Enterprise Security Management - Detection and Prevention

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

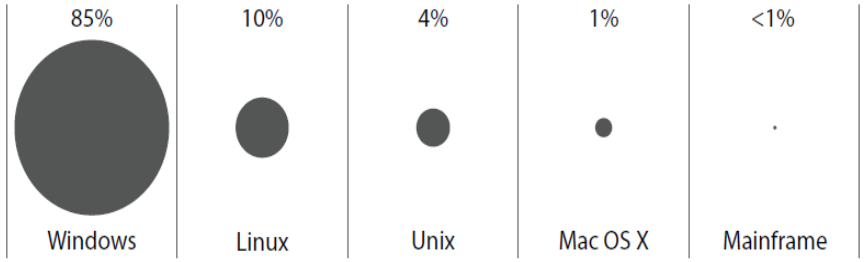
Agenda

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

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

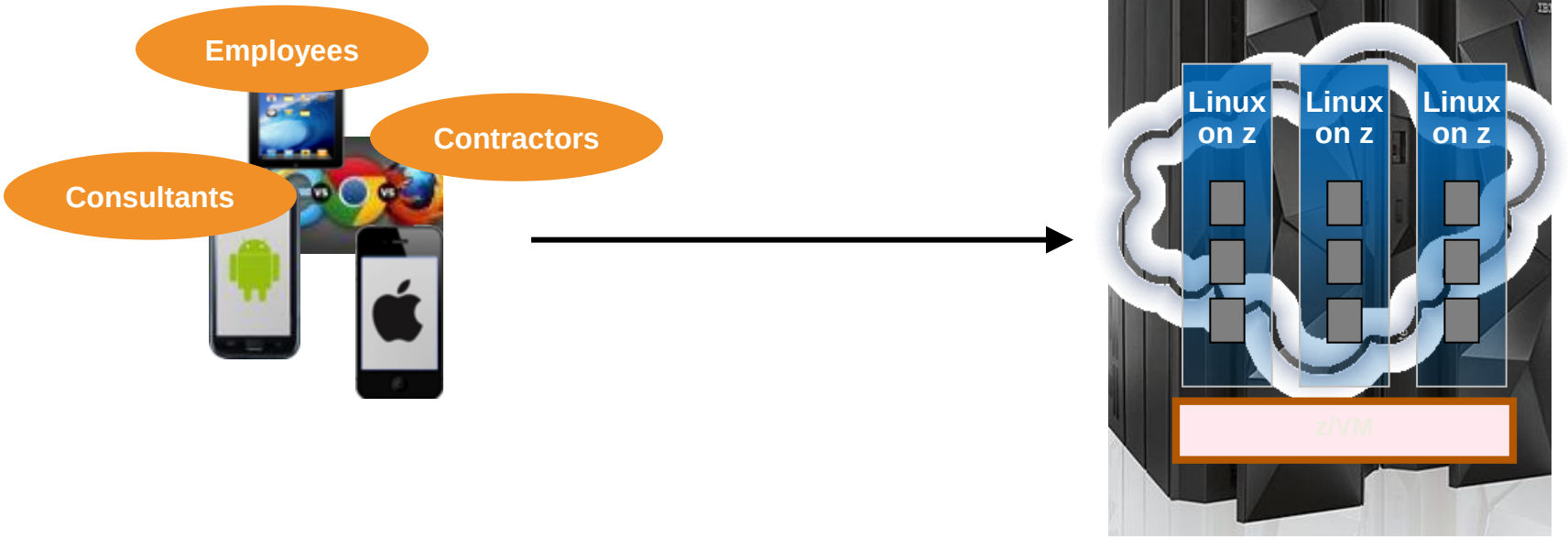
Common z/OS Security Vulnerabilities create points of entry for Insiders

- 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

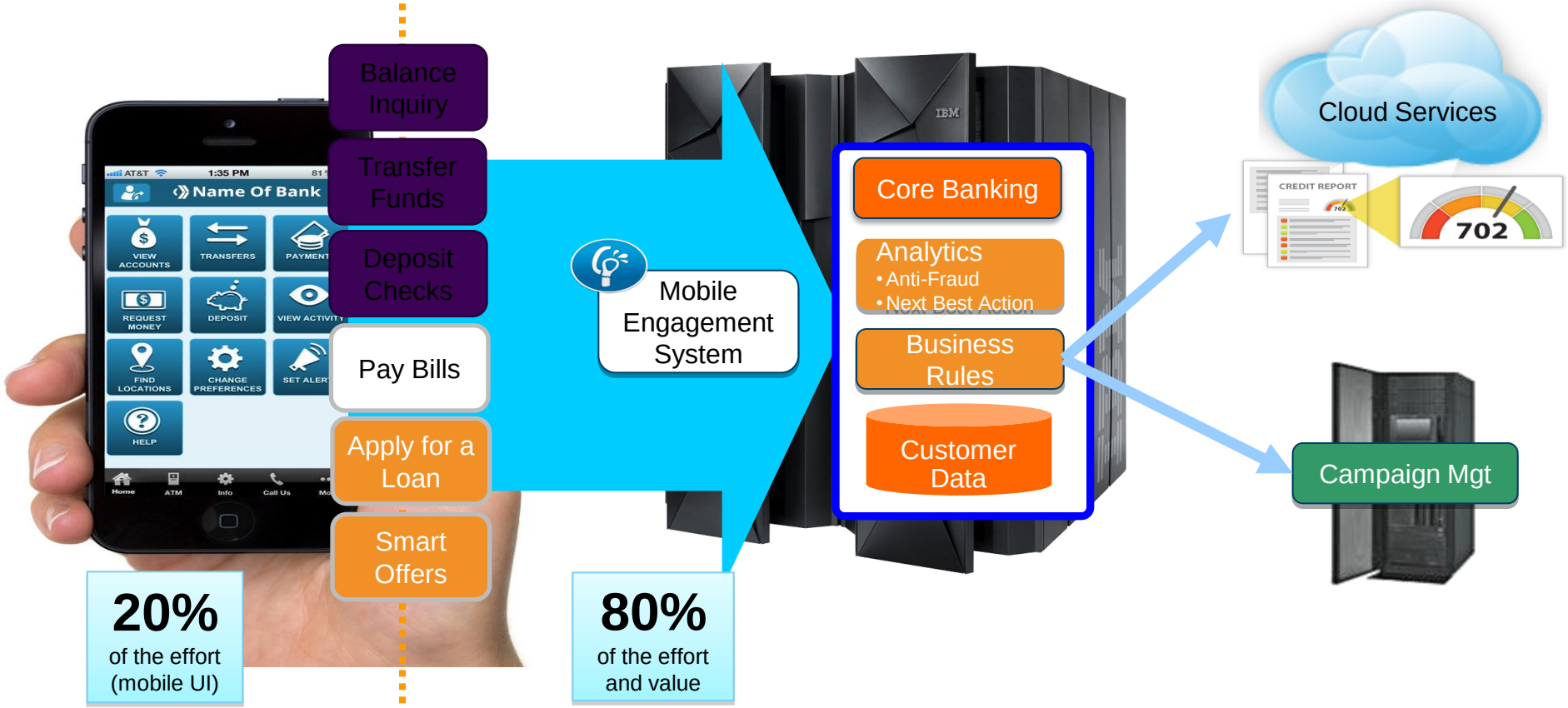
System z Cloud Scenario #1: Private Cloud with Linux on z

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



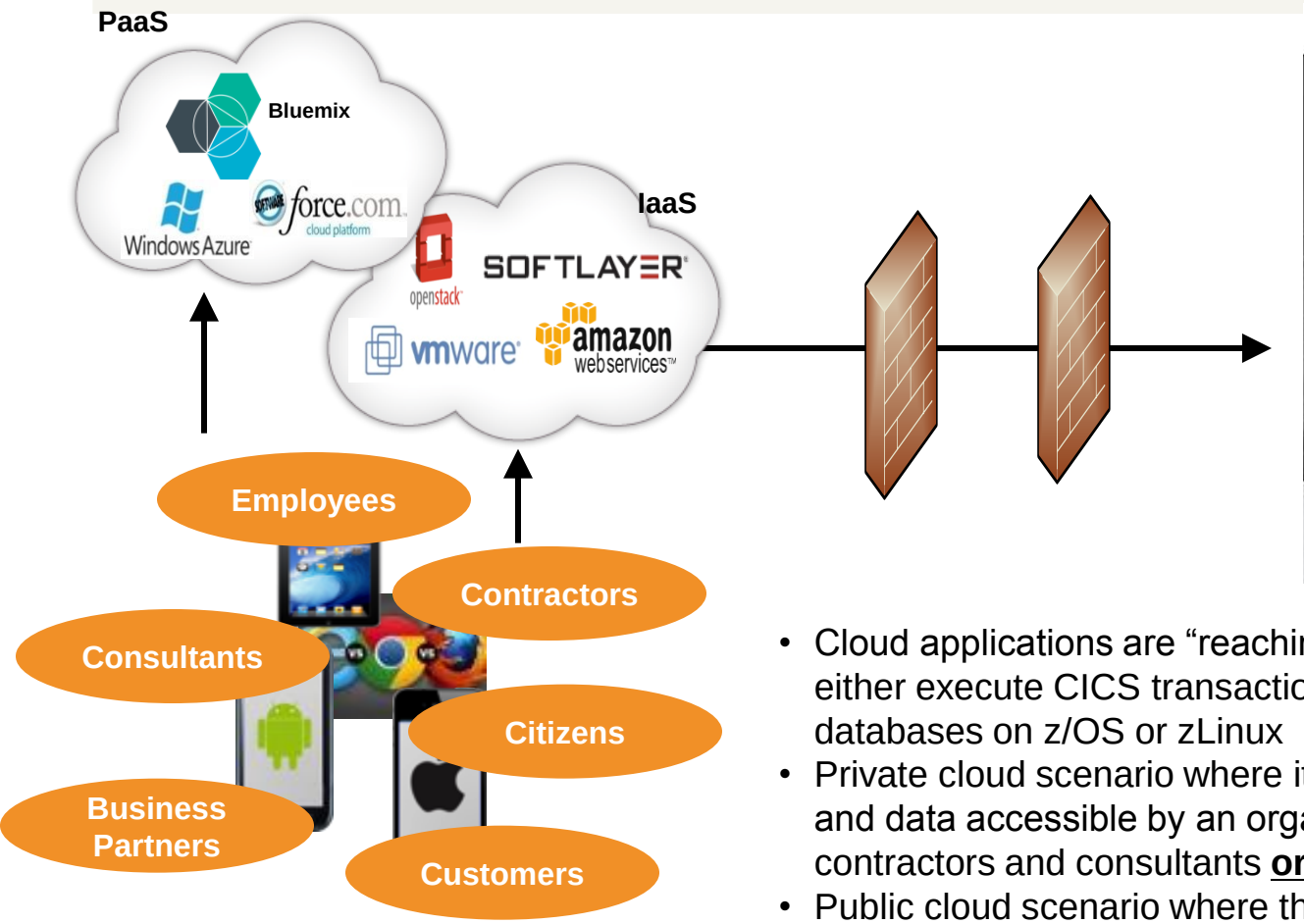
- Web servers, portals, applications and data reside on the VM's on System z utilizing zLinux
- Theoretically, this would be equivalent to a VMWare ESX server type of deployment
- Likely, it would only involve applications and data accessible by an organization's employees, contractors and consultants.

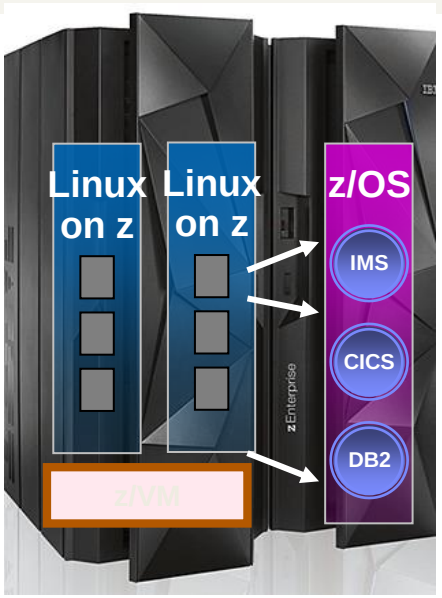
System z Cloud Scenario #2: z/OS Software as a Service



System z Cloud Scenario #3: Hybrid Cloud

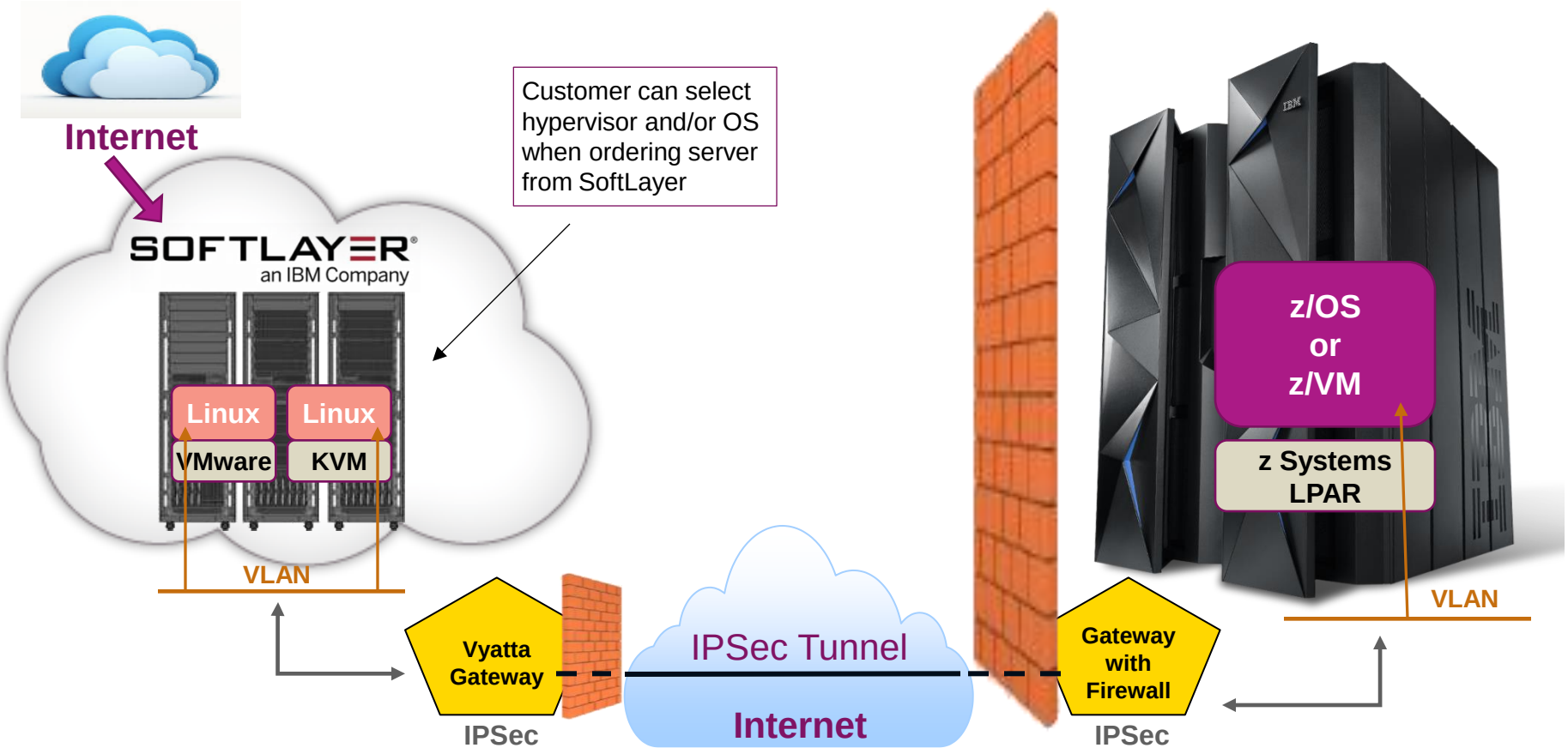
Enterprise applications moved to public cloud environments, including IaaS and PaaS, and integrating with Systems of Record deployed on System z within the enterprise





- 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 **or**
- 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.

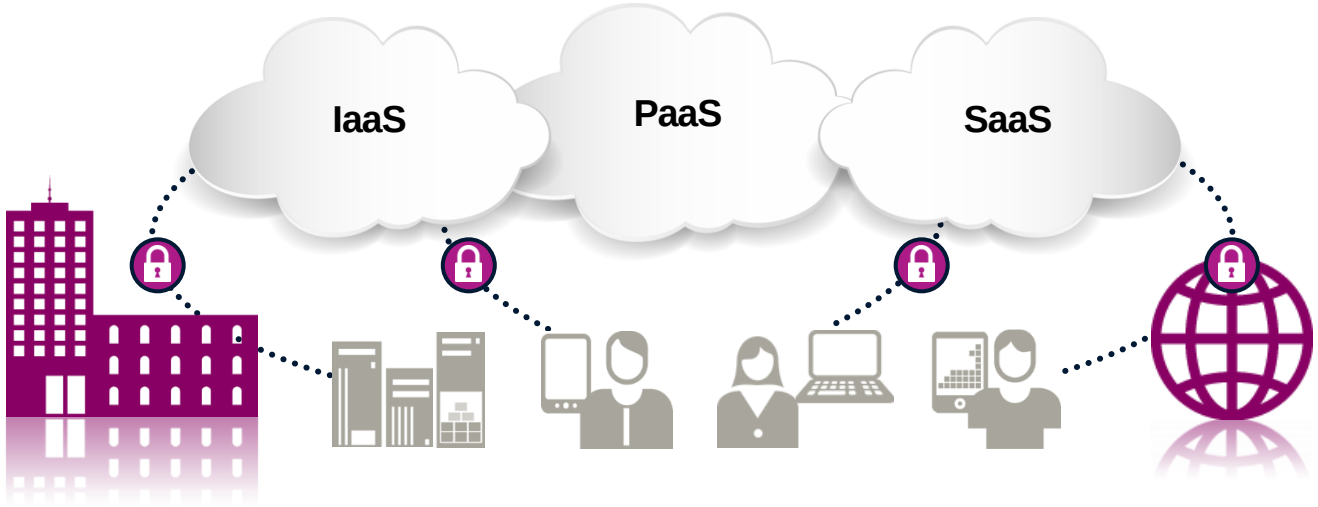
Gateway as a Service

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



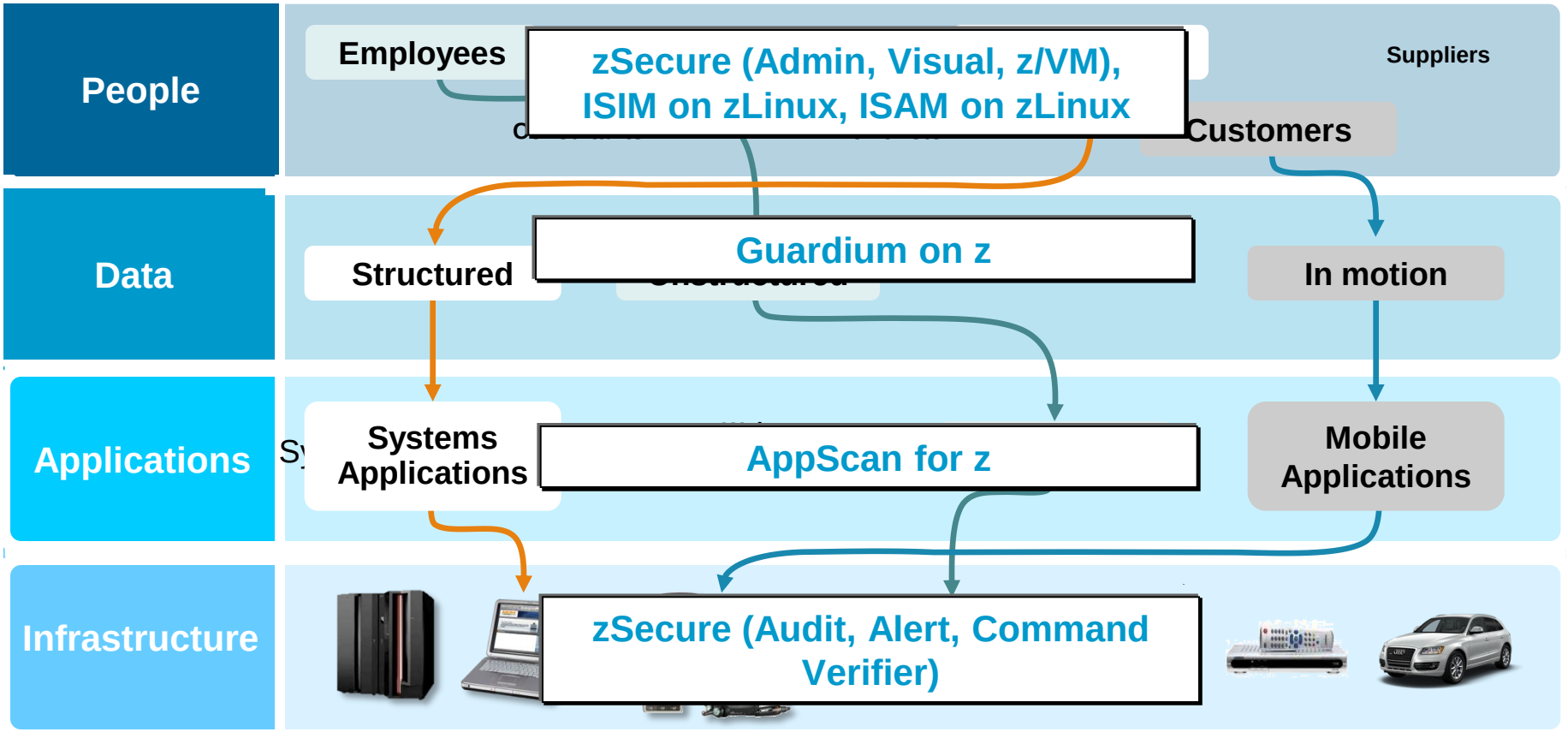
So, let's talk about the security requirements for such a powerful and dynamic system

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.



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

QRadar for z

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

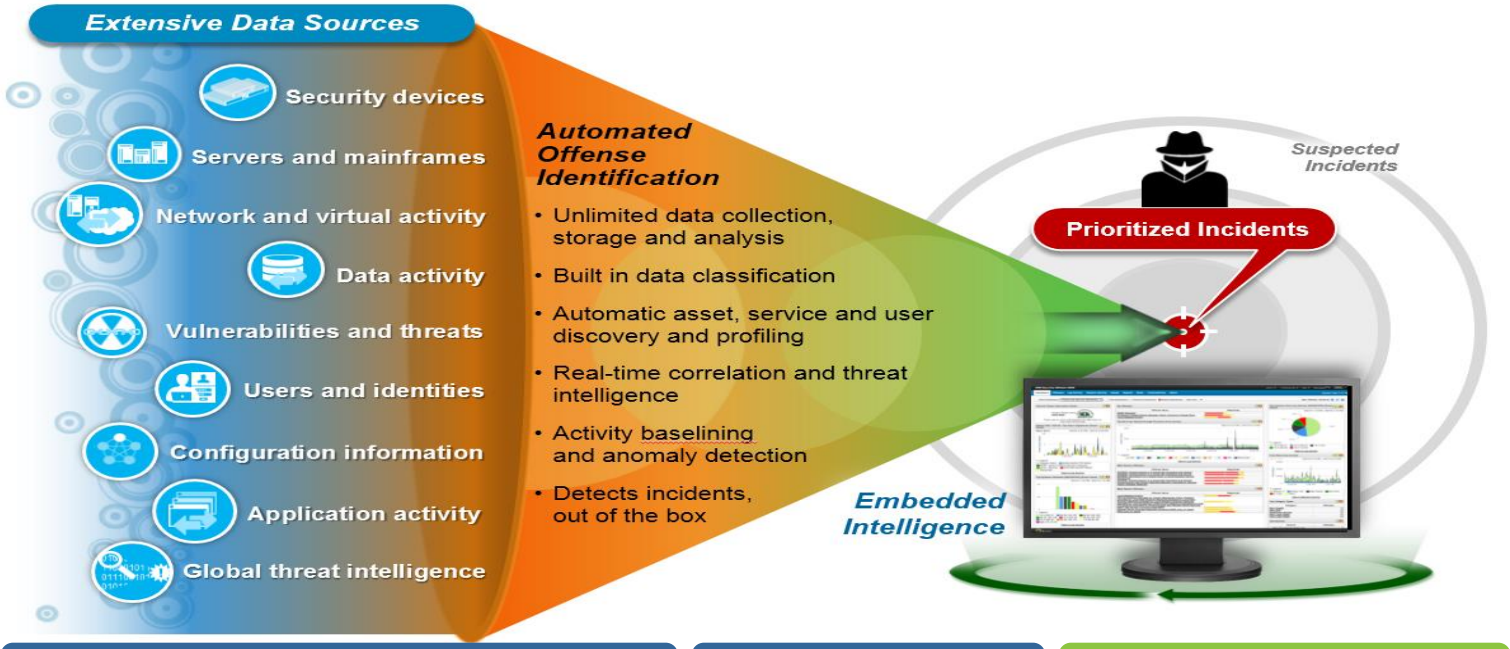
Better predicting risks to your business

- 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 + 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

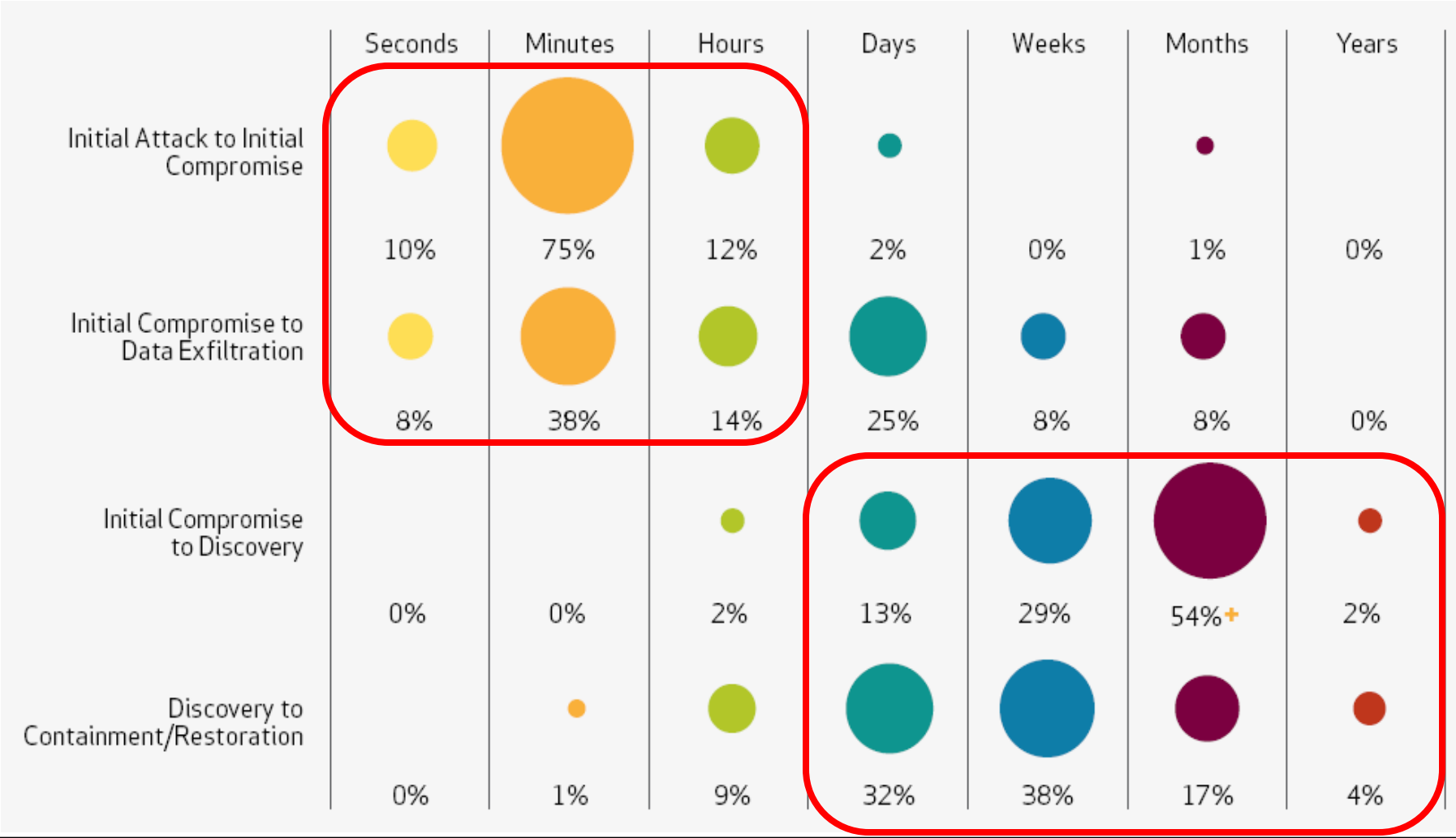
Client Benefits:

- 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



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)

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

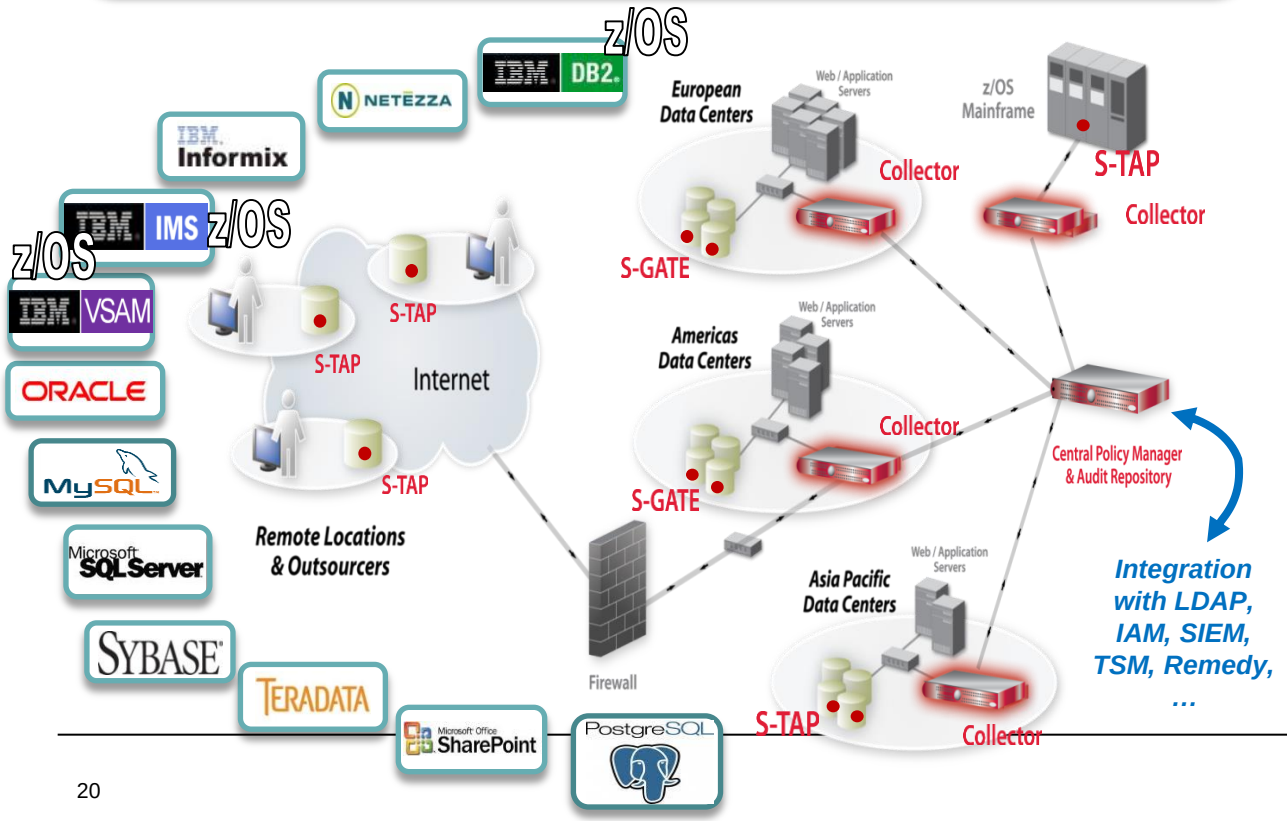
IBM Enterprise Key Management Foundation for Integrated Key Management

- 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

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

IBM Guardium Provides Real-Time Database Security & Compliance

- ✓ **Continuous, policy-based, real-time monitoring of all database activities, including actions by privileged users**
- ✓ **Database infrastructure scanning for missing patches, misconfigured privileges and other vulnerabilities**
- ✓ **Data protection compliance automation**



Key Characteristics

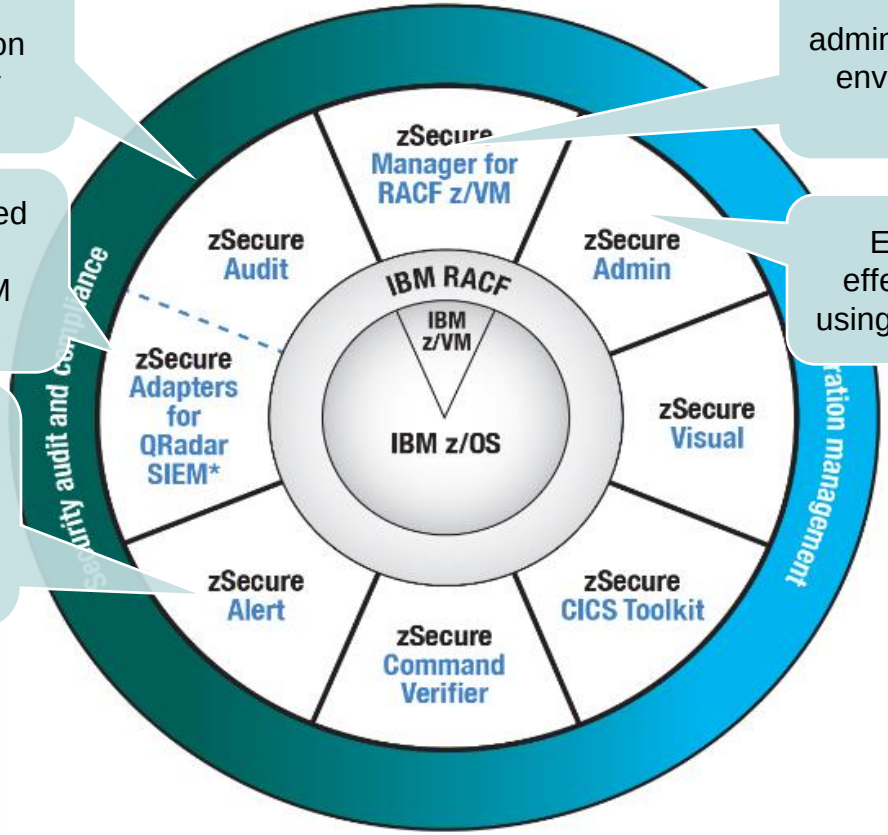
- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect unauthorized & suspicious activity
- Granular, real-time policies
- *Who, what, when, how*
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

IBM Security zSecure Suite: Helps address those unique security challenges that may impact the mainframe

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



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

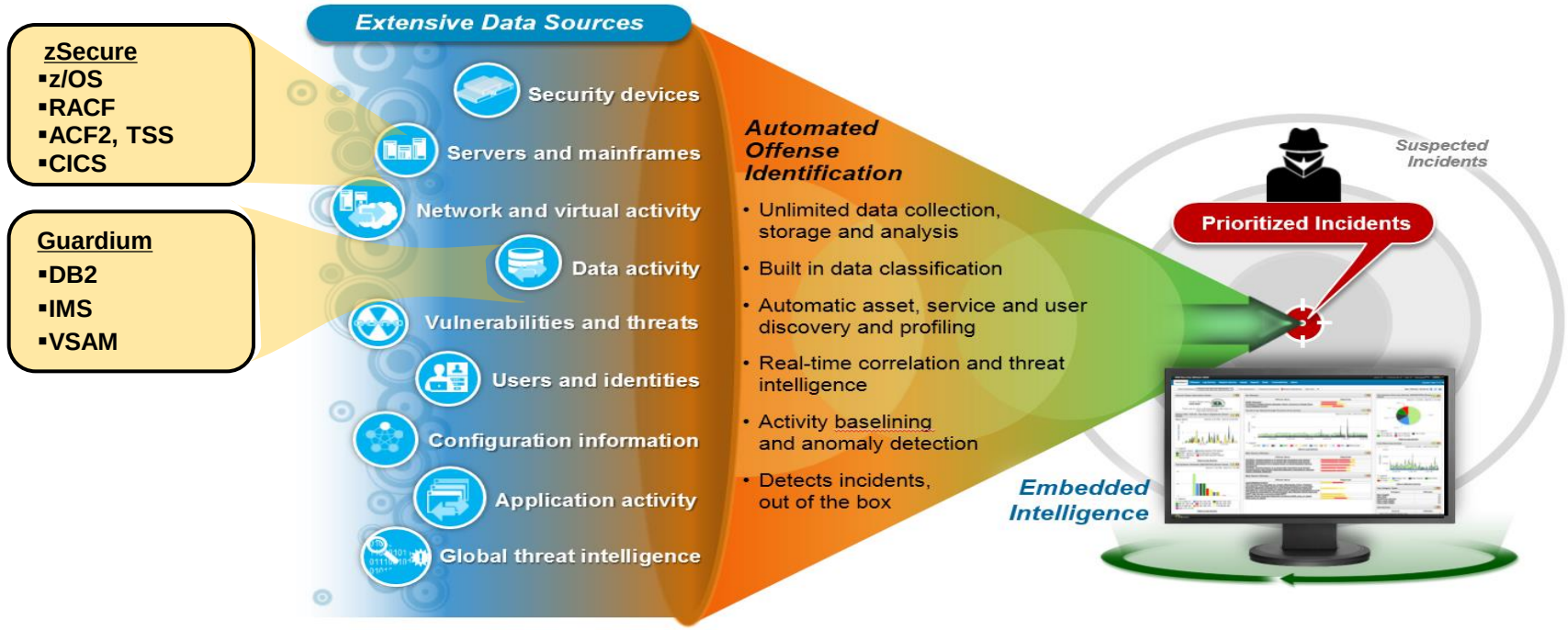
Combined audit and administration for RACF in the VM environment including auditing Linux on System z

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

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



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

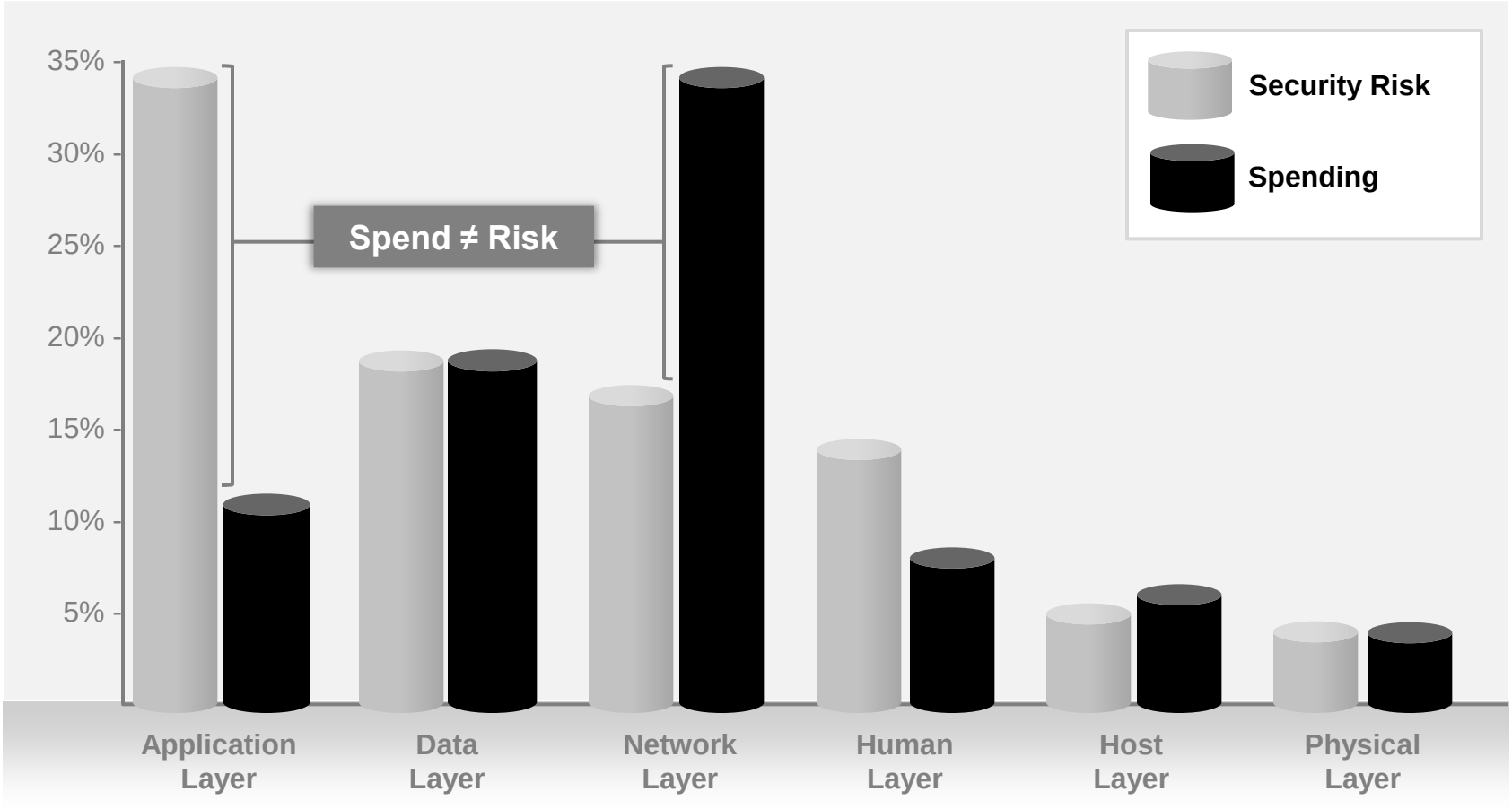
- ✓ Centralized view of mainframe and distributed network security incidents, activities and trends
- ✓ Creates automatic alerts for newly discovered vulnerabilities experiencing active 'Attack Paths'
- ✓ Produces increase accuracy of risk levels and offense scores, and simplified compliance reporting
- ✓ 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

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

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

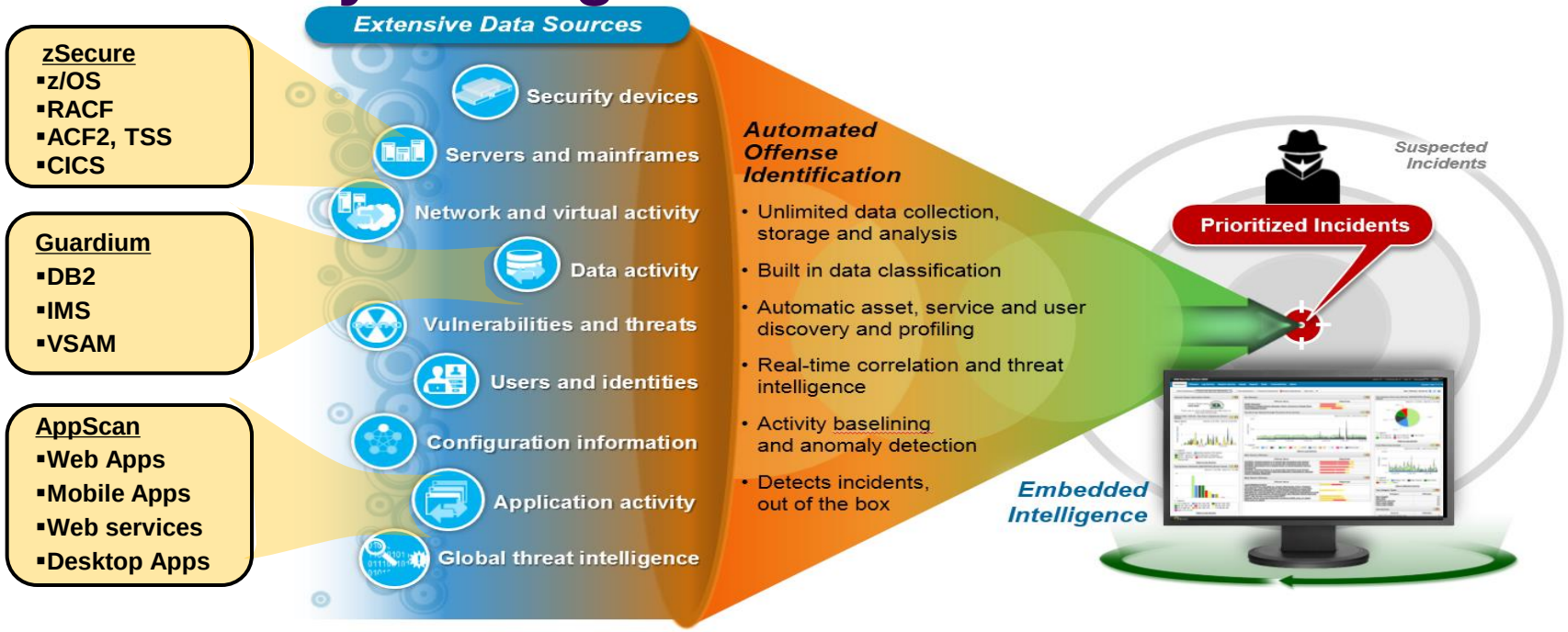
Interactive Analysis

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



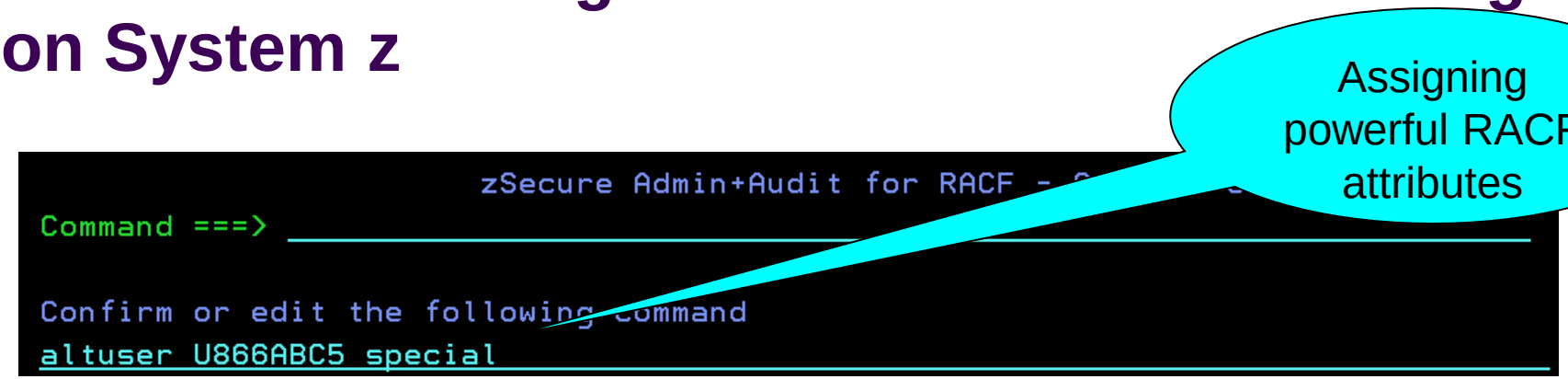
Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

- ✓ 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

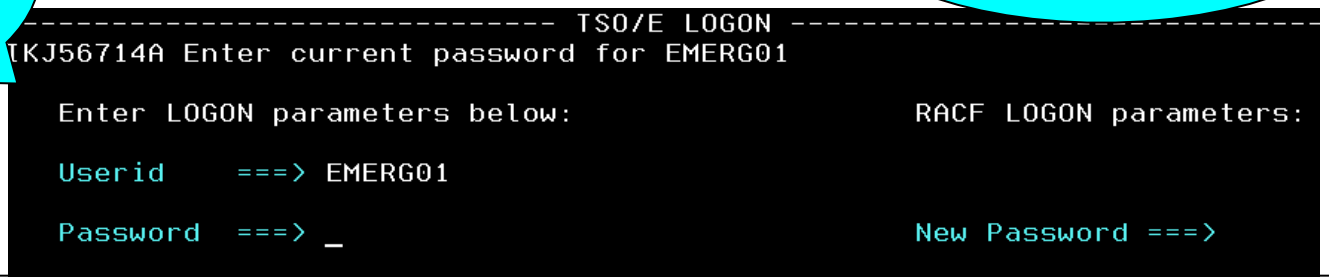


Assigning powerful RACF attributes

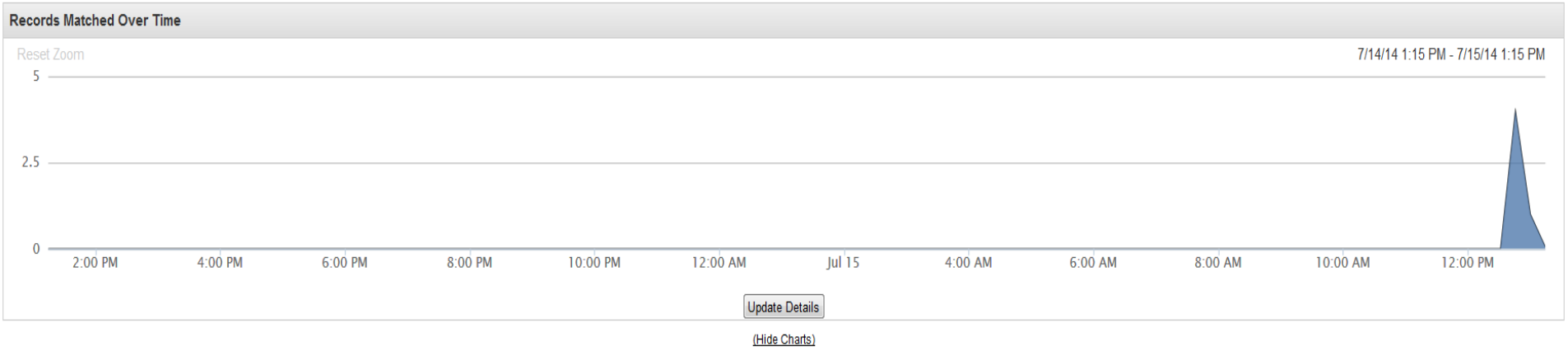
```
SETPROG APF,ADD,DSNAME=PEASEJ.LOADLIB,SMS
CSV410I SMS-MANAGED DATA SET PEASEJ.LOADLIB ADDED TO APF LIST
```

Modifying the Trusted Computing Base

Logon with powerful emergency user IDs



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**

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