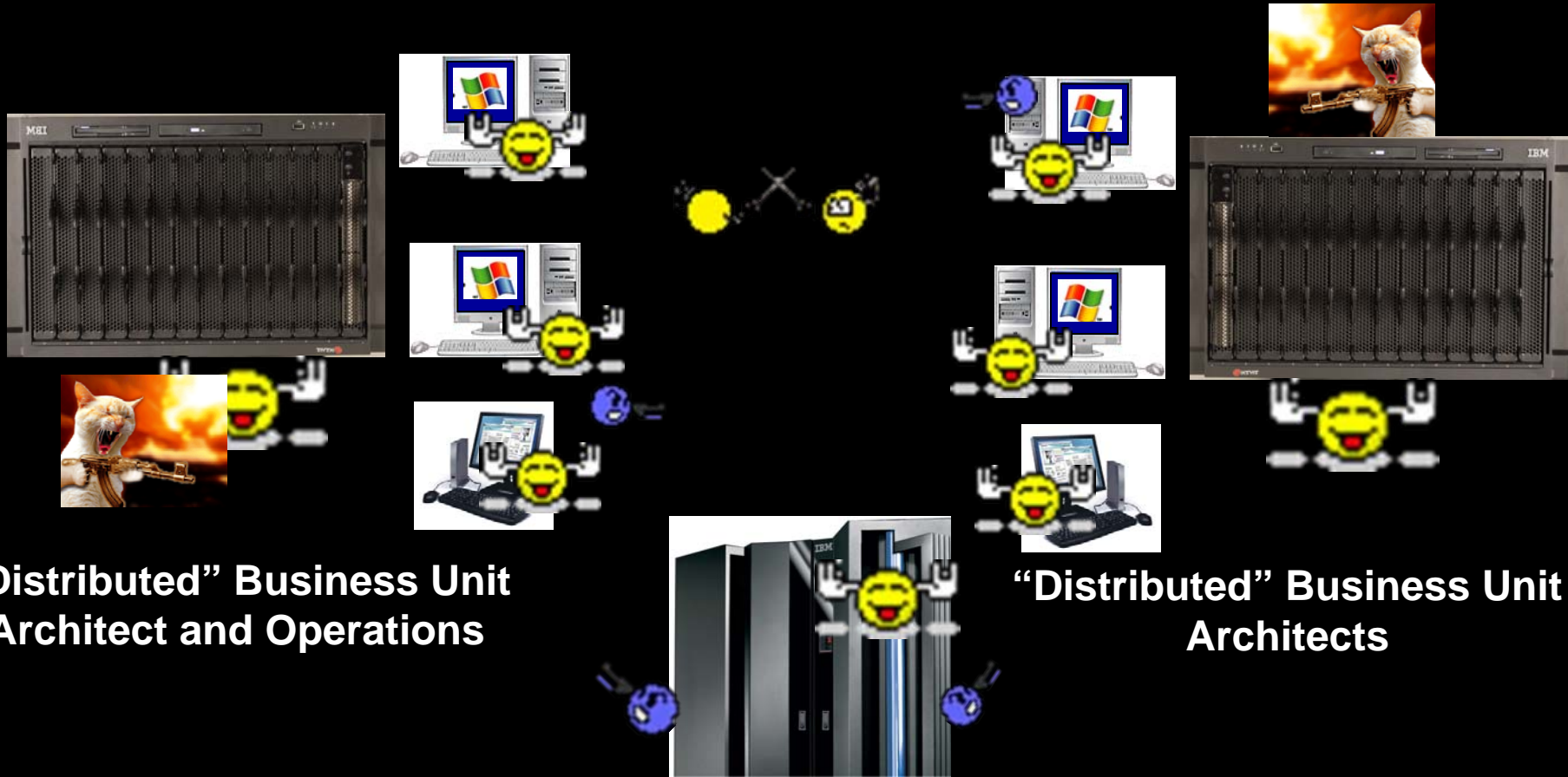# zEnterprise: Security and Risk Hub

Agenda

- **Why all of the data breaches?**

- **The "Silver Bullet" in your Security, Risk Strategy: zEnterprise**

- **The "Fort Knox" of Cloud Computing**

- **Case Studies, Client Examples**

- **How to get Started**

How did we get into this huge data breach problem? Lost Centralized Control of the Data.

"Distributed" Business Unit Architect and Operations

"Distributed" Business Unit Architects

"Centralized" Glass House Operations

Real Customer Problem

Point of Sale

Wireless Store Infrastructure

Point of Sale

Hacker

Store Manager

Bank

Distribution center

HQ

- Store uses WEP wireless for Point of Sale devices
- POS processes cards with banks
- **Common password on all store systems**
- **Security patches not applied to store systems**
- **Hacker plugs in and gets copies of all transactions**
- Problem detected and store systems are getting fixed.
- Mainframe folks are happy they are bullet proof
- **Hypothesis: Mainframe could help secure stores if they use good procedures**
- Store managers run inventory transactions to mainframe
- **No encryption on sign in**
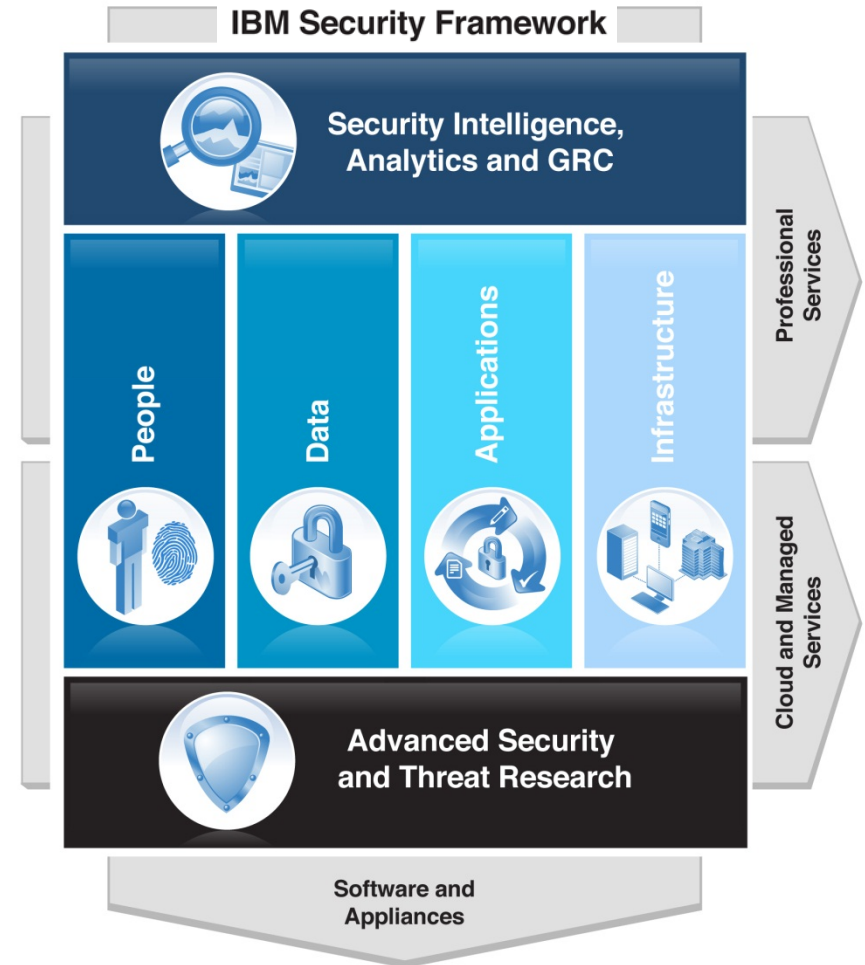- **No audit records analyzed**

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

IBM Security Systems

- Only vendor in the market with end-to-end coverage of the security foundation
- 6K+ security engineers and consultants
- Award-winning X-Force® research
- Largest vulnerability database in the industry

Intelligence • **Integration** • **Expertise**

IBM Security Framework

Security Intelligence, Analytics and GRC

People

Data

Applications

Infrastructure

Advanced Security and Threat Research

Professional Services

Cloud and Managed Services

Software and Appliances

System z Security Conferences and Training

- **System z Training Available:**

  - Onsite from IBM Services

  - SHARE

  - System z Technical University

  - Impact

  - Information on Demand

  - Pulse

2012 RSA Security Conference

- **Largest Security Conference in the World**

  - US: San Francisco, February 27-March 2, 2012

- **RSA Europe**

- **RSA Asia**

- **http://www.rsaconference.com/index.htm**

- **Highlights……**

RSA CONFERENCE | Where The World Talks Security

IT-Security made in Germany

Federal Ministry of Economics and Technology   TeleTrusT

USA 2012   February 27 - March 2 | Moscone Center | San Francisco

IBM's FORT KNOX: zEnterprise

System z Security, Risk, & Fraud Strategy: Looking at 2012 and Beyond

The Enterprise Security Hub

Jack Jones, System z Security -- johnjone@us.ibm.com
Greg Boyd, System z Cryptography -- boydg@us.ibm.com
Rich Skinner, IBM Risk, Security Executive Advisor--rcs@us.ibm.com
Glinda Cummings – Tivoli Security for zEnterprise
Kelly Ozley – System z Security BUE

Forrester Survey –
"Please rank which operating system category you feel is inherently more secure?"

April 10, 2007
Operating System Vendors: Do More To Help Users With Server Security
by Jennifer Albornoz Mulligan

	Rank	
More secure	1	Mainframe
	2	Unix
	3	Macintosh
	4	Linux
Less secure	5	Windows

Figure 3 - Security Decision-Makers' Opinions On OSes' Security

- Source: Forrester Research, Inc. 41887
- Base: 75 decision-makers responsible for server security

System z Evaluations & Certifications

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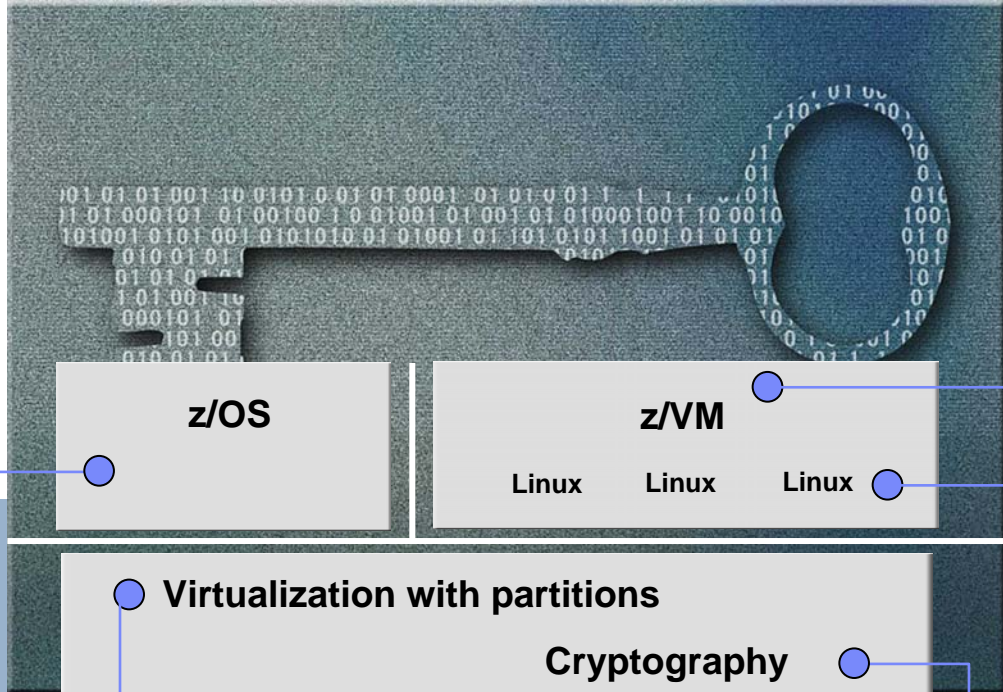
z/VM

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

- System Integrity Statement

z/OS

z/VM

Linux   Linux   Linux

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

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

9
- Statement of Integrity

Virtualization with partitions

Cryptography

- 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)

Recent 2012 System z Certifications

- **IBM RACF for z/OS 1.12 has achieved Common Criteria certification at Evaluation Assurance Level 5 (EAL5)**

- **IBM's® z/OS® Version 1 R. 13 System ICSF PKCS#11 Cryptographic Module Receives FIPS 140-2 Certification – February 23, 2012**

- **IBM's® z/OS® Version 1 Release 13 System SSL Cryptographic Module Receives FIPS 140-2 Certification – March 20, 2012**

zEnterprise Enables Consolidation of Workloads
IBM Security Solutions Enable Consolidation of Security Management

z/OS
z/VM
z/VSE
z/TPF
Linux

Z for Business

HMC

POWER7 BUILT ON Power

Driven by System x

Linux

AIX

Windows
Datapower

Unified Resource Manager

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

Authentication
Authorization
Administration
Auditing

RACF

Administration
Data & Applications
Networks
z/OS
Architecture
Hardware

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
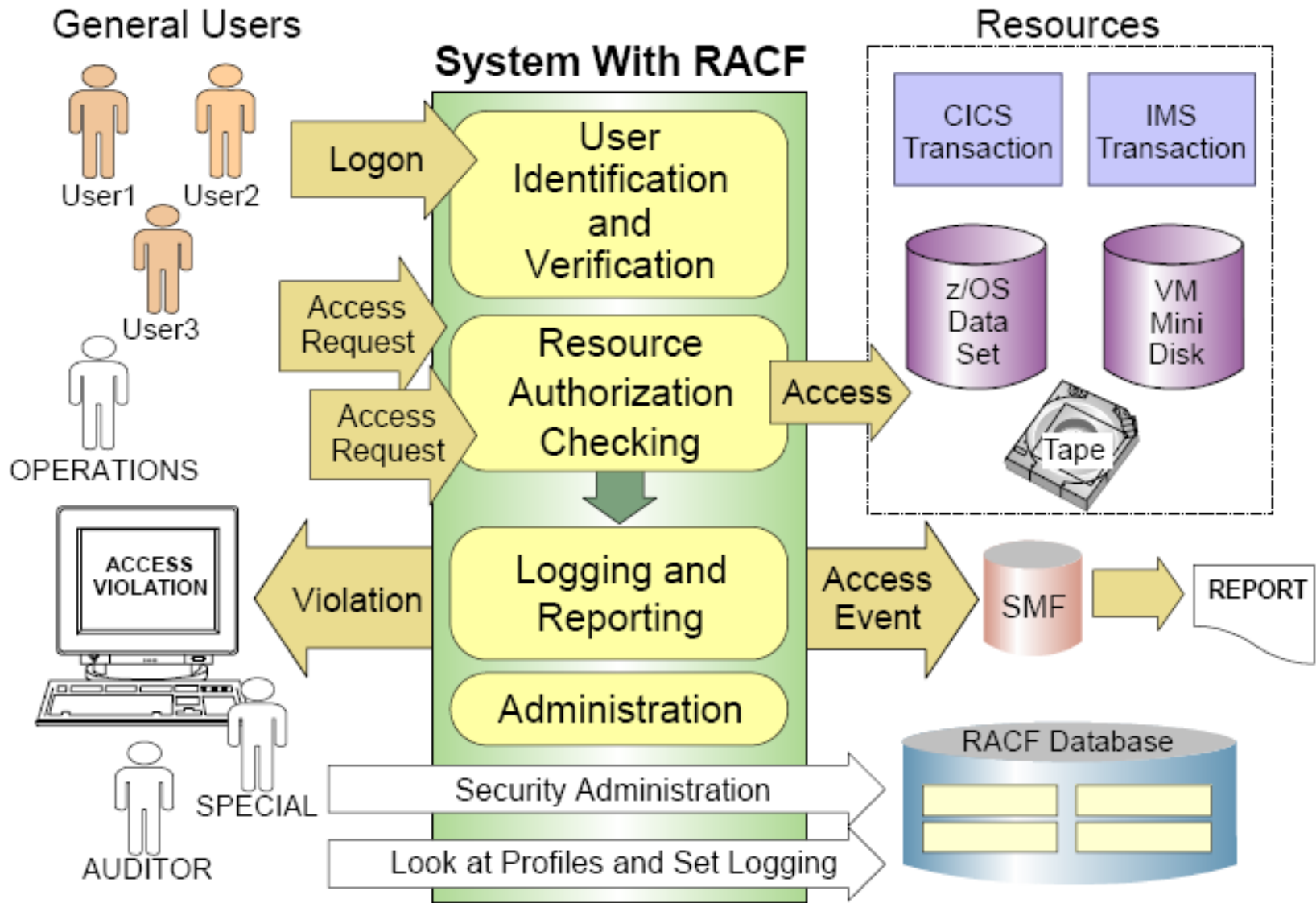
Enterprise Encryption Solutions

System z Encryption Infrastructure

Encryption hardware acceleration with every processor

GP Processor	GP Processor

zAAP (Java)	zIIP (IPSec)

IFL (Linux)

Tamper-resistant encryption processing
Keys never in the clear

Trusted Key Entry

Crypto Express2	Crypto Express2
Crypto Express3	Crypto Express3

Key Storage

Encryption service management and optimization

ICSF, RACF, SMF

CKDS

PKDS   TKDS

z/OS

Linux on z

Crypto access

Encryption Solutions

- Tape
- Disk Encryption
- Internet Access
- Web applications
- Java Applications
- Certificate Authority
- Encryption Facility File Exchange
- Databases
- Smart Cards
- POS / ATM
- zBX (zEnterprise Blades)
- Distributed Key Mgmt System (DKMS)
- ISKLM - Encryption Key Lifecycle Mgr

Protocol stack view of z TCP/IP Security Functions

Protect the system

z/OS CS TCP/IP applications use SAF to authenticate users and prevent unauthorized access to datasets, files, and SERVAUTH protected resources..

Application layer
- SAF protection
- Application specific
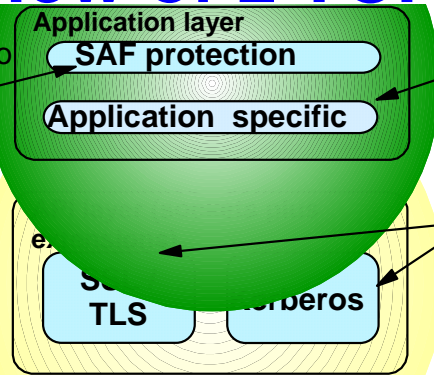
Protect data in the network

Examples of application protocols with built-in security extensions are SNMPv3, DNS, and OSPF.

Both Kerberos and SSL/TLS are located as extensions to the sockets APIs and applications have to be modified to make use of these security functions. Both SSL/TLS and Kerberos are connection-based and only applicable to TCP (stream sockets) applications, not UDP.

ex...
- SSL TLS
- Kerberos
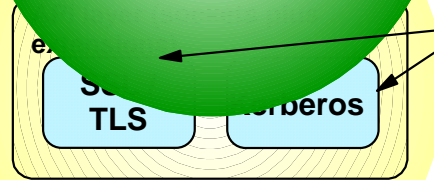
The SAF SERVAUTH class is used to prevent unauthorized user access to TCP/IP resources (stack, ports, networks)

- SAF protection
- AT-TLS
- Intrusion Detection Services
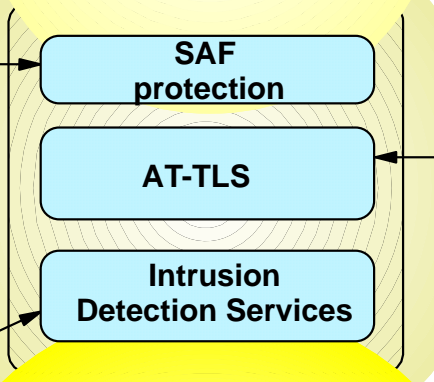
AT-TLS is TCP/IP stack service that provides SSL/TLS services at the TCP transport layer and is transparent to upper-layer protocols. It is avaliable to TCP applications in all programming languages except PASCAL.

Intrusion detection services protect against attacks of various types on the system's legitimate (open) services. IDS protection is provided at both the IP and transport layers.

IP Networking layer
- Intrusion Detection Services
- IP Filtering
- IPSec

IP packet filtering blocks out all IP traffic that this systems doesn't specifically permit.
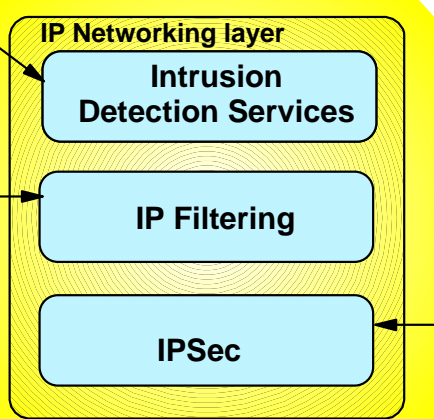
IPSec resides at the networking layer and is transparent to upper-layer protocols, including both transport layer protocol and application protocol.

zEnterprise Enhanced Security for Workloads

- Consolidated Systems

- Cloud Servers and Virtual Systems

- Data Hubs

- Security Services

Garanti Bank – Turkey: The adoption of IBM's System z reinforced Garanti's strategy to deliver fast and secure banking services 24-hours a day, ensuring fast, scalable, robust, flexible, cost-effective and **secure environment across different channels** - banking branches, ATMs, POSs, Internet and mobile channels.
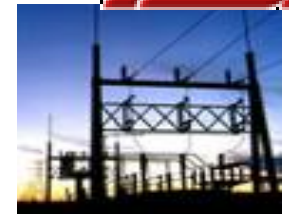
"The HP, Oracle infrastructure simply couldn't support our growing business," said Danny Gurizzan, executive vice president of operations, **Payment Solution Providers (PSP).** "By teaming with IBM, we are actively pursuing new clients and opportunities, confident that our technology can keep pace and hold operating costs to a minimum. Further, selecting the IBM mainframe gives PSP instant credibility with potential clients thanks to its **well-known security and reliability**."

http://www-03.ibm.com/press/us/en/pressrelease/34329.wss

Point of Sale

http://www.prnewswire.com/news-releases/new-ibm-system-z-mainframe-servers-at-turkish-garanti-bank-help-introduce-new-services-124862844.html

zSecure References: Norwich Union improved efficiency and reduced errors

NORWICH UNION
an AVIVA company

Business Challenge:
- Needed to facilitate compliance with identity and access management initiatives
- Needed strategic, robust solution to keep up with high demand for security and audit reports, and with often-complex security requests

Solution:
- IBM Tivoli zSecure Admin, enables efficient RACF administration with fewer resources
- IBM Tivoli zSecure Audit for RACF automatically analyses and reports on security events and exposures

"IBM Tivoli zSecure software gives us a simple, powerful way to comply with identity and access management initiatives, and to assure auditors that preventative, detective and corrective controls are installed."
Phil Secker, Security Support Manager, Norwich Union

Allied Irish Banks streamlines compliance and risk management efforts – and stays ahead of threats

AIB

Value
- **Delivered an expected reduction in administration effort**
- **Strengthened security efforts with deep, proactive auditing of the security configuration**
- **Enabled staff to respond more quickly to configuration errors and security breaches**

Solution
zSecure software
Transformed the banking system completely by implementing the solution on IBM System z platform on z/OS
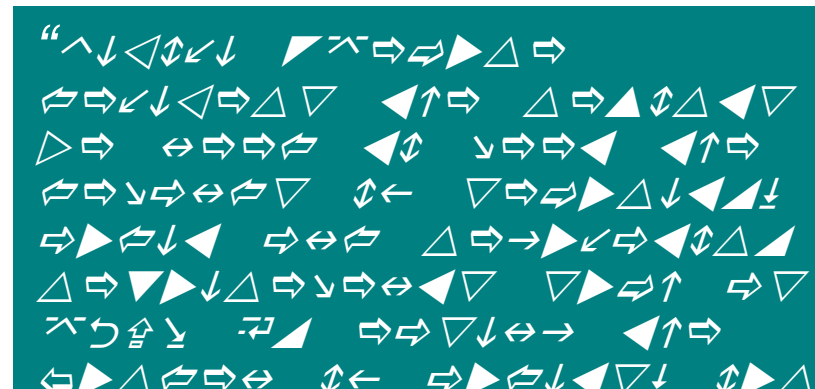
Banco do Brasil **saves over $16 M a year** **System z as a Certificate Authority**

Requirement: Establish a more secure enterprise network after outsourcing network management

Solution:

- Created a VPN (Virtual Private Network) between each device in the network
- Established "Trust" using digital certificates
- Saved millions annually by hosting digital certificates on z/OS

BANCO DO BRASIL

- **30 million accounts**
- **4,000 locations**
- **20 million transactions per day**
- **Hosting certificates for all network devices at branch offices**

Branch offices

Employees

Securing the Internet
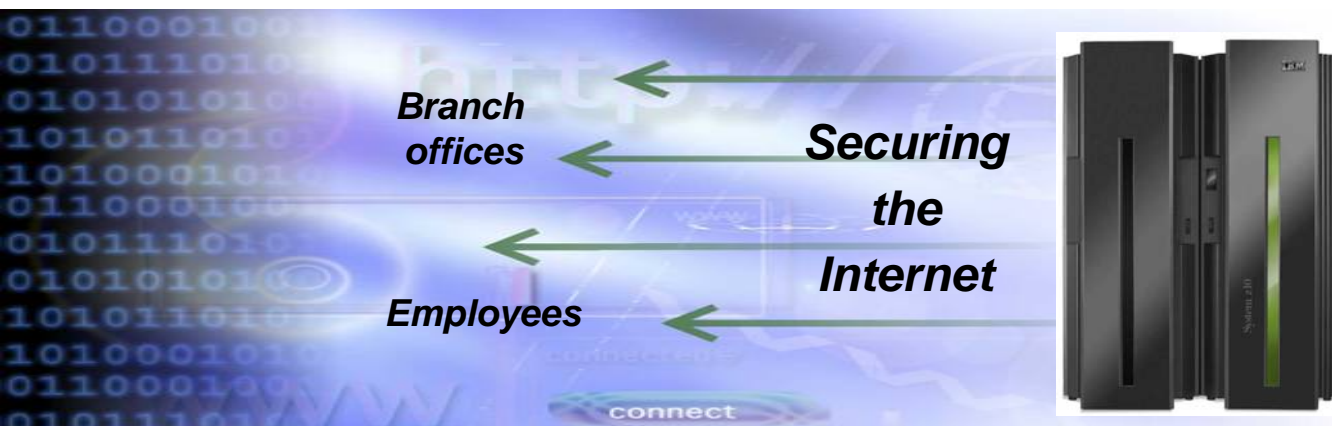
Large Bank / Payments Processer

- Migrated from Encryption Appliances to System z Infrastructure

- 6-9 Months

- Over 100 Million Encryption Transactions a day on peak days

- Other Initiatives

  - **Certificate Authority**

  - **Tape Encryption**

  - **File Encryption**

  - **Network Encryption**

  - **Secure Vault: DB2**

- Have saved over $2million USD on Encryption Hardware

Bank Itáu **Offers Secure Smart Card Solution with System z Encryption**

- *Problem*
  - To ensure the security of its 12 million issued debit cards, the Bank needed to replace its regular cards with security chip-enabled smart cards.
  - Performance bottleneck with current security servers processing smart cards

- *Solution*
  - Leverage superior mainframe security, eliminating separate security servers and migrating smart card solution to the mainframe
  - ▶ Installed mainframe PCI Cryptographic Coprocessor cards
    - ▶ Encryption keys generated and stored on cards used for smart card authentication
    - ▶ Expect to scale to support 15M smart cards

- *Benefit*
  - Reduce fraud from stronger smart card security, while lowering costs, and increased efficiency

> *The IBM Crypto solution offers considerable scope for expansion and is expected to comfortably support all 12 million smart cards when the rollout is complete.*

PII Repository / Secure Vault on System z.
Utilizing infrastructures with EAL5 and FIPS 140-2 Level 4 Security Certifications.

Tivoli Federated Identity Manager w/WebSphere

RACF w/zSecure and Communications Server

z/OS

RACF w/ zSecure Tooling

ICSF

Encryption

Data

Centralized PII (Credit Card Numbers, Social Security Numbers, Addresses, etc. stored and protected in a central repository.
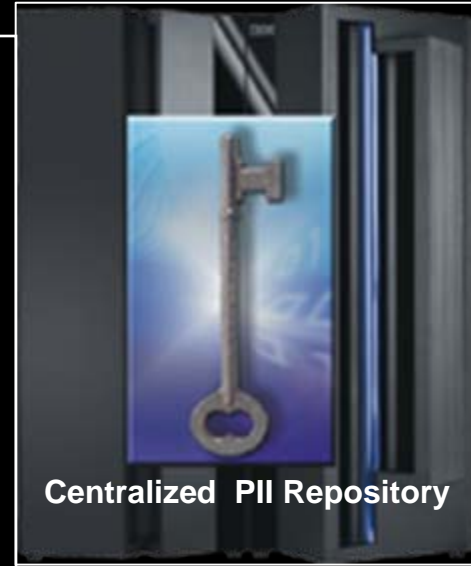
Centralized PII Repository

Linux

Windows

Unix
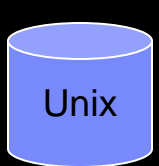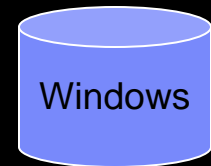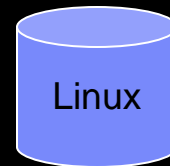
PII is no longer stored in the disparate data stores. Only the Reference Number is stored. If PII is needed, then the system will pull this information from the Central Repository.

Central Repository Structure

Unique Identifier	SS #	CC #	Address

Success:

Ways to get started……..

But I don't know anything about security, risk..

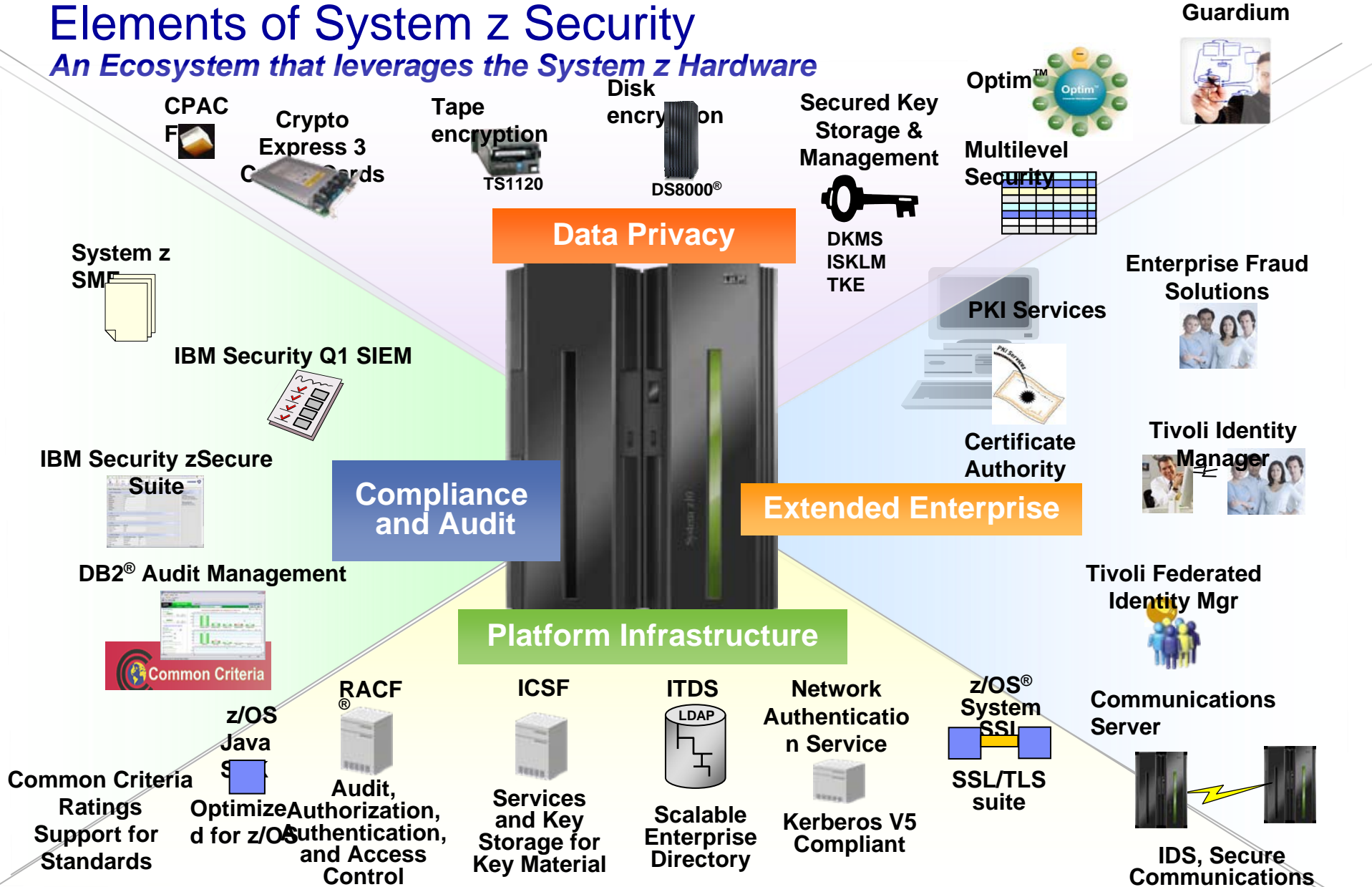How can I work with the Chief Security Officer or Chief Risk Officer?

End to End Entry Points to Success

http://www-03.ibm.com/security/

•Security, Risk Assessment
  Auditing / Compliance Reporting for RACF / ACF2
  Services Engagement: can be high level or detailed

•Executive Security, Risk, Fraud, and Compliance Briefing
  End to End Executive Session on IBM Strengths

•Security, Risk Workshop
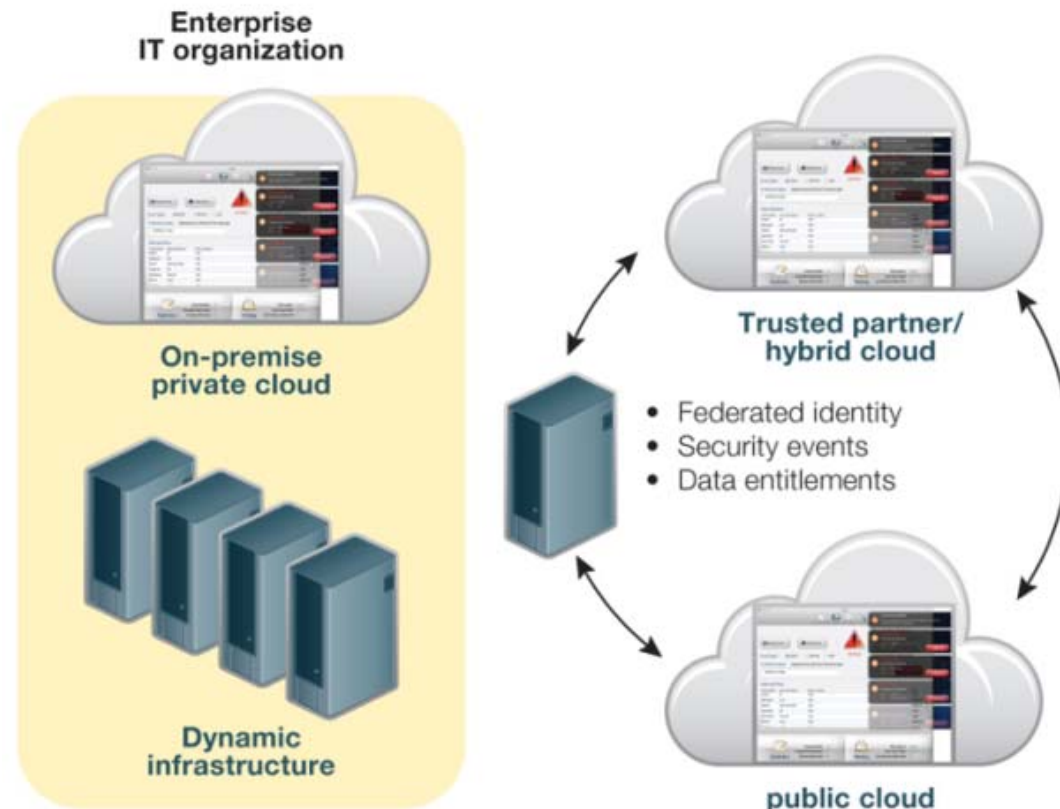 Focuses on Particular Initiative

Elements of System z Security

An Ecosystem that leverages the System z Hardware

Guardium

CPAC F

Crypto Express 3 Cards

Tape encryption
TS1120

Disk encryption
DS8000®

Secured Key Storage & Management
DKMS ISKLM TKE

Optim™

Multilevel Security

Data Privacy

System z SMF

IBM Security Q1 SIEM

PKI Services

Enterprise Fraud Solutions

IBM Security zSecure Suite

Compliance and Audit

Certificate Authority

Extended Enterprise

Tivoli Identity Manager

DB2® Audit Management

Common Criteria

Platform Infrastructure

Tivoli Federated Identity Mgr

Common Criteria Ratings Support for Standards

z/OS Java SDK
Optimized for z/OS

RACF®
Audit, Authorization, Authentication, and Access Control

ICSF
Services and Key Storage for Key Material

ITDS
LDAP
Scalable Enterprise Directory

Network Authentication Service
Kerberos V5 Compliant

z/OS® System SSL
SSL/TLS suite

Communications Server

IDS, Secure Communications

X-Force 2011 Trend Report: Challenges of cloud security

- We saw a number of high profile cloud breaches in 2011 affecting well-known organizations and large populations of their customers

- Customers looking at cloud environments should consider:
    – Cloud-appropriate workloads
    – Appropriate service level agreements (SLAs)
    – Lifecycle approaches to deployment that include exit strategies should things not work out

Securing access to cloud-based applications and services

Enterprise IT organization

On-premise private cloud

Dynamic infrastructure

Trusted partner/ hybrid cloud

- Federated identity
- Security events
- Data entitlements

public cloud

System z has been running a cloud-centric environment for 40+ years, do the same issues exist?

Cloud Computing

Security is one of the top concerns of cloud, as enterprises drastically rethink the way IT resources are designed, deployed and consumed

Our focus is in two areas of cloud security

1 **Security from the Cloud**   **2** **Security for the Cloud**

Cloud-based Security Services

Public cloud Off premise

Use cloud to deliver security as-a-Service *- focusing on services such as vulnerability scanning, web and email security, etc.*

Secure usage of Public Cloud applications – *focusing on Audit, Access and Secure Connectivity*

Securing the Private Cloud stack *– focusing on building security into the cloud infrastructure and its workloads*

Private cloud On premise

IBM Project Green - Virtualization Hub

- **Expecting substantial savings in multiple dimensions: energy, software and system support costs**

- **The consolidated environment will use 80% less energy**

- **This transformation is enabled by the System z's sophisticated virtualization capability**

- **Provides world class security**

IBM'S PROJECT BIG GREEN SPURS GLOBAL SHIFT TO LINUX ON MAINFRAME

Plan to shrink 3,900 computer servers to about 30 mainframes targets 80 percent energy reduction over five years

Optimized environment to increase business flexibility

ARMONK, NY, August 1, 2007 – In one of the most significant transformations of its worldwide data centers in a generation, IBM (NYSE: IBM) today announced that it will consolidate about 3,900 computer servers onto about 30 System z mainframes running the Linux operating system.
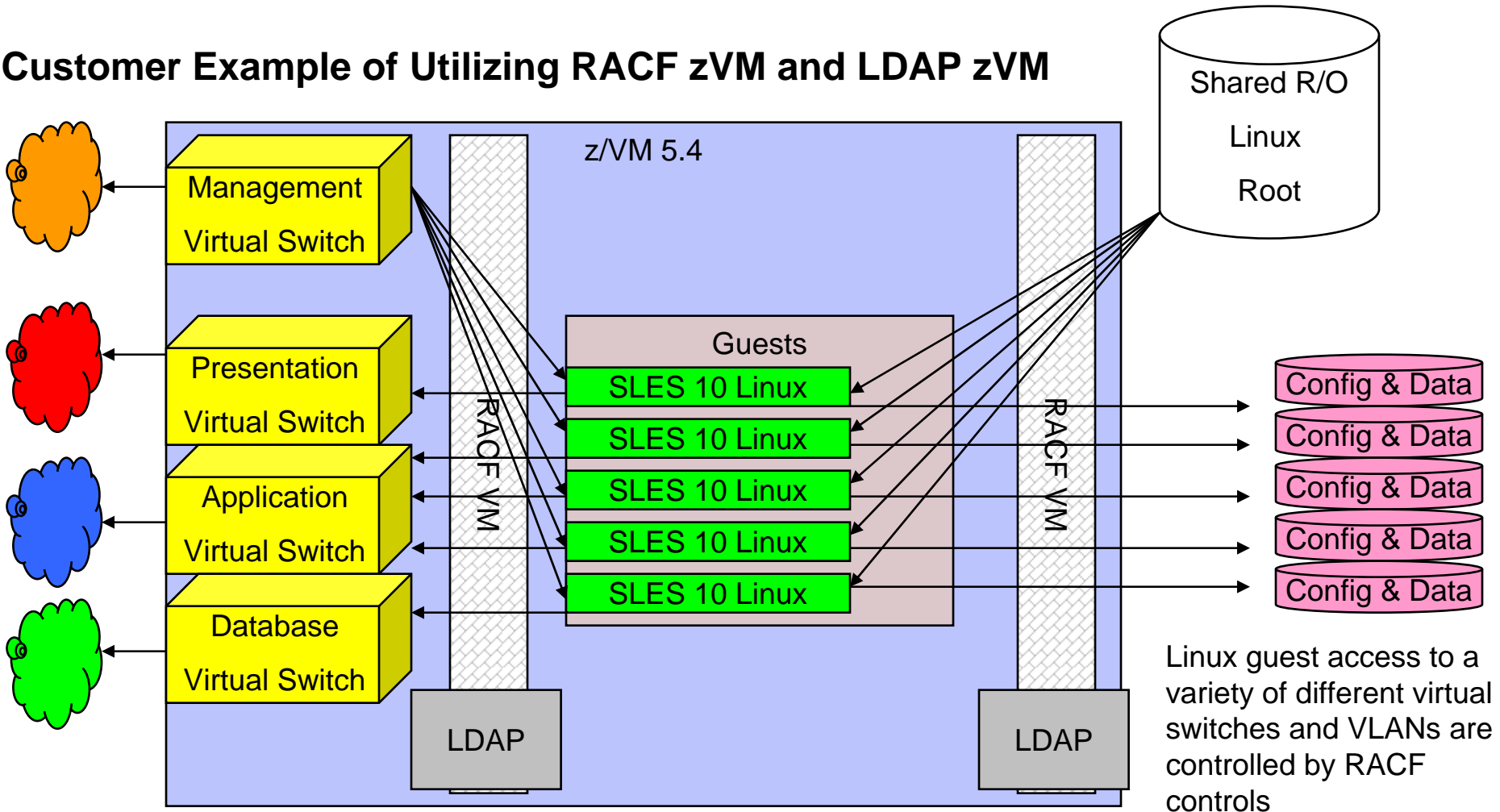
Security

Economics

Energy Efficiency

Did you know there is a RACF zVM? Linux on z workloads.

Customer Example of Utilizing RACF zVM and LDAP zVM

Management Virtual Switch

Presentation Virtual Switch

Application Virtual Switch

Database Virtual Switch

z/VM 5.4

RACF VM

Guests
- SLES 10 Linux
- SLES 10 Linux
- SLES 10 Linux
- SLES 10 Linux
- SLES 10 Linux

RACF VM

LDAP

LDAP

Shared R/O Linux Root

Config & Data
Config & Data
Config & Data
Config & Data
Config & Data

Linux guest access to a variety of different virtual switches and VLANs are controlled by RACF controls

Encryption Management & Controls

PKI

Crypto Cloud

Lifecycle Manager

Backup Tapes

SSL or IPSec

Data at Rest

Personal Authentication

Looking for a Secure, Proven Cloud Infrastructure: System z

Security for the Cloud

Public / Private Cloud
Secure Application Hosting
Secure Data Vault

Security from the Cloud

Trusted Identities
Fraud, Risk Analytics
Data Protection

**Securing Cloud
with IBM Security Systems**

Security Intelligence ● People ● Data ● Apps ● Infrastructure

oration

Security Services for the Enterprise

- **A sampling of Recent 3rd Party Vendor Solutions**

- **Security Services to run on the System z Cloud**

ibm.com/security