



Enterprise Security – Helping businesses lower risk and costs

Jose Castano
Director: System z Growth Initiatives
castano@us.ibm.com



Trademark

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

BladeCenter*	IBM*	InfoSphere	System z*	zEnterprise*
CICS*	IBM (logo)*	MQSeries*	WebSphere*	z/OS*
DB2*	IMS	HiperSockets	X-Force*	
Guardium*	Informix*	RACF*		

* 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



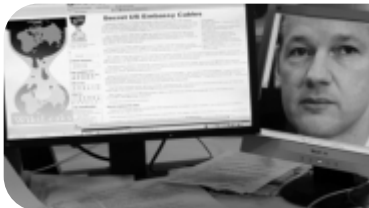
CONSUMERIZATION OF IT

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



New Industry Trends Bring Security Challenges to Business

The cost of data loss has increased by 68% over the past five years¹

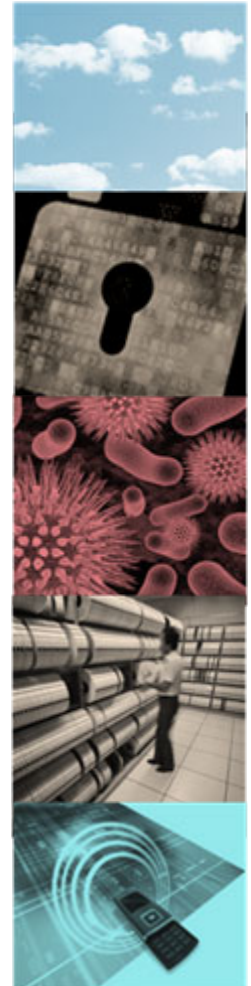
Today's applications with huge data volumes means protection of data is a key imperative

77% of execs believe that adopting cloud computing makes protecting privacy more difficult²

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 concern³

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



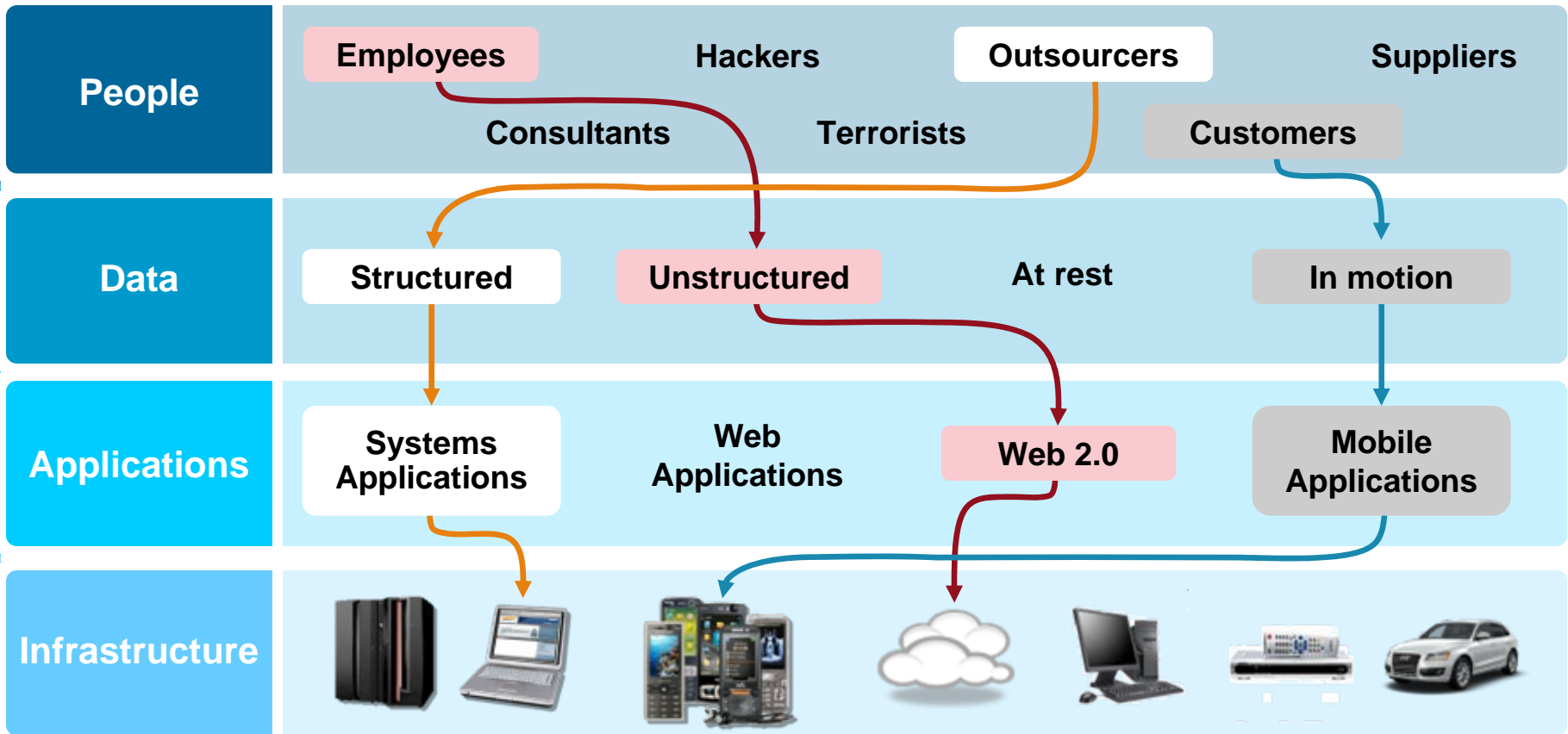
Redefining the challenge of securing your business

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



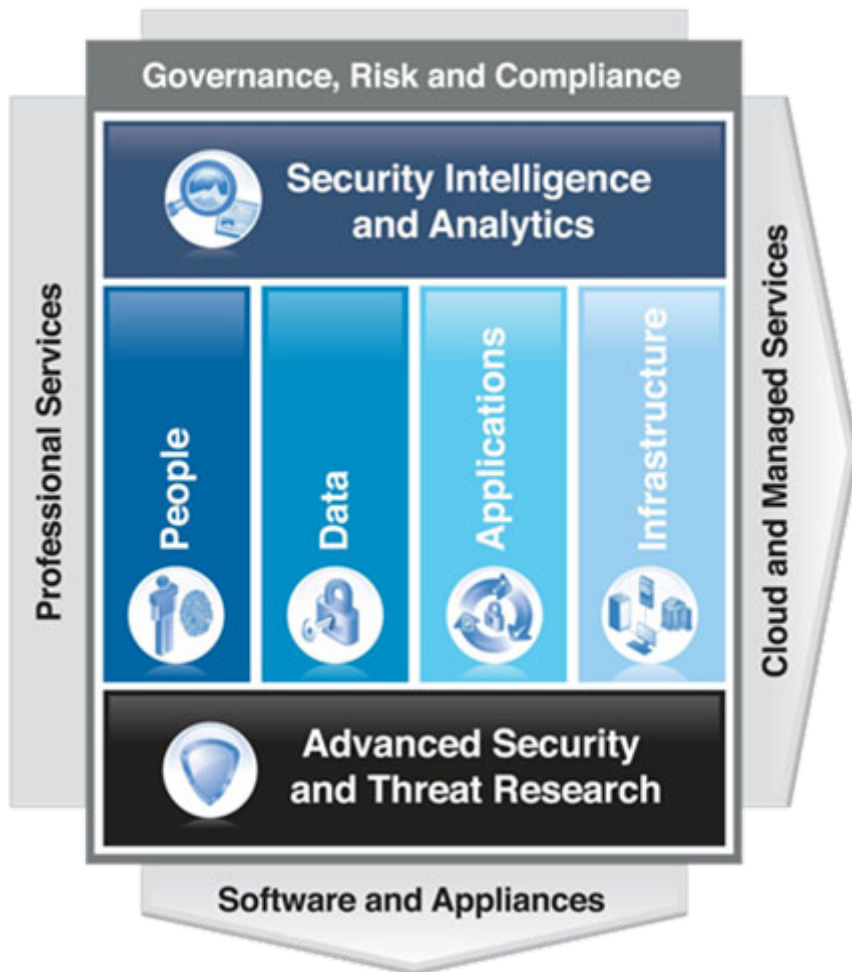
- 77% of firms feel cyber-attacks harder to detect and 34% low confidence to prevent
- 75% felt effectiveness would increase with end-to-end solutions

As a result, the Security market is shifting

	Traditional Focus <i>Governance and Compliance</i>	Emerging Focus <i>Risk Management</i>
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

IBM's security framework... Intelligence Integration Expertise



Security Intelligence and Analytics

Optimize security management with additional context, automation and integration across domains



People

Mitigate the risks associated with user provisioning and access to corporate resources



Data

Understand, deploy, and properly test controls for access to and usage of sensitive data



Applications

Keep applications secure, protected from malicious or fraudulent use, and hardened against failure



Infrastructure

Help protect and maintain compliance of networks, servers, storage, endpoints and mobile devices

IBM Security approach to answer the CSO Challenge: Manage Cost, Decrease Complexity, Improve Effectiveness, Assure Agility



Designed to....



- Enable innovation through secured infrastructure and platforms
- Reduce number and complexity of required security controls
- Reduce redundant security expenses
- Improve organizational and operational agility and resiliency
- Deliver needed visibility, control and automation

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 security server provides the foundation for consistent identity and access mgmt across the stack
 - One policy across z/OS resource managers
- Integrated Public key infrastructure reduces cost and risk of managing digital ids
 - Integrates w/RACF and utilize HW crypto for the security of keys



- Integrated accelerated tamper proof Hardware Cryptography
 - Open standards with Enterprise IBM PKCS #11 targeted to the public sector
 - IBM's Common Crypto Architecture (CCA) supporting needs of banking and finance
- Enterprise management of keys and certificates targeting for financial customers



- Memory protection to protect your most critical transactional systems
- Use Application Transparent Transport Layer Security to secure sensitive communications without incurring costly application changes



- Secured connection with Linux® virtual servers (Linux for IBM System z®) in the box
- Intra-Ensemble Data Network point to point and non-sniffable



- Consistent auditing and reporting using a centralized model
- Strong focus on crypto functions required by the Banking/Finance industries
- Centralized hardware based key management that helps customers comply with standards like PCI-DSS

Security with Core z/OS Middleware

Centralized Integrated Security

EAL5 certified

Administration

**CICS, IMS, WAS
Applications
DB2, IMS, VSAM
Messages&Queues**

Middleware

Network

Virtualization

Hardware

Architecture



- Authentication / Authorization / Administration / Auditing
 - Application and database security without modifying applications
 - Use WebSphere® with RACF® for end-to-end, authentication and authorization



- Granular security implementation for DB2®, CICS®, IMS™, WAS, MQSeries® and z/OS® resources
- Protecting data InfoSphere™ Guardium® Data Encryption
- Labeled DB2 and z/OS security for secured multi-tenancy



- Integrated LDAP capabilities provide enterprise application registry
- Optimized Java environment permits transparent use of platform security
- Open PKCS#11 Crypto facilitates the porting of applications



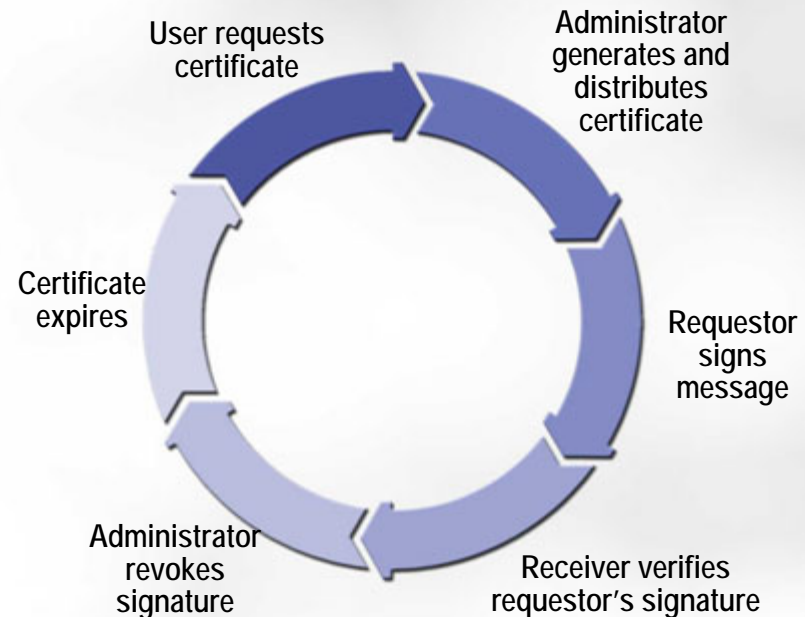
- Support of System Secure Sockets Layer (SSL), digital certificates, and key repositories
- Built-in defenses to ensure high availability of the system against denial-of-service attacks
- Network IPS front end fraud and threat detection



- Granular and detailed logging provided by z/OS Resource Mangers – eg - DB2, CICS, IMS, MQ and z/OS
 - Provides the basis for capabilities with zSecure and Guardium®

Digital certificate hosting with z/OS PKI Services

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



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

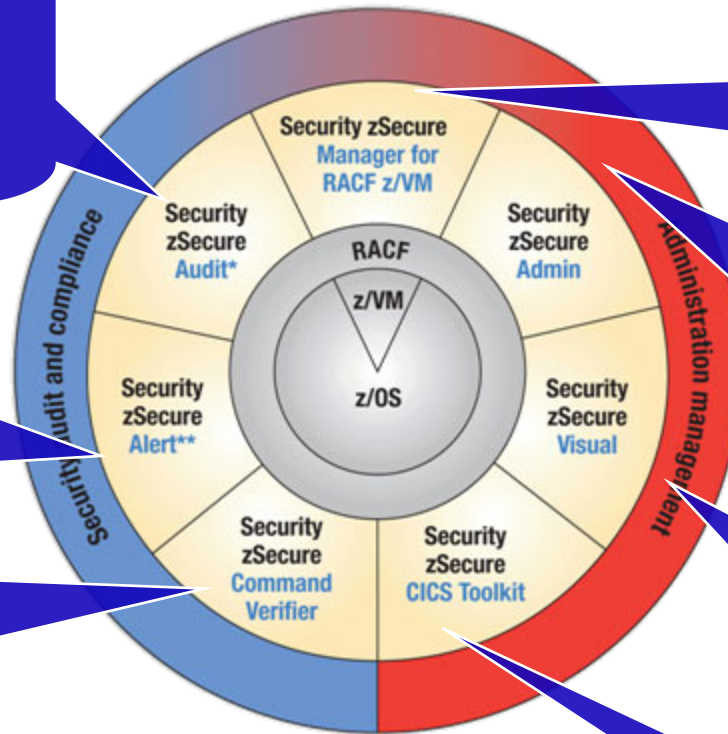
IBM Enterprise Key Management Foundation for Integrated Key Management

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



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

IBM Security zSecure suite products and benefits



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

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. Provides RACF cleanup, database merge, database compare and RACF offline

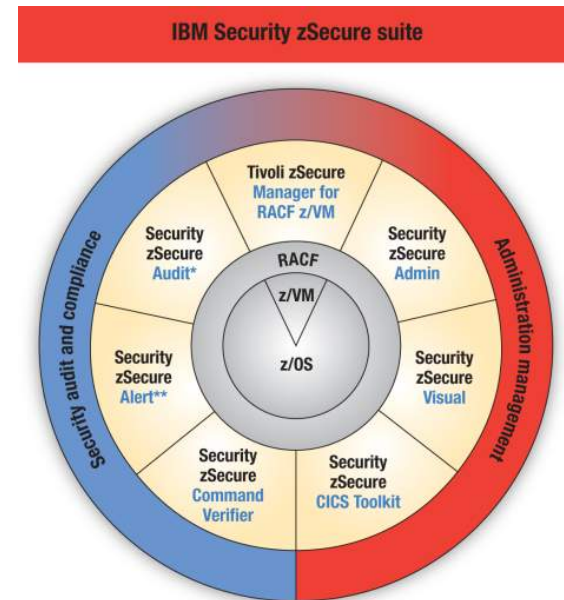
Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows-based GUI for RACF administration

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

- Automate audit, monitoring and compliance with repeatable – sustainable processes
- Simplify security administration and provisioning
- Reduce costs, improve ROI, assist in improving z/OS security
- Consolidate an centralize security management

Security zSecure Suite Benefits:

- **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**



*Also available for ACF2™ and Top Secret®

**Also available for ACF2

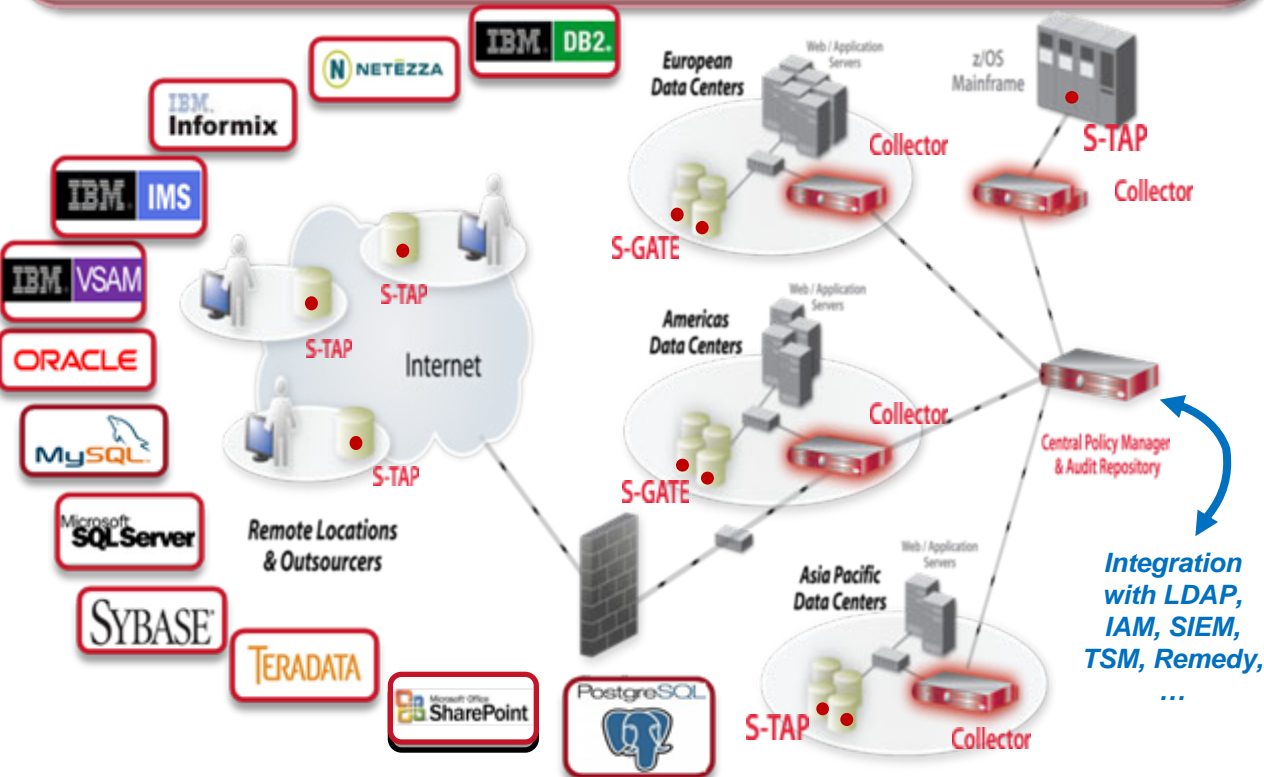
IBM can save customers up to 70% in auditing overhead on mainframe

IBM Guardium Provides Real-Time Database Security and Compliance

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

Key Characteristics

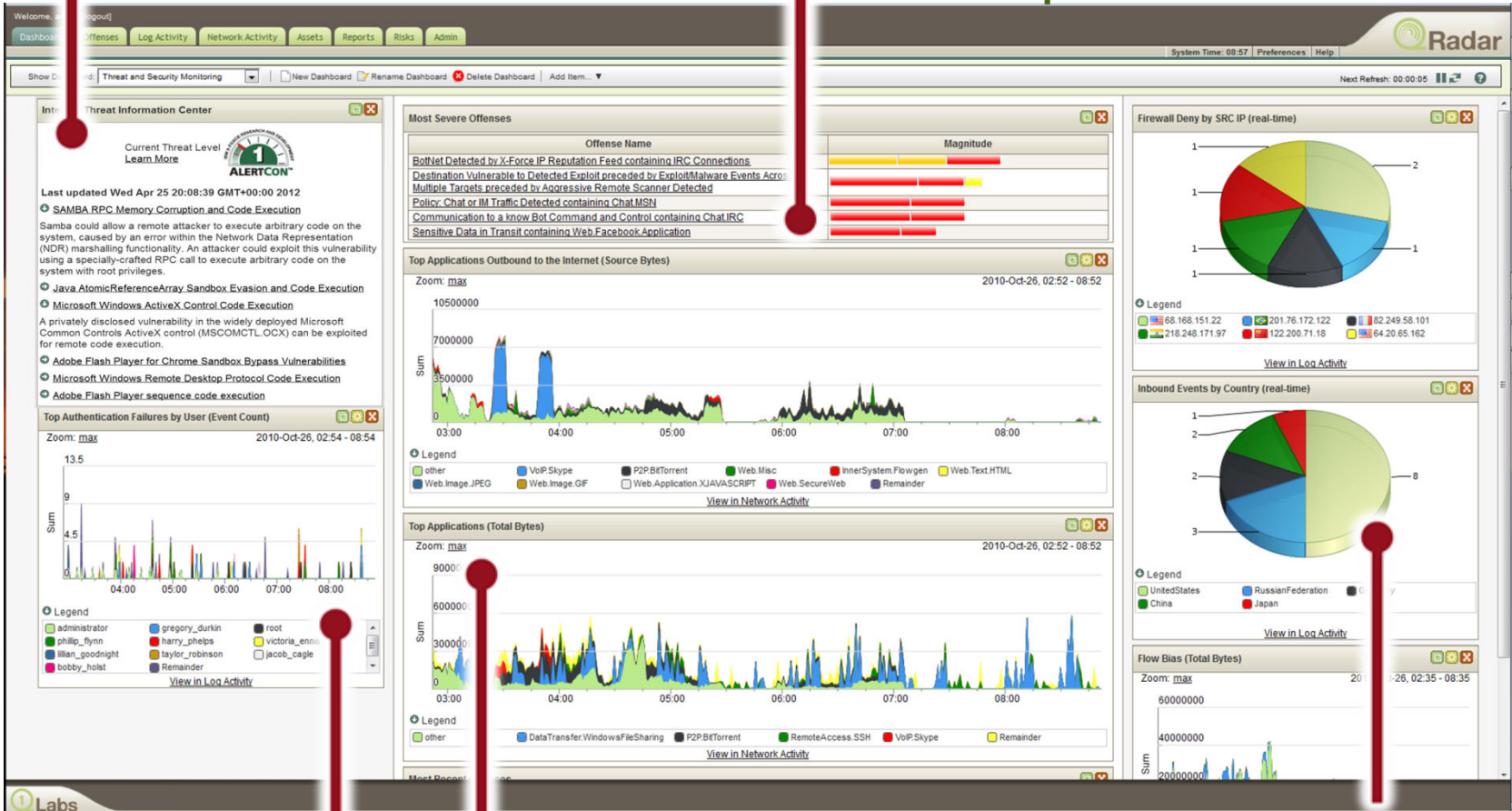
- Single Integrated Appliance
- Non-invasive/disruptive, cross-platform architecture
- Dynamically scalable
- SOD enforcement for DBA access
- Auto discover sensitive resources and data
- Detect or block unauthorized and suspicious activity
- Granular, real-time policies
 - *Who, what, when, how*
- Prepackaged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



Security Intelligence: QRadar provides security visibility

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation

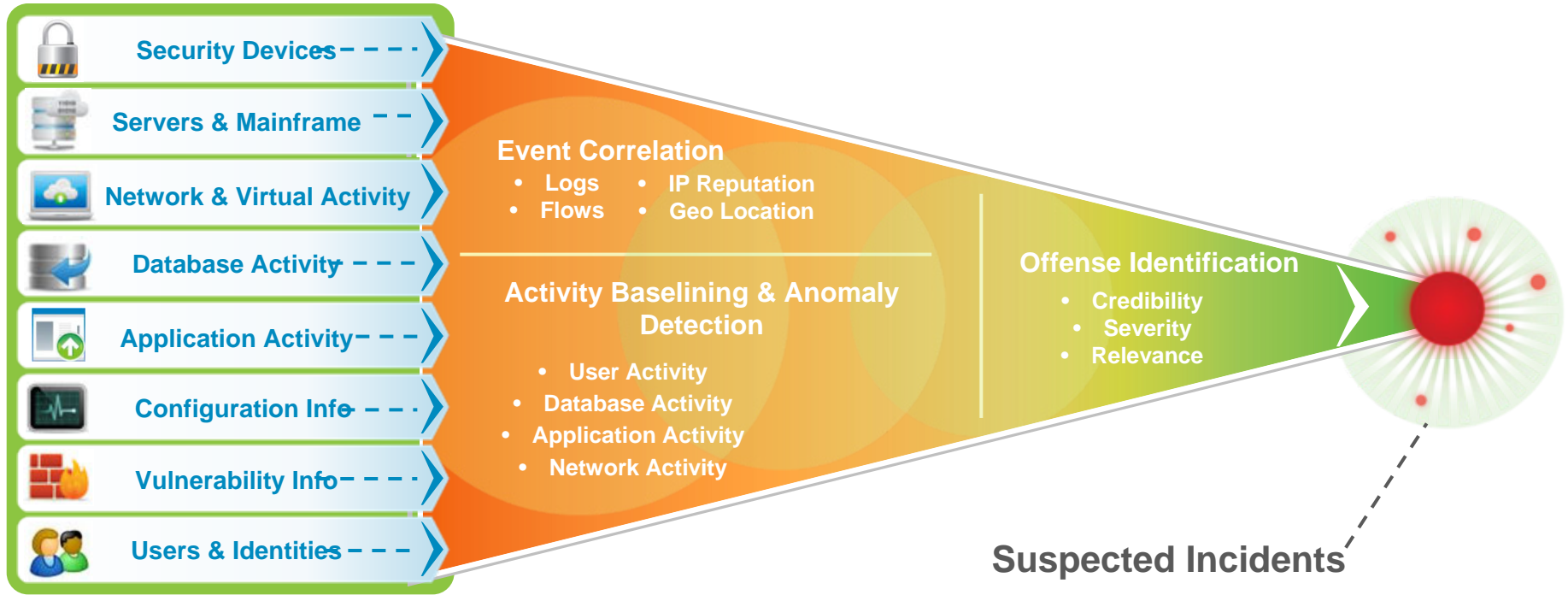


Identity and User Context

Real-time Network Visualization and Application Statistics








Inbound Security Events

QRadar: Context and Correlation Drive Deep Insight and Accurate Detection



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

System z “built in” at every level provides maximum protection - x86 bolted on security provides opportunities for vulnerabilities and complexity

Component	Mainframe	Distributed
Data Encryption 	Built in, scalable, tamper resistant encryption – bullet proof	Typically third party appliances requires integration - more expensive and potentially more vulnerable
Integrated Security across the lifecycle of data 	From transaction to archive, from access to network to storage, data access and encryption is integrated into the platform	Requires multiple components and add on SW solutions with different key's, policies, and procedures.
Consistent Policy Based Access 	Consistent policy based access and authentication with a single point of control for accountability	Multiple tools with different access controls, & different repositories increases risk of unauthorized access
Secured Isolation 	Workload protection of customer data with hardware enforced isolation	Multiple isolated solutions without the advantages of central control making data on cloud more vulnerable to interception
Public Key Infrastructure 	Built in secure, highly available centralized key repository and management	Appliances can create single points of failure and be difficult to achieve highly scalable configurations
Auditing 	Granular auditing using extremely detailed records for accurate and comprehensive reporting	Multiple often inconsistent audit systems making regulatory compliance difficult
Network Security 	Network security built-in – secured HiperSockets™ and networks also provides economic, secure communication to IBM zEnterprise® BladeCenter® Extension (zBX) and within the CPC	Lack of built in security requires more firewalls and additional secured network infrastructure

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*



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
Hardware
Cryptography

1977
DES Encryption
Unit

1985
Crypto Operating
System

2004
Multilevel
Security MLS

2012
RACF Evaluated
at EAL5+

2013
Enterprise
Key
Management
Foundation



ibm.com/security

© **Copyright IBM Corporation 2013. All rights reserved.** The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.