Demonstrating Governance, Risk, and Compliance for your Mainframe

Speaker Name and Title

Trademark

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

DataPower*

DB2*

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.

The world is becoming more digitized and interconnected, opening the door to emerging threats and leaks…

DATA EXPLOSION

The age of Big Data – the explosion of digital information – has arrived and is facilitated by the pervasiveness of applications accessed from everywhere

CONSUMERIZATION OF IT

With the advent of Enterprise 2.0 and social business, the line between personal and professional hours, devices and data has disappeared

EVERYTHING IS EVERYWHERE

Organizations continue to move to new platforms including cloud, virtualization, mobile, social business and more

ATTACK SOPHISTICATION

The speed and dexterity of attacks has increased coupled with new actors with new motivations from cyber crime to terrorism to state-sponsored intrusions

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

New Industry Trends Bring Security Challenges to Business

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

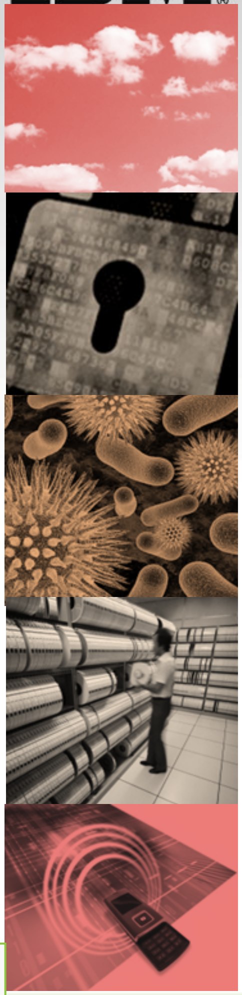
Today's applications with huge data volumes means protection of data is a key imperative

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?

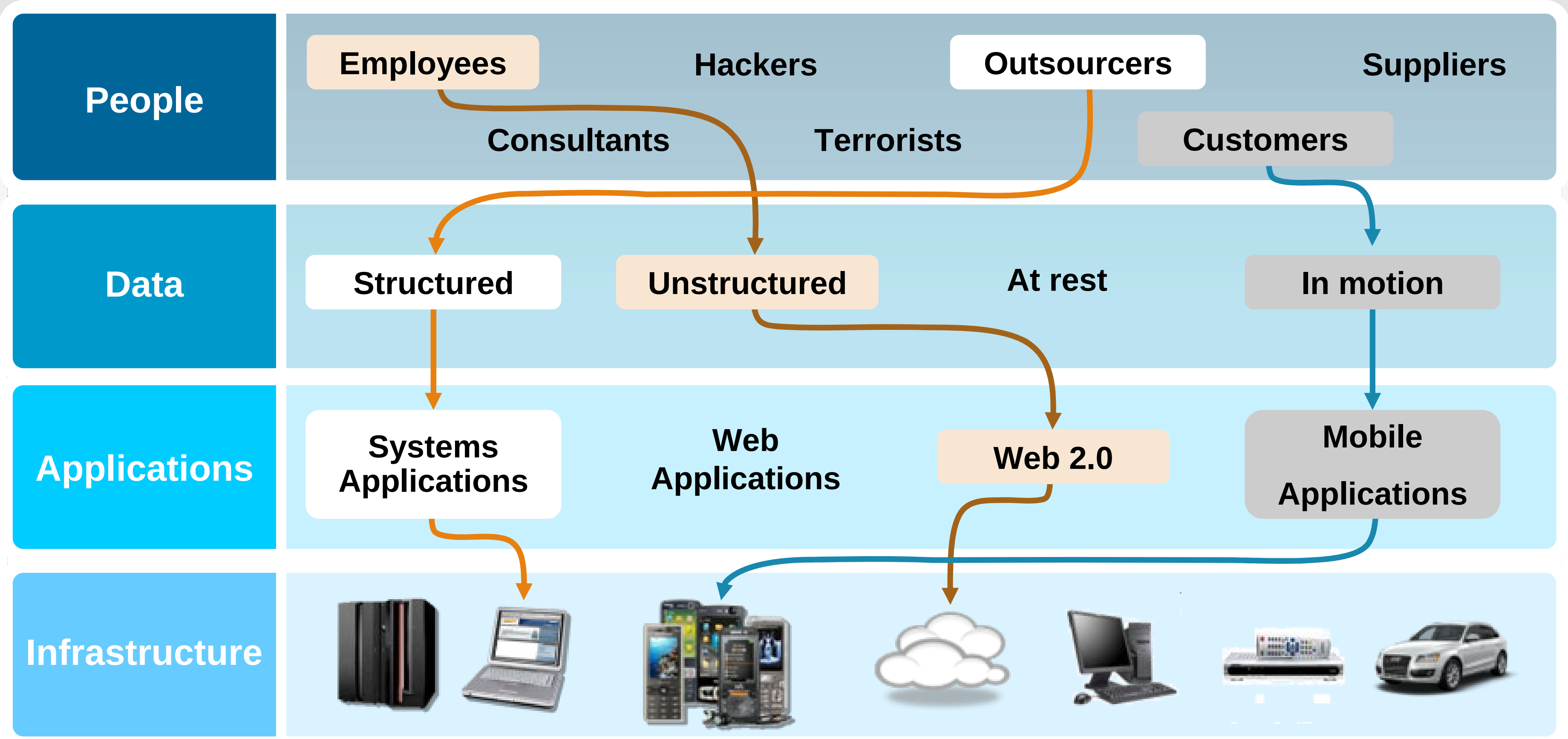
Redefining the challenge of securing your business

[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

The attack surface for a typical business is growing at an exponential rate



People

Employees

Hackers

Outsourcers

Suppliers

Consultants

Terrorists

Customers

Data

Structured

Unstructured

At rest

In motion

Applications

Systems Applications

Web Applications

Web 2.0

Mobile Applications

Infrastructure

- **77%** of firms feel cyber-attacks harder to detect and **34%** low confidence to prevent
- **75%** felt effectiveness would increase with end-to-end solutions

JK 2012-04-26

As a result, the Security market is shifting

	Traditional Focus *Governance and Compliance*	**Emerging Focus** *Risk Management*
Security strategy	React when breached	Continual management
Speed to react	Weeks/months	Realtime
Executive reporting	None	Operational KPIs
Data tracking	Thousands of events	Millions of events
Network monitoring	Server	All devices
Employee devices	Company issued	Bring your own
Desktop environment	Standard build	Virtualization
Security enforcement	Policy	Audit
Endpoint devices	Annual physical inventory	Automatically managed
Security technology	Point products	Integrated
Security operations	Cost Center	Value Driver

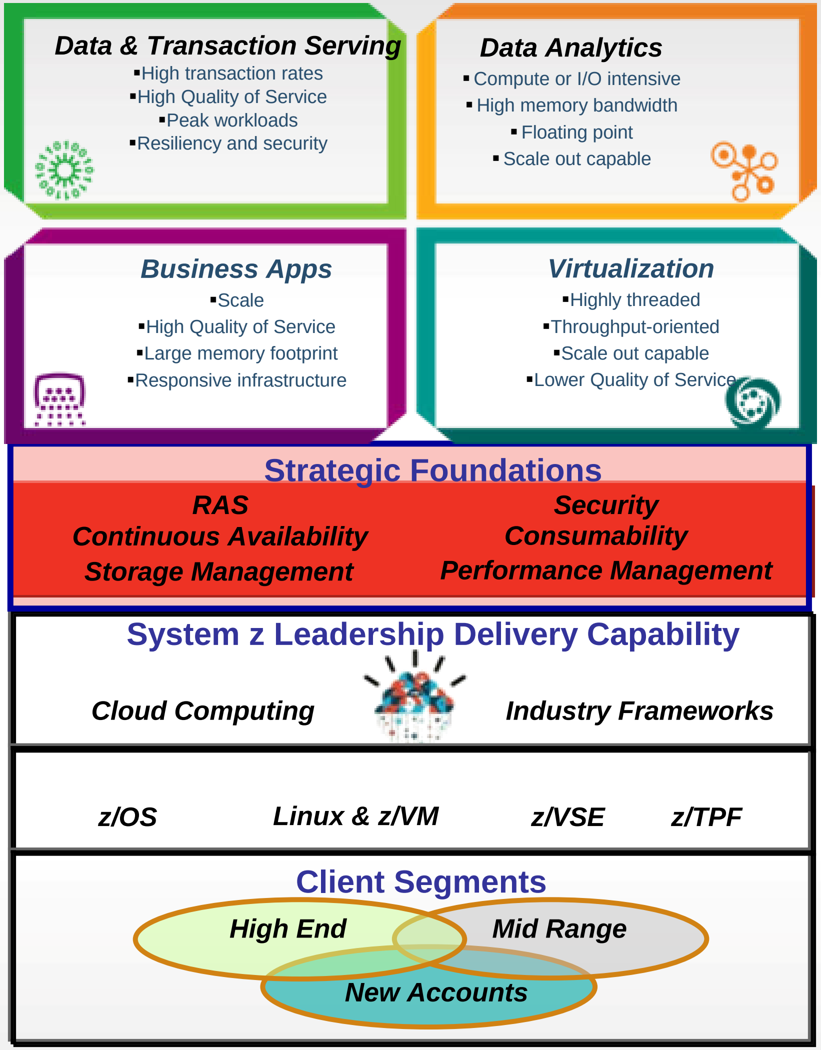
Source**:** Client Insights 27-Jun-11, *An Evaluation of the Security & Risk Opportunity; Assessing a New Approach to Competitive Differentiation,* Ari Sheinkin

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

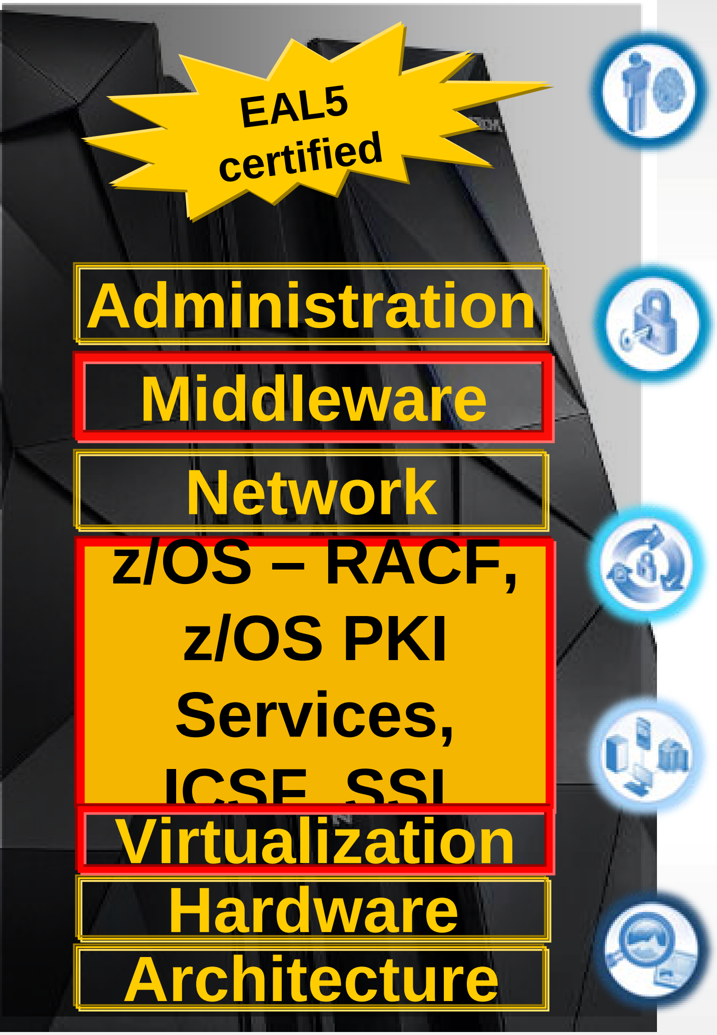
Cloud Computing *Industry Frameworks*

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

Client Segments

Security with Core System z Infrastructure

System z Security Architected and Integrated



EAL5 certified

Administration

Middleware

Network

z/OS – RACF, z/OS PKI Services, ICSF, SSL

Virtualization

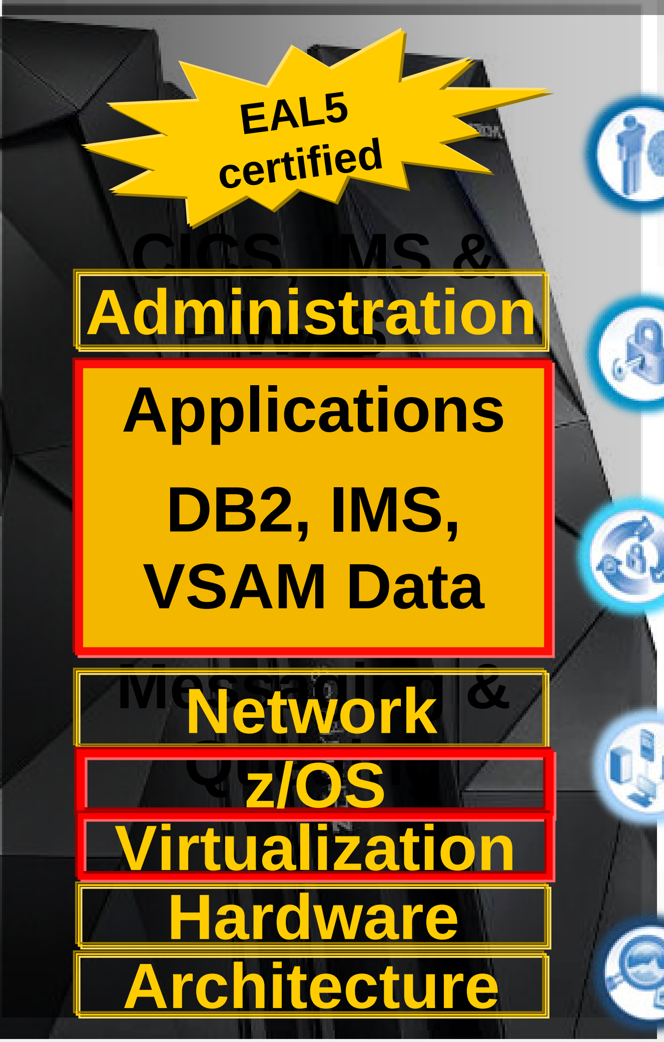
Hardware

Architecture

- ✓ Integrated accelerated tamper proof Hardware Cryptography supporting two different architectures:
  - •Open standards with Enterprise IBM PKCS #11 targeted to the public sector
  - •IBM's Common Crypto Architecture (CCA) supporting needs of banking and finance
- ✓ Secure your business critical assets with tamper resistant high speed through clear key and secure key encryption
- ✓ High speed encryption that keeps sensitive keys private, ideal for securing high volume business transactions
- ✓ Trusted Key Entry (TKE) Workstation to securely enter master keys
- ✓ EKMF enterprise management of keys and certificates targeting for financial customers
- ✓ Use Application Transparent Transport Layer Security to secure sensitive communications without incurring costly application changes
- ✓ Memory protection to protect your most critical transactional systems
- ✓ Built-in defenses to ensure high availability of the system against denial-of-service attacks
- ✓ Network IPS front end fraud and threat detection
- ✓ Evaluate inbound encrypted data for suspect activity
- ✓ Labeled DB2 and z/OS security for secured multi-tenancy
- ✓ Consistent auditing and reporting using a centralized model integrated with event management
- ✓ Strong focus on crypto functions required by the Banking/Finance industries

Security with Core z/OS Middleware

Centralized Integrated Security



EAL5 certified

CICS, IMS &

Administration

Applications

DB2, IMS, VSAM Data

Messaging &

Network

z/OS

Virtualization

Hardware

Architecture

- ✓ Authentication / Authorization / Administration / Auditing
  - ✓Application and database security without modifying applications - Applicable at almost no cost for new workload
  - ✓Tracking of activity to address audit and compliance requirement
  - ✓Use WebSphere® with RACF for end-to-end, authentication and authorization
- ✓ Granular security implementation for many DB2, CICS, IMS, WAS, MQ and z/OS resources
- ✓ Protecting sensitive and confidential data with Data Encryption solutions for DB2 and IMS databases with InfoSphere™ Guardium® Data Encryption
- ✓ Code signing for Program Objects in PDSEs
- ✓ Access to crypto features inside of applications
- ✓ Support of System Secure Sockets Layer (SSL), digital certificates, and key repositories
- ✓ Secured connection with Linux virtual servers (Linux for System z) in the box
- ✓ Tools for audit and compliance – Everything is logged by DB2, CICS, IMS, MQ and z/OS

How IBM leverages security best practices

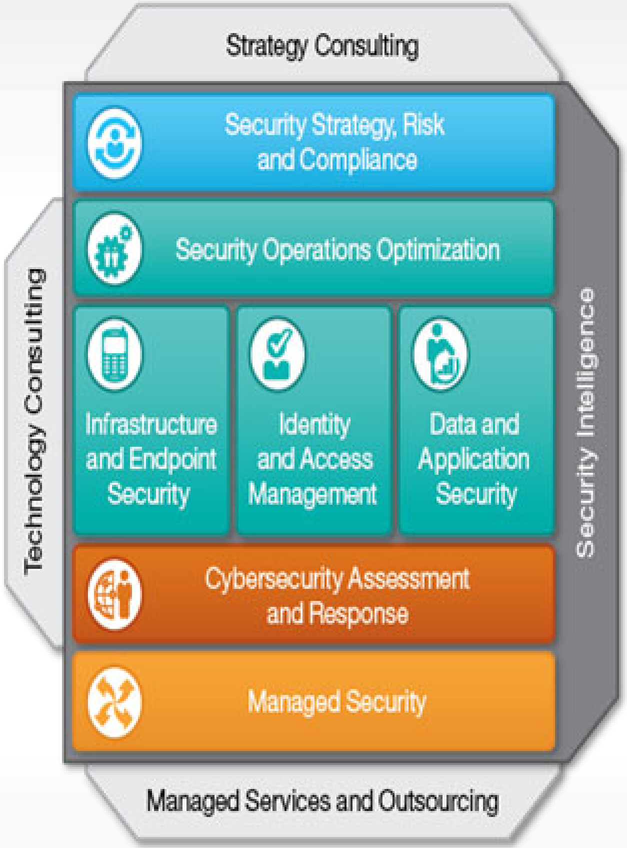
1. Build a risk-aware culture and management system

2. Manage security incidents with greater intelligence

3. Defend the mobile and social workplace

4. Security-rich services, by design

5. Automate security “hygiene”



Strategy Consulting

Technology Consulting

Security Strategy, Risk and Compliance

Security Operations Optimization

Infrastructure and Endpoint Security

Identity and Access Management

Data and Application Security

Cybersecurity Assessment and Response

Managed Security

Security Intelligence

Managed Services and Outsourcing

6. Control network access and help assure resilience

7. Address new complexity of cloud and virtualization

8. Help manage third-party security compliance

9. Better secure data and protect privacy

10. Help manage the identity lifecycle

Protect People, Identities throughout your Extended Enterprise

- Integrated authentication and access control provided by RACF®
- 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.

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

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™

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.

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

Guardium Data Activity Monitoring

✓**Activity Monitoring**

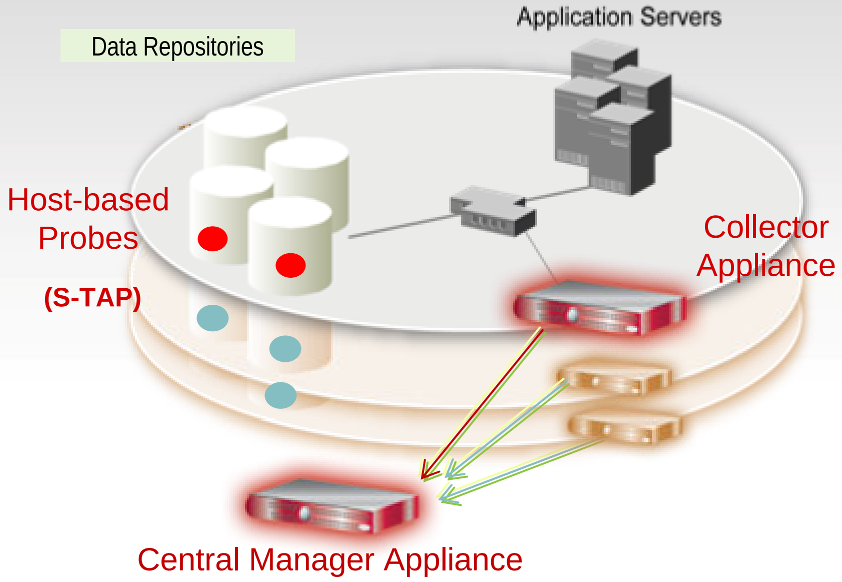
Continuous, policy-based, real-time monitoring of all data traffic activities, including actions by privileged users

✓**Blocking & Masking**

Data protection compliance automation

✓**Vulnerability Assessment**

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

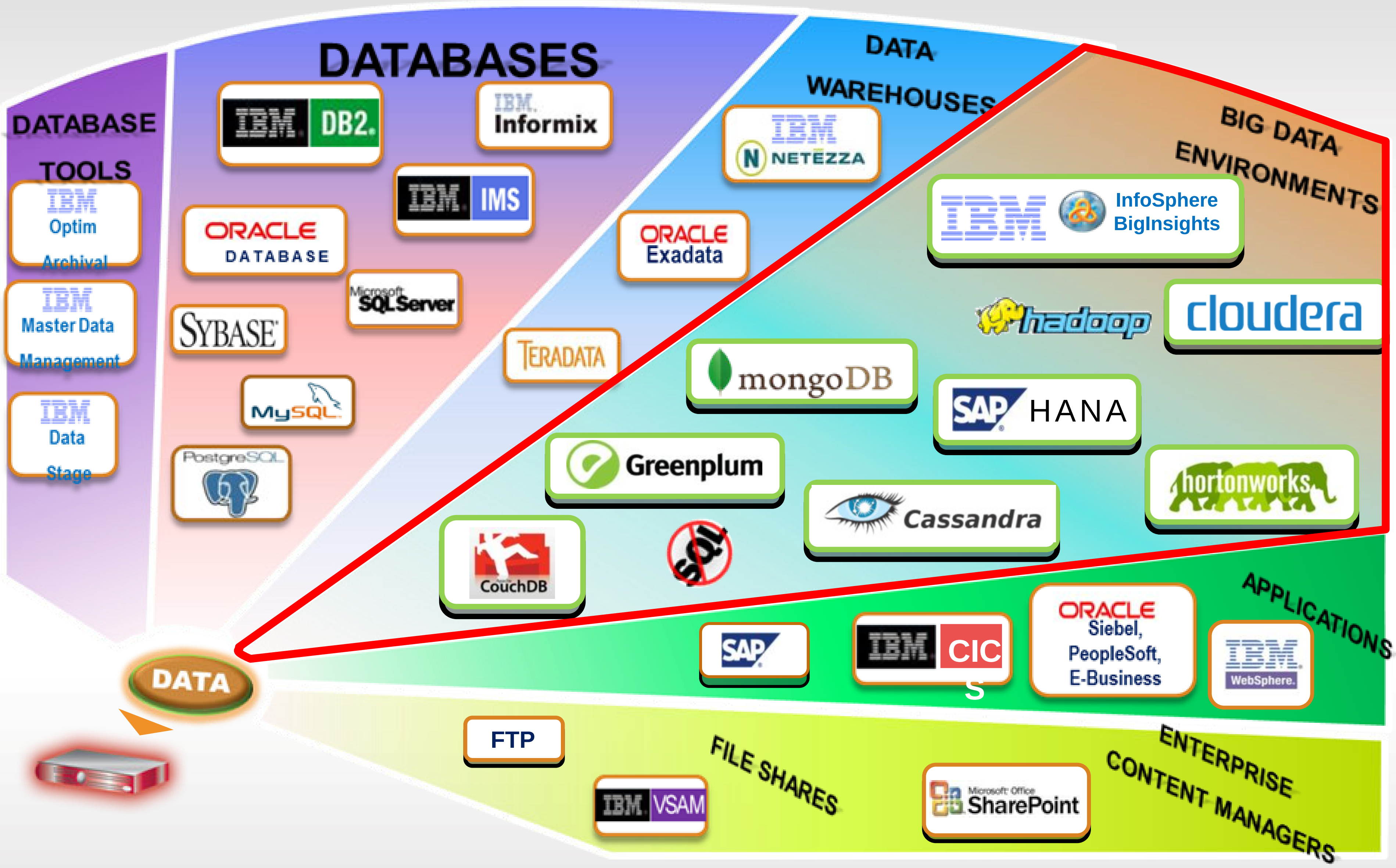


Key Characteristics

- 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*

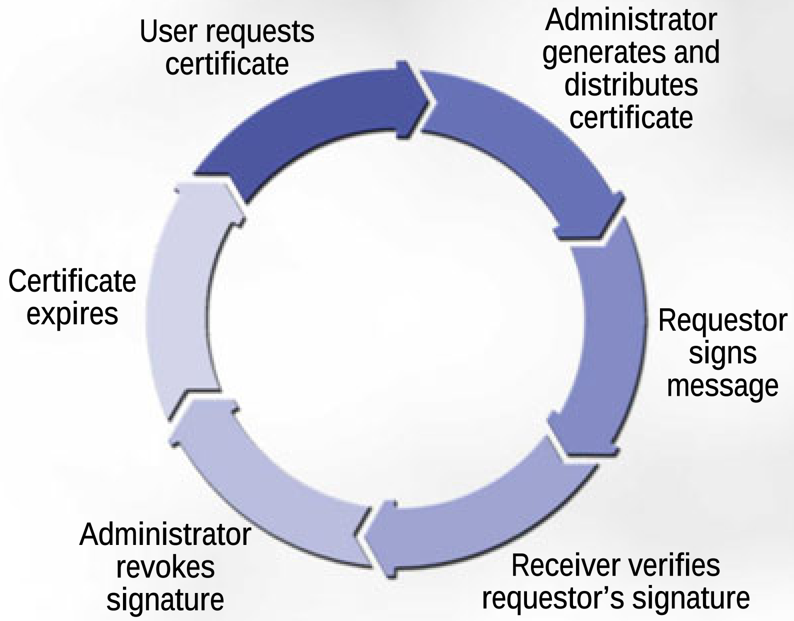
- 100% visibility including local DBA access
- Minimal performance impact
- Does not rely on resident logs that can easily be erased by attackers, rogue insiders
- No environment changes
- Prepackaged vulnerability knowledge base and compliance reports for SOX, PCI, etc.
- Growing integration with broader security and compliance management vision

Extend Activity Monitoring to Big Data, Warehouses, File Shares



Digital certificate hosting with z/OS PKI Services

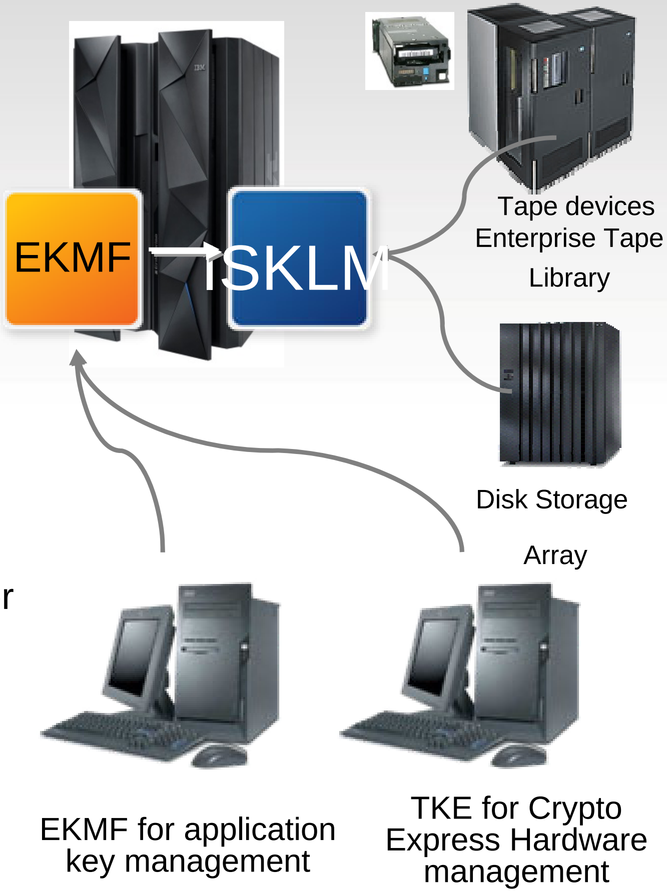
- A Certificate Authority solution built into z/OS
- Can provide significant TCO advantage over third party hosting
- Provides full certificate life cycle mgmt
  - **User requests driven via Web pages**
  - **Browser or server certificates**
  - **Automatic or administrator approval process**
  - **End 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**
  - **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

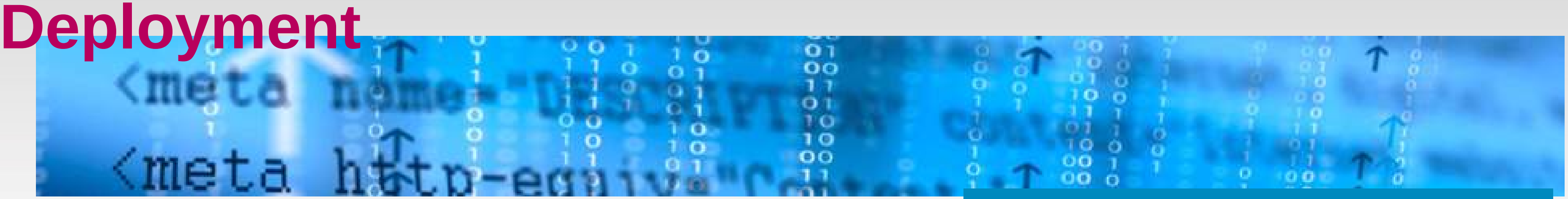
IBM Enterprise Key Management Foundation for Integrated Key Management

- 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

Secure Applications From Design through Deployment



- Use Application Transparent Transport Layer Security to secure sensitive communications without incurring costly application changes
- Hardware enforced storage protect keys -- memory protection to protect your most critical transactional systems
- Prevent execution of malicious or erroneous security changes with zSecure Command Verifier
- Protect application paging data automatically with Flash Express
- Use WebSphere® with RACF for end-to-end, authentication and authorization
- Scan and protect web applications for vulnerabilities

Reduce the cost of fixing a security defect by up to 200x by finding vulnerabilities early in the development cycle

IBM zEnterprise Solutions

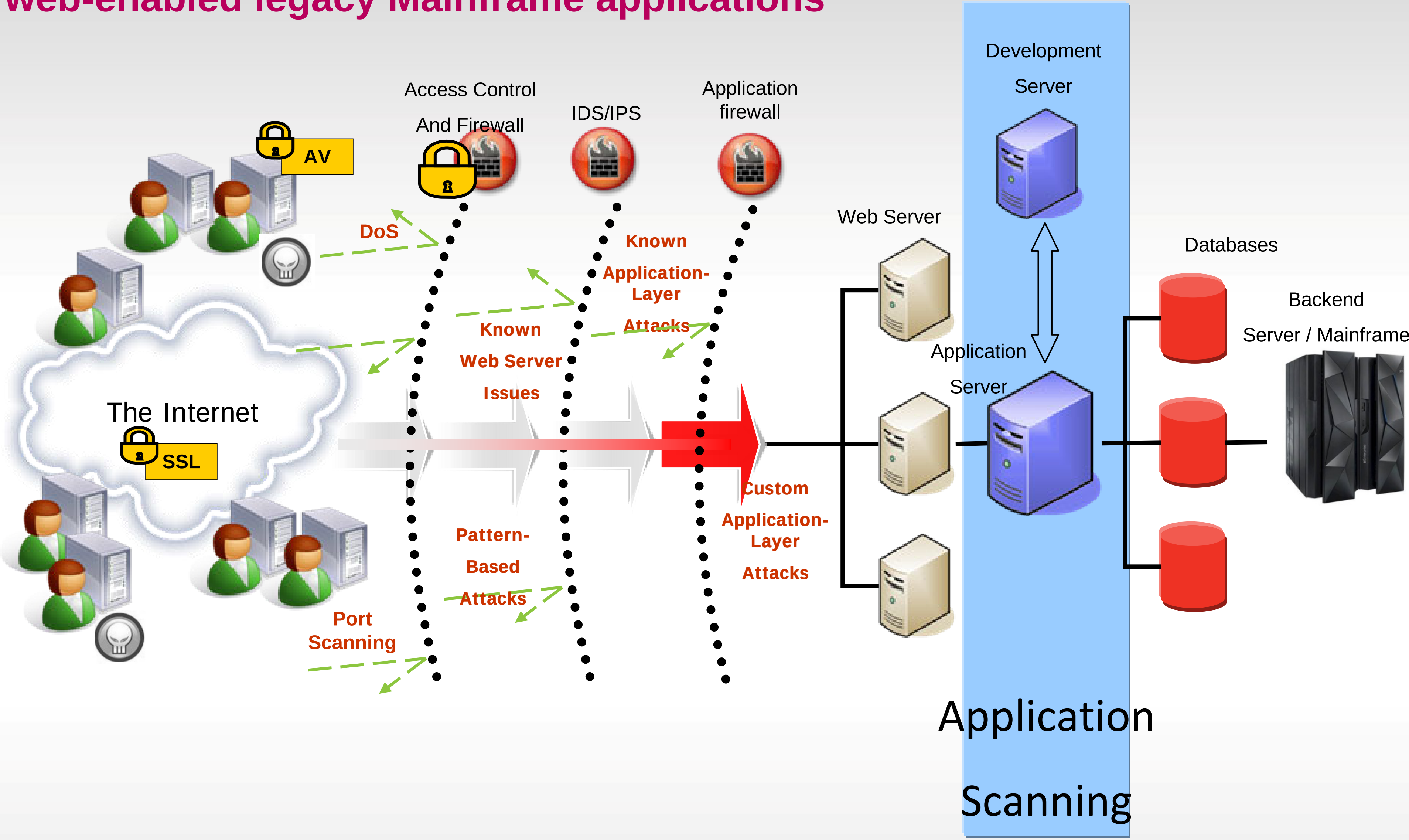
- Comm Server AT-TLS
- Storage Protection of z
- Flash Express
- zSecure Command Verifier
- WebSphere Application Server
- Rational® AppScan®

41% of all security vulnerabilities in 2011 were found in Web applications. System z architecture is fortified against such attacks.

IBM X-Force® 2011 Trend and Risk Report

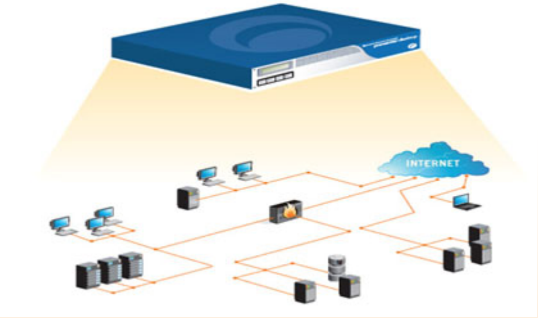
Secure new business models and interfaces that require additional security mechanisms through the zEnterprise stack

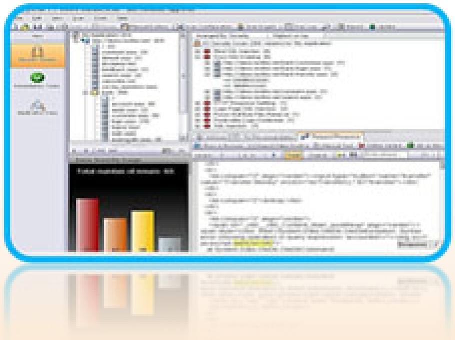
Application security scanning is an essential component of protecting web-enabled legacy Mainframe applications



Using AppScan for Dynamic Application Security Testing (DAST) identifies more vulnerabilities in web applications

1. Scan applications and code
2. Analyze and identify issues
3. Report: Detailed, actionable





- AppScan Dynamic Analysis:
  - Analyze live web applications
  - Use during testing
  - Uses HTTP tampering
- Types of DAST Tests AppScan Sends:
  - Application - Tests that focus on the specific web application being scanned, based of the pages, parameters, and other components discovered during the Explore
  - Infrastructure - Tests that focus more on the environment in which a web application is hosted, encompassing: Web Server, Application Server, Framework, Database and OS.
  - Third Party Components - Check the server for 3rd Party Technologies known to have vulnerabilities, or are un-patched.

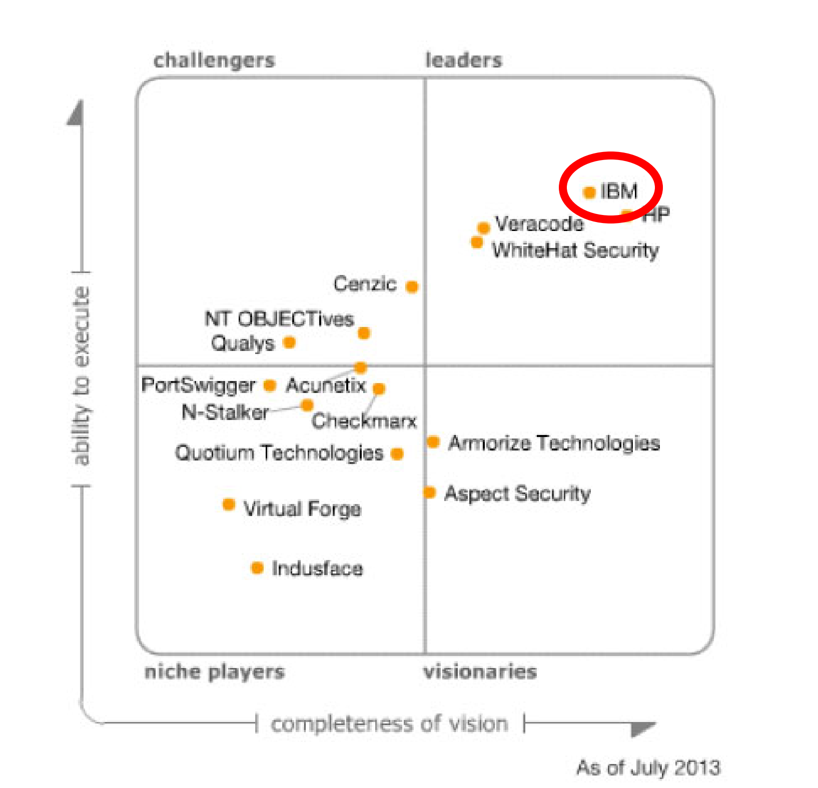
Gartner has recognized IBM as a leader in the Magic Quadrant for Application Security Testing (AST)

Magic Quadrant for Dynamic Application Security Testing

Neil MacDonald, Joseph Feiman

July 2, 2013

“The market for application security testing is changing rapidly. Technology trends, such as mobile applications, advanced Web applications and dynamic languages, are forcing the need to combine dynamic and static testing capabilities, which is reshaping the overall market.”



Source: Gartner (July 2013)

This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The link to the Gartner report is available upon request from IBM.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose

zEnterprise software: Mobile

1.7M+

apps in the world today

70B

apps will be downloaded in 2013

6x and 3x

the number of Android and iOS versions Google and Apple respectively have released compared to major Microsoft® Windows® versions

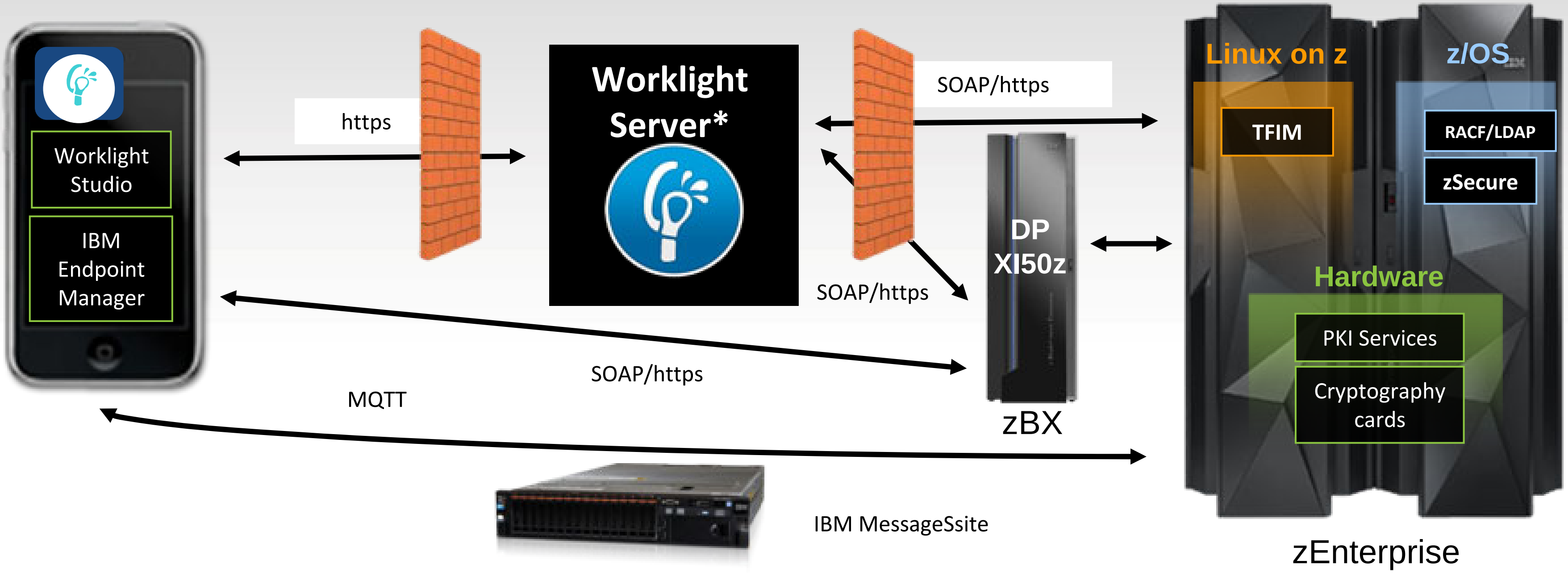
Build mobile web, hybrid, and native apps connecting to zEnterprise data

Complete lifecycle security

Sharing of apps in a cloud environment

Building, connecting, and securing zEnterprise data to mobile devices to provide a better customer experience

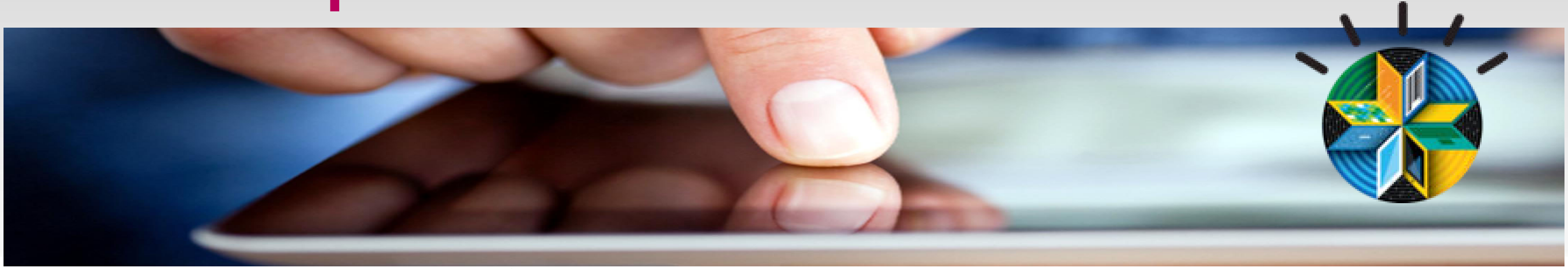
End to end security from mobile to the mainframe



- **End to end capability of mobile users identity permits, syncing of LDAP, auditing of transactions, simplified identity mapping** with zSecure and RACF®
- **Advanced scalability of encryption processing** with System z cryptography cards
- **Centralized certificate management** with z/OS PKI services, RACF and zSecure
- **Secured integration gateway for System z services, centralized key management and mobile access policy capabilities** with DataPower XI50z
- **High level security to backend applications** via HiperSockets or IEDN support with Worklight Server

**Worklight Server can also reside on Linux on z*

zEnterprise software solutions for Mobile



Build and Connect

- **Native JSON support** and conversion between JSON and data structures with **NEW!** **CICS® Transaction Server Feature Pack for Mobile Extensions V1.0 and NEW! DB2 11 for z/OS**
- **Development of multiplatform mobile applications** with **NEW!** **IBM Worklight V6** and **NEW!** **Rational® Developer for the Enterprise v9**

Manage and Secure

- **Secure access to System z data on mobile devices and integration with LDAP on zEnterprise BC12** with **IBM Endpoint Manager**
- **Easy-to-use security enhanced integration and IMS integration for mobile devices** with **NEW!** **IBM WebSphere® DataPower® Gateway Appliances V6**

Extend and Transform

- **Extend mobile devices to WebSphere MQ** on z/OS with **NEW!** **IBM Mobile Messaging client pack** updates
- **View of dashboards, reports, etc** on mobile devices with **NEW!** **Cognos Mobile**

Key customer Cloud security concerns

- Manage the registration and control the access of thousands or even millions of Cloud users in a cost-effective way
- Ensure the safety and privacy of critical enterprise data in Cloud environments without disrupting operations
- Provide secure access to applications in the Cloud
- Manage patch requirements for virtualized systems
- Provide protection against network threat and vulnerabilities in the Cloud
- Protect virtual machines
- Achieve visibility and transparency in Cloud environments to find advanced threats and meet regulatory and compliance requirements

"It was much nicer before people started storing all their personal information in the cloud."

Four steps to data security in the Cloud

1

Understand, define policy

- Discover where sensitive data resides
- Classify and define data types
- Define policies and metrics

2

Secure and protect

- Encrypt, redact and mask virtualized databases
- De-identify confidential data in non-production environments

3

Actively monitor and audit

- Monitor virtualized databases and enforce review of policy exceptions
- Automate and centralize the controls needed for auditing and compliance (e.g., SOX, PCI)
- Assess database vulnerabilities

4

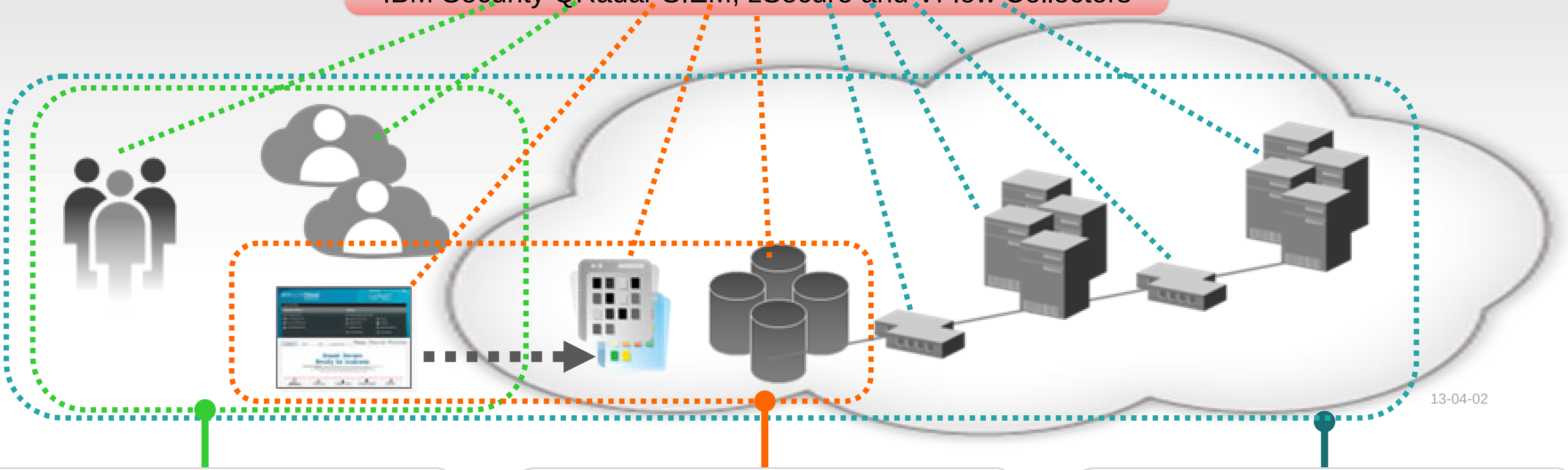
Establish compliance and security intelligence

- Automate reporting customized for different regulations to demonstrate compliance in the Cloud
- Integrate data activity monitoring with security information and event management (QRadar SIEM)

SmartCloud Security Capabilities

IBM SmartCloud Security Intelligence

IBM Security QRadar SIEM, zSecure and VFlow Collectors



IBM SmartCloud Security

Identity Protection

Administer, secure, and extend identity and access to and from the cloud

- IBM Security Identity and Access Management Suite
- IBM Security Federated Identity Manager - Business Gateway
- IBM Security Privileged Identity Manager
- IBM Security zSecure portfolio

IBM SmartCloud Security

Data and Application Protection

Secure enterprise databases

Build, test and maintain secure cloud applications

- IBM InfoSphere Guardium
- IBM Security AppScan Suite
- IBM AppScan OnDemand (hosted)
- IBM Security Key Lifecycle Manager

IBM SmartCloud Security

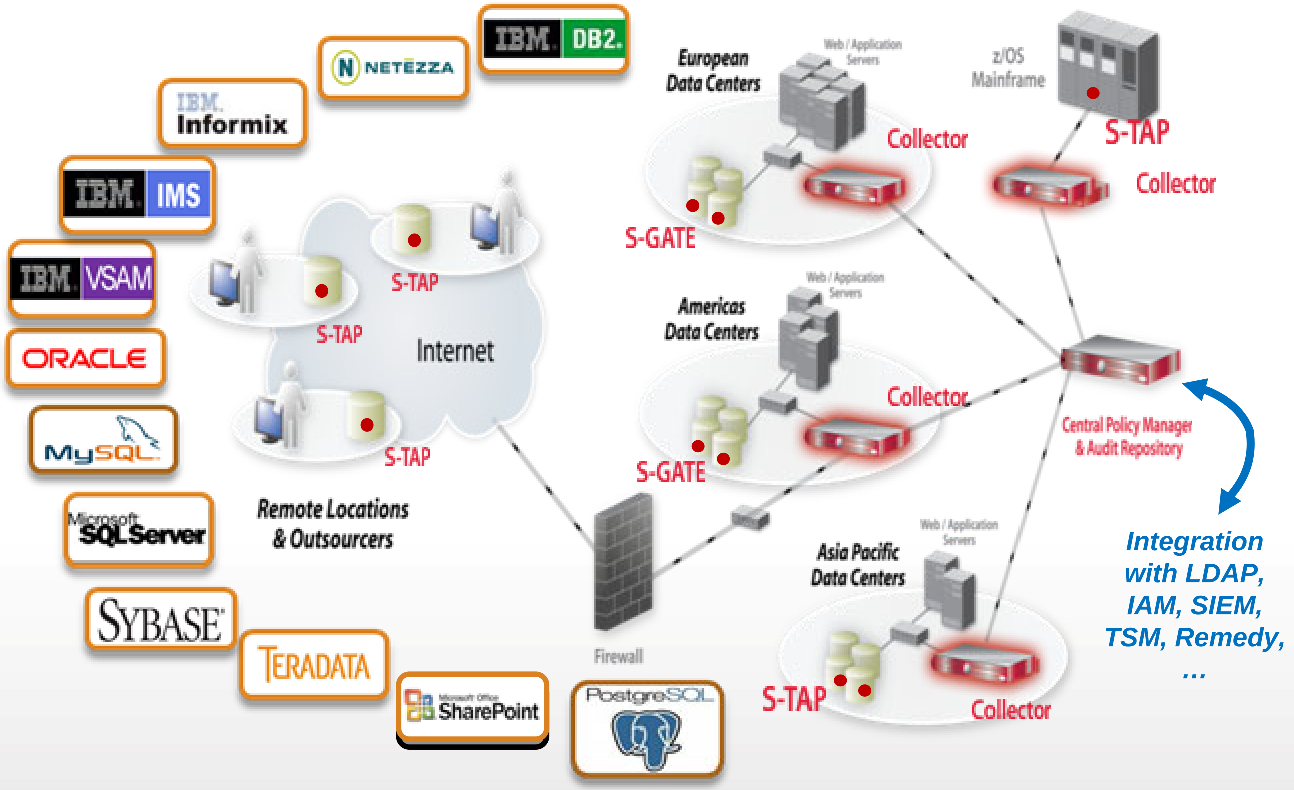
Threat Protection

Prevent advanced threats with layered protection and analytics

- IBM SmartCloud Patch
- IBM Security Network IPS and Virtual IPS
- IBM Security Virtual Server Protection for VMware
- IBM Security zSecure Manager for RACF z/VM

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

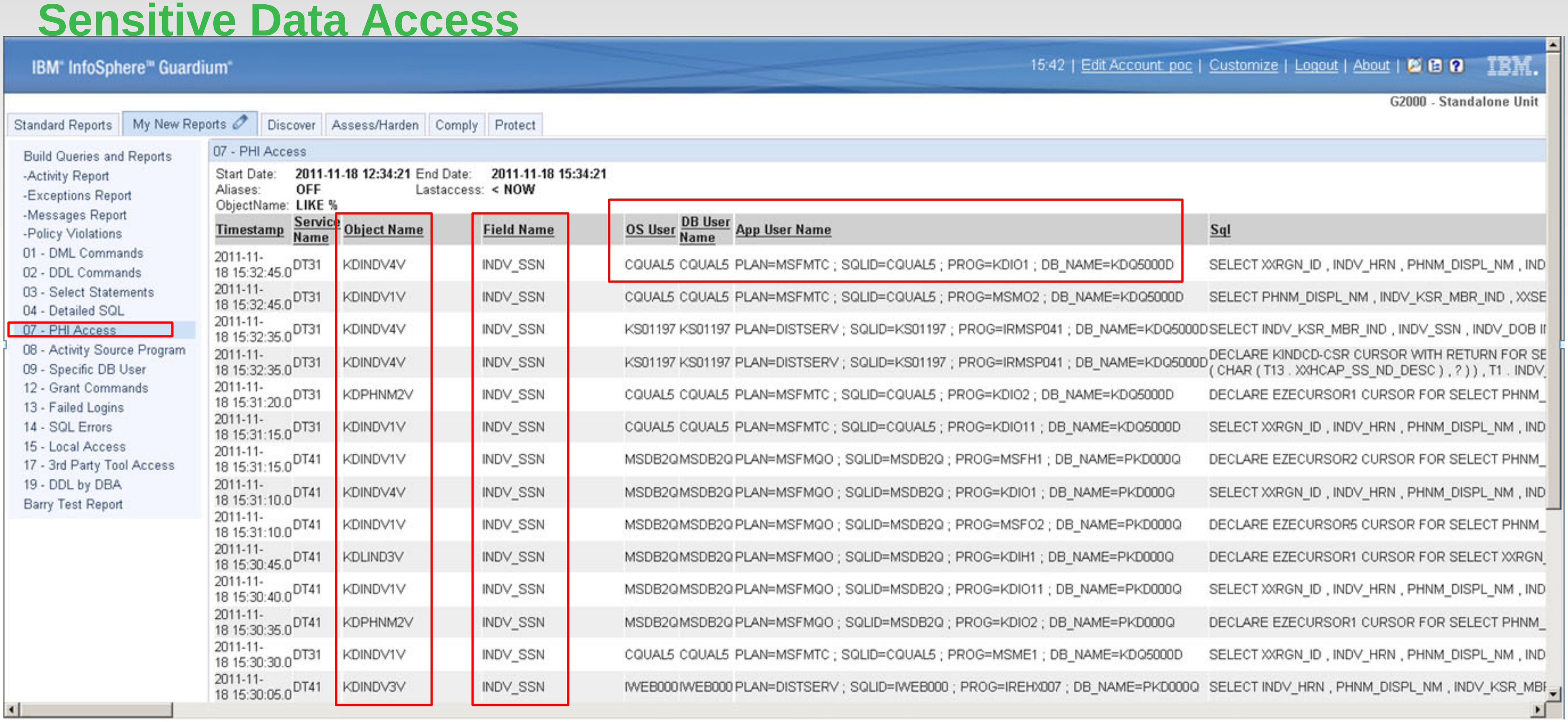
- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized & suspicious activity
- Granular, real-time policies
  - *Who, what, when, how*
- Prepackaged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

Guardium Monitoring on System z - Recent Enhancements

- Termination of suspicious DB2 activity
  - Terminate a DB2 thread that a Guardium policy has flagged as high risk
- Many new System z RACF vulnerability tests
  - directly or via zSecure Integration
- New Entitlement Reporting for z
  - DB2 Catalog and RACF via zSecure
- New monitoring of DataSet activity (sequential and partitioned)
- Centralized IMS management
- Expanded DB2 monitoring including DB2 start and stop
- Resiliency across network or server outages
  - Consistent across all platforms
- Appliance based policy administration
  - Consistent with Distributed policies on Guardium UI

Guardium Reporting

Sensitive Data Access



07 - PHI Access

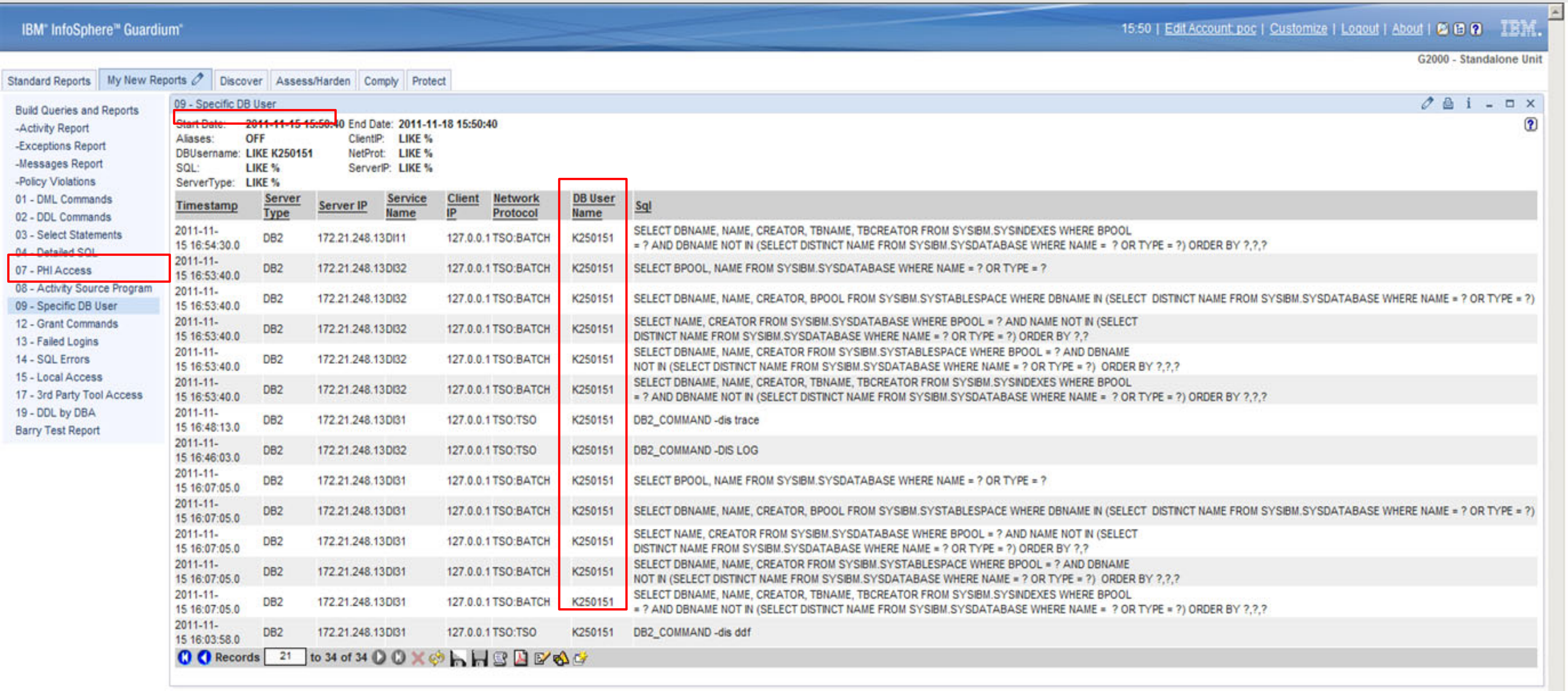
Start Date: 2011-11-18 12:34:21 End Date: 2011-11-18 15:34:21
Aliases: OFF Lastaccess: < NOW
ObjectName: LIKE %

Timestamp	Service Name	Object Name	Field Name	OS User	DB User Name	App User Name	Sql
2011-11-18 15:32:45.0	DT31	KDINDV4V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTC ; SQLID=CQUAL5 ; PROG=KDIO1 ; DB_NAME=KDQ5000D	SELECT XXRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:32:45.0	DT31	KDINDV1V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTC ; SQLID=CQUAL5 ; PROG=MSMO2 ; DB_NAME=KDQ5000D	SELECT PHNM_DISPL_NM , INDV_KSR_MBR_IND , XXSE
2011-11-18 15:32:35.0	DT31	KDINDV4V	INDV_SSN	KS01197	KS01197	PLAN=DISTSERV ; SQLID=KS01197 ; PROG=IRMSP041 ; DB_NAME=KDQ5000D	SELECT INDV_KSR_MBR_IND , INDV_SSN , INDV_DOB I
2011-11-18 15:32:35.0	DT31	KDINDV4V	INDV_SSN	KS01197	KS01197	PLAN=DISTSERV ; SQLID=KS01197 ; PROG=IRMSP041 ; DB_NAME=KDQ5000D	DECLARE KINDCD-CSR CURSOR WITH RETURN FOR SE (CHAR (T13 . XXHCAP_SS_ND_DESC) , ?)) , T1 . INDV_
2011-11-18 15:31:20.0	DT31	KDPHNM2V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTC ; SQLID=CQUAL5 ; PROG=KDIO2 ; DB_NAME=KDQ5000D	DECLARE EZECURSOR1 CURSOR FOR SELECT PHNM_
2011-11-18 15:31:15.0	DT31	KDINDV1V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTC ; SQLID=CQUAL5 ; PROG=KDIO11 ; DB_NAME=KDQ5000D	SELECT XXRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:31:15.0	DT41	KDINDV1V	INDV_SSN	MSDB2Q	MSDB2Q	PLAN=MSFMQO ; SQLID=MSDB2Q ; PROG=MSFH1 ; DB_NAME=PKD000Q	DECLARE EZECURSOR2 CURSOR FOR SELECT PHNM_
2011-11-18 15:31:10.0	DT41	KDINDV4V	INDV_SSN	MSDB2Q	MSDB2Q	PLAN=MSFMQO ; SQLID=MSDB2Q ; PROG=KDIO1 ; DB_NAME=PKD000Q	SELECT XXRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:31:10.0	DT41	KDINDV1V	INDV_SSN	MSDB2Q	MSDB2Q	PLAN=MSFMQO ; SQLID=MSDB2Q ; PROG=MSFO2 ; DB_NAME=PKD000Q	DECLARE EZECURSOR5 CURSOR FOR SELECT PHNM_
2011-11-18 15:30:45.0	DT41	KDLIND3V	INDV_SSN	MSDB2Q	MSDB2Q	PLAN=MSFMQO ; SQLID=MSDB2Q ; PROG=KDIH1 ; DB_NAME=PKD000Q	DECLARE EZECURSOR1 CURSOR FOR SELECT XXRGN_
2011-11-18 15:30:40.0	DT41	KDINDV1V	INDV_SSN	MSDB2Q	MSDB2Q	PLAN=MSFMQO ; SQLID=MSDB2Q ; PROG=KDIO11 ; DB_NAME=PKD000Q	SELECT XXRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:30:35.0	DT41	KDPHNM2V	INDV_SSN	MSDB2Q	MSDB2Q	PLAN=MSFMQO ; SQLID=MSDB2Q ; PROG=KDIO2 ; DB_NAME=PKD000Q	DECLARE EZECURSOR1 CURSOR FOR SELECT PHNM_
2011-11-18 15:30:30.0	DT31	KDINDV1V	INDV_SSN	CQUAL5	CQUAL5	PLAN=MSFMTC ; SQLID=CQUAL5 ; PROG=MSME1 ; DB_NAME=KDQ5000D	SELECT XXRGN_ID , INDV_HRN , PHNM_DISPL_NM , IND
2011-11-18 15:30:05.0	DT41	KDINDV3V	INDV_SSN	IWEB000	IWEB000	PLAN=DISTSERV ; SQLID=IWEB000 ; PROG=IREHX007 ; DB_NAME=PKD000Q	SELECT INDV_HRN , PHNM_DISPL_NM , INDV_KSR_MB

Ability to Monitor Access to Objects and Fields Containing Sensitive Data

Guardium Report

Specific User Activity



09 - Specific DB User

Start Date:	2011-11-15 15:50:40	End Date:	2011-11-18 15:50:40
Aliases:	OFF	ClientIP:	LIKE %
DBUsername:	LIKE K250151	NetProt:	LIKE %
SQL:	LIKE %	ServerIP:	LIKE %
ServerType:	LIKE %		

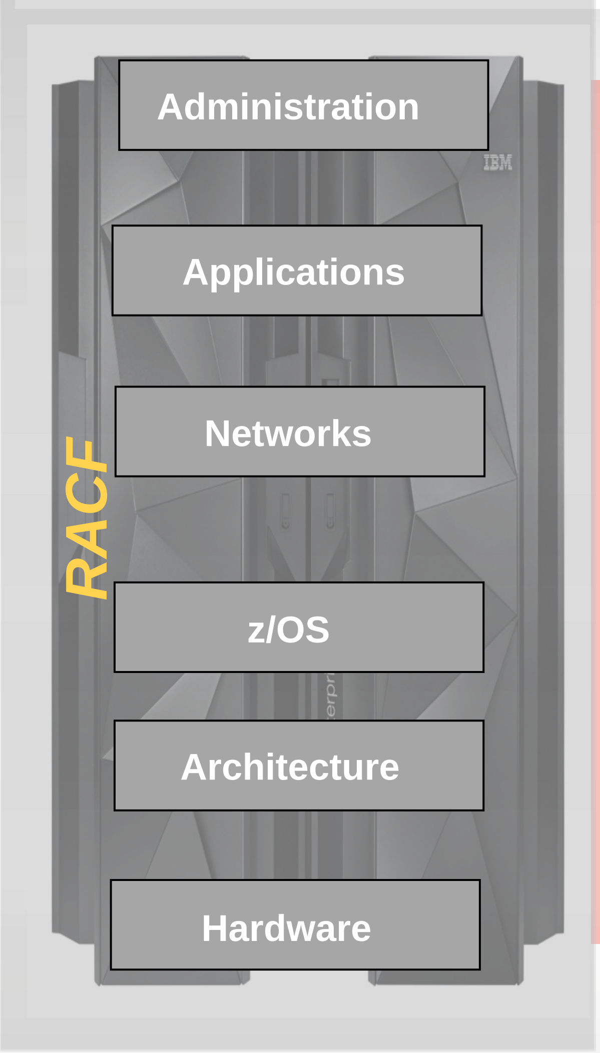
Timestamp	Server Type	Server IP	Service Name	Client IP	Network Protocol	DB User Name	Sql
2011-11-15 16:54:30.0	DB2	172.21.248.13	DI11	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR, TBNAME, TBCREATOR FROM SYSIBM.SYSINDEXES WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:53:40.0	DB2	172.21.248.13	DI32	127.0.0.1	TSO:BATCH	K250151	SELECT BPOOL, NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?
2011-11-15 16:53:40.0	DB2	172.21.248.13	DI32	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR, BPOOL FROM SYSIBM.SYSTABLESPACE WHERE DBNAME IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?)
2011-11-15 16:53:40.0	DB2	172.21.248.13	DI32	127.0.0.1	TSO:BATCH	K250151	SELECT NAME, CREATOR FROM SYSIBM.SYSDATABASE WHERE BPOOL = ? AND NAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?
2011-11-15 16:53:40.0	DB2	172.21.248.13	DI32	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR FROM SYSIBM.SYSTABLESPACE WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:53:40.0	DB2	172.21.248.13	DI32	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR, TBNAME, TBCREATOR FROM SYSIBM.SYSINDEXES WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:48:13.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:TSO	K250151	DB2_COMMAND -dis trace
2011-11-15 16:46:03.0	DB2	172.21.248.13	DI32	127.0.0.1	TSO:TSO	K250151	DB2_COMMAND -DIS LOG
2011-11-15 16:07:05.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:BATCH	K250151	SELECT BPOOL, NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?
2011-11-15 16:07:05.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR, BPOOL FROM SYSIBM.SYSTABLESPACE WHERE DBNAME IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?)
2011-11-15 16:07:05.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:BATCH	K250151	SELECT NAME, CREATOR FROM SYSIBM.SYSDATABASE WHERE BPOOL = ? AND NAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?
2011-11-15 16:07:05.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR FROM SYSIBM.SYSTABLESPACE WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:07:05.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:BATCH	K250151	SELECT DBNAME, NAME, CREATOR, TBNAME, TBCREATOR FROM SYSIBM.SYSINDEXES WHERE BPOOL = ? AND DBNAME NOT IN (SELECT DISTINCT NAME FROM SYSIBM.SYSDATABASE WHERE NAME = ? OR TYPE = ?) ORDER BY ?,?,?
2011-11-15 16:03:58.0	DB2	172.21.248.13	DI31	127.0.0.1	TSO:TSO	K250151	DB2_COMMAND -dis ddf

Records 21 to 34 of 34

Ability to Report on a Specific User’s Activity

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

Authentication
Authorization
Administration
Auditing



RACF

Administration

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

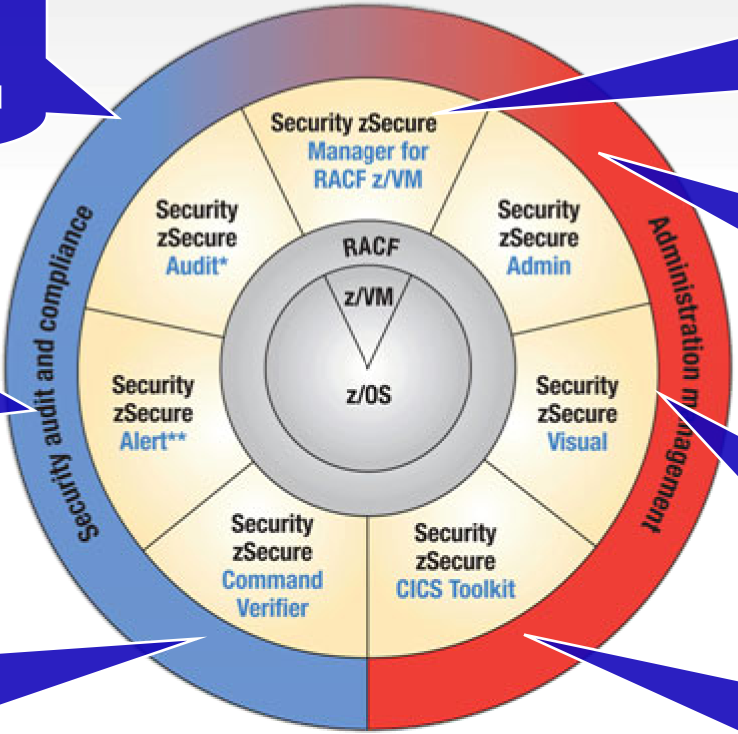
Serving mainframe enterprises for over 30 years

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 and Guardium VA.

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

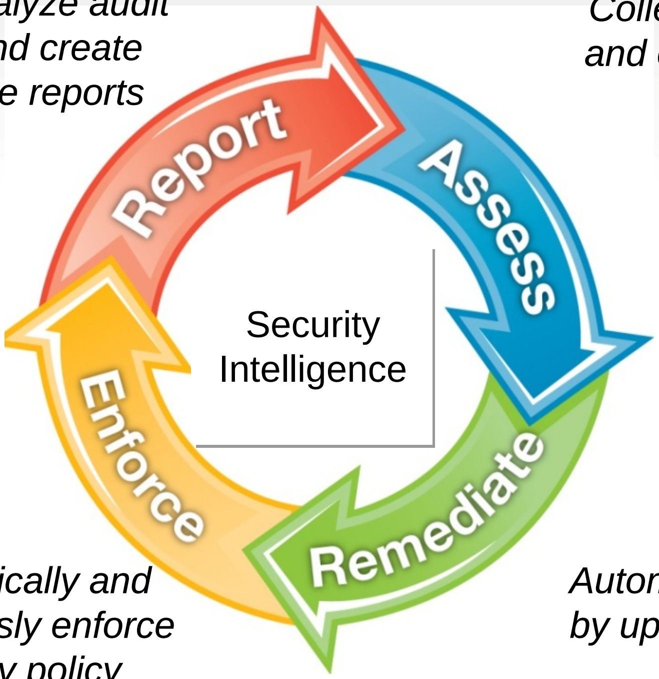
Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

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

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

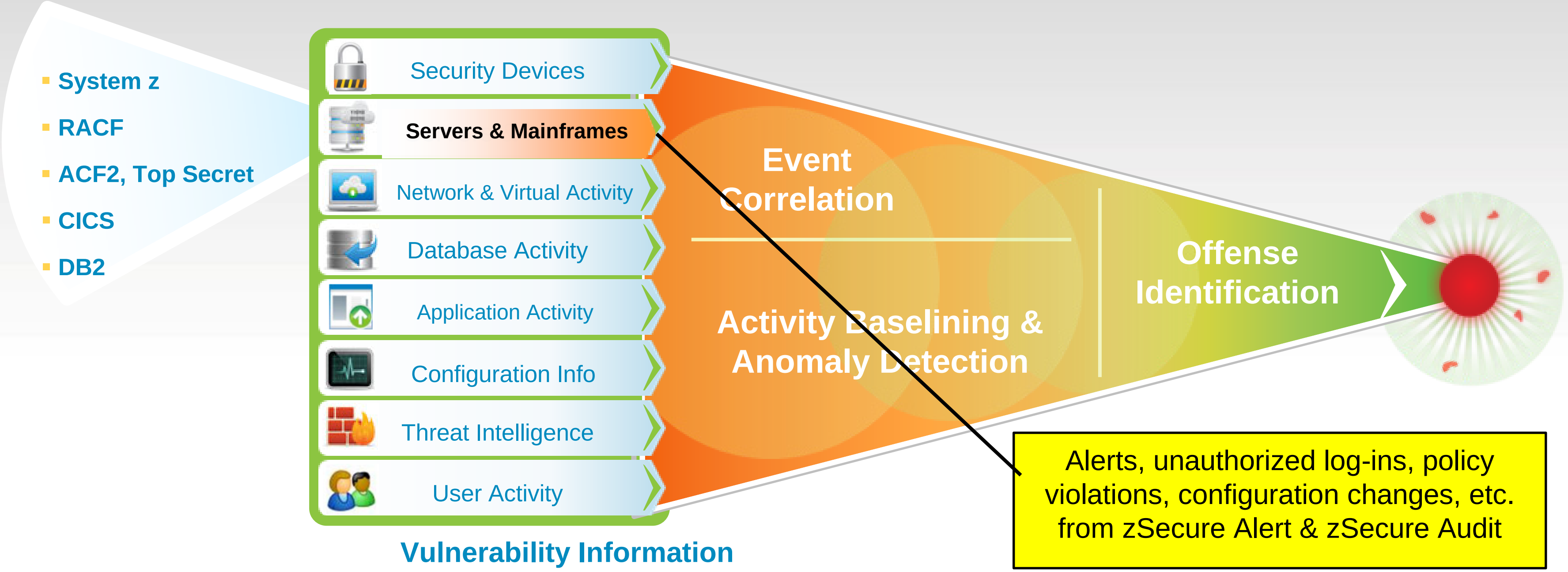


Automatically and continuously enforce security policy

Automate corrective actions by updating access controls

IBM Security zSecure Compliance and Auditing With QRadar

zSecure & QRadar improve your Security Intelligence

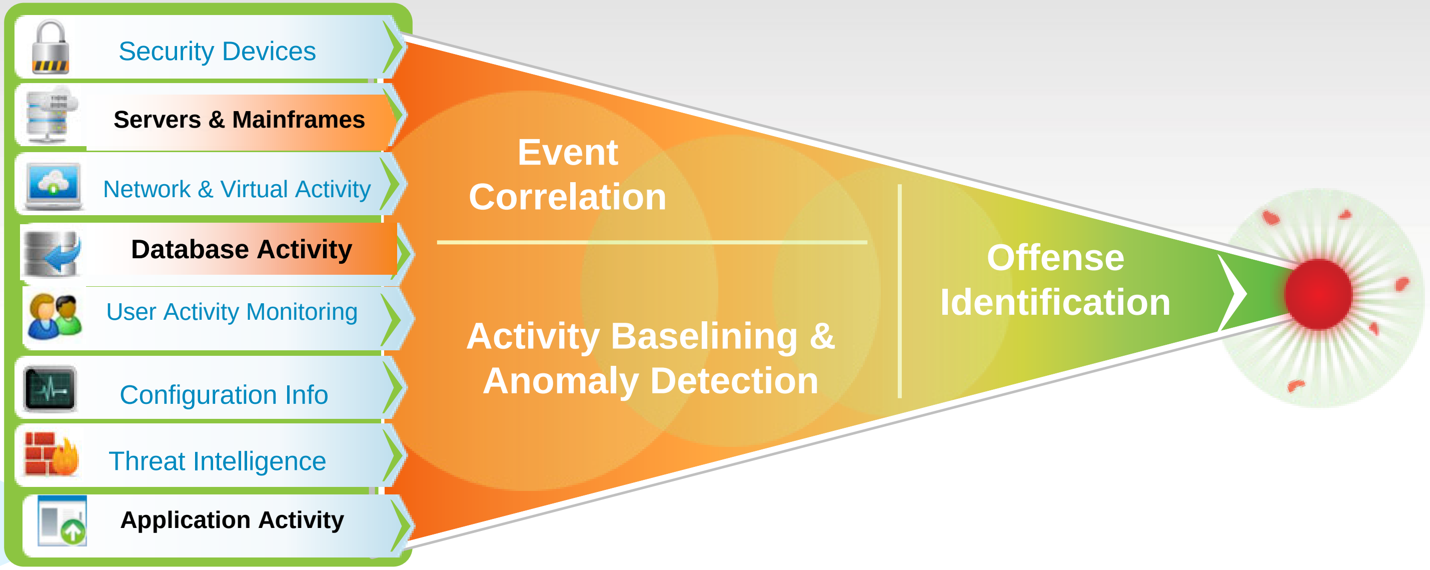


Alerts, unauthorized log-ins, policy violations, configuration changes, etc. from zSecure Alert & zSecure Audit

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

AppScan protecting your Host and Distributed applications improves your Security Intelligence



- Complex, multi-tiered applications involving the mainframe

Vulnerability Information

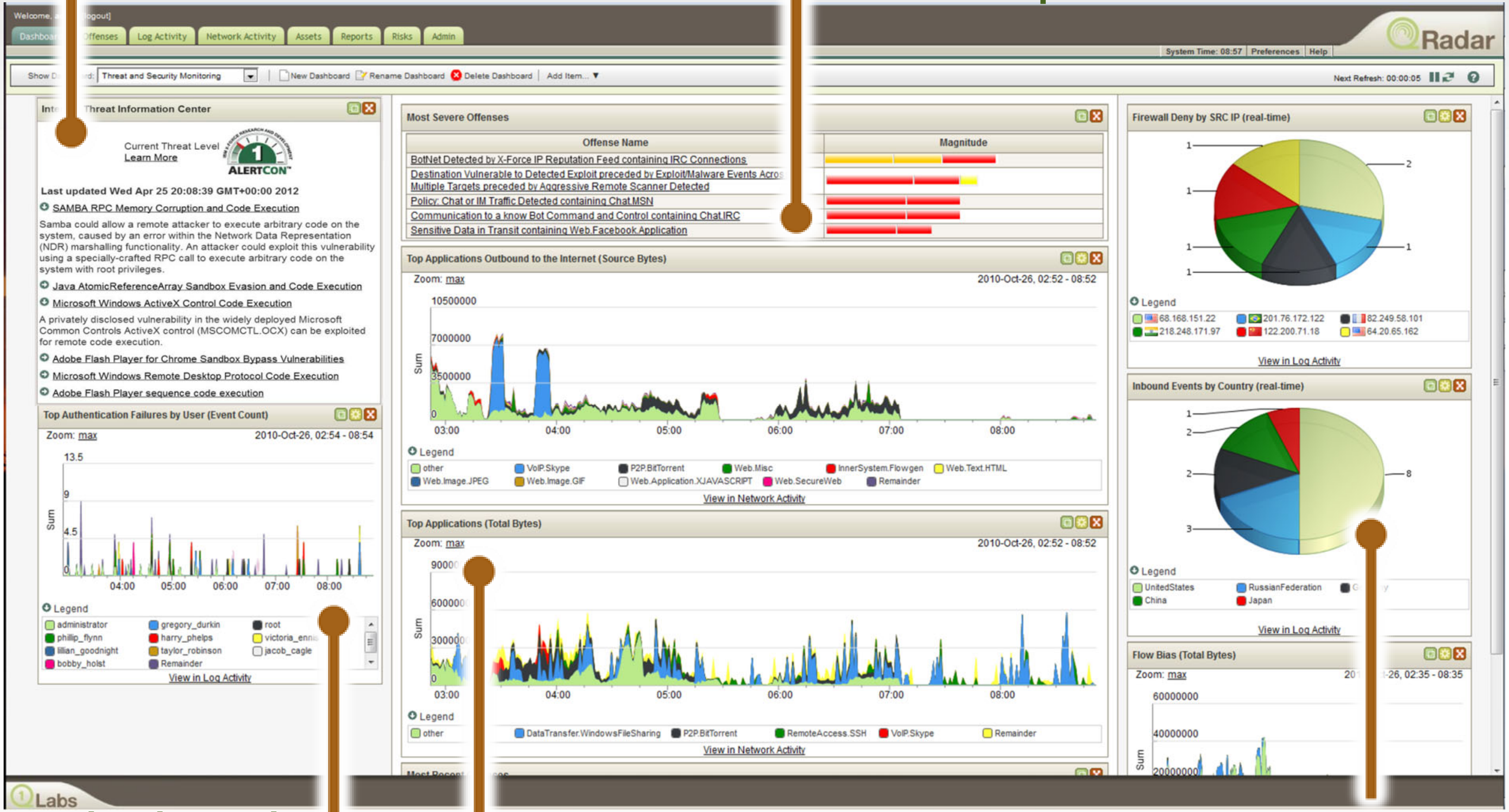
Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

- ✓ Centralized view of mainframe and distributed network security incidents, activities and trends
- ✓ Better real-time threat identification and prioritization correlating vulnerabilities on distributed and host platforms
- ✓ Produces increase accuracy of risk levels and offense scores, and simplified compliance reporting
- ✓ Provides the best level of detection and protection against advanced persistent threats

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
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

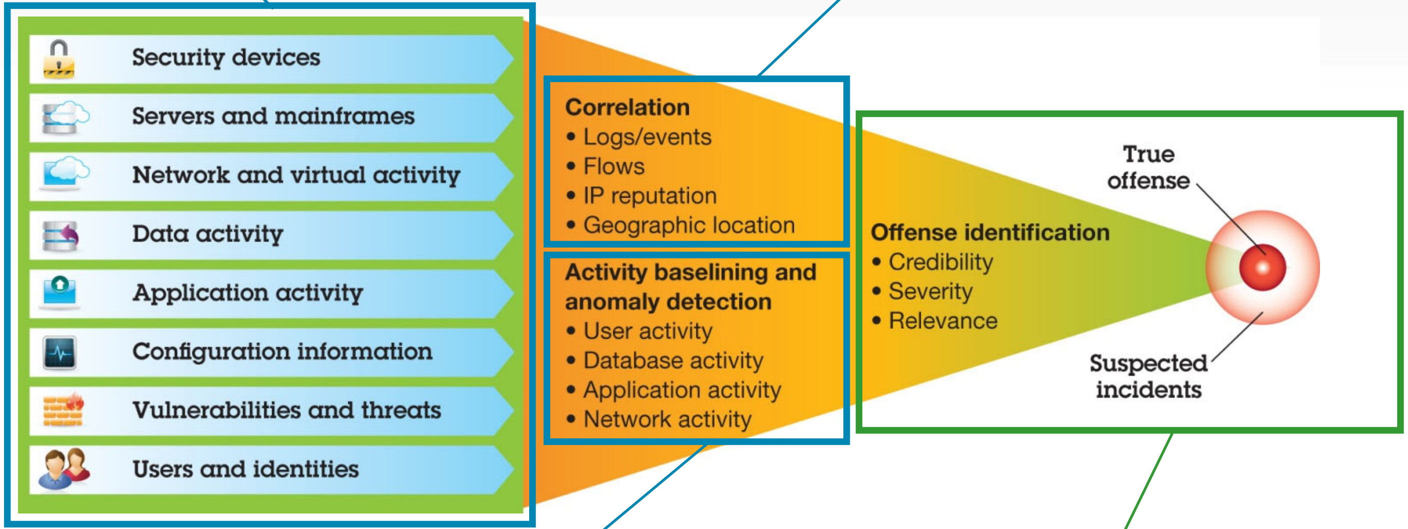
Leverage advanced analytics across all stages of the attack

Monitor everything

Logs, network traffic, user activity

Correlate intelligently

Connect the dots of disparate activity



Detect anomalies

Unusual yet hidden behavior

Prioritize for action

Attack high-priority incidents

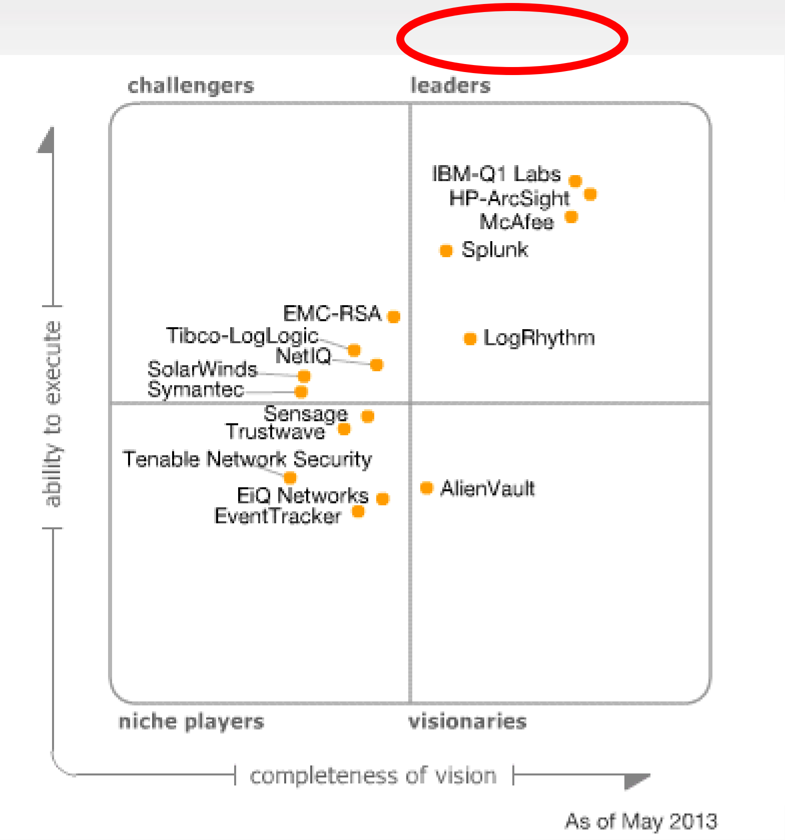
Gartner has recognized IBM as a leader in The Magic Quadrant for Security Information and Event Management

Magic Quadrant for Security Information and Event Management

Mark Nicolett, Kelly M. Kavanagh

May 7, 2013

Broad adoption of SIEM technology is being driven by the need to detect threats and breaches, as well as by compliance needs. Early breach discovery requires effective user activity, data access and application activity monitoring.



This Magic Quadrant graphic was published by Gartner, Inc. as part of a larger research note and should be evaluated in the context of the entire report. The Gartner report is available upon request from IBM.

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose

zEnterprise Big Data Security Solutions

- **Up to 70% of corporate production data may still reside on mainframes**
- **Enhanced DB2, CICS, and IMS data protection** with RACF, Guardium, Optim, and zSecure
- **Improved data integrity with automated auditing and compliance capabilities** with zSecure, Guardium, and IBM Security QRadar
- **Data security classification** with RACF, Guardium, and Optim
- **Sensitive data encryption** with DB2, Guardium, Optim and SKLM for z/OS

The need for bulletproof infrastructure has never been greater – zEnterprise 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*

System z Technical Strategic Priorities

Data Server of Choice

Stack Performance

- Get workload done faster
- Scale capacity with workload
- Co-optimize hardware & software

Data-Serving

- Deliver more data … faster

Business Analytics

- Integrated Stack
- Workload-optimized
- OLTP -> OLTAP

Most Secure & Reliable

Security

- Auditable protection of data
- Simplify management & compliance
- Security Analytics

System Availability

- IT analytics for monitoring & resiliency

Sysplex Availabiity

- Enhanced GDPS
- Active-active solutions
- Asynchronous data replication
- Simplification and automation

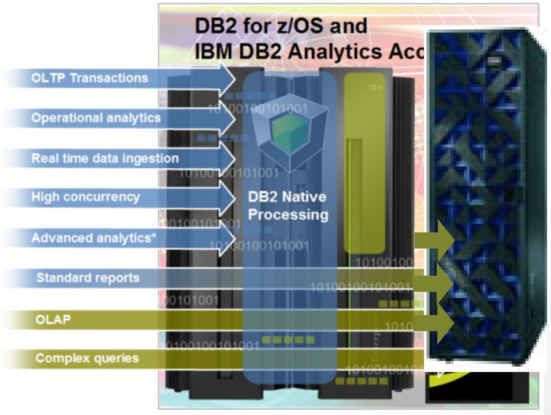
Enterprise Cloud Leadership

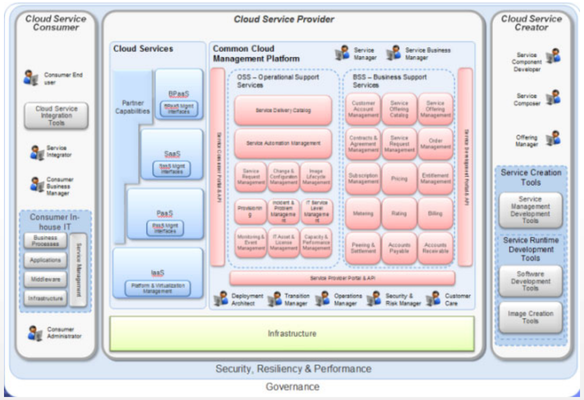
Enterprise Cloud

- Enable cloud-based delivery
- Dynamic shared infrastructure
- Common Cloud Stack
- Isolation for multi-tenancy

Heterogeneous & Mobile Workloads

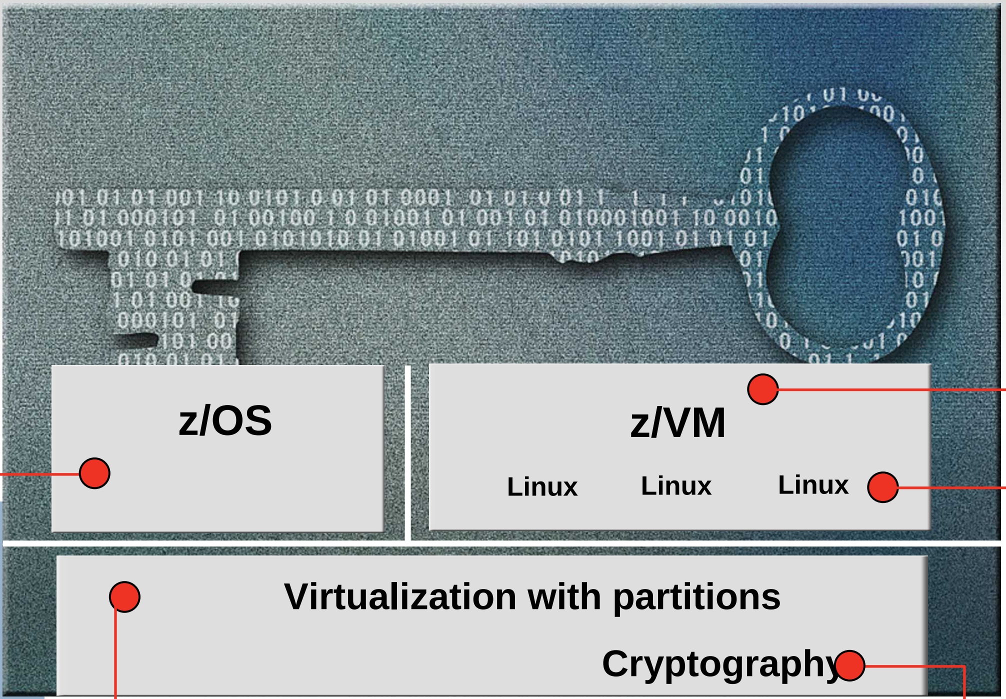
- Linux consolidation
- Extend platform management
- Cross-platform integration
- Industry Solutions
- Integrate mobile workloads




Cloud Service Consumer
Consumer End user
Cloud Service Integration Tools
Service Integrator
Consumer Business Manager
Consumer In-house IT
Business Processes
Applications
Middleware
Infrastructure
Service Management
Consumer Administrator
Cloud Service Provider
Cloud Services
Partner Capabilities
BPaaS
SaaS
PaaS
IaaS
Platform & Virtualization Management
Common Cloud Management Platform
Service Manager
Service Business Manager
OSS – Operational Support Services
Service Delivery Catalog
Service Automation Management
Service Request Management
Change & Configuration Management
Image Lifecycle Management
Provisioning
Incident & Problem Management
IT Service Level Management
Monitoring & Event Management
IT Asset & License Management
Capacity & Performance Management
BSS – Business Support Services
Customer Account Management
Service Offering Catalog
Service Offering Management
Contracts & Agreement Management
Service Request Management
Order Management
Subscription Management
Pricing
Entitlement Management
Metering
Rating
Billing
Peering & Settlement
Accounts Payable
Accounts Receivable
Service Provider Portal & API
Deployment Architect
Transition Manager
Operations Manager
Security & Risk Manager
Customer Care
Infrastructure
Cloud Service Creator
Service Component Developer
Service Composer
Offering Manager
Service Creation Tools
Service Management Development Tools
Service Runtime Development Tools
Software Development Tools
Image Creation Tools
Security, Resiliency & Performance
Governance

System z 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 , z/OS 1.13 (OSPP)
- Common Criteria EAL5+

RACF V1R12 (OSPP)

RACF V1R13 (OSPP)

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

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

- System zEC12
  - Common Criteria EAL5+ with specific target of evaluation -- LPAR: Logical partitions

- Crypto Express2 Coprocessor, Crypto Express3 & Crypto Express4s

  - FIPS 140-2 level 4 Hardware Evaluation
  - Approved by German ZKA
- CP Assist

  - FIPS 197 (AES)
  - FIPS 46-3 (TDES)
  - FIPS 180-3 (Secure Hash)

z/VM

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

- System Integrity Statement

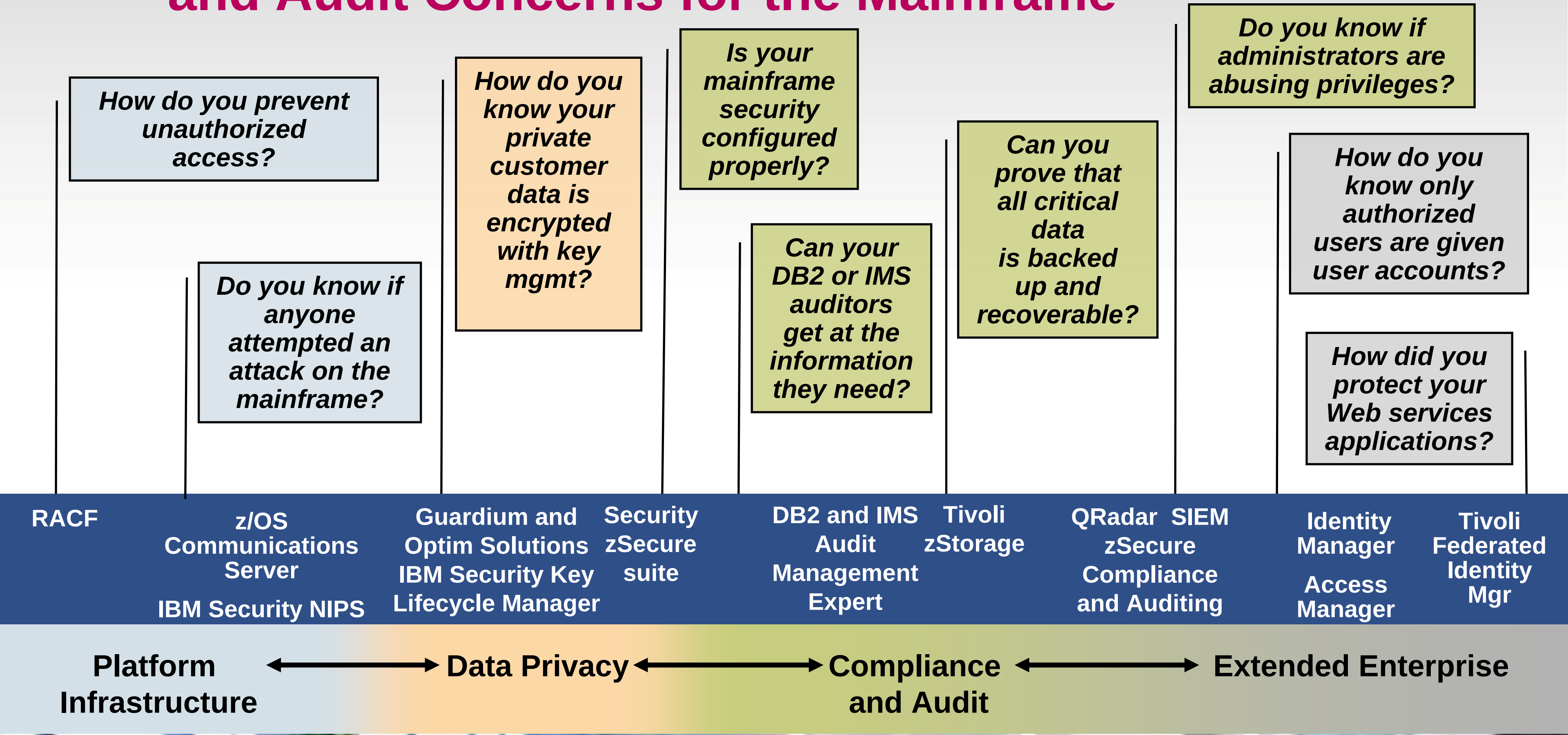
Linux on System z

- Common Criteria
  - SUSE SLES11 SP2 certified at EAL4+ with OSPP
  - Red Hat EL6.2 EAL4+ with CAPP and LSPP

- OpenSSL - FIPS 140-2 Level 1 Validated

- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

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

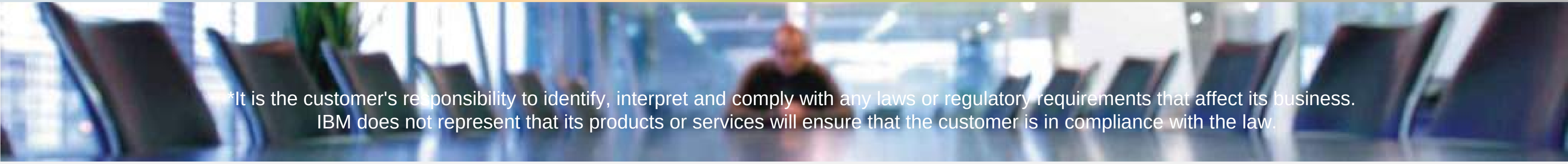
zSecure Compliance and Auditing

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.

Ultimate Security

Reinforce customer trust

"Colony Brands puts Customer Trust and Loyalty as top priorities within the organization. We are proud to leverage IBM's zEnterprise throughout our organization due to the **Trusted, Proven, and Secure** nature of the platform. …"

- *Todd Handel, Director, IT Strategy and Architecture*

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.*

"IBM Security zSecure benefited Itaú Unibanco risk areas by reducing the IT risks that could have a direct impact on the bank's operational risk."

Ineida Moura, Information Security Manager, Itaú Unibanco

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

IBM System z has Secured Systems for over 40 Years.
IBM is Security Ready.

Security, Built-in, by Design

“The mainframe has survived many challenges …. IBM has done this by keeping the IBM System z platform up to date with the changing times, while retaining the fundamental characteristics such as security that define enterprise-class computing at the highest level.”*

*Masabi Group, David Hill, Analyst, November 14, 2012

Security Innovation Spanning Four Decades

1970	1977	1985	2004	2012	2013
Hardware Cryptography	DES Encryption Unit	Crypto Operating System	Multilevel Security MLS	RACF® Evaluated at EAL5+	Enterprise Key Management Foundation

ibm.com/security