workloads
- Security is built into every level of the z Systems structure
  - Processor
  - Hypervisor
  - Operating system
  - Communications
  - Storage
  - Applications
- The Mainframe became the worlds premier business platform, in part due to this security
  - 80% of all active code runs on the Mainframe
  - 80% of enterprise business data is housed on the Mainframe
  - Source: 2013 IBM zEnterprise Technology Summit
- However… Several factors combine to make the Mainframe a desirable target

Distribution of Data Breaches by Operating Systems



Source: Verizon 2011 Data Breach Investigations Report

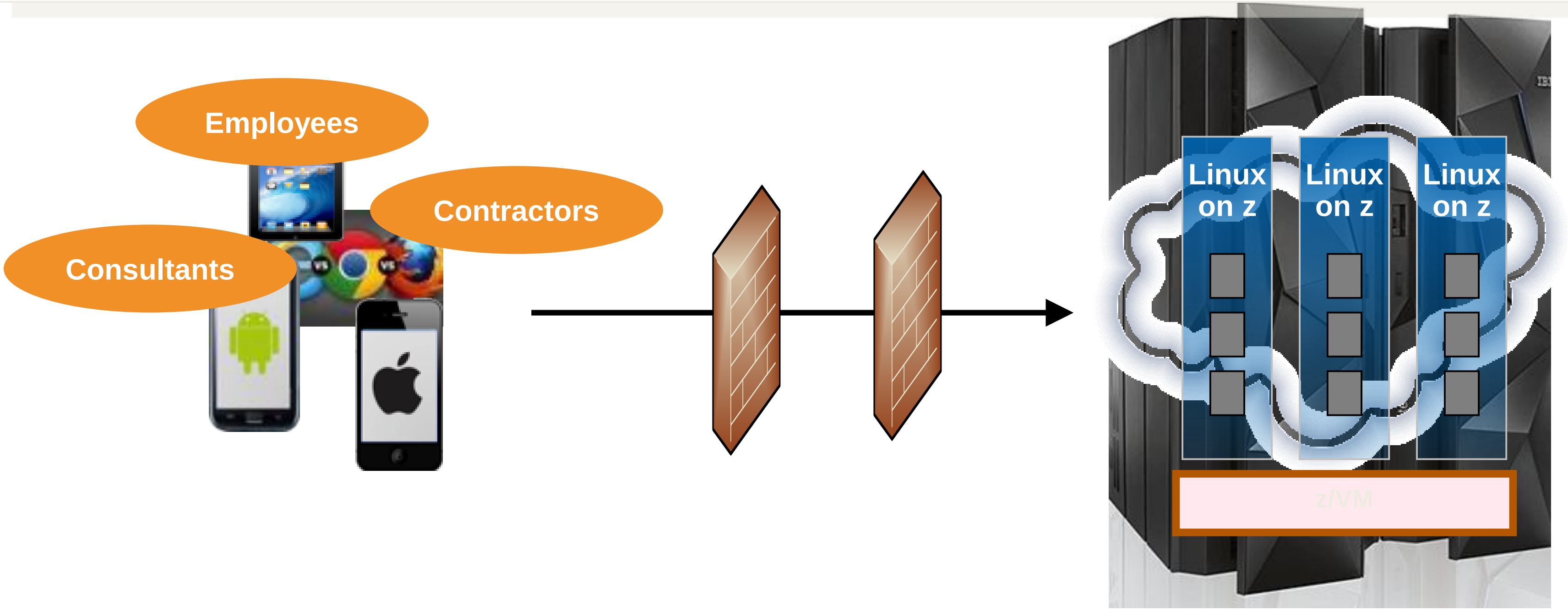
Mainframe is under-appreciated in today’s distributed-centric world

> *“Most IT staff view the mainframe as just another network node, and frequently more thought goes into protecting PCs than into securing mainframes from intrusion.”*

Dan Woods, The Naked Mainframe, Forbes.com

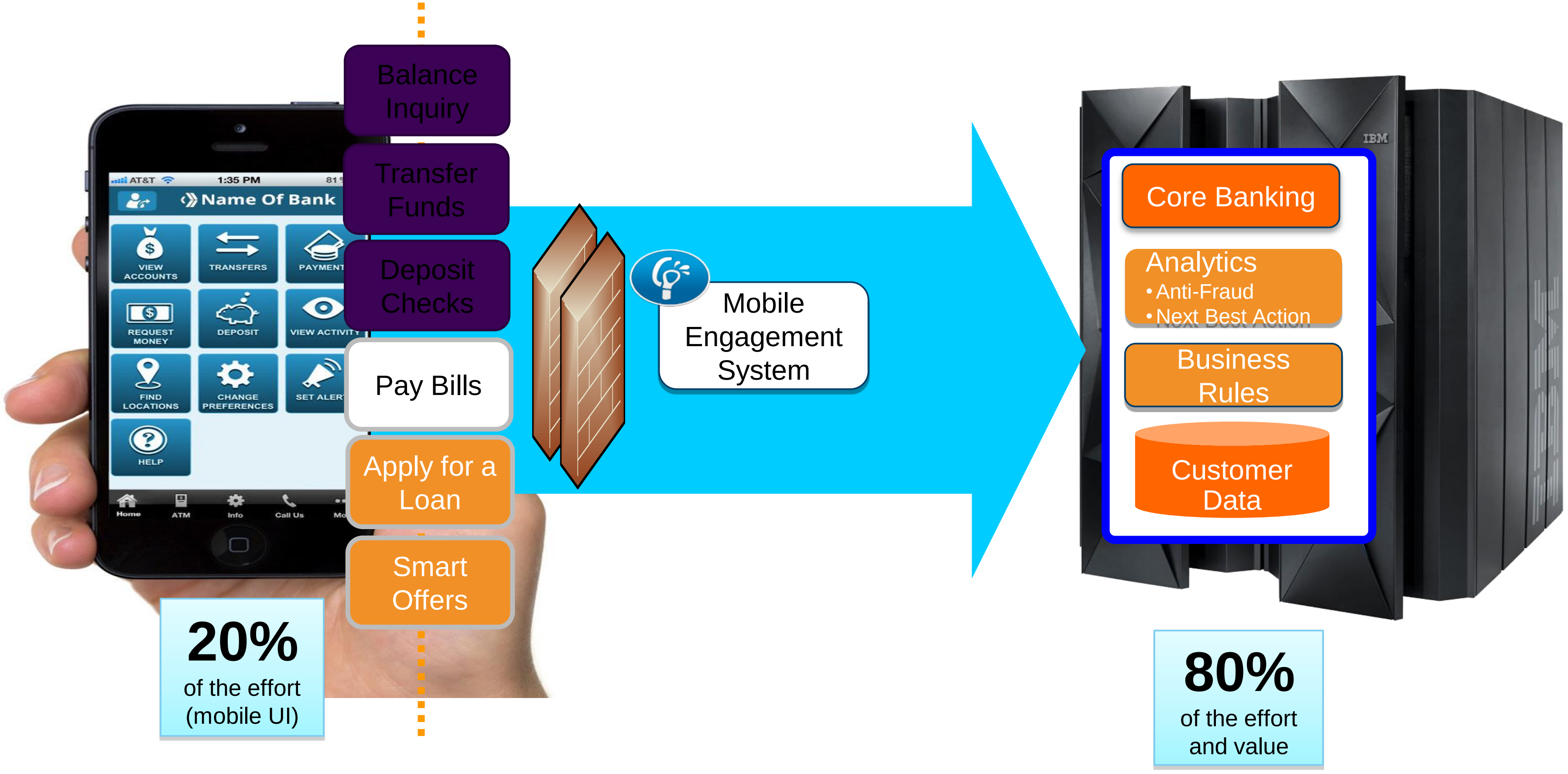
System z Cloud Scenario #1: Private Cloud with Linux on z

Multiple workloads from distributed platforms consolidated into a single, scalable footprint utilizing Linux on z



- Web servers, portals, applications and data reside on the VM’s on System z
- Theoretically, this would be equivalent to a VMWare ESX server type of deployment

System z Cloud Scenario #2: z/OS Software as a Service



Balance Inquiry

Transfer Funds

Deposit Checks

Pay Bills

Apply for a Loan

Smart Offers

Mobile Engagement System

Core Banking

Analytics
- Anti-Fraud
- Next Best Action

Business Rules

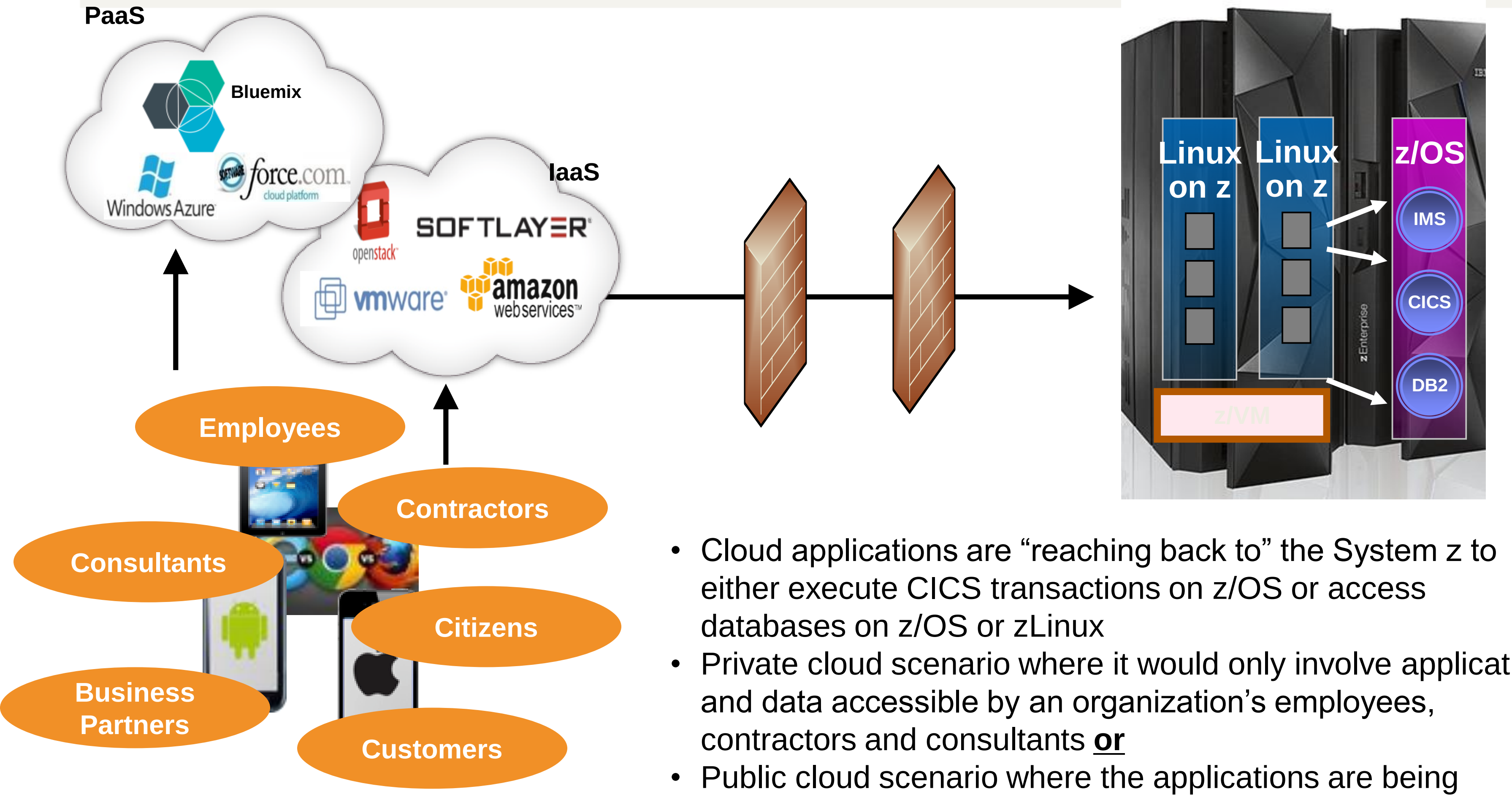
Customer Data

20%
of the effort
(mobile UI)

80%
of the effort
and value

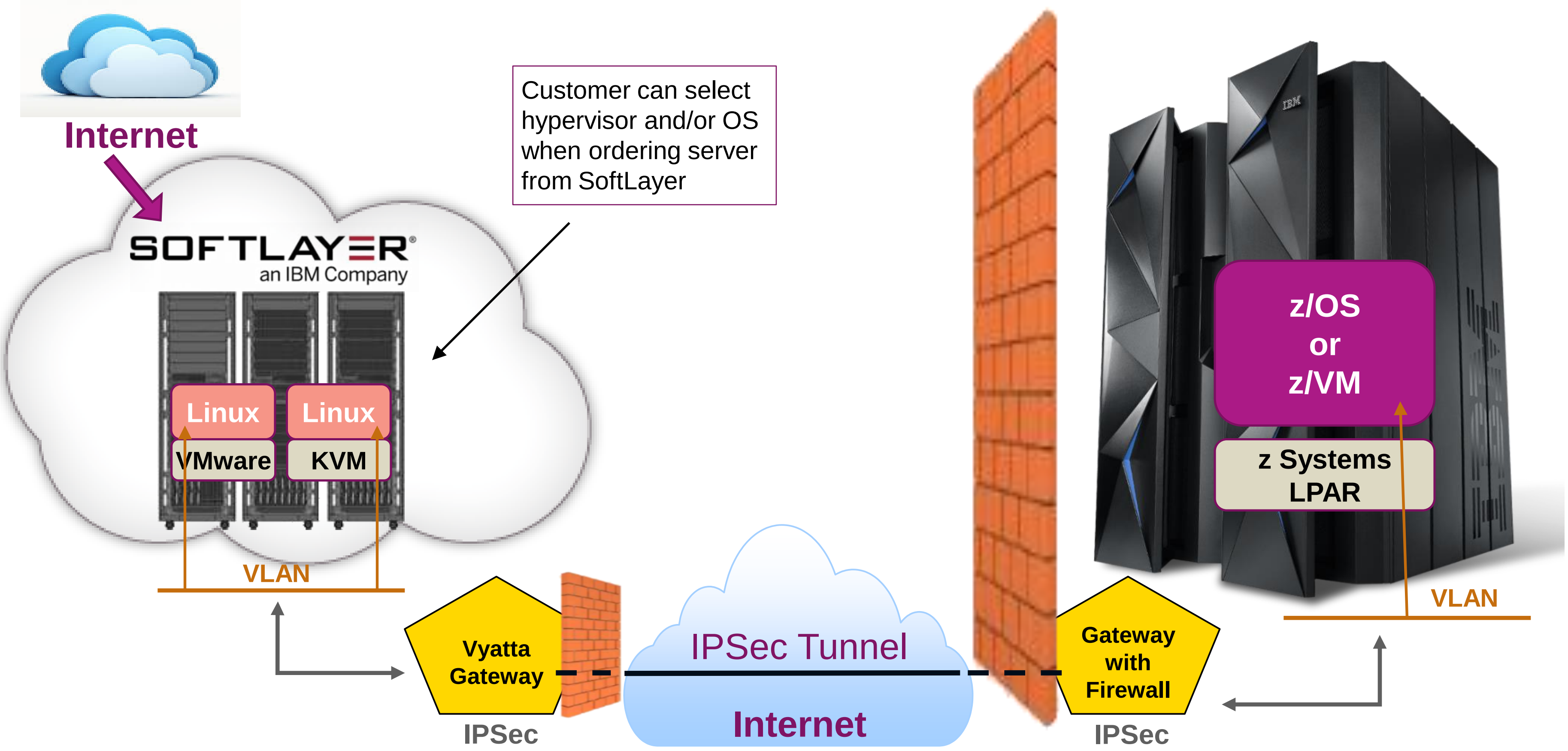
System z Cloud Scenario #3: Hybrid Cloud

Enterprise applications moved to public cloud environments, including IaaS and PaaS, and integrating with Systems of Record deployed on System z within the enterprise



- Cloud applications are "reaching back to" the System z to either execute CICS transactions on z/OS or access databases on z/OS or zLinux
- Private cloud scenario where it would only involve applications and data accessible by an organization's employees, contractors and consultants <u>**or**</u>
- Public cloud scenario where the applications are being accessed by customers, clients, citizens, etc.

z Systems Hybrid Cloud Connect Test Drive Architecture



SoftLayer

Use SoftLayer Portal to acquire server (either bare metal or virtual), storage and establish VLANs.

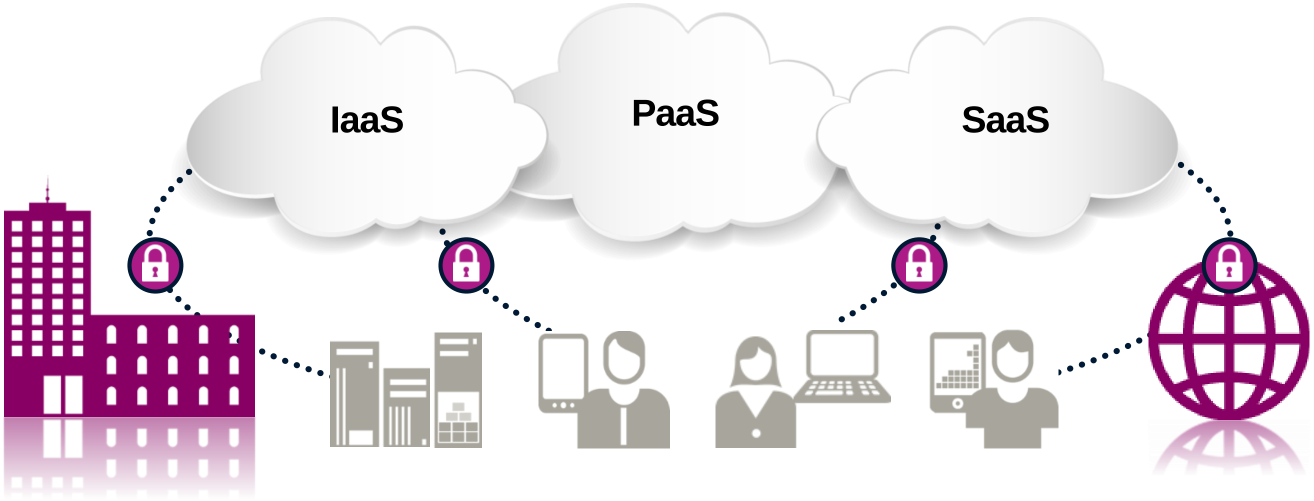
Gateway as a Service

Use GaaS Portal to route VLANs and IP traffic through Vyatta gateway. Also establish IPSec and firewall on Vyatta gateway.

On-Premise

z Systems of Record is used to maintain secure and operational control of data.

Securing the Cloud Environment



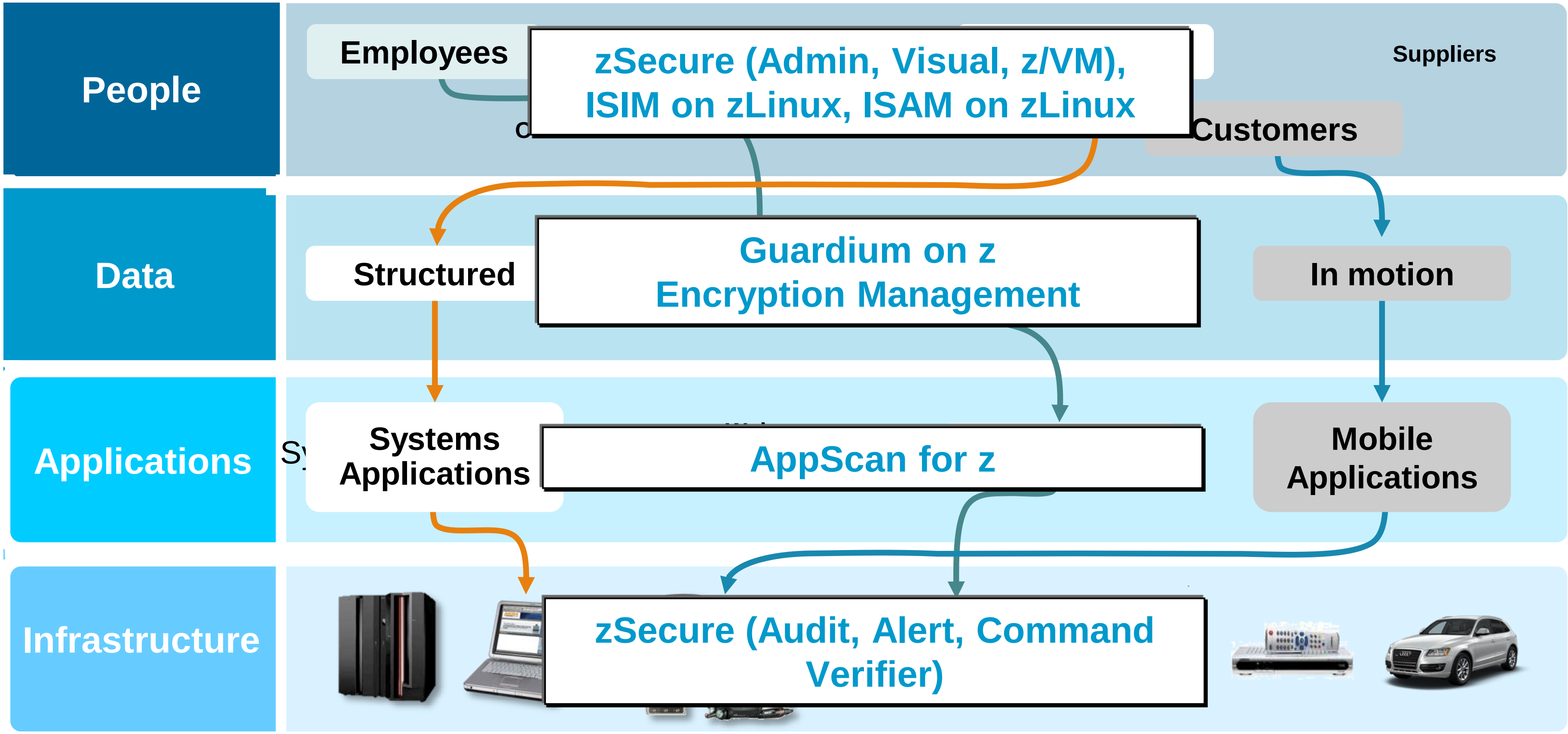
So, let’s talk about the security requirements for such a powerful and dynamic system

You will need to be able to:

- Secure the hypervisor, i.e. z/VM
- Provide administrator access to the VM’s
- Be able to Provision users to the applications and data
- Manage and Control access to the applications and data
- Monitor, Alert, Audit and Report on accesses to and attempted access to the applications and data
- Detect and Prevent against vulnerabilities, threats, malware and fraud
- Safeguard the data and protect from data loss

Does this sound familiar?

Addressing security issue is a complex, four-dimensional puzzle, requiring multiple layers of integrated defense.



People

Employees

zSecure (Admin, Visual, z/VM), ISIM on zLinux, ISAM on zLinux

Suppliers

Customers

Data

Structured

Guardium on z
Encryption Management

In motion

Applications

Systems Applications

AppScan for z

Mobile Applications

Infrastructure

zSecure (Audit, Alert, Command Verifier)

Attempting to protect the perimeter is not enough – siloed point products and traditional defenses cannot adequately secure the enterprise

QRadar for z

JK 2012-04-26

Common z/OS Security Vulnerabilities create points of entry for Insiders

- Absent, or poorly conceived, security design
- 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 disks between environments, i.e. Development, Test and Production
- Lax access controls allowing users elevated privileges
- Poor data management practices concerning access to data, copying of data and reuse of data, etc.

Source: IBM Pre-Sale Mainframe Security Health Checks

Agenda

- Changing Mainframe Threat Landscape
- **Enterprise Security Intelligence**
- Protecting Data
- Protecting Applications
- Managing the Changing Threat Landscape

Business challenges addressed by Security Intelligence

Detecting threats

- Arm yourself with comprehensive security intelligence

Consolidating data silos

- Collect, correlate and report on data in one integrated solution

Detecting insider fraud

- Next-generation SIEM with identity correlation

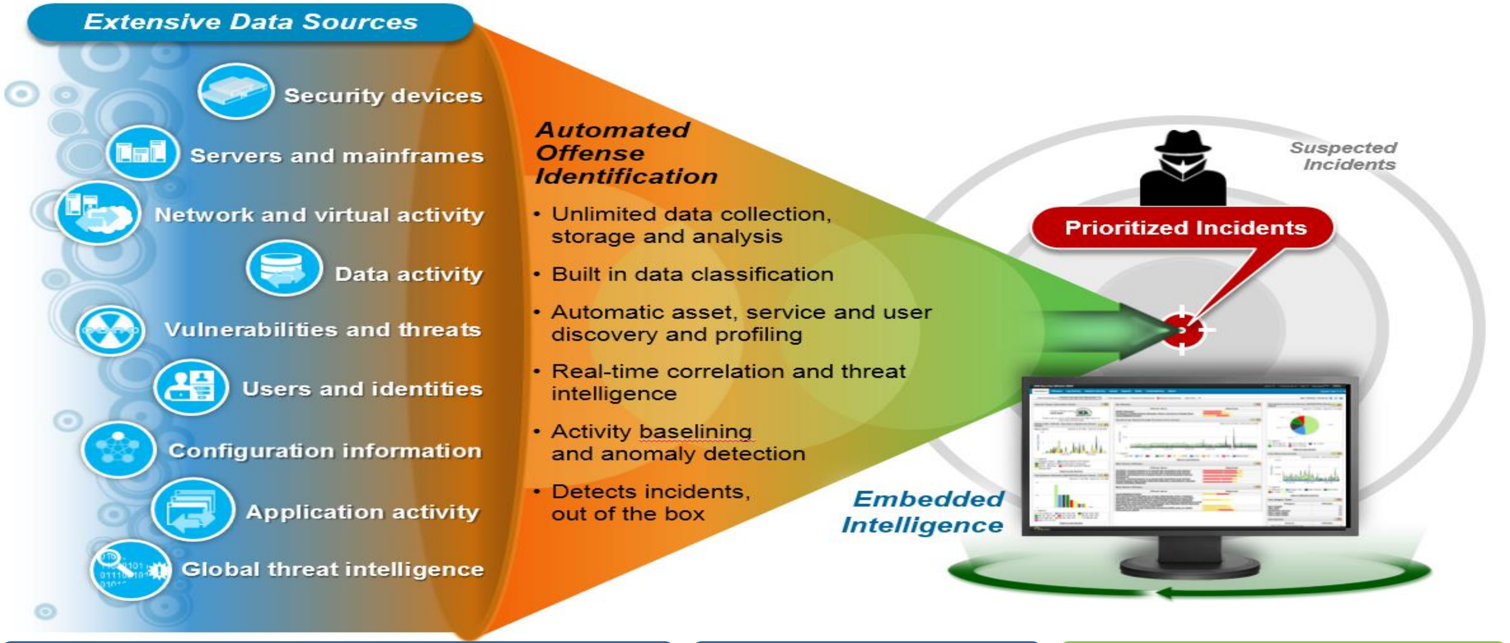
Better predicting risks to your business

- Full life cycle of compliance and risk management for network and security infrastructures

Addressing regulation mandates

- Automated data collection and configuration audits

QRadar is IBM’s Security Intelligence Solution



Extensive Data Sources

- Security devices
- Servers and mainframes
- Network and virtual activity
- Data activity
- Vulnerabilities and threats
- Users and identities
- Configuration information
- Application activity
- Global threat intelligence

Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents, out of the box

Embedded Intelligence

Suspected Incidents

Prioritized Incidents

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Core Capabilities:

- Real-time correlation of events, network flows, vulnerabilities, assets, and threat intelligence
- Flow capture and analysis to support deep application insight
- Automated dashboards & numerous report templates out of the box
- Workflow management to track threats and ensure resolution
- Scalable architecture to support largest enterprise deployments

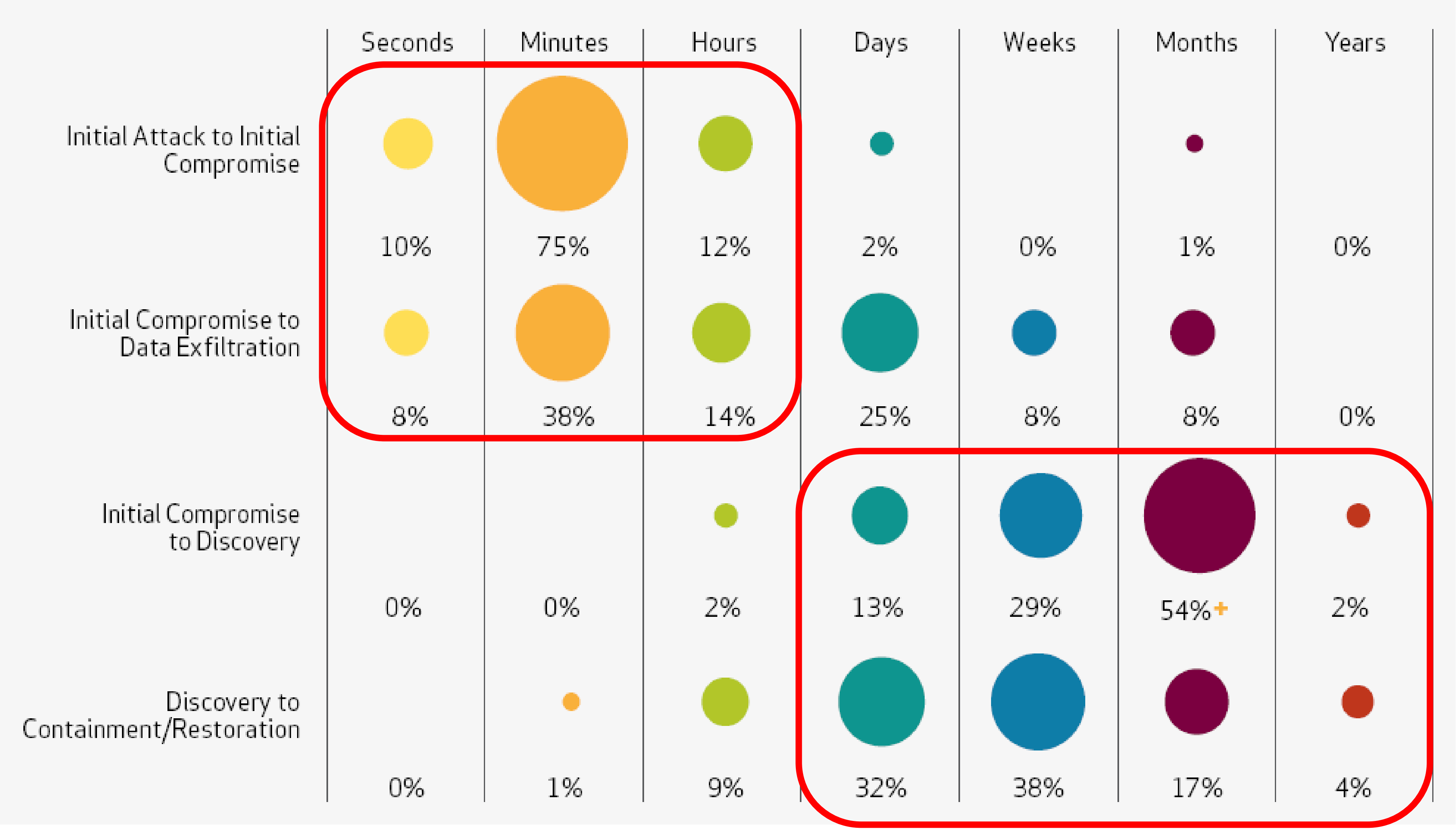
Client Benefits:

- Reduce the risk and severity of security breaches
- Remediate security incidents faster and more thoroughly
- Ensure regulatory and internal policy compliance effectively
- Reduce manual effort of security intelligence operations

Agenda

- Changing Mainframe Threat Landscape
- Enterprise Security Intelligence
- **Protecting Data**
- Protecting Applications
- Managing the Changing Threat Landscape

Compromises occur in minutes and can take weeks to months to discover and remediate

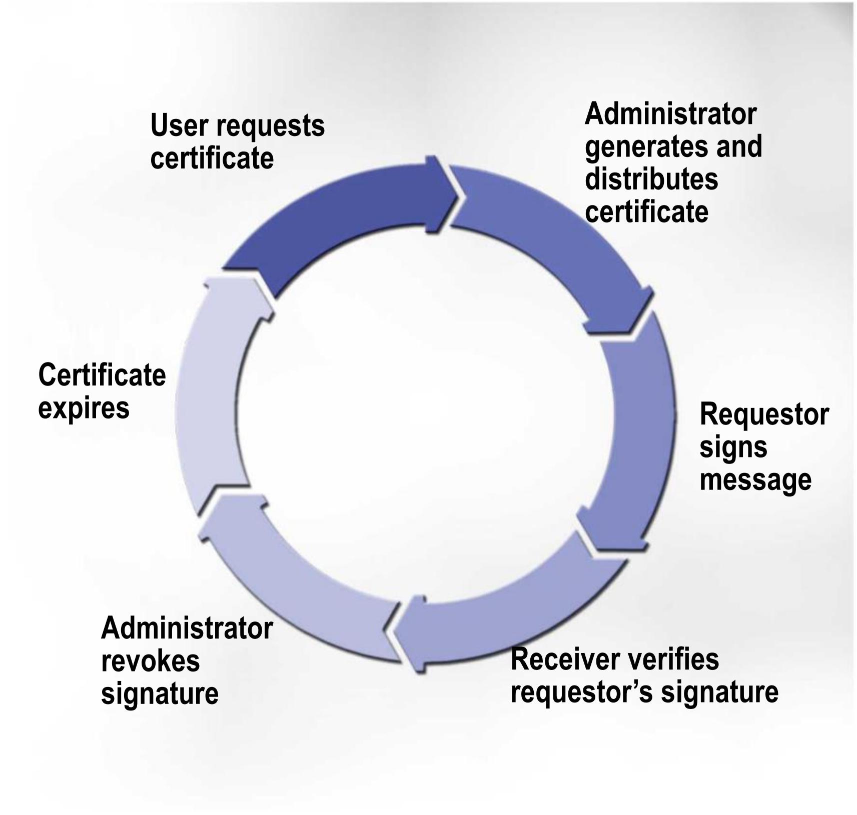


	Seconds	Minutes	Hours	Days	Weeks	Months	Years
Initial Attack to Initial Compromise	10%	75%	12%	2%	0%	1%	0%
Initial Compromise to Data Exfiltration	8%	38%	14%	25%	8%	8%	0%
Initial Compromise to Discovery	0%	0%	2%	13%	29%	54%+	2%
Discovery to Containment/Restoration	0%	1%	9%	32%	38%	17%	4%

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf?CMP=DMC-SMB_Z_ZZ_ZZ_Z_TV_N_Z038

Digital certificate hosting with z/OS PKI Services

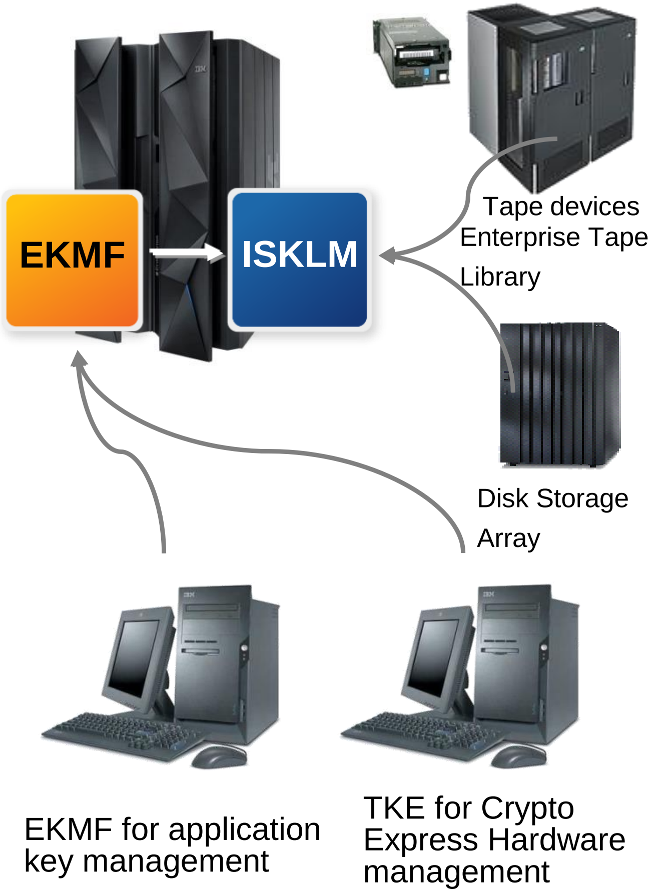
- A Certificate Authority solution built into z/OS
- Can provide significant TCO advantage over third party hosting
- Provides full certificate life cycle mgmt
  - User requests driven via Web pages
  - Browser or server certificates
  - Automatic or administrator approval process
  - End user/administrator revocation process
    - Supports CRL (Certificate Revocation List) and OCSP (Online Certificate Status Protocol)
  - Supports SCEP (Simple Certificate Enrollment Protocol) for network device certificate lifecycle management
  - *New* with z/OS R13 Support for the Certificate Management Protocol (CMP)


User requests certificate
Administrator generates and distributes certificate
Requestor signs message
Receiver verifies requestor's signature
Administrator revokes signature
Certificate expires

Banco do Brasil saves an estimated $16 M a year in digital certificate costs by using the PKI services on z/OS

IBM Enterprise Key Management Foundation for Integrated Key Management

- IBM Enterprise Key Management Foundation powered by DKMS Centralized key lifecycle management with single point of control, policy, reporting, and standardized processes for compliance
  - EMV & PCI Standards
- EKMF provides proven experience in the enterprise key management space
  - Capabilities tailored to the needs of the banking and finance community
  - Adherence to key banking and finance standards
- Trusted Key Entry (TKE) workstation provides a secure environment for the management of crypto hardware and host master keys
- ISKLM for z/OS provides proven key serving and management for self encrypting tape and disk storage capabilities to devices
- The capabilities of EKMF, TKE, and ISKLM provides an optimum solution that addresses the needs of multiple client and marketplace needs


EKMF
ISKLM
Tape devices
Enterprise Tape
Library
Disk Storage
Array
EKMF for application key management
TKE for Crypto Express Hardware management

IBM's EKMF provides the foundation for Integrated and Extensible Key Management

A comprehensive suite of products

zSecure Audit

Vulnerability analysis for the mainframe infrastructure; automatically analyze and report on security events and monitor compliance

zSecure Adapters for QRadar

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

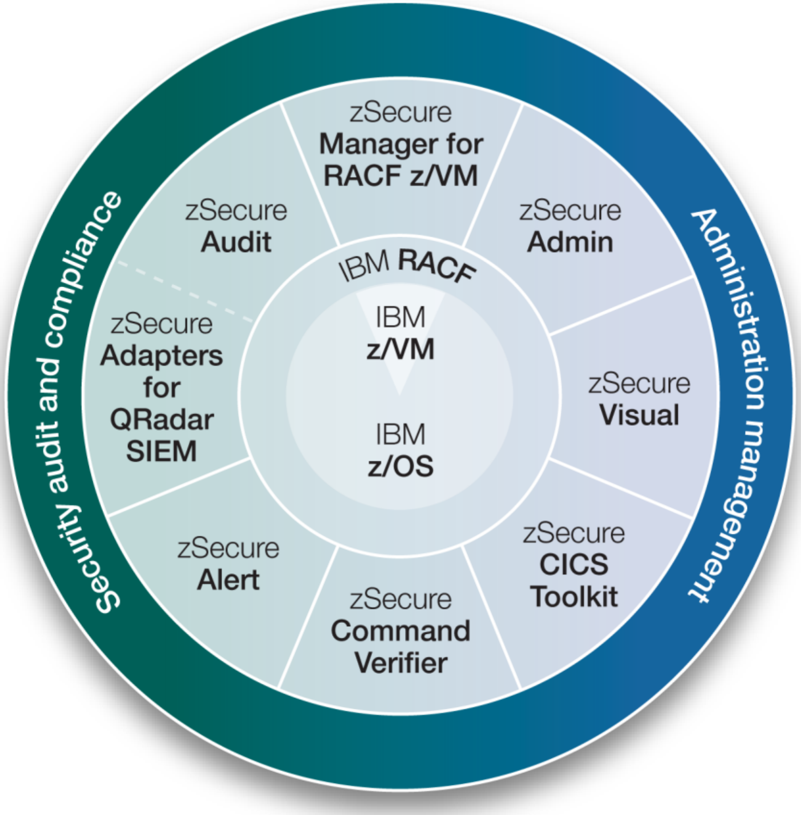
zSecure Alert

Real-time mainframe threat monitoring of intruders and alerting to identify misconfigurations that could hamper compliance

zSecure Command Verifier

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

IBM Security zSecure suite



Note:

- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

zSecure Manager for RACF z/VM

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

zSecure Admin

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

zSecure Visual

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

zSecure CICS Toolkit

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

IBM Security zSecure suite automated capabilities

Security audit and compliance

Enhanced data collection z
of SMF audit information from:

- RACF, DB2, CICS, IMS, MQ, SKLM, WAS, UNIX, Linux on System z, OMEGAMON XE on z/OS, FTP, Communication Server, TCP/IP, PDSE and more

Automated remediation
to detect and prioritize potential threats with security event analysis

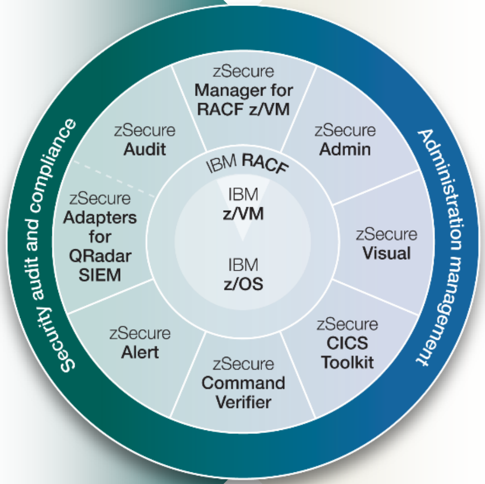
Real-time alerts of potential threats and vulnerabilities

Compliance monitoring and reporting

- PCI-DSS, STIGs, GSD331, and site-defined requirements

Comprehensive customized audit reporting

Detect harmful system security settings with automated configuration change checking



Administration management

Reduce administrative overhead
with security management tasks

Prevent abuse of special roles and authorization
with privileged user monitoring

Enforce security policies
by blocking dangerous commands and potential errors

RACF data set cleanup
of unused security profiles and inactive / terminated users

IBM Security zSecure Administration and Visual

zSecure Admin

Improves the efficiency of admin and audit tasks with highly usable ISPF panels with overtype capability

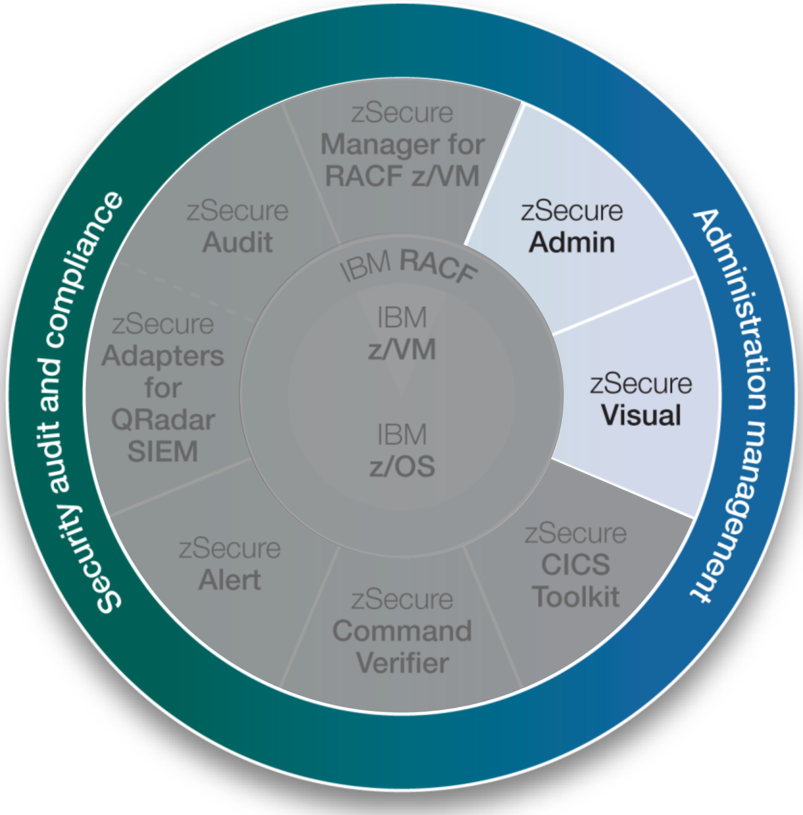
- Enables offline RACF database management and helps with merging RACF databases
- Provides access monitoring for RACF database cleanup and verifying validity of defined security
- Apply updates to multiple live RACF databases with or without RRSF from one single session
- Apply command to multiple profiles showing on a display
- Digital certificate administration with use case templates

zSecure Visual

Windows based GUI modernizes and helps with RACF consumability

- Specify once, execute on multiple systems
- Drag and drop administration

IBM Security zSecure suite



Note:
- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

IBM Security zSecure Compliance and Auditing *(excluding adapters)*

zSecure Audit

Provides highly customizable reporting and analysis of audit records (SMF etc.)

- Includes events and compliance information from RACF and ACF2 as well as subsystems such as DB2, CICS, IMS, MQ and more
- Reports on Compliance Framework for regulations including PCI-DSS, GSD331, and STIGS
- Collects, formats and sends enriched security information to QRadar SIEM for enterprise wide analysis and threat detection

zSecure Alert

Provides real time threat monitoring extending RACF and ACF2 real time notification capabilities

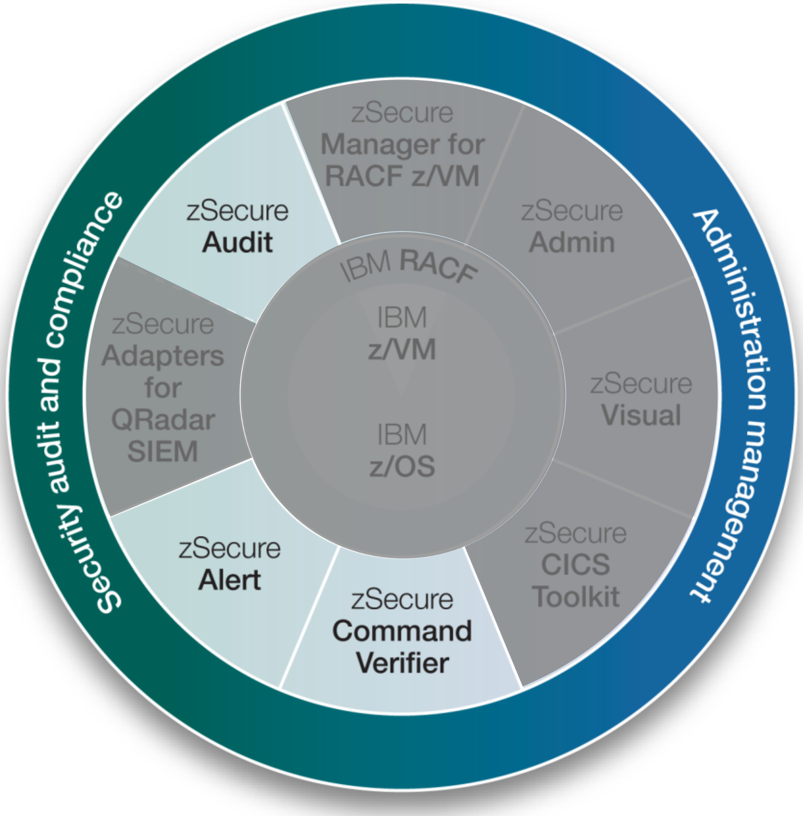
- Monitors for status changes in z/OS, RACF, and ACF2
- Alerts on PCI data

zSecure Command Verifier

Helps to control and maintain compliance by preventing RACF commands that are erroneous or do not adhere to corporate security policy

- Reduce database pollution by preventing noncompliant commands
- Reduce the risk of security breaches and failed audits caused by internal errors and noncompliant commands, enforce naming conventions

IBM Security zSecure suite



Note:

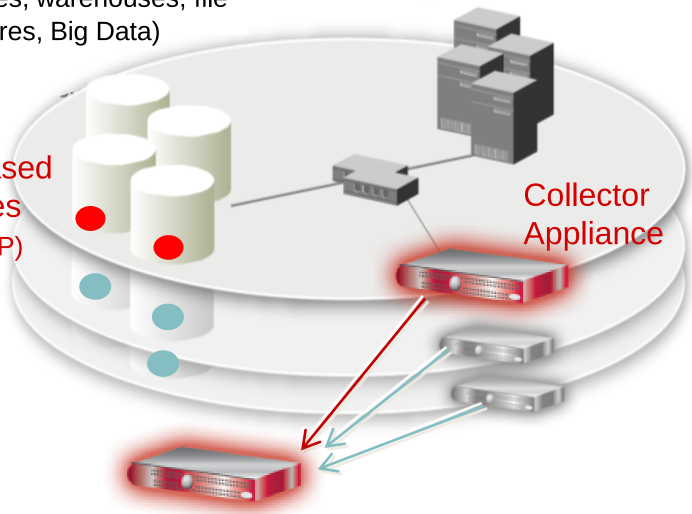
- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

IBM InfoSphere Guardium provides real-time data activity monitoring for security & compliance

✓ **Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users**

✓ **Database infrastructure scanning for missing patches, mis-configured privileges and other vulnerabilities**

✓ **Data protection compliance automation**



Data Repositories

(databases, warehouses, file shares, Big Data)

Application Servers

Host-based Probes (S-TAP)

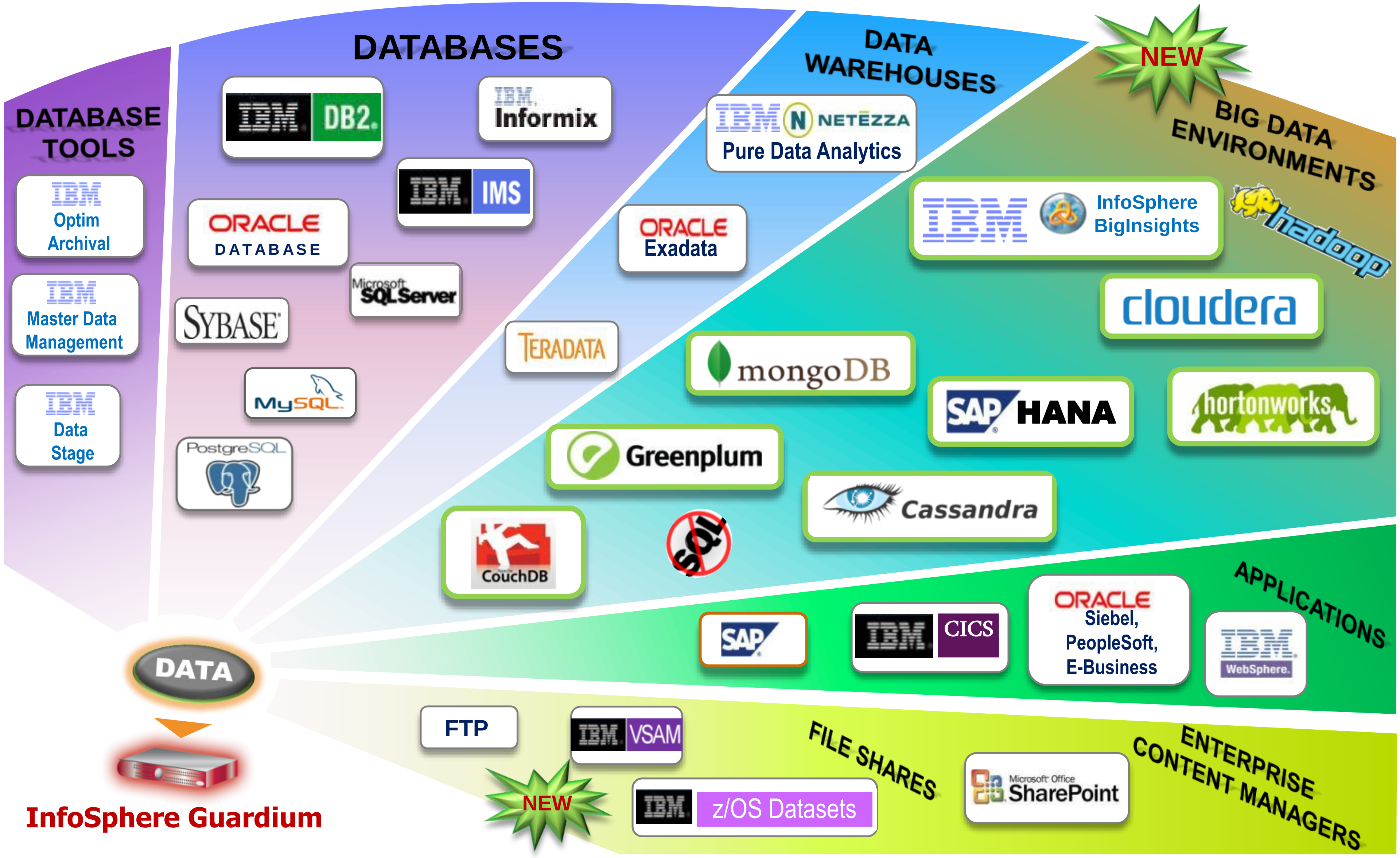
Collector Appliance

Central Manager Appliance

Key Characteristics

- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized & suspicious activity
- Granular, real-time policies
  - *Who, what, when, how*
- 100% visibility including local DBA access
- Minimal performance impact
- Does not rely on resident logs that can easily be erased by attackers, rogue insiders
- No environment changes
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Extend real-time Data Activity Monitoring to also protect sensitive data in data warehouses, Big Data Environments and file shares



DATABASE TOOLS

IBM Optim Archival

IBM Master Data Management

IBM Data Stage

DATABASES

IBM DB2

IBM Informix

IBM IMS

ORACLE DATABASE

Microsoft SQL Server

SYBASE

MySQL

PostgreSQL

TERADATA

DATA WAREHOUSES

IBM NETEZZA Pure Data Analytics

ORACLE Exadata

NEW

BIG DATA ENVIRONMENTS

IBM InfoSphere BigInsights

hadoop

cloudera

mongoDB

SAP HANA

hortonworks

Greenplum

Cassandra

CouchDB

SQL

APPLICATIONS

SAP

IBM CICS

ORACLE Siebel, PeopleSoft, E-Business

IBM WebSphere

FILE SHARES

FTP

IBM VSAM

NEW

IBM z/OS Datasets

ENTERPRISE CONTENT MANAGERS

Microsoft Office SharePoint

DATA

InfoSphere Guardium

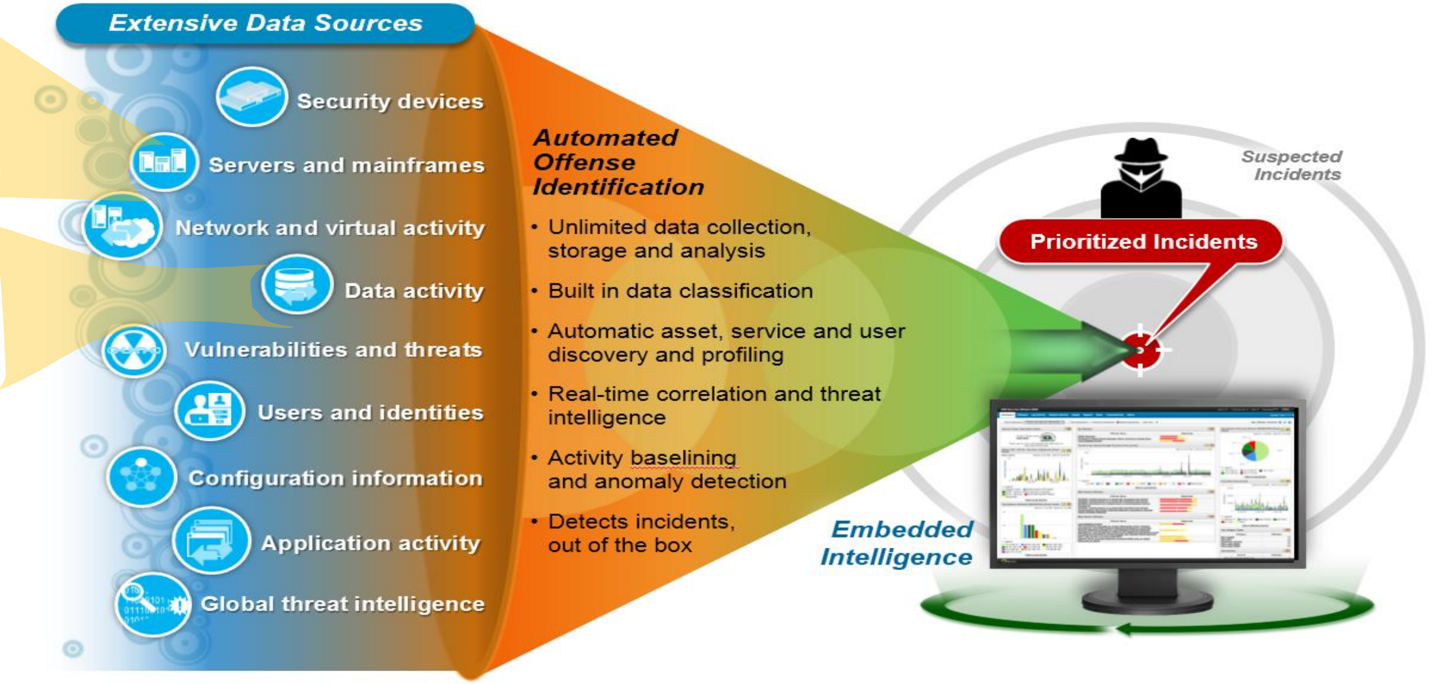
zSecure, Guardium and QRadar provide a Complementary Solution

Domain:	Security Server	Operating System	Data	Security Intelligence
Endpoints:	RACF, ACF2, Top Secret	z/OS	DB2, IMS, VSAM	All
Solution:	zSecure Admin, Visual	zSecure Audit, Alert	Guardium	QRadar SIEM
Automated cleanup of unused, obsolete and under-protected access permissions	●			
Externalization of DB2 security into RACF, including automated clean-up of prior DB2 access permissions	●			
Separation of duties in provisioning access	●			
Continuous, policy-based, real-time monitoring		●	●	
Infrastructure scanning for missing patches, misconfigurations and other vulnerabilities		●	●	
Automated Compliance Protection		●	●	
Knowledge base for compliance reports with SOX, PCI DSS, etc.		●	●	
Provides contextual and actionable surveillance to detect and remediate enterprise threats				●
Identifies changes in behavior against applications, hosts, servers and network.				●
Correlates, analyzes and reduces realtime data into actionable offenses				●

zSecure, Guardium & QRadar improve your Security Intelligence

zSecure
- **z/OS**
- **RACF**
- **ACF2, TSS**
- **CICS**

Guardium
- **DB2**
- **IMS**
- **VSAM**



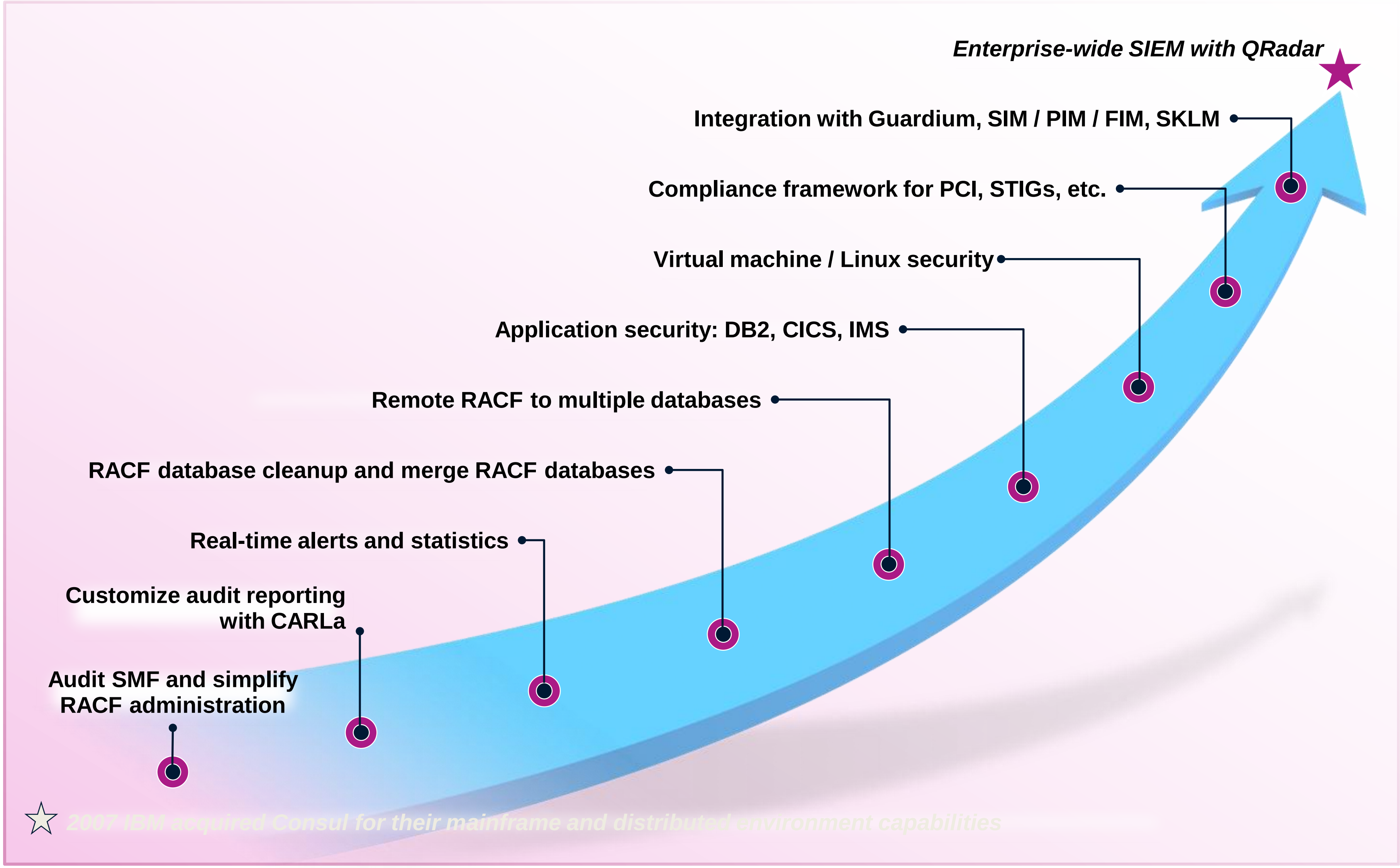
Automated Offense Identification

- Unlimited data collection, storage and analysis
- Built in data classification
- Automatic asset, service and user discovery and profiling
- Real-time correlation and threat intelligence
- Activity baselining and anomaly detection
- Detects incidents, out of the box

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

✓ Centralized view of mainframe and distributed network security incidents, activities and trends
✓ Creates automatic alerts for newly discovered vulnerabilities experiencing active ‘Attack Paths’
✓ Produces increase accuracy of risk levels and offense scores, and simplified compliance reporting
✓ QRadar supports the zLinux and the most common Applications and Databases deployed on zLinux for Cloud

IBM zSecure capabilities to help reach security maturity



Enterprise-wide SIEM with QRadar ★

Integration with Guardium, SIM / PIM / FIM, SKLM

Compliance framework for PCI, STIGs, etc.

Virtual machine / Linux security

Application security: DB2, CICS, IMS

Remote RACF to multiple databases

RACF database cleanup and merge RACF databases

Real-time alerts and statistics

Customize audit reporting
with CARLa

Audit SMF and simplify
RACF administration

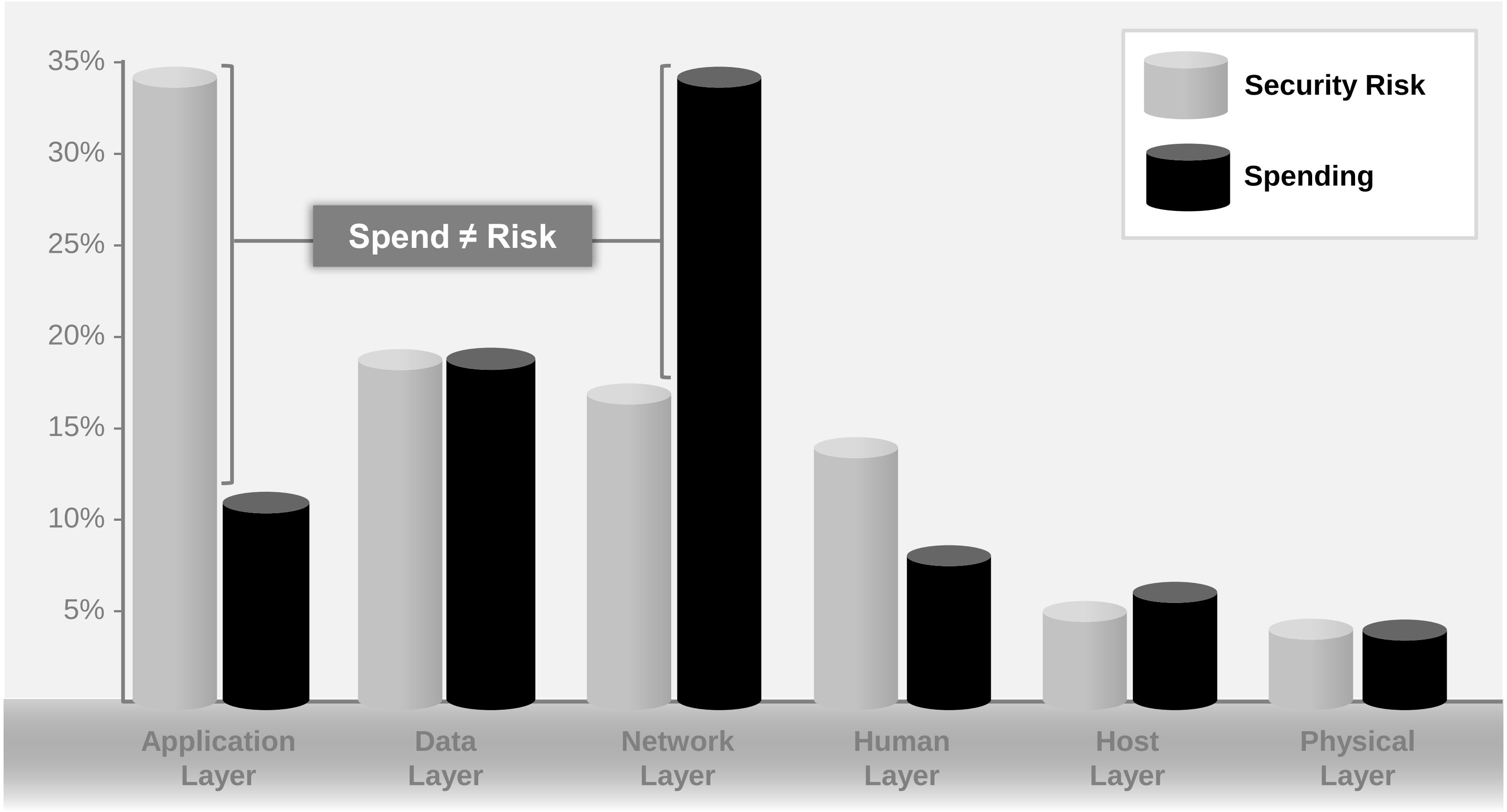
☆ *2007 IBM acquired Consul for their mainframe and distributed environment capabilities*

Agenda

- Changing Mainframe Threat Landscape
- Enterprise Security Intelligence
- Protecting Data
- **Protecting Applications**
- Managing the Changing Threat Landscape

Application security spending for our customers

Where are your “security risks” versus their “spend”?



Many clients do not prioritize application security in their environments

Source: *The State of Risk-Based Security Management,* Research Study by Ponemon Institute, 2013

Application security management

Inventory assets

Application inventory

- Create an application profile template
- Build an inventory of applications
- Describe each application

Assess business impact

Asset classification

- Classify applications
- Determine business impact
- Prioritize assets

Prioritize vulnerabilities

Vulnerabilities in application context

- Assess for vulnerabilities
- Prioritize vulnerabilities based on severity and application context

Measure status and progress

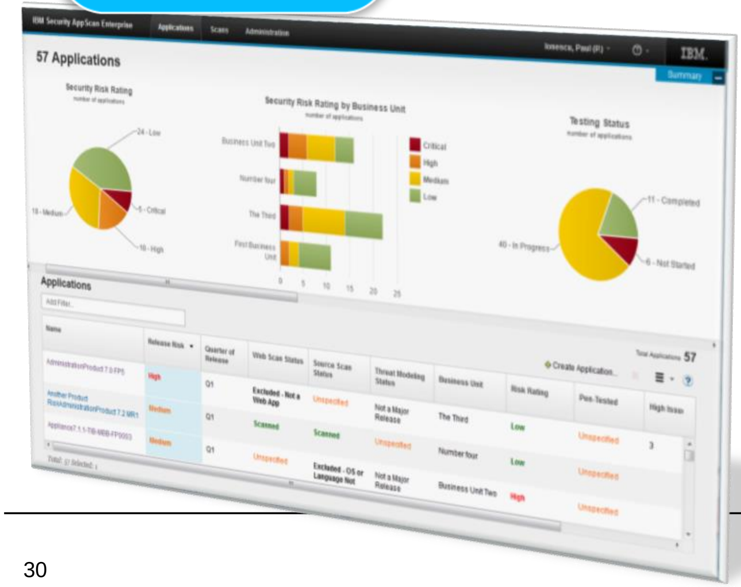
Risk assessment and progress metrics

- Determine overall risk status
- View applications that present highest risk
- Evaluate progress

Determine compliance

Compliance reporting

- Determine compliance failures by viewing over 45 compliance reports (PCI, DISA, etc.)



Name	Release Risk	Quarter of Release	Web Scan Status	Source Scan Status	Threat Modeling Status	Business Unit	Risk Rating	Pen-Tested	High Issue
AdministrationProduct 7.0 FP5	High	Q1	Excluded - Not a Web App	Unspecified	Not a Major Release	The Third	Low	Unspecified	3
Another Product RiskAdministrationProduct 7.2 MR1	Medium	Q1	Scanned	Scanned	Unspecified	Number four	Low	Unspecified	
Appliance7.1.1-TIB-MBB-FP0003	Medium	Q1	Unspecified	Excluded - OS or Language Not	Not a Major Release	Business Unit Two	High	Unspecified	

Total: 57 Selected: 1

Test applications: OWASP Top 10, SANS Top 25, etc.

Dynamic Analysis

Dynamic analysis ("black-box")

- AppScan sends mutated HTTP requests to a running app and examines how the app responds

Static Analysis

Static analysis ("white-box")

- AppScan examines application source code and traces data flow from 'source' to 'sink' to check if user input is sanitized

Interactive Analysis

Interactive analysis (*"glass-box"*)

- *Like "black-box",* includes an agent on target Web server
- Discovers more vulnerabilities

Mobile Application Analysis

Mobile application analysis

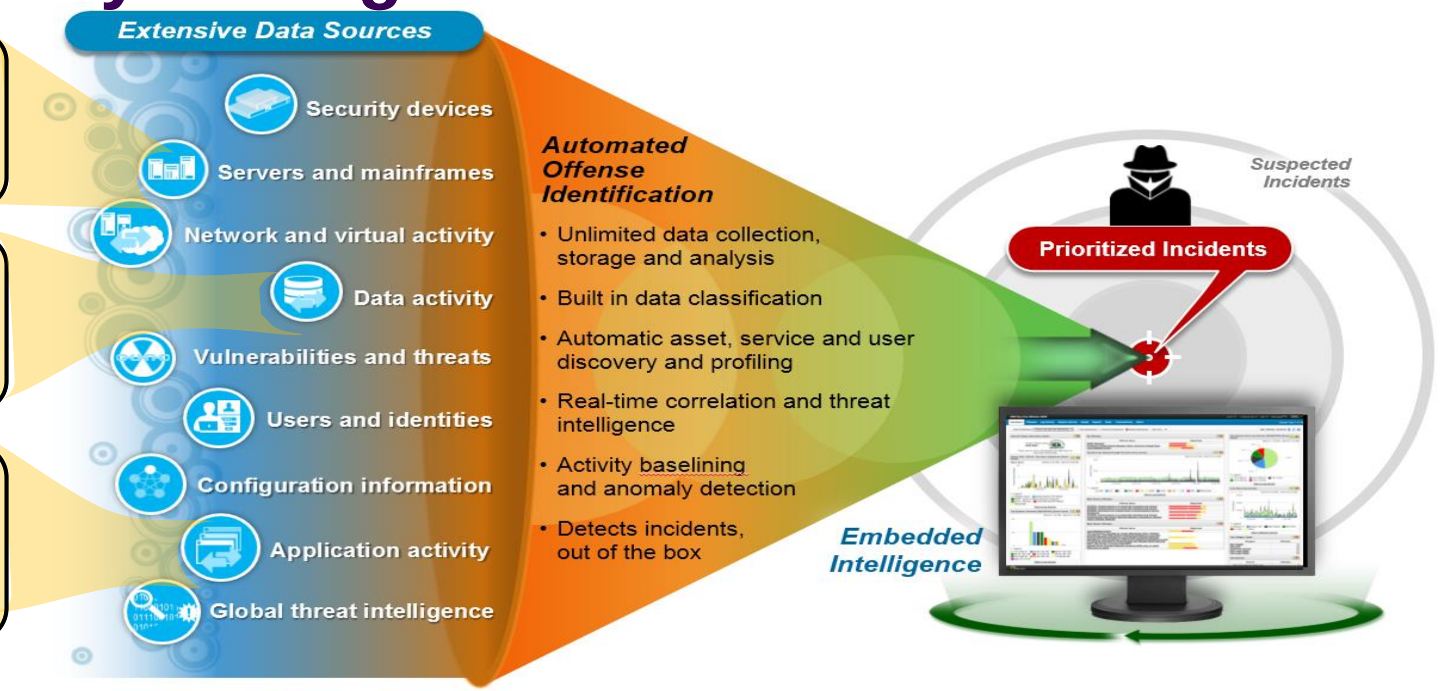
- Source code analysis of iOS and Android apps
- Full trace analysis, covers over 20K APIs

zSecure, Guardium, AppScan & QRadar improves your Security Intelligence

zSecure
- z/OS
- RACF
- ACF2, TSS
- CICS

Guardium
- DB2
- IMS
- VSAM

AppScan
- Web Apps
- Mobile Apps
- Web services
- Desktop Apps


Extensive Data Sources
Security devices
Servers and mainframes
Network and virtual activity
Data activity
Vulnerabilities and threats
Users and identities
Configuration information
Application activity
Global threat intelligence
Automated Offense Identification
• Unlimited data collection, storage and analysis
• Built in data classification
• Automatic asset, service and user discovery and profiling
• Real-time correlation and threat intelligence
• Activity baselining and anomaly detection
• Detects incidents, out of the box
Embedded Intelligence
Suspected Incidents
Prioritized Incidents

Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

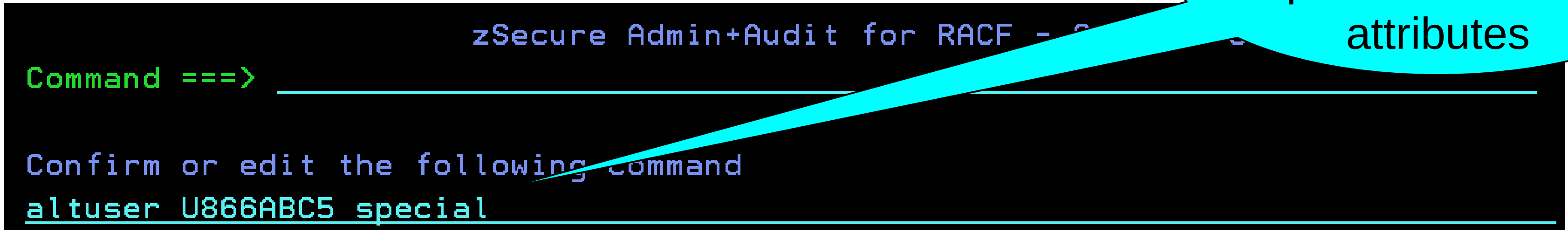
- ✓ Centralized view of mainframe and distributed network security incidents, activities and trends
- ✓ Creates automatic alerts for newly discovered vulnerabilities experiencing active ‘Attack Paths’
- ✓ Produces increase accuracy of risk levels and offense scores, and simplified compliance reporting
- ✓ QRadar supports the zLinux and the most common Applications and Databases deployed on zLinux for Cloud

Agenda

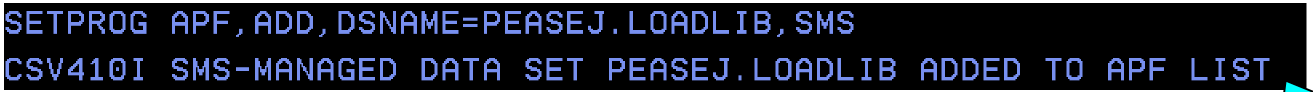
- Changing Mainframe Threat Landscape
- Enterprise Security Intelligence
- Protecting Data
- Protecting Applications
- **Managing the Changing Threat Landscape**

Scenario – Privileged User Activities occurring on System z

Assigning powerful RACF attributes



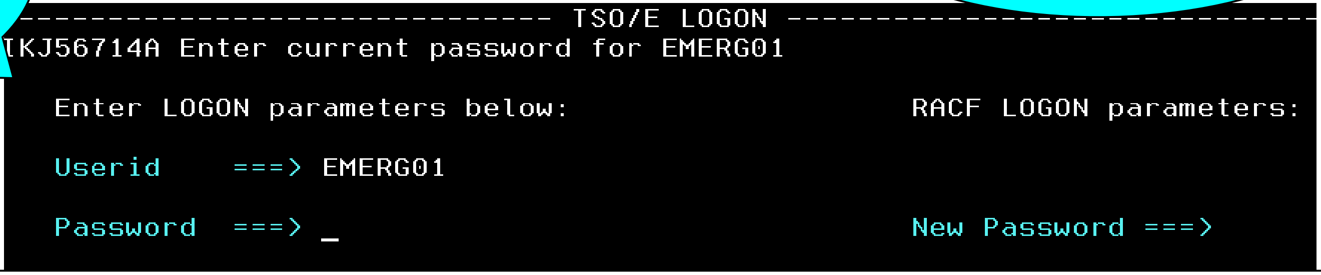
```
                 zSecure Admin+Audit for RACF - 
Command ===> 

Confirm or edit the following command
altuser U866ABC5 special
```



```
SETPROG APF,ADD,DSNAME=PEASEJ.LOADLIB,SMS
CSV410I SMS-MANAGED DATA SET PEASEJ.LOADLIB ADDED TO APF LIST
```

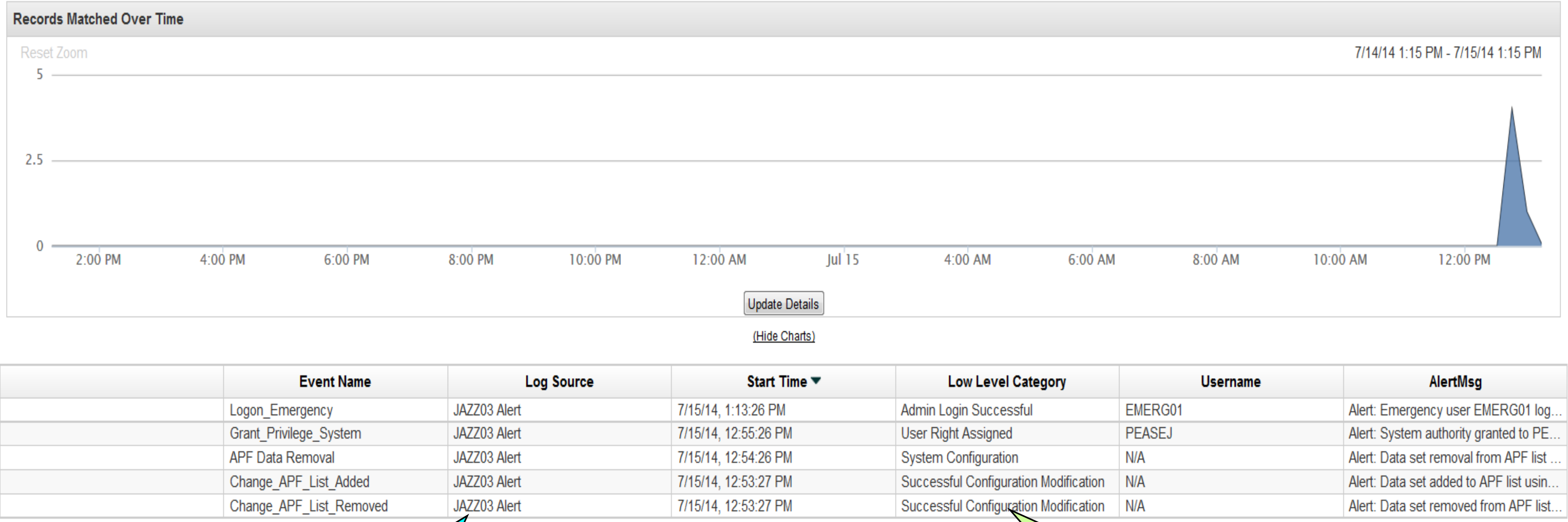
Modifying the Trusted Computing Base

Logon with powerful emergency user IDs



```
------------------------------- TSO/E LOGON -----------------------------------
IKJ56714A Enter current password for EMERG01

  Enter LOGON parameters below:                    RACF LOGON parameters:

  Userid    ===> EMERG01

  Password  ===> _                                 New Password ===>
```

Scenario – Monitoring Privileged User activities in QRadar



	Event Name	Log Source	Start Time ▼	Low Level Category	Username	AlertMsg
	Logon_Emergency	JAZZ03 Alert	7/15/14, 1:13:26 PM	Admin Login Successful	EMERG01	Alert: Emergency user EMERG01 log...
	Grant_Privilege_System	JAZZ03 Alert	7/15/14, 12:55:26 PM	User Right Assigned	PEASEJ	Alert: System authority granted to PE...
	APF Data Removal	JAZZ03 Alert	7/15/14, 12:54:26 PM	System Configuration	N/A	Alert: Data set removal from APF list ...
	Change_APF_List_Added	JAZZ03 Alert	7/15/14, 12:53:27 PM	Successful Configuration Modification	N/A	Alert: Data set added to APF list usin...
	Change_APF_List_Removed	JAZZ03 Alert	7/15/14, 12:53:27 PM	Successful Configuration Modification	N/A	Alert: Data set removed from APF list...

Events sent to QRadar, seconds later

Collected and sent to QRadar by **zSecure Alert**

Mainframe Security Control Overview

- **Format:** The MSCR is facilitated by an IBM Security Architect, and one or two additional technical experts will facilitate this half-day workshop.
- **What to Expect:** This workshop focuses on high-level concepts at the architecture and policy level. We begin by gathering baseline information about the vision and current state of your security program. For each control we will map your existing solutions and processes and help you self-assess your as-is maturity, and identify your to be goal.
- **Your Participation:** Key participants are a management leader and a technical leader, each who have an understanding of your security program, and authority to identify next step actions. Typical roles include the CISO or Director of Security, and a Security Architect or technical leader, Technical Support Manager, Applications Manager.
- **What' s Produced:** You will receive a report that documents your maturity level, and specific, 'very next actions' for each control not at the desired state. The output of this activity is considered IBM and Customer Confidential.
- **Cost:** This no-fee workshop is an investment both of your and IBM' s time, and provides significant value to your organization.

What you can expect as a result of completing this workshop

- Understanding of your current security posture.
- Measurement of the opinions of target maturity required in the organization to be successful.
- How security capabilities are implemented in your business through People, Process and Technology.
- Better understanding of how your security program can reduce business risk.
- Understanding of the remaining risks you bear.

The need for bulletproof infrastructure has never been greater – IBM z Systems is the foundation for a secure enterprise

- ✓ Designed for the highest level of security for commercial platforms
- ✓ Consistent policy based security management
- ✓ Protects critical data with encryption and key management
- ✓ Delivers a secure foundation for enterprise cloud
- ✓ Helps meet compliance and audit requests
- ✓ Monitors potential threats with vigilance

- *52% lower security administrative costs*
- *Highest security rating for commercially available servers*
- *Savings of up to 70% of audit and compliance overhead*
- *90% of business applications run on mainframe technology*

Questions

Resources

White Papers:

- Safeguard Enterprise Compliance and Remain Vigilant against Threats:
  - http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03013USEN&attachment=WGW03013USEN.PDF
- Get Actionable Insight with Security Intelligence for Mainframe Environments:
  - http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03063USEN&attachment=WGW03063USEN.PDF
- Creating the Ultimate Security Platform:
  - http://www.ibm.com/common/ssi/cgi-bin/ssialias?subtype=WH&infotype=SA&appname=SWGE_WG_WG_USEN&htmlfid=WGW03031USEN&attachment=WGW03031USEN.PDF

YouTube Videos:

- System z Security Intelligence with IBM zSecure and IBM QRadar:
  - https://www.youtube.com/watch?v=f2iSFjMNI6s&list=UUlAgZm2OXFpX8WoMsOpWoXA
- How Swiss Re Manages Mainframe Security Compliance:
  - https://www.youtube.com/watch?v=RR_-NaHaO_8