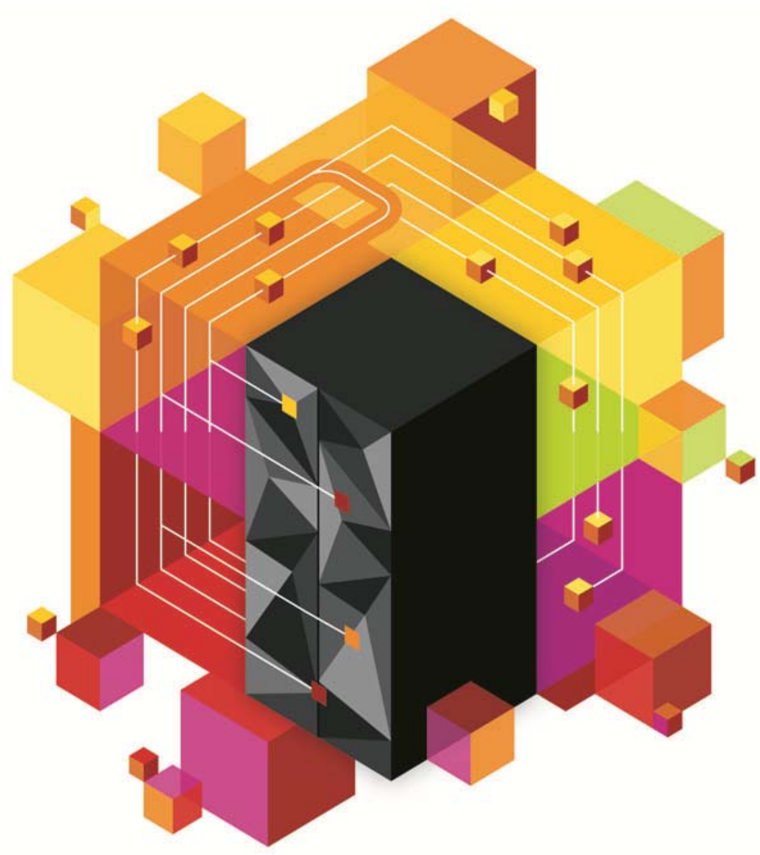
IBM zEnterprise Technology Summit

System z continues to be the ultimate security platform



Speaker:

Date:

Security – Is good enough … enough?

Security vigilance begins with the fundamental design built in from the start

Security vulnerabilities need multifaceted defenses

Being reactive is not good enough, anticipate the worst

Security must contain and prevent damage from escalating

Track intrusion attempts, notify immediately, understand patterns of attack

Security must adhere to standards, even the new ones

Fundamental security designed into the infrastructure increases protection

Mainframe security

What's the 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

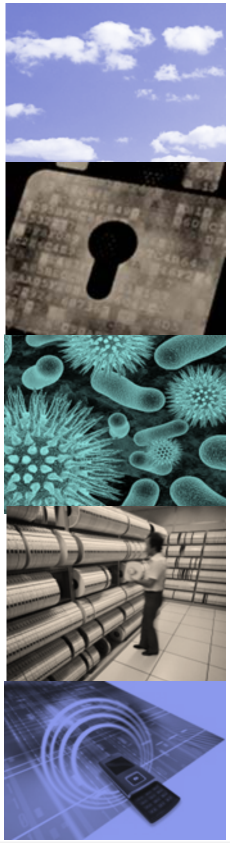
$ Lost customer business

$ Problem remediation

$ Claims from trusted vendors and business partners

$$ Damage to brand image

New Industry Trends Bring Security Challenges to Business



The cost of data loss has increased by 68% over the past five years[1]

Today’s applications with huge data volumes means protection of data is a key imperative

77% of execs believe that adopting cloud computing makes protecting privacy more difficult[2]

Security risks abound around the sharing of common cloud infrastructure

More than one half of security leaders say mobile security is their greatest near-term technology concern[3]

Emerging mobile and social applications can generate new use cases and also new risks

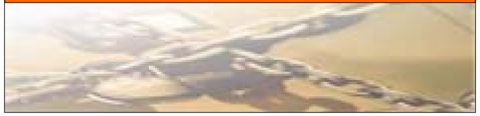
Are you security ready?

Redefining the challenge of securing your business

[1] Source: Computerweekly.com March 20, 2012 www.computerweekly.com/news/2240147054/Cost-of-data-breach-up-68
[2] Source: IBM's Institute for Business Value 2010 Global IT Risk Study
[3] Source: IBM 2012 CISO study

Security Challenges Specific to the Mainframe

Ensuring Compliance



Increasing Complexity

Rising Costs

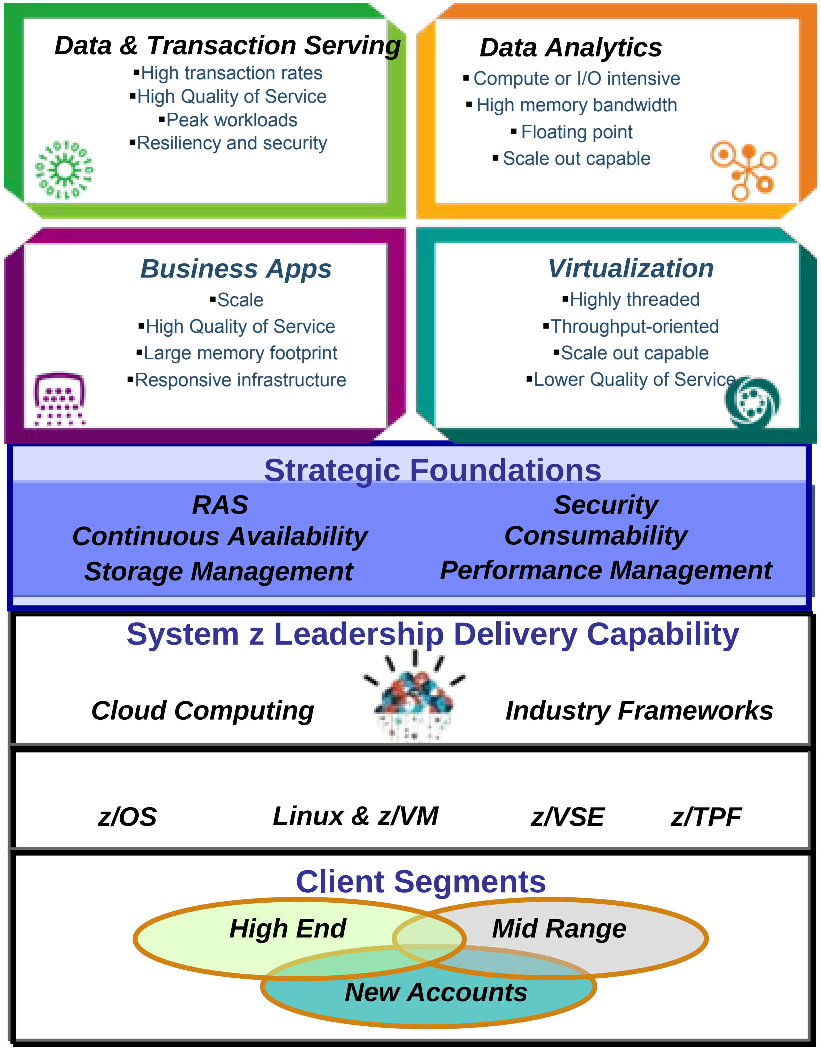
Visibility

- **Compliance:**
  - Compliance verification is a manual task with alerts coming after a problem has occurred, if at all
- **Complexity:**
  - The mainframe is an integral component of many large business services, making the identification and analysis of threats very complex and creating a higher risk to business services
  - Systems are vulnerable to the unmanaged activities of privileged users.
- **Cost:**
  - Mainframe security administration is usually a manual operation, or relies upon old, poorly documented scripts.
  - Administration is done by highly skilled mainframe resources that are usually in short supply.
- **Visibility:**
  - Mainframe processes, procedures, & reports are often siloed from the rest of the organization

Security is one of the strategic foundations of System z

- **Integrated security that spans from:**
  - Hardware
  - Firmware
  - Hypervisors
  - System z Operating Systems
  - Middleware and applications
  - Network
- **Integrated security that spans to an zEnterprise ensemble**
- **Hardware and firmware assists enhance security QoS**
- **System z security is integrated at all “levels” of the platform**
- **From a strategic view -- multiple security strategies converge -- to create unified view of security on System z**

Optimizing System z for Strategic Workloads & Industry-based Initiatives



Data & Transaction Serving
- High transaction rates
- High Quality of Service
- Peak workloads
- Resiliency and security

Data Analytics
- Compute or I/O intensive
- High memory bandwidth
- Floating point
- Scale out capable

Business Apps
- Scale
- High Quality of Service
- Large memory footprint
- Responsive infrastructure

Virtualization
- Highly threaded
- Throughput-oriented
- Scale out capable
- Lower Quality of Service

Strategic Foundations

RAS
Continuous Availability
Storage Management

Security
Consumability
Performance Management

System z Leadership Delivery Capability

Cloud Computing
Industry Frameworks

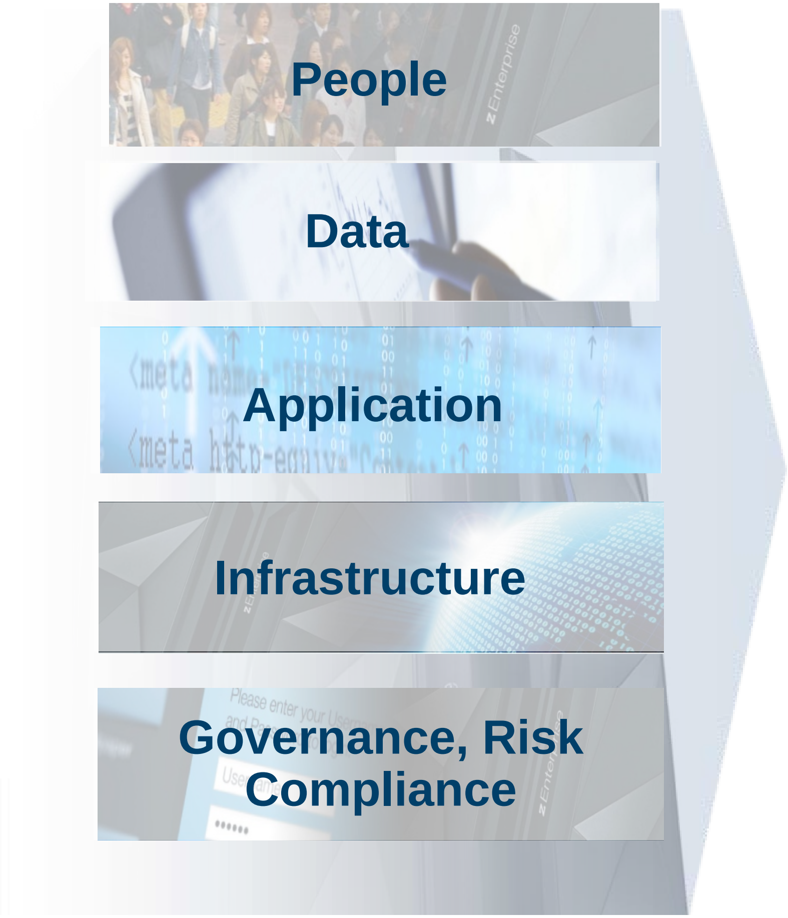
z/OS *Linux & z/VM* *z/VSE* *z/TPF*

Client Segments

High End
Mid Range
New Accounts

zEnterprise - Ultimate security to protect your mission critical assets

Deeply Integrated Security Throughout the Stack



People

Data

Application

Infrastructure

Governance, Risk Compliance

from IBM Security Framework

- ✓ Consistent policy based user authentication, access control, audit and management
- ✓ Encrypt critical data, at rest and in flight, with centralized key management
- ✓ Detect application vulnerabilities early to contain potential problems
- ✓ Create a secured virtualized pool of resources as a foundation for private cloud
- ✓ Reduce operational risk. Improved compliance to evolving regulations and audit responsiveness

Protect People, Identities throughout your Extended Enterprise

- Centrally manage identities and access rights across the enterprise
- Establish a unique, trusted identity and provide accountability for all user activities
- Deliver a scalable digital certificate solution based using IBM System z® as a trusted certificate authority
- Use IBM Enterprise PKCS #11 (Public Key Cryptography Standard) to provide outstanding levels of security
- CCA architecture provides many cryptographic key management and generation functions
- Achieve Role Based Access Control
- Leverage trusted identity and context for additional administrative and fine-grained authority on DB2®

Up to 52% lower security administrative costs efforts on mainframe

IBM zEnterprise® Solutions

- RACF®, LDAP, Identity propagation
- IBM Security zSecure
- Tivoli® Federated Identity Manager
- System z as a Certificate Authority
- ICSF support of PKCS #11
- DB2 and RACF security

IBM Enterprise PKCS #11 to provide digital signatures with the highest levels of assurance; designed for FIPS 140-2 Level 4 requirements.

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

Maintain Confidentiality of Data and Protect Your Critical Assets

- Secure your business critical assets with tamper resistant crypto cards
- High speed encryption that keeps sensitive keys private, ideal for securing high volume business transactions
- Centralized key management to manage your encryption keys (z/OS PKI infrastructure)
- EKMF enterprise management of keys and certificates targeting for financial customers
- Trusted Key Entry (TKE) Workstation to securely enter master keys
- Encrypt DB2 and IMS™ data with InfoSphere™ Guardium® Data Encryption
- Encrypt sensitive data before transferring it to media for archival purposes or business partner exchange
- Protect and mask sensitive z/OS data with Optim™

Secure and encrypt your data throughout its lifecycle using entitled crypto or tamper resistant cards

The Crypto Express co-processors have achieved FIPs 140-2 level 4 hardware evaluation

IBM zEnterprise Solutions

- Crypto Express4s
- ICSF
- EKMF, TKE Workstation
- Guardium DB2 Encryption, Dynamic Access Managament
- IBM Security Key Lifecycle Manager
- z/OS Encryption Facility
- Optim for data masking

The zEC12 can perform up to 19,000 SSL handshakes per second when using four Crypto Express4S adapters configured as accelerators.

Defend Against Network Attacks and Intrusions

- Built-in defenses to ensure high availability of the system against denial-of-service attacks
  - Network IPS front end fraud and threat detection
  - Policy-based network communications managed through RACF for consistent policy enforcement
- Secured communications to the zBX with IEDN and INMN networks
  - HiperSockets™ for high speed secured communications across LPARS
  - Advanced threat detection with real-time alerting from zSecure and QRadar
- Evaluate inbound encrypted data for suspect activity

Integrated intrusion detection in the network stack that works even with encrypted sessions.

IBM zEnterprise Solutions

- RACF, Comm. Server AT-TLS, SSL, IPSec
- Intrusion protection and defense mechanisms (Comm Server)
- Secured Internal networks (INMN IEDN)
- IBM Security Network IPS appliance
- HiperSockets communications
- QRadar SIEM with zSecure Alert

2011 Average Organizational Cost per Data Breach in US was $5.5M* . Only IBM zEnterprise offers end to end encryption.

IBM System Communications Server serves as a line of defense with Communication Server Intrusion Detection and Intrusion Prevention Services

*Symantec's 2011 Annual Study: U.S. Cost of a Data Breach

Manage Compliance to Reduce Risk and Improve Governance

- Reduce operational risk with exhaustive audit, reporting and control capabilities
- Consistent auditing and reporting using a centralized model integrated with event management
- Enforced separation of duties preventing any one individual from having uncontrolled access
- Customizable compliance monitoring, audit, reporting with RACF and zSecure
- Prevent issuance of problematic commands with RACF command verification
- Continued drumbeat of health checks to catch potential problems early

68% of CIOs selected Risk Management and Compliance as one of the most important visionary plan elements (CIO Study 2011)

IBM zEnterprise Solutions

- z/OS Audit Records (SMF)
- RACF and SAF
- zSecure Audit
- zSecure Command Verifier
- QRadar SIEM
- Optim
- Healthchecks

Customers can save up to 70% of their audit and compliance overhead with centralized security audit and compliance reporting and more.*

"zSecure delivers the reports we need to meet the demands of security, audit and regulatory requirements such as SOX. By easing the burden of audits, our security administrators can focus their time on improving security quality." ***— Source: Damien Dunne, Mainframe Systems Manager, Allied Irish Banks***

Meet regulatory and corporate mandates; achieve improved governance by driving consistent security policy

*Based on a European Insurance Co's input to IBM BVA using IBM zSecure

Deliver Isolation to Provide Integrity and Trust for a Smarter Cloud

- System z PR/SM™ hypervisor maintains strict isolation and compartmentalization between workloads
- Fast clear key operations (CPACF), secure keys or protected keys
- World class security certifications: Common Criteria EAL 5+, FIPS 140-2 level 4
- Labeled DB2 and z/OS security for secured multi-tenancy
- HiperSockets for fast, secured in-memory communications between LPARs
- SAF interface provides automatic built-in centralized control over system security processing
- Storage protect keys safeguards memory access
- Only authorized programs use sensitive system functions; protects against misuse of control
- IBM backed "Integrity Statement" in effect for decades

Common Criteria EAL5+ allows your many workloads to be concurrently hosted & securely isolated

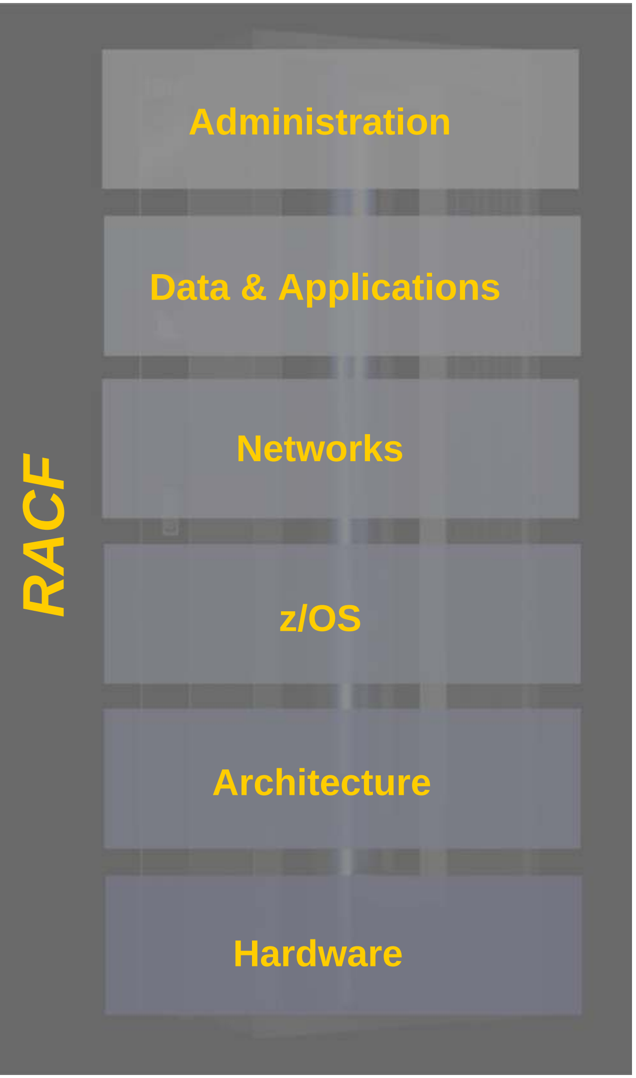
IBM zEnterprise Solutions

- PR/SM at EAL 5+, RACF at EAL 5
- Multi-Level Security on z/OS and DB2
- z/Secure Manager for RACF z/VM®
- HiperSockets
- System z hardware
  - Storage protection key
  - APF Authorization
  - Integrity Statement

IBM is unique in having published an Integrity Statement for z/OS and z/VM, in place for over three decades

System z security is hardwired throughout the server, network and infrastructure. It cannot be bypassed

Resource Access Control Facility (RACF)
The backbone of mainframe security



Enables application and database security without modifying applications

Can reduce security complexity and expense:

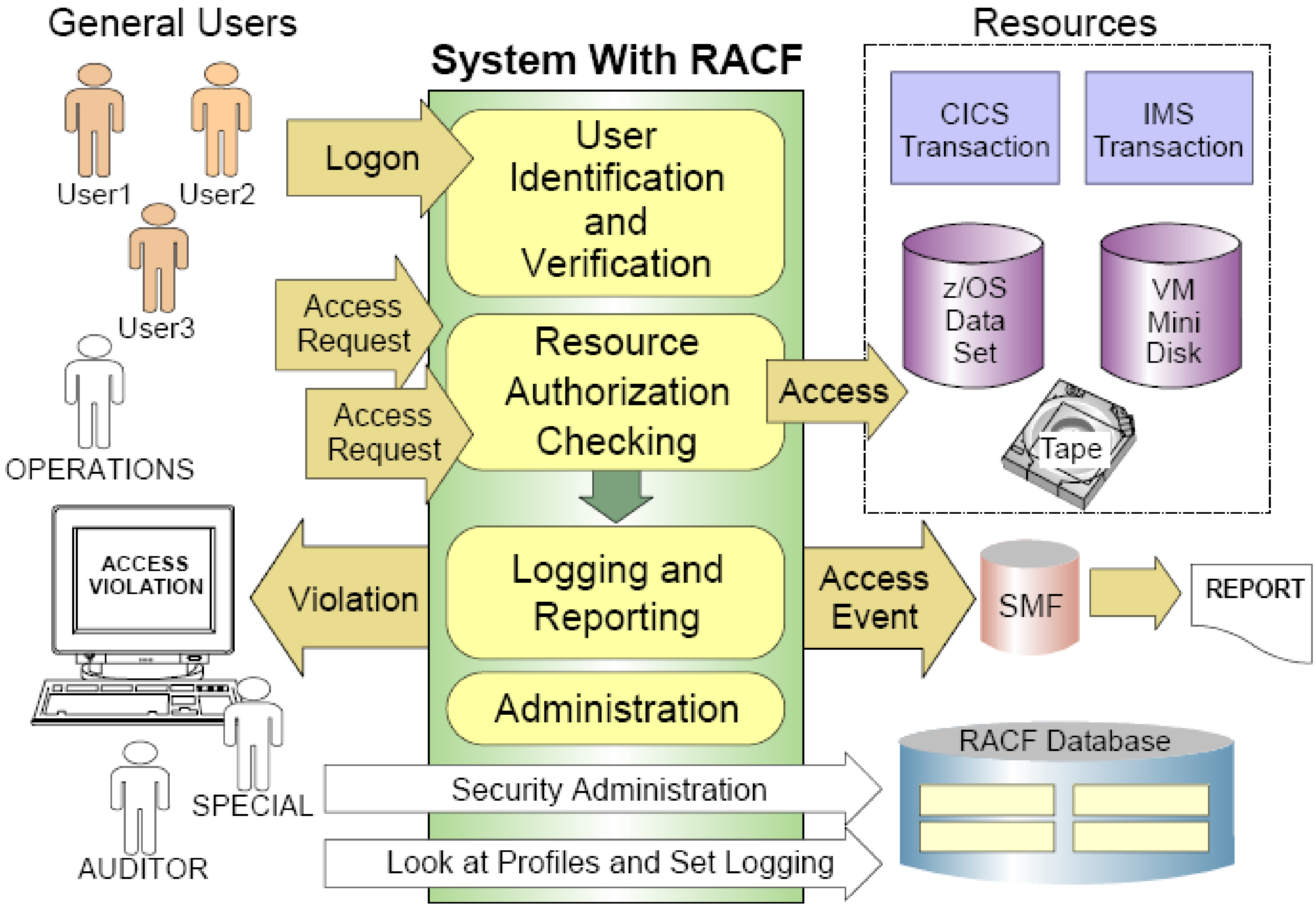
- Central security process that is easy to apply to new workloads or as user base increases
- Tracks activity to address audit and compliance requirements

Integration with distributed system security domain

Checking for “Best Practices” with z/OS HealthChecker

Serving mainframe enterprises for over 30 years

RACF Features and Functions



Typical problems

- **Large and complex environment**
  - ➢ Existing tools not scalable or flexible to meet evolving business requirements

- **In-house written software**
  - ➢ Often out of date; new releases of z/OS + RACF each year
- **Manual and time consuming tasks**
  - ➢ No time to focus on improving quality of Security and Service
- **Regulatory and compliance demands (E.g. PCI-DSS)**
  - ➢ Failed an audit or assessment
- **Failed Internal or External Audits**
  - ➢ Significant weaknesses in controls that were not previously detected
- **Excessive and unused access in the security database**
  - ➢ No regular and automated clean-up to improve security and performance

And there’s more . . .

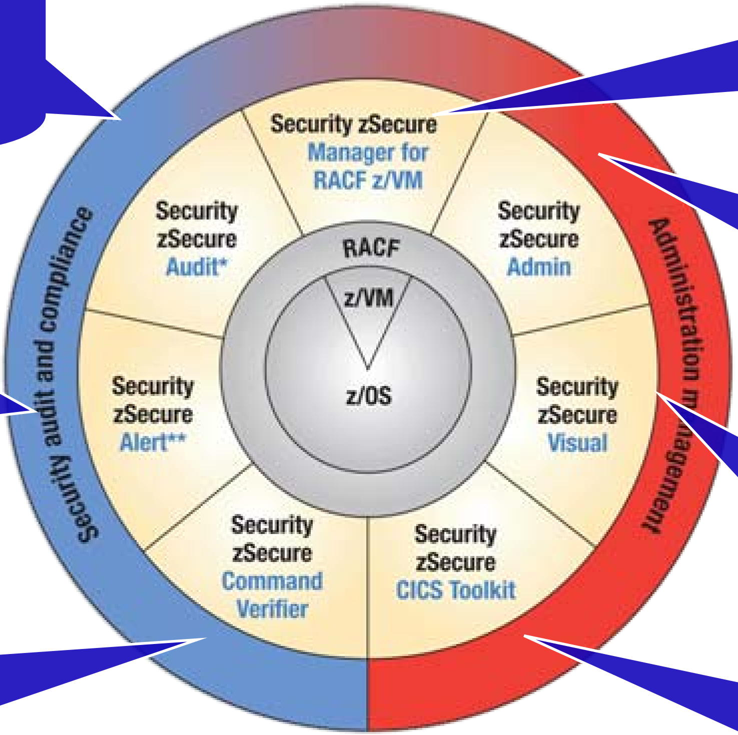
- **Segregation of duties are not enforced**
  - Conflicting access permissions in business or IT departments
- **Privileged users are not adequately monitored or “controlled”**
  - Inappropriate actions go undetected
- **Policies and procedures are not adhered to**
  - RACF commands issued that weaken controls
- **Processes and procedures are not structured or repeatable**
  - How and what did we use before?
- **System or application outages caused by Security Administrators**
  - A RACF command that should have been prevented
- **Concerns around skills and knowledge of System z Security**
  - Existing toolset does not improve capability

IBM Security zSecure suite products

Vulnerability analysis for your mainframe infrastructure. Automatically analyze and report on security events detect security exposures, and report to SIEMs.

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

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


Security audit and compliance
Administration management
Security zSecure Manager for RACF z/VM
Security zSecure Admin
Security zSecure Visual
Security zSecure CICS Toolkit
Security zSecure Command Verifier
Security zSecure Alert**
Security zSecure Audit*
RACF
z/VM
z/OS

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

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

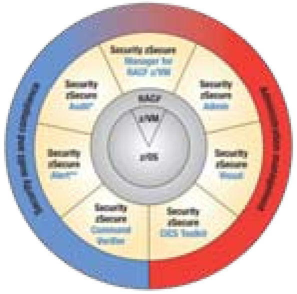
Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

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

Security zSecure Suite Benefits

Consolidate and centralize security management
Leverage the mainframe as your enterprise security hub

- **Simplify security administration and provisioning:**
  - Reduce administration time, effort and cost
  - Enable de-centralized administration
  - Quick response time, enabling business
  - Reduce training time needed for new administrators
  - Enforce security policy and implement best practices
- **Automate audit, monitoring and compliance:**
  - Pass audits more easily, improve security posture
  - Save time and costs through improved security and incident handling to manage risk
  - Increase operational effectiveness
- **Reduce costs and improve ROI**



IBM can save customers up to 70% in auditing overhead on mainframe

zSecure provides with significant business value

zSecure	IBM's Significant Product Capabilities	IBM's Business Value
Enhanced Administration	• Automated cleanup of orphan accounts • Offline change management & change modeling • RACF DB merges • Cascading permissions for Group Tree Structures	• Helps improve security at lower labor cost • Aids in reducing costs by avoiding configuration mistakes • Eases labor cost for directory merges • Helps reduce labor cost by more efficient group management
Auditing & Compliance	• Customizable reports • Automated risk classification • Broad coverage of audit control points • Security Intelligence to identify and manage Trusted Users • Exceptional coverage of security event records, including TCP/IP, CICS, DB2, & IMS	• Can provide report that match business model / business requirements • Helps optimize labor utilization by prioritizing tasks • Aids in reducing cost by helping eliminate outages not detected by non-IBM solutions • Address business risk by helping to find segregation of duties exposure

zSecure provides with significant business value

zSecure	IBM's Significant Product Capabilities	IBM's Business Value
Alerting	• Can capture unauthorized back door changes to RACF, Security Policies • Extensive coverage of real time audit control points, especially network	• Can reduce cost by helping eliminate outages not detected by competition
Command Verification	• Auditing of RACF changes by Privileged Users	• Can complete audit in seconds, not days, reducing labor cost
Visual Administration	• Real time, on line updates • Integrates w/ HR Systems (PeopleSoft, SAP, etc.) • Roles based administration for separation of duties • Manage from a single screen	• Permits changes in minutes, not overnight • Enables better business control by providing access for only current employees & contractors • Helps minimize business risk by enabling segregation of duties • Aids in reducing labor cost and errors
CICS based administration	• Externalizes authentication from the application	• Can lower application development and maintenance costs

Solving Customer Security Challenges in Mainframe Environments

z/OS, z/VM and Linux on System z

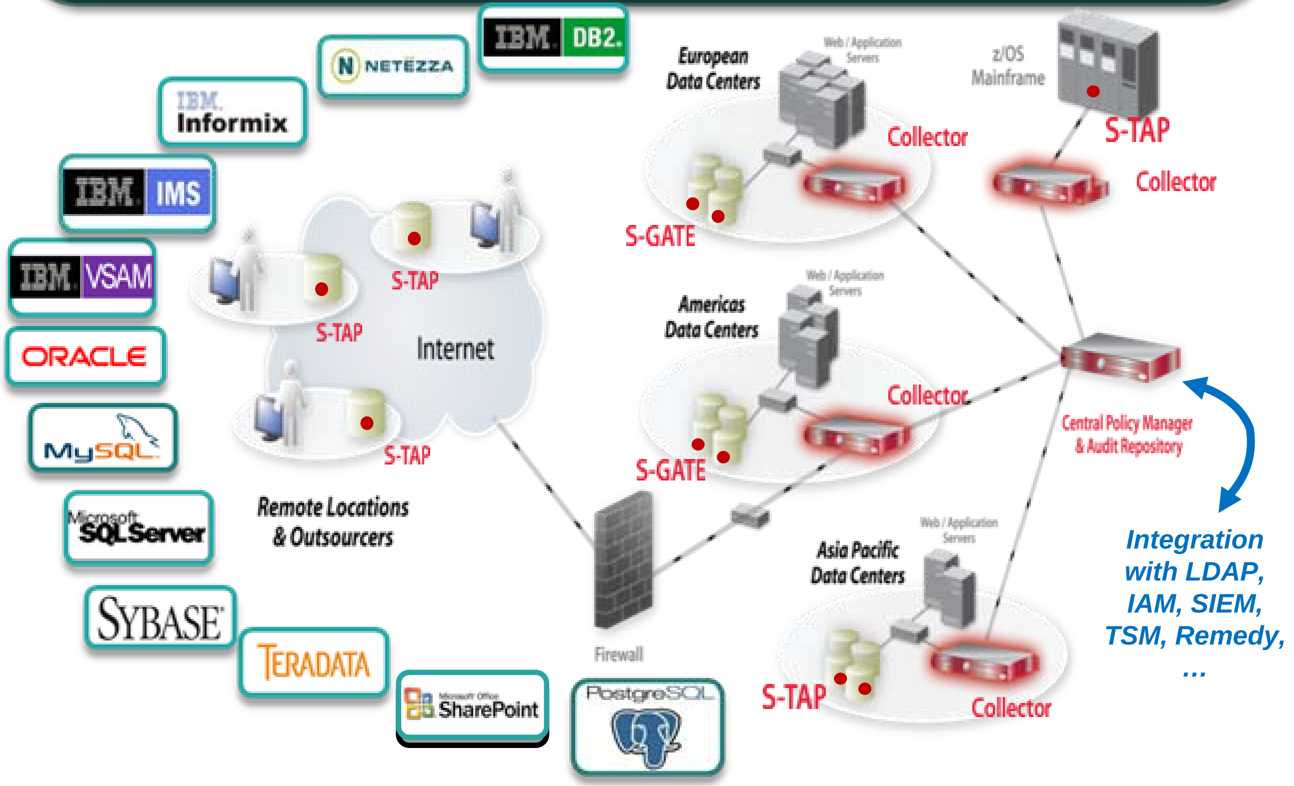
NORWICH UNION an AVIVA company	Automate continuous compliance to address worldwide industry standards and regulations	Assure auditors that preventative, detective and corrective controls are installed
AIB	Improve administrator effectiveness with built-in best practices	Reduced identity and access security management overhead and costs with integrated security management
AVIVA	Protect and ensure the integrity of sensitive enterprise data	Leveraged IBM technologies to track and redact medical information from imaged documents.
	Simplify mainframe administration and auditing for consolidated systems and workloads	Establish user identification services for compliance and governance

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



Integration with LDAP, IAM, SIEM, TSM, Remedy, …

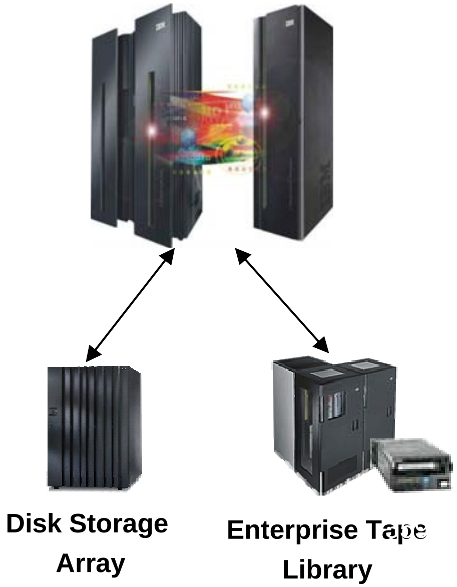
Key Characteristics

- 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*
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Security Key Lifecycle Manager for z/OS V1.1

Attributes of encryption and key management:

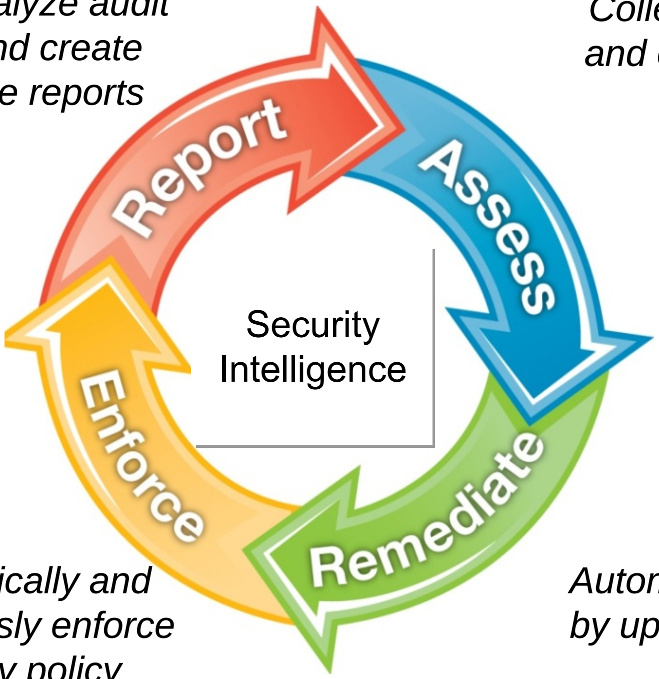
- Encryption in storage hardware does not hurt performance
- Encryption and key management doesn't require changing applications, middleware, JCL, operating systems
  - Key management completely separate from the data path
  - Storage arrays and libraries contact the key manager on behalf of the application and hosts doing I/O
    - With disk arrays done at power up
    - With tape libraries at each cartridge mount
- Encryption and key management fits into your operations management
  - Separation of duties
  - Leverage investments in high availability and security



ISKLM V1.1 benefits:

- Easy upgrade from EKM, easy SMPE install
- Still supports ICSF, RACF, crypto express hardware
- Writes SMF records type 83 subtype 6
- Supports all of the latest system z centric storage – tape and disk
- No longer requires DB2 or SSRE

Customers need security intelligence: automated continuous compliance to address worldwide industry standards and regulations



Monitor, analyze audit records and create compliance reports

Collect information, assess, and establish security policy

Automatically and continuously enforce security policy

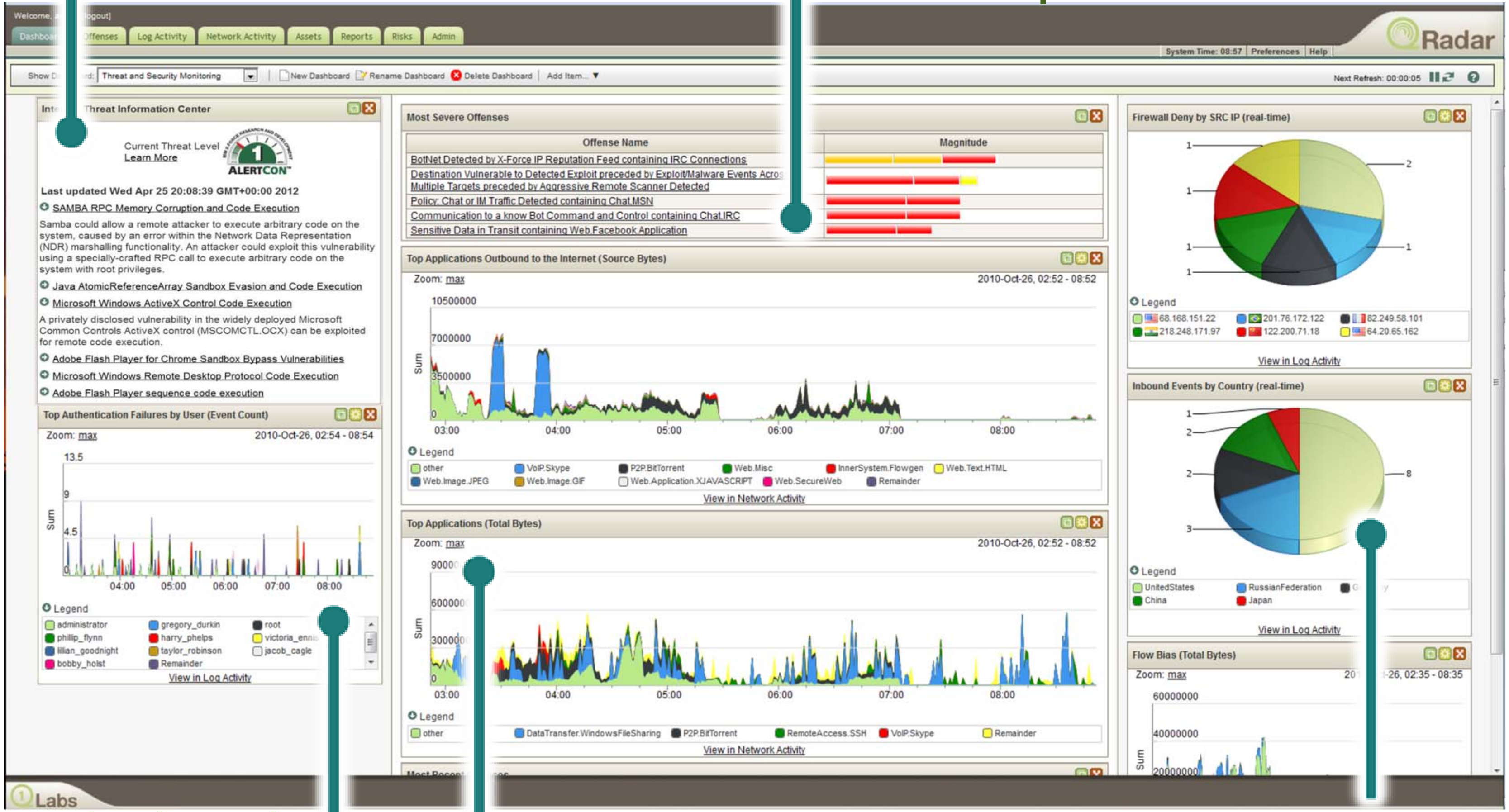
Automate corrective actions by updating access controls

IBM Security zSecure Compliance and Auditing With QRadar

Security Intelligence: *QRadar provides security visibility*

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



Internet Threat Information Center

Current Threat Level 1 ALERTCON™
Learn More

Last updated Wed Apr 25 20:08:39 GMT+00:00 2012

- SAMBA RPC Memory Corruption and Code Execution

Samba could allow a remote attacker to execute arbitrary code on the system, caused by an error within the Network Data Representation (NDR) marshalling functionality. An attacker could exploit this vulnerability using a specially-crafted RPC call to execute arbitrary code on the system with root privileges.

- Java AtomicReferenceArray Sandbox Evasion and Code Execution
- Microsoft Windows ActiveX Control Code Execution

A privately disclosed vulnerability in the widely deployed Microsoft Common Controls ActiveX control (MSCOMCTL.OCX) can be exploited for remote code execution.

- Adobe Flash Player for Chrome Sandbox Bypass Vulnerabilities
- Microsoft Windows Remote Desktop Protocol Code Execution
- Adobe Flash Player sequence code execution

Most Severe Offenses

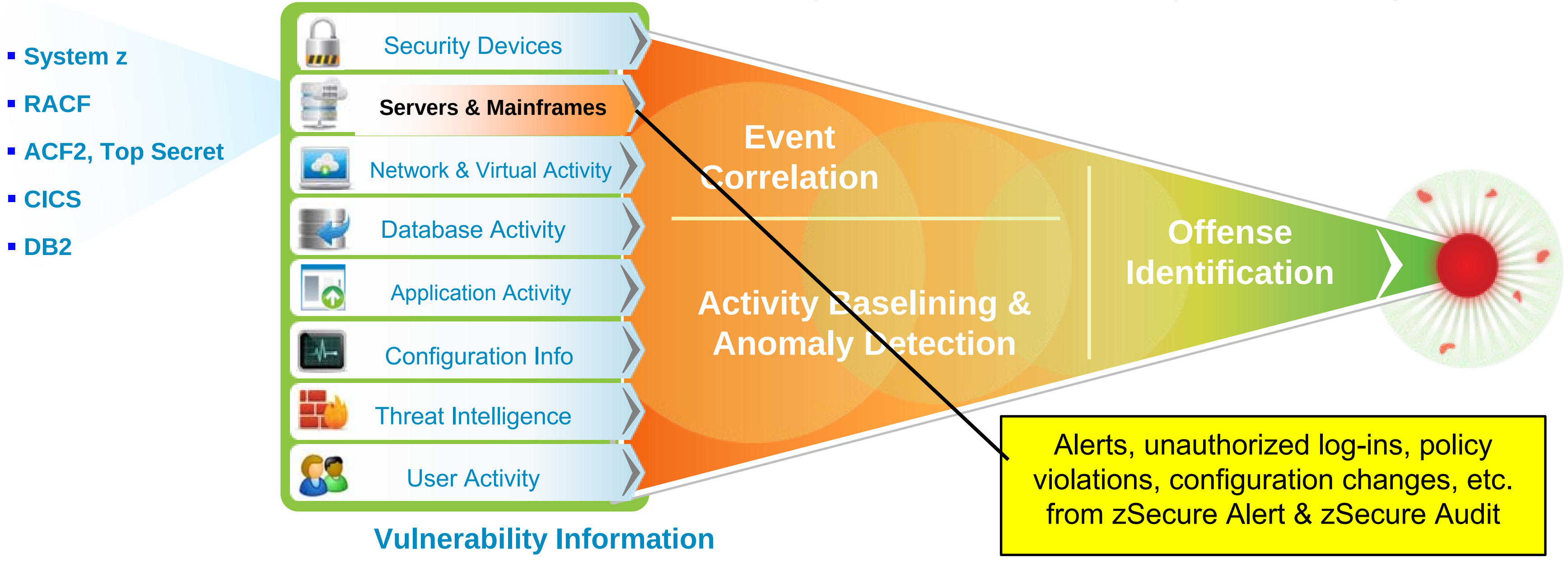
Offense Name	Magnitude
BotNet Detected by X-Force IP Reputation Feed containing IRC Connections	
Destination Vulnerable to Detected Exploit preceded by Exploit/Malware Events Acros Multiple Targets preceded by Aggressive Remote Scanner Detected	
Policy: Chat or IM Traffic Detected containing Chat.MSN	
Communication to a know Bot Command and Control containing Chat.IRC	
Sensitive Data in Transit containing Web.Facebook.Application	

Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

zSecure & QRadar improve your Security Intelligence



- System z
- RACF
- ACF2, Top Secret
- CICS
- DB2

Security Devices

Servers & Mainframes

Network & Virtual Activity

Database Activity

Application Activity

Configuration Info

Threat Intelligence

User Activity

Vulnerability Information

Event Correlation

Activity Baselining & Anomaly Detection

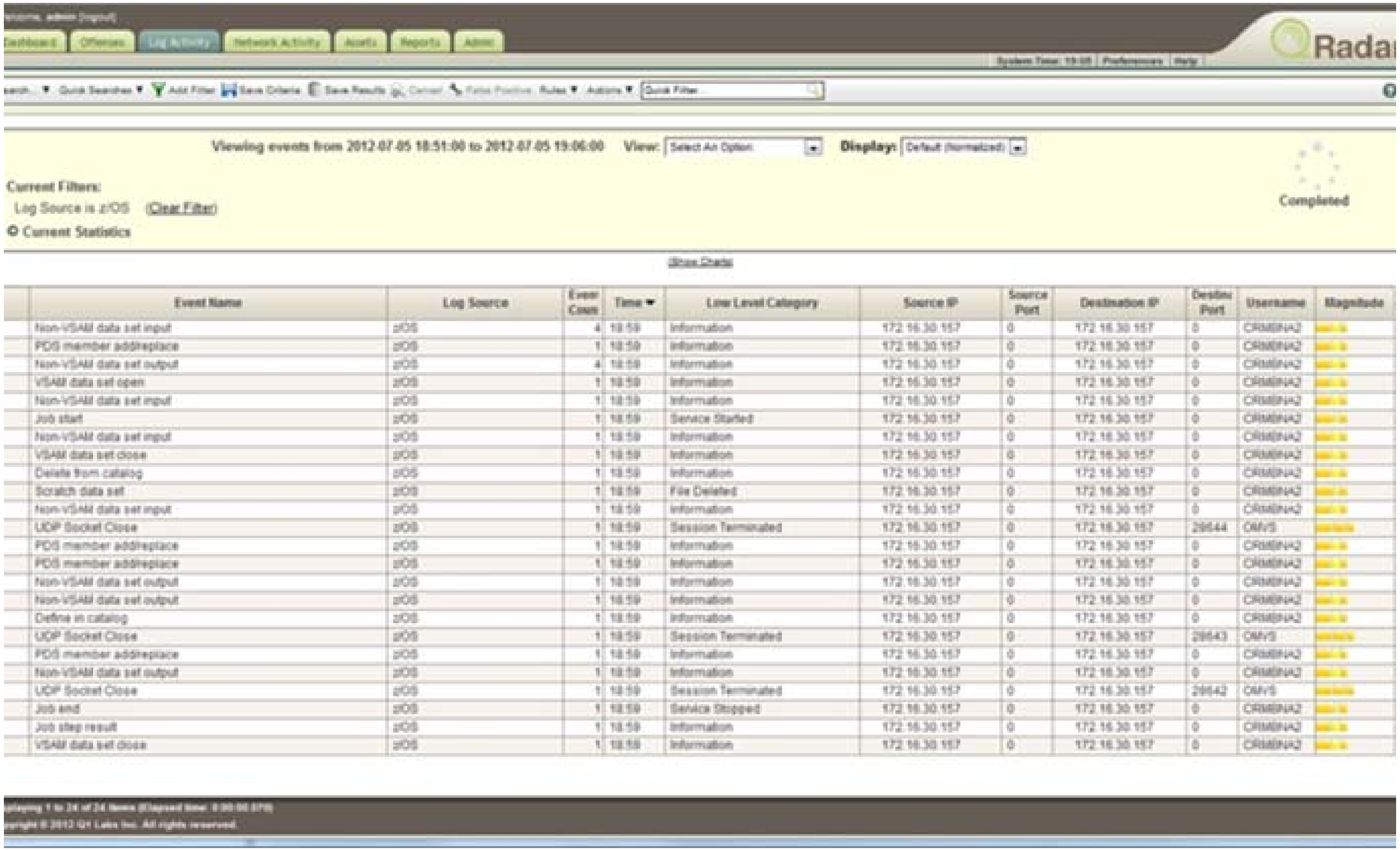
Offense Identification

Alerts, unauthorized log-ins, policy violations, configuration changes, etc. from zSecure Alert & zSecure Audit

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

- ✓ Centralized view of mainframe and distributed network security incidents, activities and trends
- ✓ Better real-time threat identification and prioritization correlating vulnerabilities with zSecure Alert
- ✓ SMF data set feeds increase accuracy of risk levels and offense scores and simplify compliance reporting with zSecure Audit

Integrated SMF log data and supporting details



Viewing events from 2012-07-05 18:51:00 to 2012-07-05 19:06:00 View: Select An Option Display: Default (Normalized)

Current Filters:
Log Source is z/OS (Clear Filter)

Event Name	Log Source	Even Coun	Time ▼	Low Level Category	Source IP	Source Port	Destination IP	Destina Port	Username	Magnitude
Non-VSAM data set input	z/OS	4	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set output	z/OS	4	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
VSAM data set open	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set input	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Job start	z/OS	1	18:59	Service Started	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set input	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
VSAM data set close	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Delete from catalog	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Scratch data set	z/OS	1	18:59	File Deleted	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set input	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
UDP Socket Close	z/OS	1	18:59	Session Terminated	172.16.30.157	0	172.16.30.157	28644	OMVS	▬
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set output	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set output	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Define in catalog	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
UDP Socket Close	z/OS	1	18:59	Session Terminated	172.16.30.157	0	172.16.30.157	28643	OMVS	▬
PDS member add/replace	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Non-VSAM data set output	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
UDP Socket Close	z/OS	1	18:59	Session Terminated	172.16.30.157	0	172.16.30.157	28642	OMVS	▬
Job end	z/OS	1	18:59	Service Stopped	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
Job step result	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬
VSAM data set close	z/OS	1	18:59	Information	172.16.30.157	0	172.16.30.157	0	CRMBNA2	▬

playing 1 to 24 of 24 items (Elapsed time: 0:00:00.079)
pyright © 2012 Q1 Labs Inc. All rights reserved.

- zSecure Audit asynchronously converts SMF data into QRadar Log Event Enhanced Format (LEEF)
- Enriched content includes environmental data, user privileges, user groups, and dataset sensitivity

Complementary capabilities by use case scenarios

QRadar target use case	zSecure Suite complementary capabilities
✓ Complex threat detection	zSecure Alert detects unauthorized logons and attempts, user behavior in violation of security policy, and instances where your core systems may be at risk
✓ Malicious activity identification	Identify dangerous configuration changes before they can be exploited
✓ User activity monitoring	Tracks privileged user activities and abuse and enforces separation of duties
✓ Compliance monitoring	zSecure Audit technology creates standard and customized reports for worldwide regulations and standards such as PCI, SOX, STIG, and more
✓ Fraud detection and data loss prevention	zSecure Alert provides real time notification of anomalous user activity including inappropriate data access
✓ Network and asset discovery	[suggest drop this]

Value of zSecure and QRadar Security Intelligence integration

- Strengthen mainframe security operations and help improve protection for critical mainframe environment

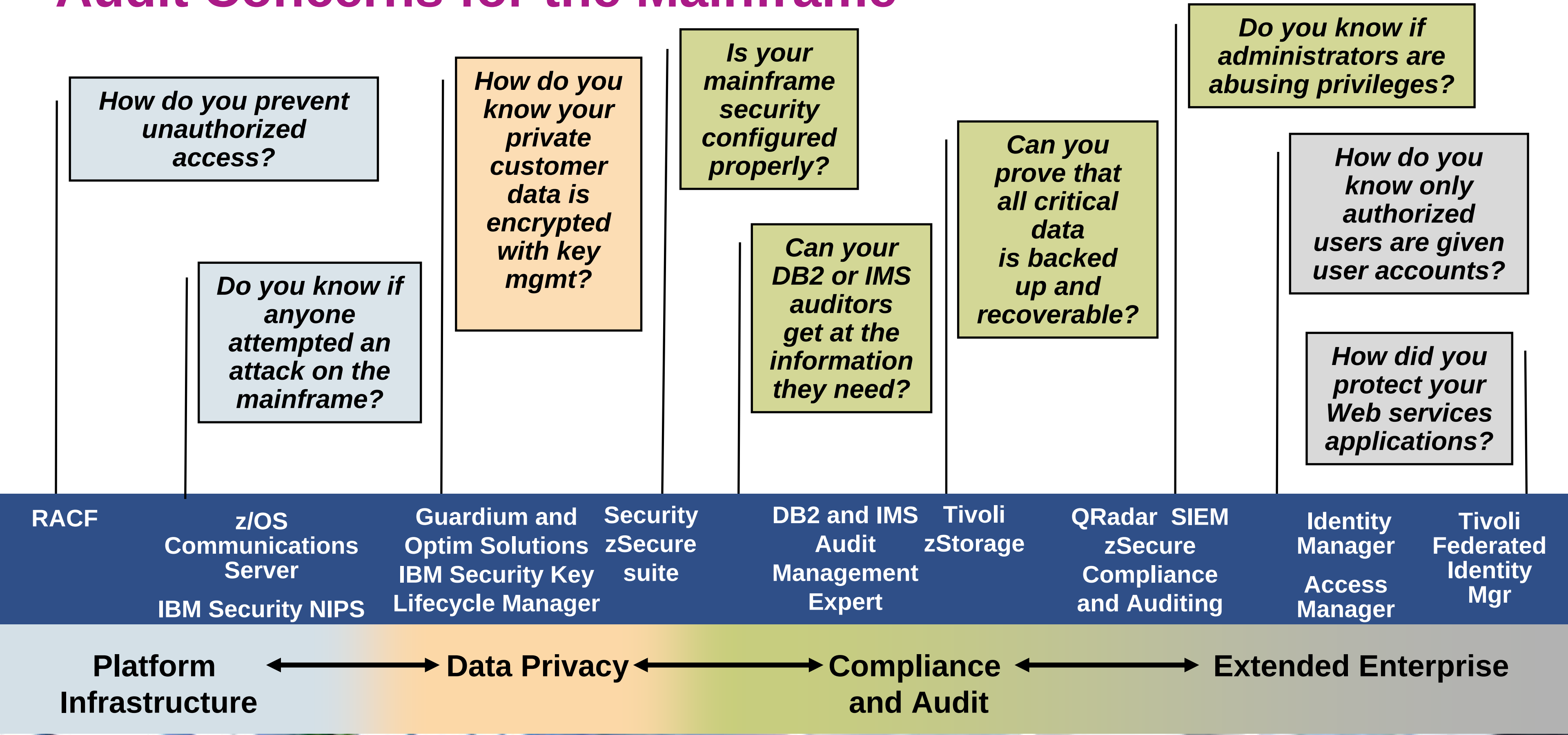
- Improve compliance visibility real-time with standards and regulations by simplifying audit and management efforts

- Consolidate enterprise security view allowing the identification and remediation of excess mainframe access, threats and concerns.

- Store event data in forensically secure database to address regulation mandates.

- Trigger complex correlation of threats, insider fraud and business risk as easy to understand “offenses” for further investigation and follow-ups

IBM Solutions Help to Address Potential Security and Audit Concerns for the Mainframe



How do you prevent unauthorized access?

Do you know if anyone attempted an attack on the mainframe?

How do you know your private customer data is encrypted with key mgmt?

Is your mainframe security configured properly?

Can your DB2 or IMS auditors get at the information they need?

Can you prove that all critical data is backed up and recoverable?

Do you know if administrators are abusing privileges?

How do you know only authorized users are given user accounts?

How did you protect your Web services applications?

RACF

z/OS Communications Server

IBM Security NIPS

Guardium and Optim Solutions

IBM Security Key Lifecycle Manager

Security zSecure suite

DB2 and IMS Audit Management Expert

Tivoli zStorage

QRadar SIEM

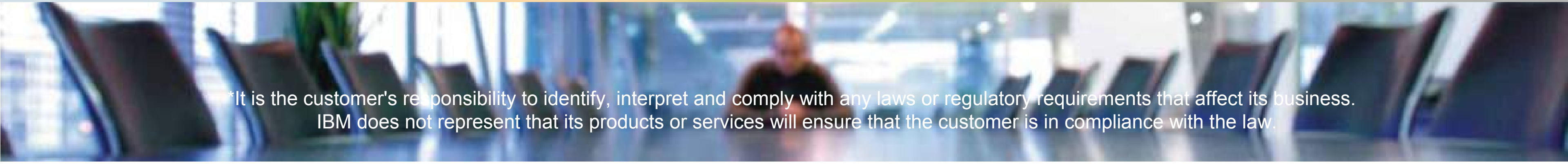
zSecure Compliance and Auditing

Identity Manager

Access Manager

Tivoli Federated Identity Mgr

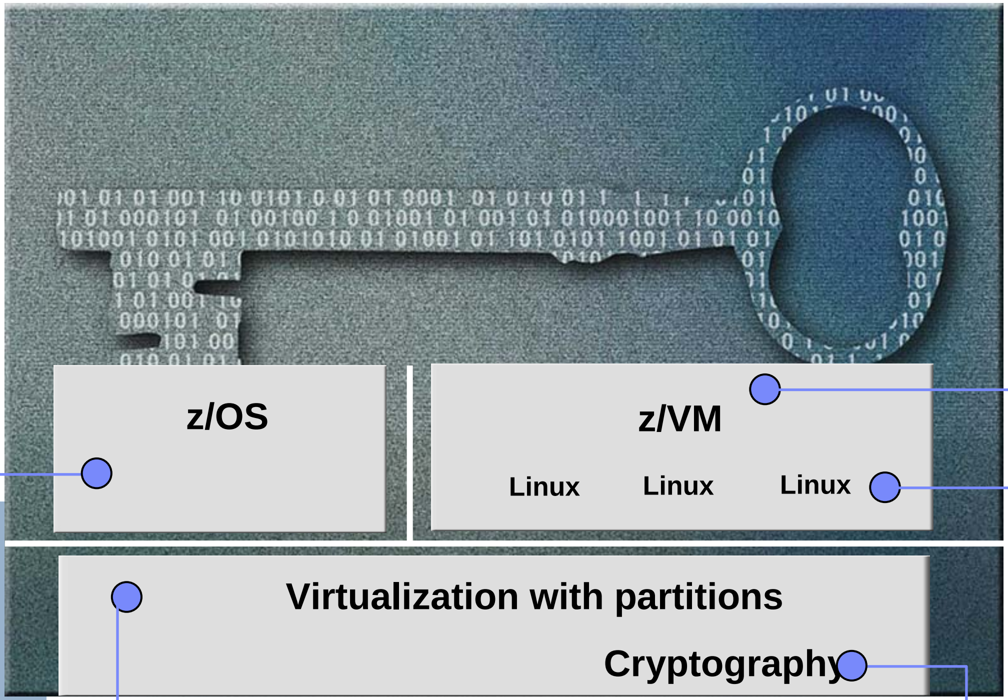
Platform Infrastructure ⟷ **Data Privacy** ⟷ **Compliance and Audit** ⟷ **Extended Enterprise**



*It is the customer's responsibility to identify, interpret and comply with any laws or regulatory requirements that affect its business. IBM does not represent that its products or services will ensure that the customer is in compliance with the law.

System z Evaluations & Certifications

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



z/OS

z/VM

Linux Linux Linux

Virtualization with partitions

Cryptography

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 + RACF (OSPP)

- Common Criteria EAL5
  - z/OS RACF 1.12 (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 →1.12
  - z/OS ICSF PKCS#11 Services – z/OS 1.11

- Statement of Integrity

- System z9 EC and z9 BC System z10 EC and z10 BC
  - Common Criteria EAL5 with specific target of evaluation -- LPAR: Logical partitions

- zEnterprise 196 & zEnterprise 114
  - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions

- Crypto Express2 & Crypto Express3 Coprocessors
  - 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)

z/VM

- Common Criteria
  - z/VM 5.3
- EAL 4+ for CAPP and LSPP

- System Integrity Statement

Linux on System z

- Common Criteria
- SUSE SLES10 certified at EAL4+ with CAPP

- Red Hat EL5 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

Mainframe is the Ultimate Security Platform

Resource Access Control Facility

Security zSecure Suite

Security Key Lifecycle Manager for z/OS

InfoSphere Guardium Family

InfoSphere Guardium Data Encryption for DB2 and IMS Databases

QRadar Security Information and Event Management

IBM Security Network Intrusion Prevention System

Communications Server & Netview for z/OS/

Solution Edition for Security

Security Identity & Access Assurance

Security Identity Manager

Security Access Manager

Security Federated Identity Manager

Security Directory Integrator

Security Directory Server

WebSphere Application Server

WebSphere DataPower Server

AppScan

Protect Your Business Assets with Ultimate Security with zEnterprise

- ✓ 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

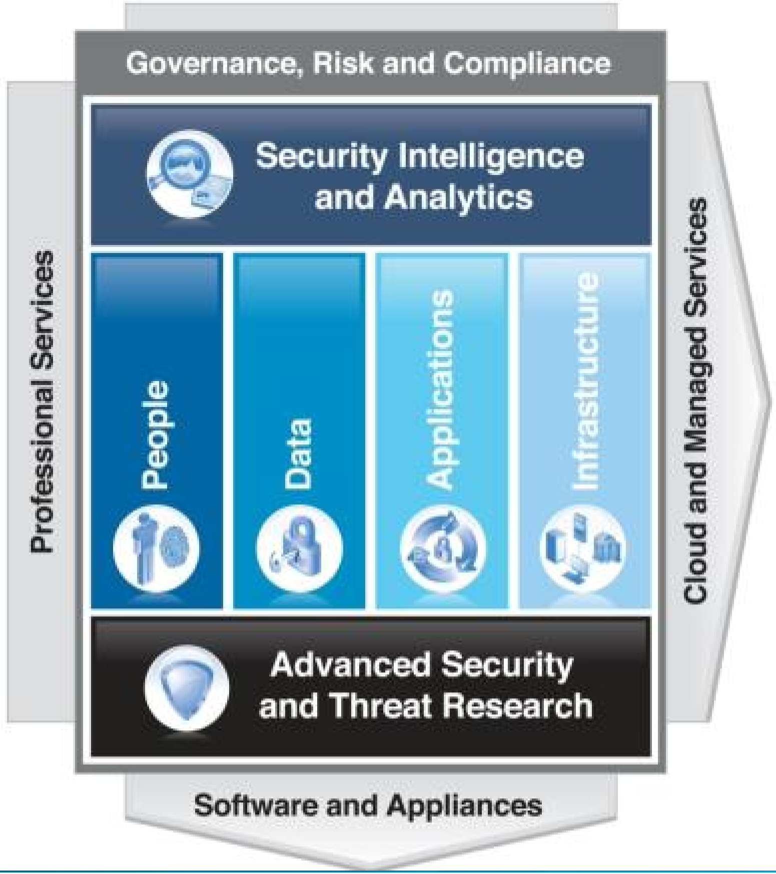
IBM zEnterprise® is the foundation for a secure enterprise

IBM Security: Delivering intelligence, integration and expertise across a comprehensive framework

IBM Security

- End-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Large vulnerability database

IBM Security Framework


Governance, Risk and Compliance
Security Intelligence and Analytics
People
Data
Applications
Infrastructure
Advanced Security and Threat Research
Professional Services
Cloud and Managed Services
Software and Appliances

Intelligence • Integration • Expertise

IBM zEnterprise. Security Ready.

….Are You?

ibm.com/security

Trademark

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

DataPower*
IBM*
IBM (logo)*
PR/SM
RACF*
System z*
zEnterprise*
z/OS*

* Registered trademarks of IBM Corporation

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Windows Server and the Windows logo are trademarks of the Microsoft group of countries.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

* Other product and service names might be trademarks of IBM or other companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.