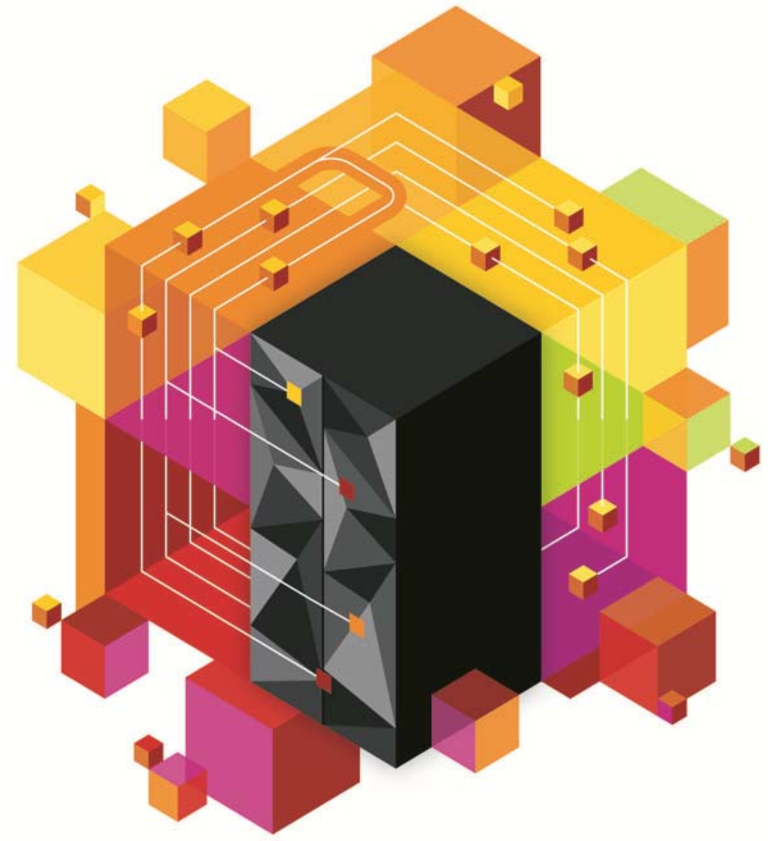
Enterprise Security – Helping Businesses lower risk and costs



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

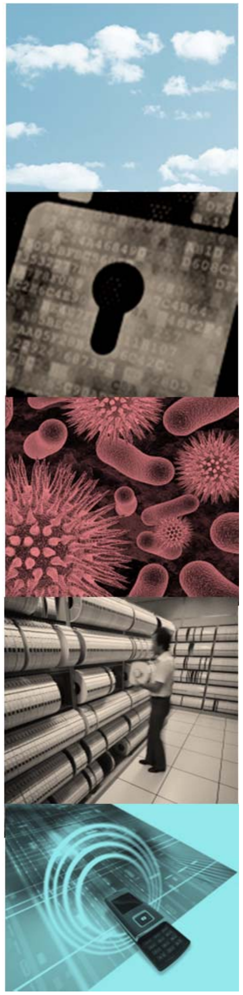
EVERYTHING IS EVERYWHERE

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

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

[1] Source: Computerweekly.com March 20, 2012 www.computerweekly.com/news/2240147054/Cost-of-data-breach-up-68

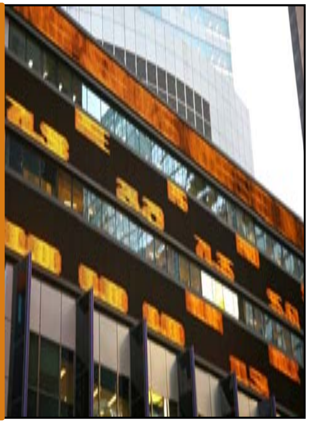
[2] Source: IBM's Institute for Business Value 2010 Global IT Risk Study

[3] Source: IBM 2012 CISO study

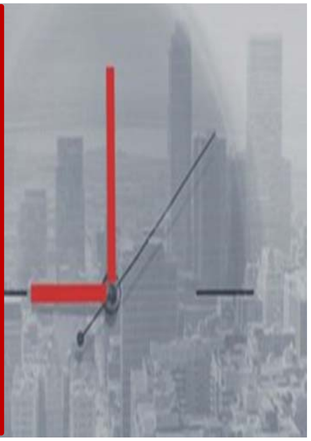
In IBM’s recent 2012 CISO study, security leaders confirm the increasing importance of security

Nearly two-thirds say **senior executives** are paying **more attention** to security issues.

Two-thirds expect to spend **more on** security over the next two years



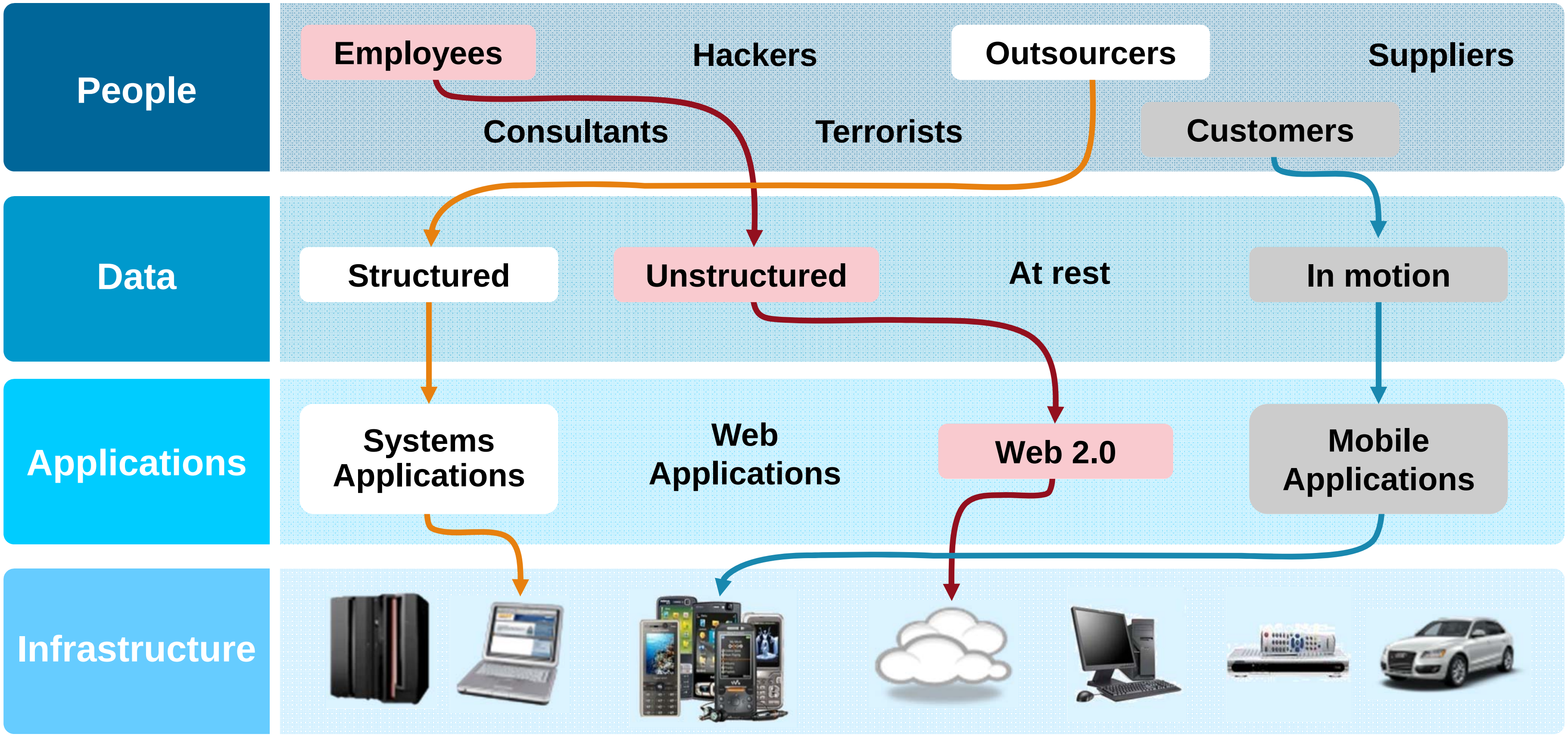
External threats are rated as a bigger challenge than internal threats, new technology or compliance.



More than one half say mobile security is their greatest near-term technology concern

Source: IBM Center for Applied Insights

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

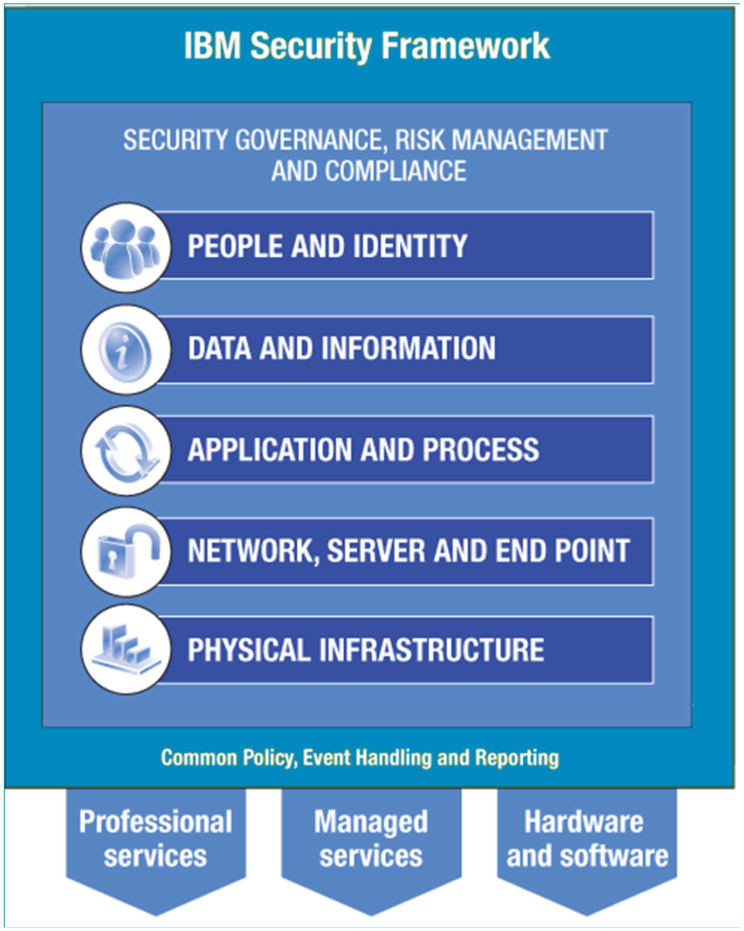
As a result, the Security market is shifting

	Traditional Focus	**Emerging Focus**
	Governance and Compliance	*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

IBM Security approach to answer the CSO Challenge:

Manage Cost, Decrease Complexity, Improve Effectiveness, Assure Agility



IBM Security Framework

SECURITY GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE

PEOPLE AND IDENTITY

DATA AND INFORMATION

APPLICATION AND PROCESS

NETWORK, SERVER AND END POINT

PHYSICAL INFRASTRUCTURE

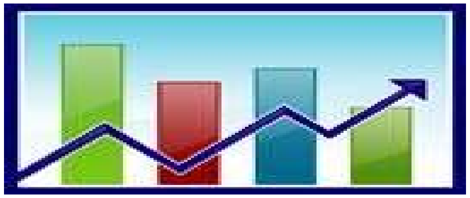
Common Policy, Event Handling and Reporting

Professional services

Managed services

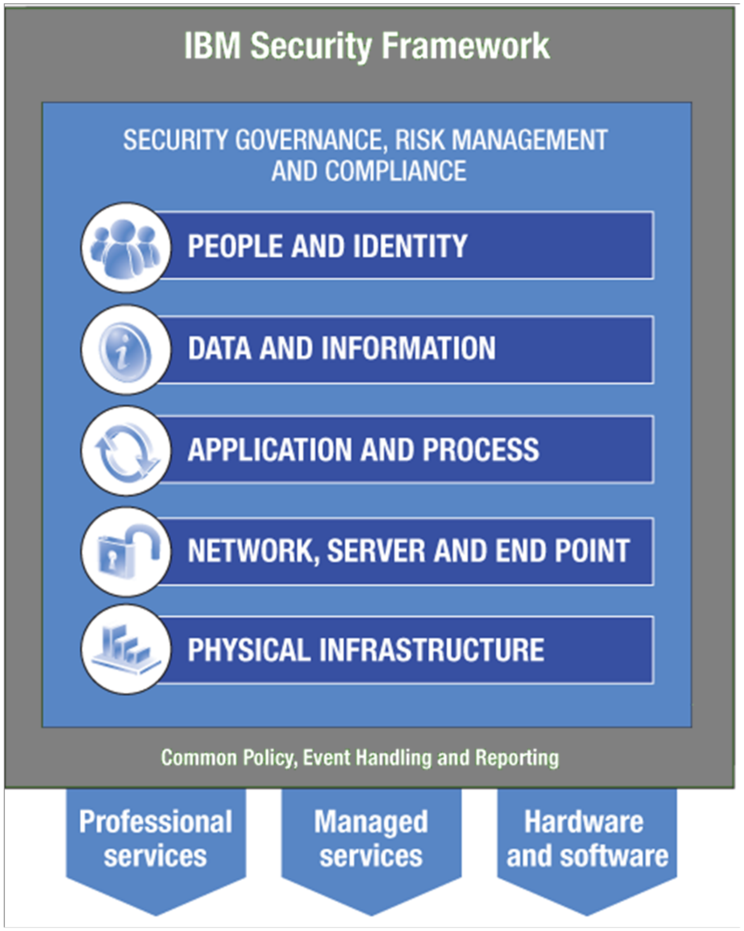
Hardware and software

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

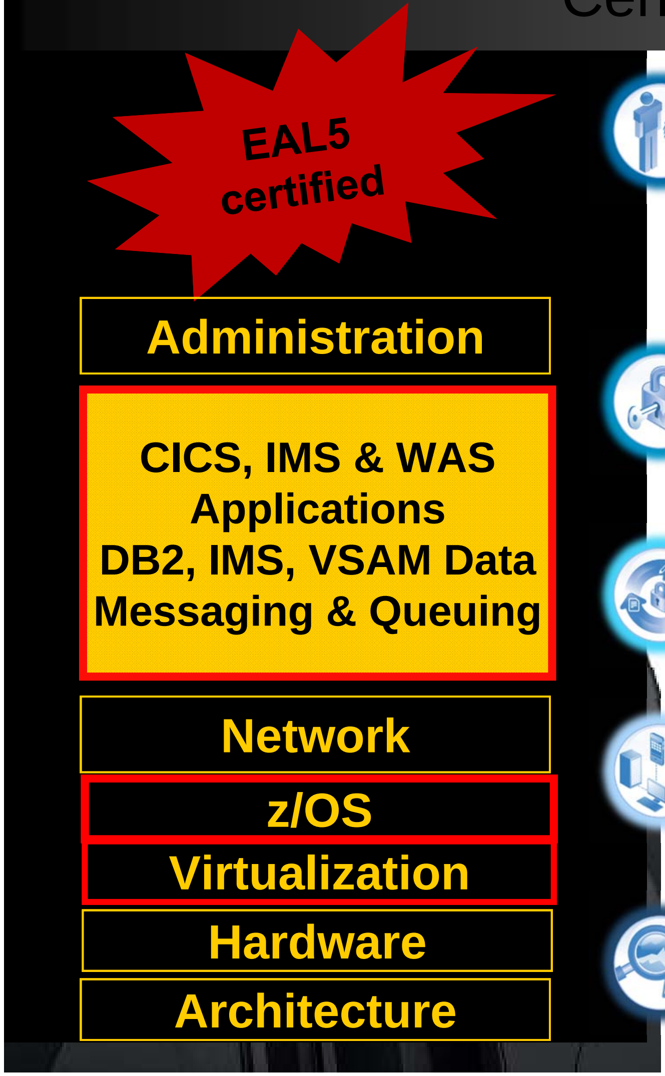
IBM Security Framework



- **IDENTITY & ACCESS**
  - Enable secure collaboration with internal and external users with controlled and secure access to information, applications and assets
- **DATA SECURITY**
  - Protect and secure your data and information assets
- **APPLICATION SECURITY**
  - Continuously manage, monitor and audit application security
- **INFRASTRUCTURE SECURITY**
  - Comprehensive threat and vulnerability management across networks, servers and end-points
- **SECURITY COMPLIANCE**
  - Demonstrable policy enforcement aligned to regulations, standards, laws, agreements (PCI, FISMA, etc..)

Security for your Workloads

Centralized Integrated Security



- 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, MQSeries® and z/OS® resources
- Protecting sensitive and confidential data with Data Encryption solutions for DB2 and IMS databases with InfoSphere™ Guardium® Data Encryption

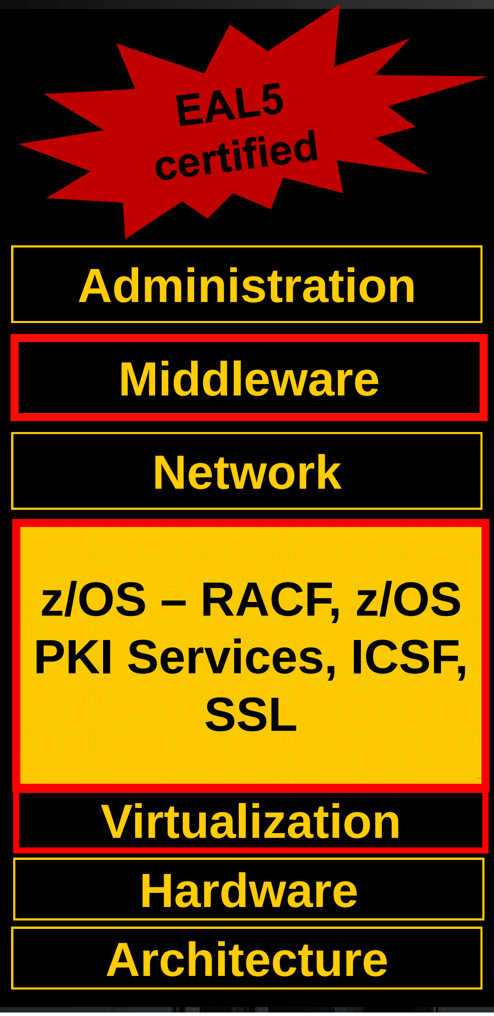
- Code signing for Program Objects in PDSEs
- Access to crypto features inside of applications

- Support of System Secure Sockets Layer (SSL), digital certificates, and key repositories
- Secured connection with Linux® virtual servers (Linux for IBM System z®) in the box

- Tools for audit and compliance – Everything is logged by DB2, CICS, IMS, MQ and z/OS

Security with Core System z Infrastructure

System z Security Architected and Integrated



- 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

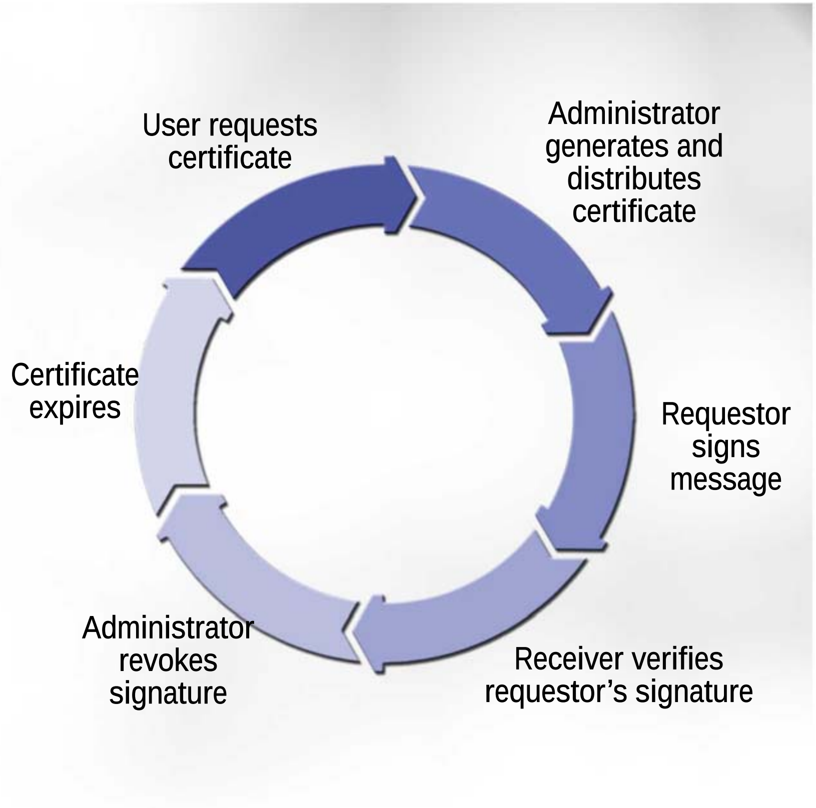
- Use Application Transparent Transport Layer Security to secure sensitive communications without incurring costly application changes
- Memory protection to protect your most critical transactional systems

- 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

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)



User requests certificate

Administrator generates and distributes certificate

Requestor signs message

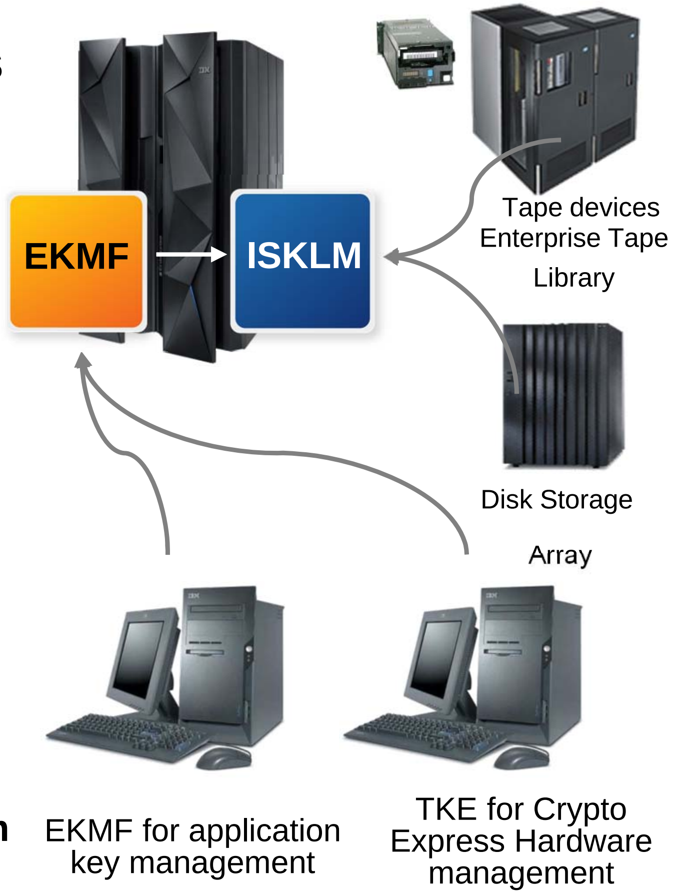
Receiver verifies requestor’s signature

Administrator revokes signature

Certificate expires

IBM Enterprise Key Management Foundation for Integrated Key Management

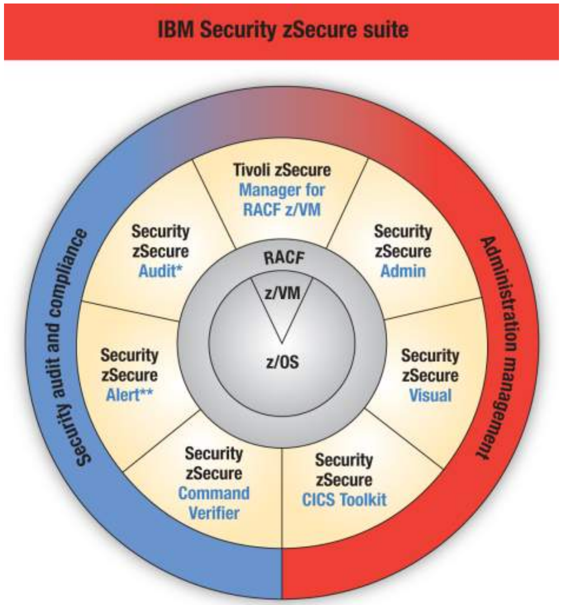
- **IBM Enterprise Key Management Foundation powered by DKMS Centralized key lifecycle management with single point of control, policy, reporting, and standardized processes for compliance**
  - EMV & PCI Standards
- **EKMF provides proven experience in the enterprise key management space**
  - Capabilities 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

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**


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

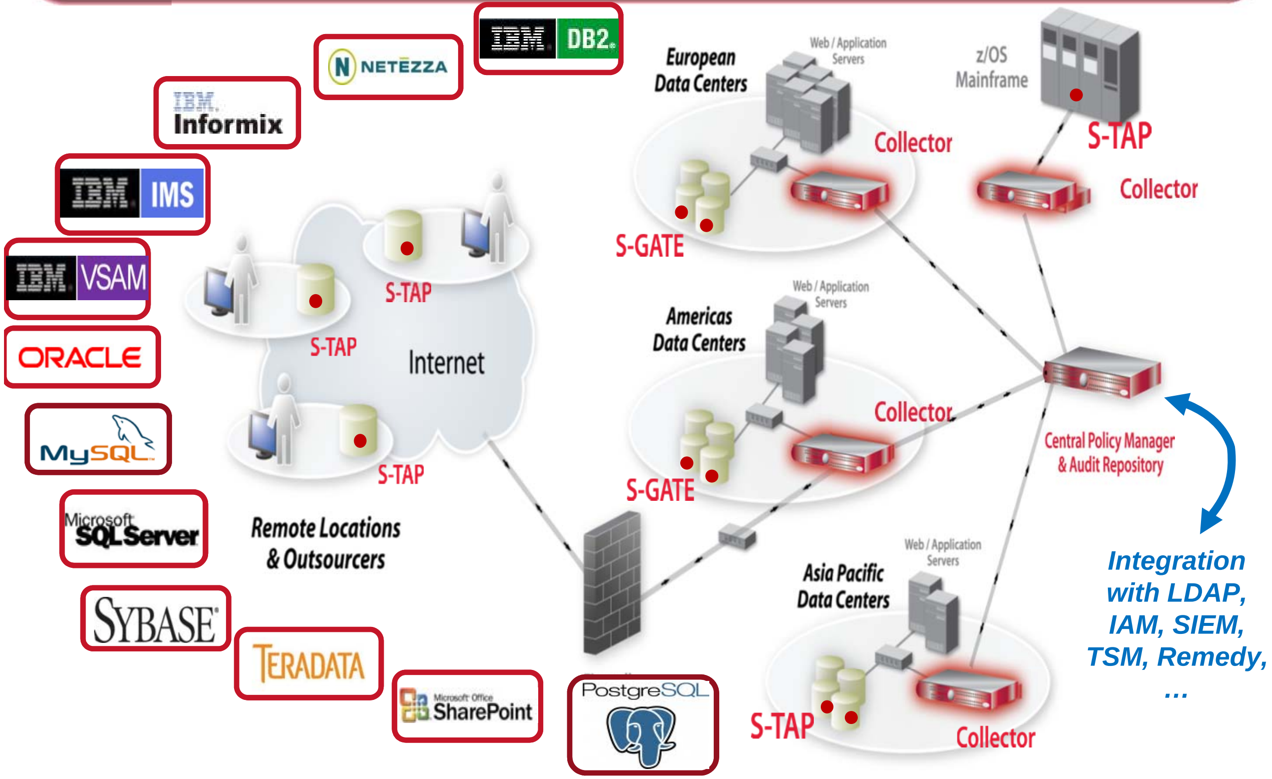
*Also available for ACF2™ and Top Secret®

**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

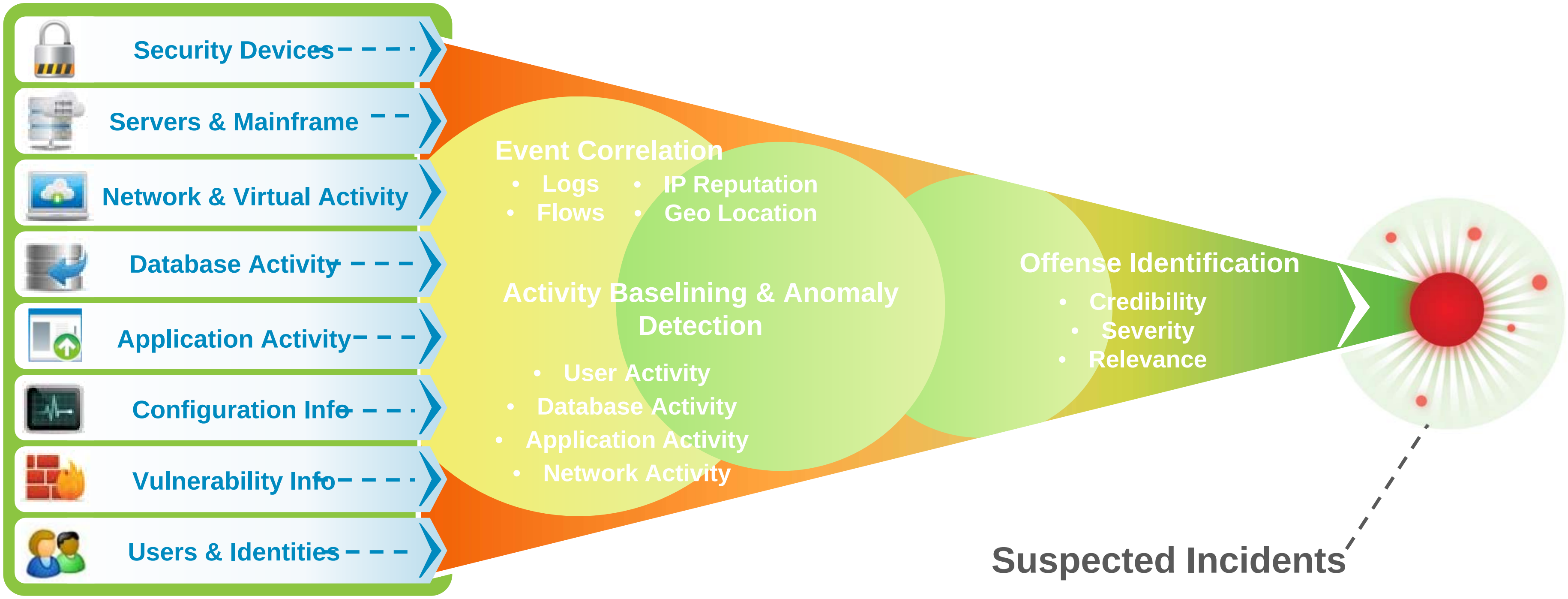


IBM DB2
NETEZZA
IBM Informix
IBM IMS
IBM VSAM
ORACLE
MySQL
Microsoft SQL Server
SYBASE
TERADATA
Microsoft Office SharePoint
PostgreSQL
European Data Centers
Web / Application Servers
z/OS Mainframe
Collector
S-TAP
Collector
S-GATE
S-TAP
S-TAP
Internet
S-TAP
Remote Locations & Outsourcers
Americas Data Centers
Web / Application Servers
Collector
S-GATE
Central Policy Manager & Audit Repository
Integration with LDAP, IAM, SIEM, TSM, Remedy, …
Asia Pacific Data Centers
Web / Application Servers
S-TAP
Collector

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

QRadar: Context and Correlation Drive Deep Insight and Accurate Detection

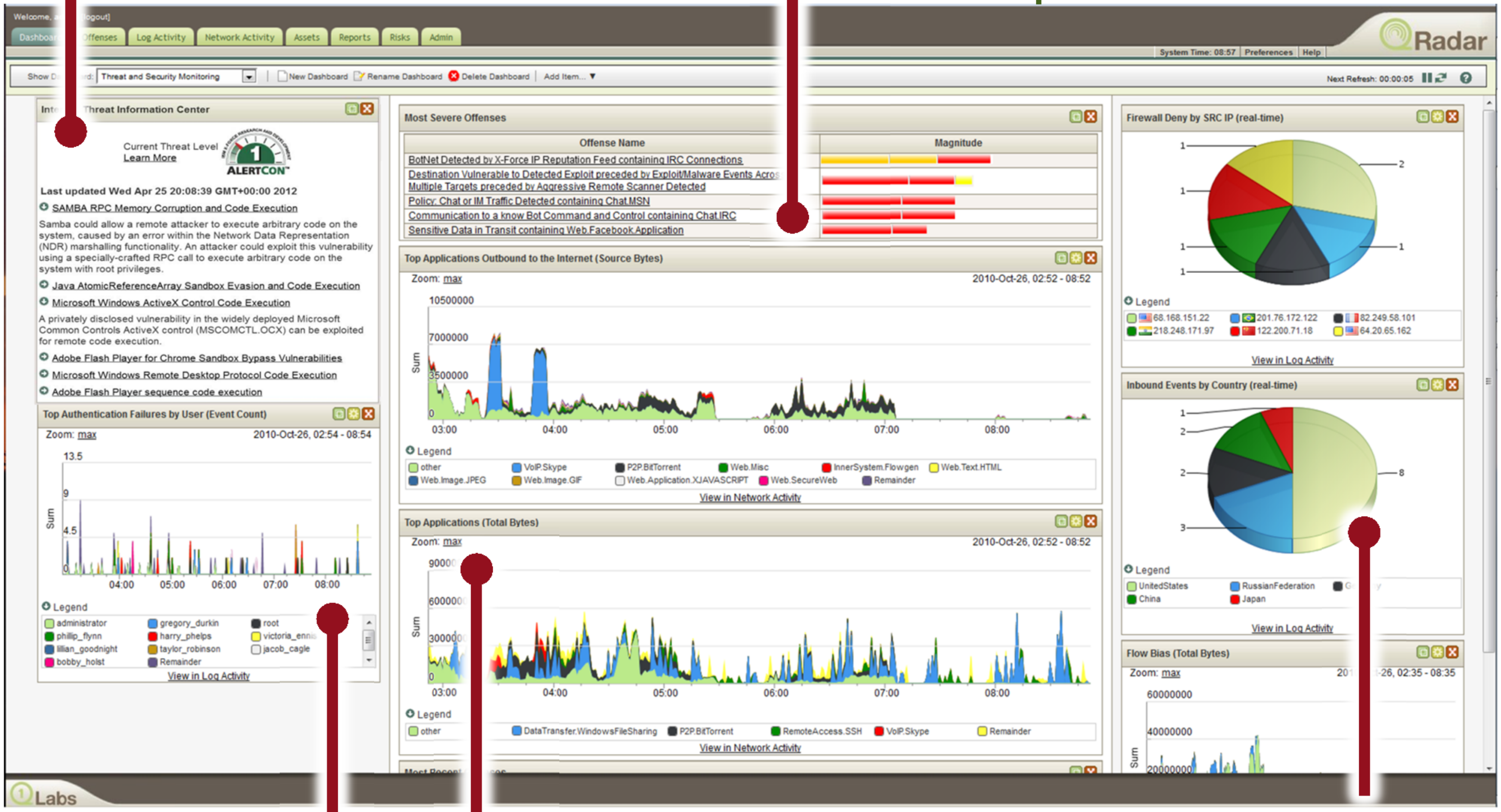


Extensive Data Sources + Deep Intelligence = Exceptionally Accurate and Actionable Insight

Security Intelligence: *QRadar provides security visibility*

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation


Welcome, a[logout]
Dashboar Offenses Log Activity Network Activity Assets Reports Risks Admin
System Time: 08:57 | Preferences | Help
QRadar
Show D rd: Threat and Security Monitoring
New Dashboard
Rename Dashboard
Delete Dashboard
Add Item... ▼
Next Refresh: 00:00:05
Labs

Inte 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	

Top Authentication Failures by User (Event Count)

Top Applications Outbound to the Internet (Source Bytes)

Top Applications (Total Bytes)

Firewall Deny by SRC IP (real-time)

Inbound Events by Country (real-time)

Flow Bias (Total Bytes)

Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

European Bank delivers secure mobile Internet banking with IBM Worklight

Background

Major European Bank needed to reduce operational complexity and cost with a single, scalable infrastructure to secure access to various back-end services from multiple mobile apps. A customized authentication mechanism empowered the bank to guarantee the security of its customers while safeguarding the trust relationship with a safe app platform that encrypts local data and delivers app updates immediately.

Customer Needs

- Extend secure access to banking apps to mobile customers
- Enhance productivity of employees to perform secure banking transactions via mobile devices
- Support for iOS, Android, and Windows Mobile

Benefits

- Authenticates requests made via HTTPS from hybrid mobile apps running on WorkLight platform to back-end services
- A custom certificates-based authentication mechanism implemented to secure back-end banking application

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	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