



IBM zEnterprise Technology Summit

**System z continues to be the
ultimate security platform**

Presenter – Title

Date



The C-suite are driving a mandate for innovation and growth



CEOs

Customer insights are the most critical investment

Engaging clients requires a step change from traditional to social media



CMOs

Customer analytics and social media are key technologies

BUT, they feel most unprepared to manage the data explosion and social media



CFOs

Pressure remains high to control costs and increase efficiency

The enterprise can succeed or fail based on how it responds to trends such as big data, social media, cloud computing, mobile and external data.

Security – Is good enough ... enough?

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

Security vulnerabilities need multifaceted defenses

Being reactive is not good enough, anticipate the worst

Security must contain and prevent damage from escalating

Track intrusion attempts, notify immediately, understand patterns of attack

Security must adhere to standards, even the new ones

Fundamental security designed into the infrastructure increases protection



Mainframe security

What's the risk?

- Disclosure of sensitive data
- Service interruption
- Corruption of operational data
- Fraud and ID Theft
- Theft of services



What's at stake?

- Customer trust
- Reputation and Brand
- Privacy
- Integrity of Information
- Legal and Regulatory Action
- Competitive Advantage



Breach cost?

- \$ Research and recovery
- \$ Notify customers
- \$ Lost customer business
- \$ Problem remediation
- \$ Claims from trusted vendors and business partners



\$\$ *Damage to brand image*

New Industry Trends Bring Security Challenges to Business

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

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

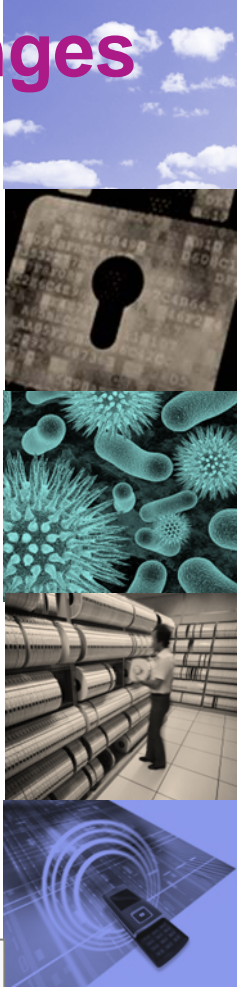
77% of execs believe that adopting cloud computing makes protecting privacy more difficult²

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

Are you security ready?



Redefining the challenge of securing your business

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

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

3 Source: IBM 2012 CISO study

Security Challenges Specific to the Mainframe

Ensuring Compliance



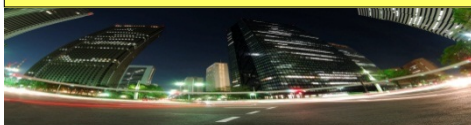
Increasing Complexity



Rising Costs



Visibility



▪ Compliance:

- Compliance verification is a manual task with alerts coming after a problem has occurred, if at all

▪ Complexity:

- The mainframe is an integral component of many large business services, making the identification and analysis of threats very complex and creating a higher risk to business services
- Systems are vulnerable to the unmanaged activities of privileged users.

▪ Cost:

- Mainframe security administration is usually a manual operation, or relies upon old, poorly documented scripts.
- Administration is done by highly skilled mainframe resources that are usually in short supply.

▪ Visibility:

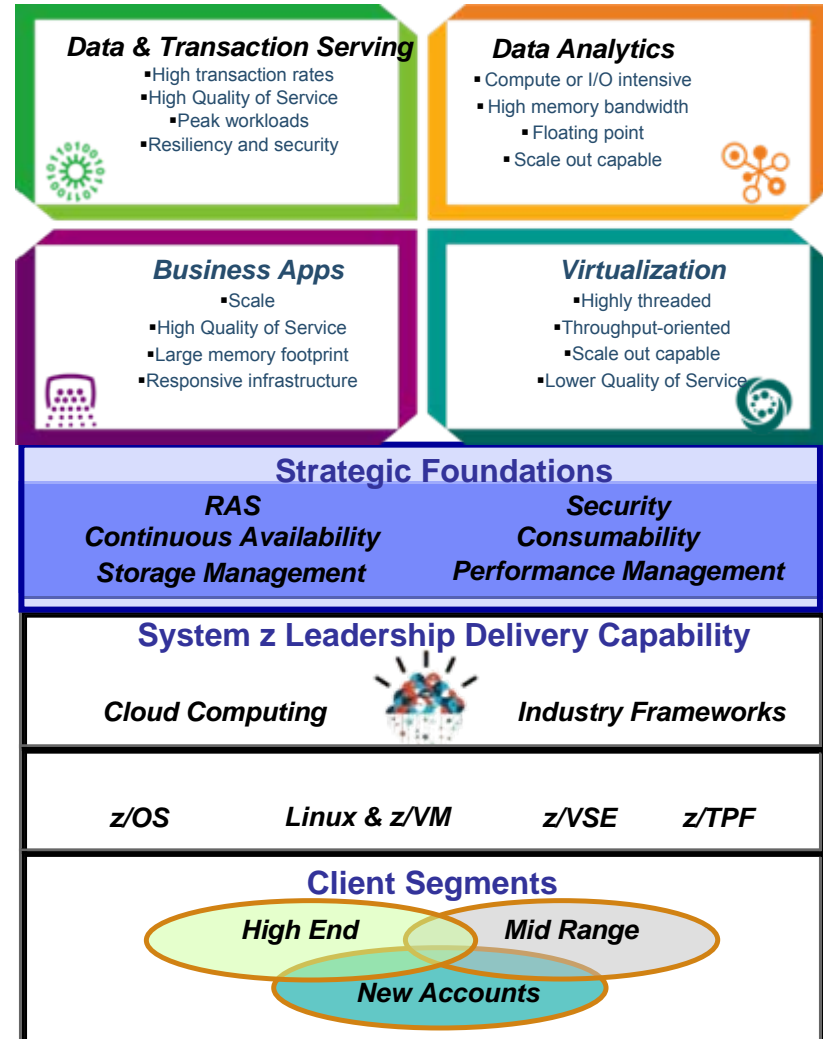
- Mainframe processes, procedures, & reports are often siloed from the rest of the organization

Security is one of the strategic foundations of System z

- **Integrated security that spans from:**
 - Hardware
 - Firmware
 - Hypervisors
 - System z Operating Systems
 - Middleware and applications
 - Network

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

Optimizing System z for Strategic Workloads & Industry-based Initiatives



zEnterprise - Ultimate security to protect your mission critical assets

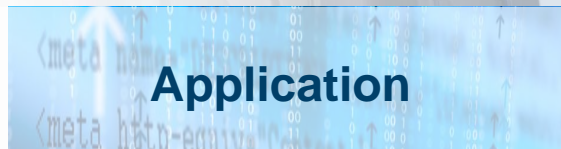
Deeply Integrated Security Throughout the Stack



- ✓ Consistent policy based user authentication, access control, audit and management



- ✓ Encrypt critical data, at rest and in flight, with centralized key management



- ✓ Detect application vulnerabilities early to contain potential problems



- ✓ Create a secured virtualized pool of resources as a foundation for private cloud



- ✓ Reduce operational risk. Improved compliance to evolving regulations and audit responsiveness

from IBM Security Framework

Defend Against Network Attacks and Intrusions

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

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

IBM zEnterprise Solutions

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

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



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

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

Protect People, Identities throughout your Extended Enterprise

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

Up to 52% lower security administrative costs efforts on mainframe

IBM zEnterprise[®] Solutions

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

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



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

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

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 Flash Express application paging data with Smart Cards
- 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 design provides a major deterrent for security attacks.

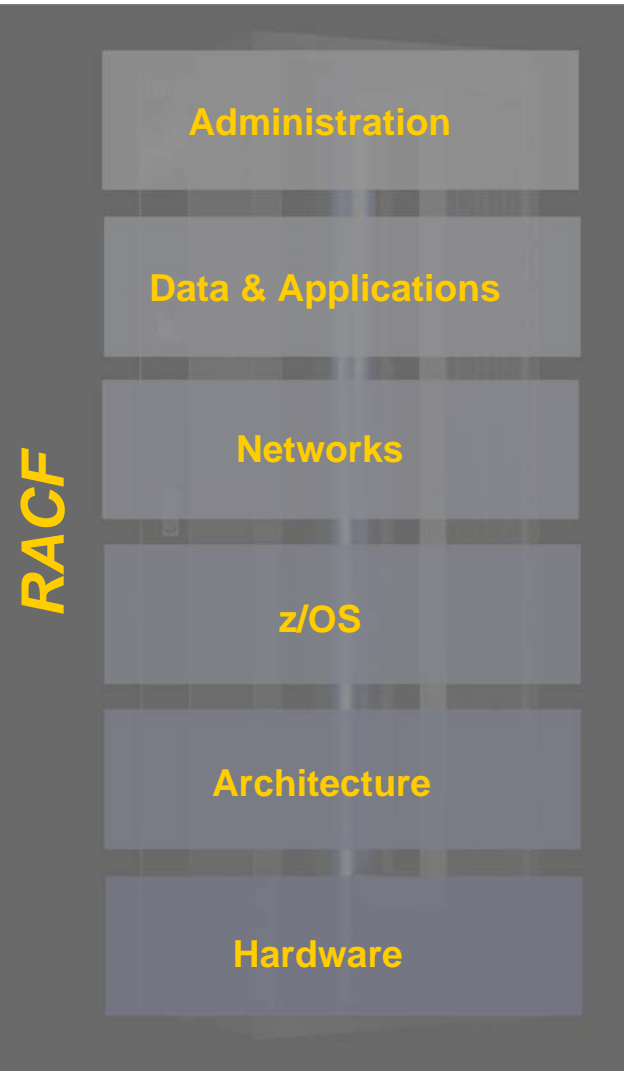
***IBM X-Force® 2011 Trend and Risk Report**



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

Resource Access Control Facility (RACF)

The backbone of mainframe security



Enables application and database security without modifying applications

Can reduce security complexity and expense:

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

Integration with distributed system security domain

Checking for “Best Practices” with z/OS HealthChecker

Serving mainframe enterprises for over 30 years

Typical problems

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



And there's more . . .

- **Segregation of duties are not enforced**
 - Conflicting access permissions in business or IT departments

- **Privileged users are not adequately monitored or “controlled”**
 - Inappropriate actions go undetected

- **Policies and procedures are not adhered to**
 - RACF commands issued that weaken controls

- **Processes and procedures are not structured or repeatable**
 - How and what did we use before?

- **System or application outages caused by Security Administrators**
 - A RACF command that should have been prevented

- **Concerns around skills and knowledge of System z Security**
 - Existing toolset does not improve capability

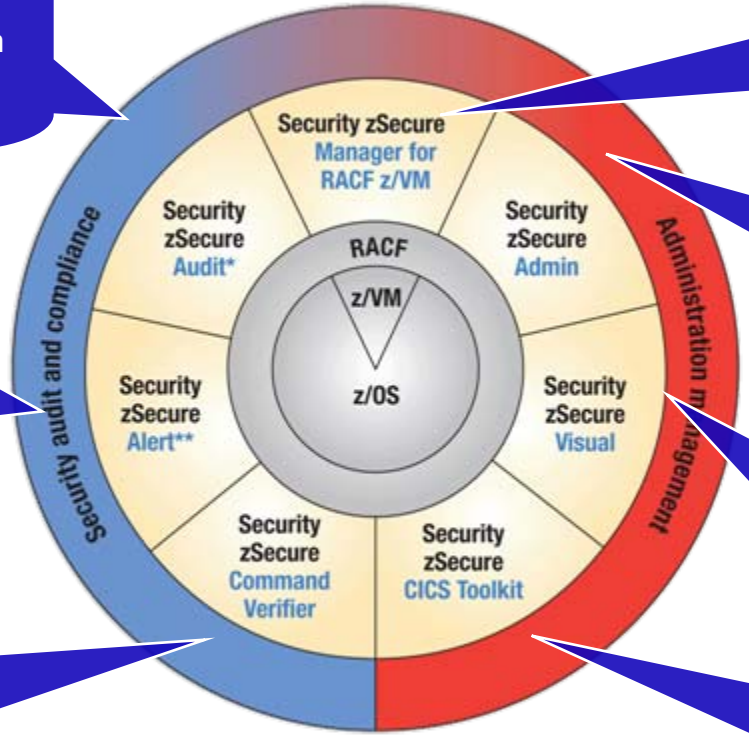


IBM Security zSecure suite products

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

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

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



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

zSecure provides significant value points

zSecure	Significant Product Capabilities	Client Business Value
Enhanced Administration	<ul style="list-style-type: none"> • Automated cleanup of orphan accounts • Offline change management & change modeling • RACF DB merges • Cascading permissions for Group Tree Structures 	<ul style="list-style-type: none"> • Helps improve security at lower labor cost • Aids in reducing costs by avoiding configuration mistakes • Eases labor cost for directory merges • Helps reduce labor cost by more efficient group management
Auditing & Compliance	<ul style="list-style-type: none"> • Customizable reports • Automated risk classification • Broad coverage of audit control points • <u>Security Intelligence to identify and manage Trusted Users</u> • Exceptional coverage of security event records, including TCP/IP, CICS, DB2, & IMS 	<ul style="list-style-type: none"> • Can provide report that match business model / business requirements • Helps optimize labor utilization by prioritizing tasks • Aids in reducing cost by helping eliminate outages not detected by non-IBM solutions • Address business risk by helping to find segregation of duties exposure

zSecure provides significant value points

zSecure	Significant Product Capabilities	Client Business Value
Alerting	<ul style="list-style-type: none"> • Can capture unauthorized back door changes to RACF, Security Policies • Extensive coverage of real time audit control points, especially network 	<ul style="list-style-type: none"> • Can reduce cost by helping eliminate outages not detected by competition
Command Verification	<ul style="list-style-type: none"> • Auditing of RACF changes by Privileged Users 	<ul style="list-style-type: none"> • Can complete audit in seconds, not days, reducing labor cost
Visual Administration	<ul style="list-style-type: none"> • Real time, on line updates • Integrates w/ HR Systems (PeopleSoft, SAP, etc.) • Roles based administration for separation of duties • Manage from a single screen 	<ul style="list-style-type: none"> • Permits changes in minutes, not overnight • Enables better business control by providing access for only current employees & contractors • Helps minimize business risk by enabling segregation of duties • Aids in reducing labor cost and errors

Solving Customer Security Challenges in Mainframe Environments

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



Automate continuous compliance to address worldwide industry standards and regulations

Assure auditors that preventative, detective and corrective controls are installed



Improve administrator effectiveness with built-in best practices

Reduced identity and access security management overhead and costs with integrated security management



Protect and ensure the integrity of sensitive enterprise data

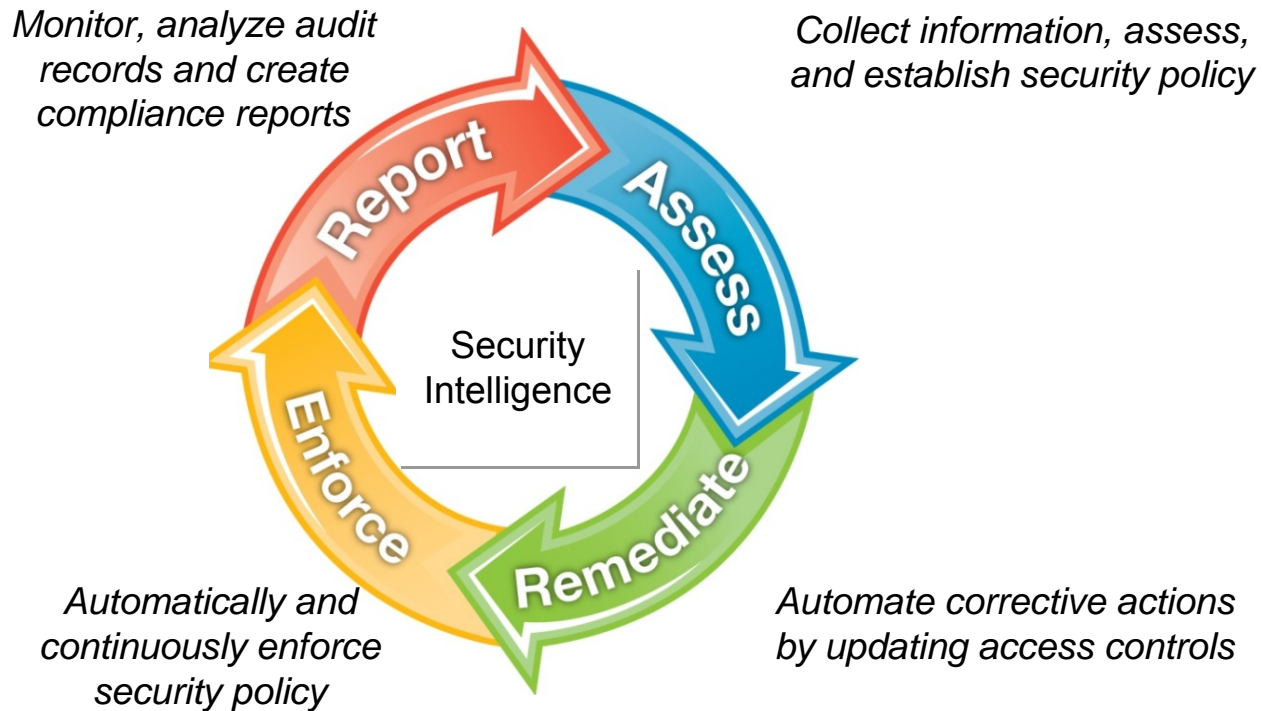
Leveraged IBM technologies to track and redact medical information from imaged documents.



Simplify mainframe administration and auditing for consolidated systems and workloads

Establish user identification services for compliance and governance

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

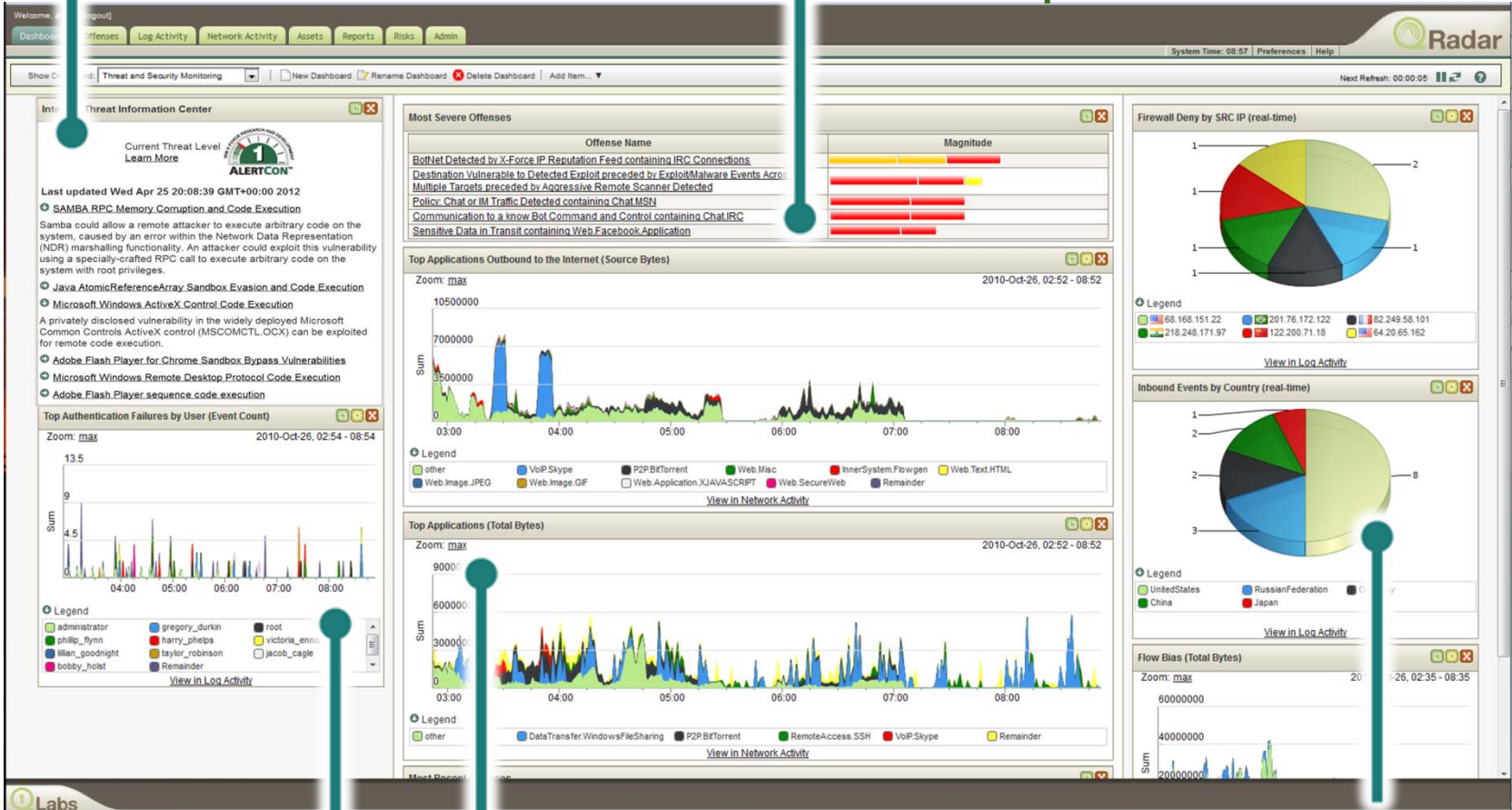


IBM Security zSecure Compliance and Auditing With QRadar

Security Intelligence: QRadar provides security visibility

IBM X-Force® Threat Information Center

Real-time Security Overview w/ IP Reputation Correlation



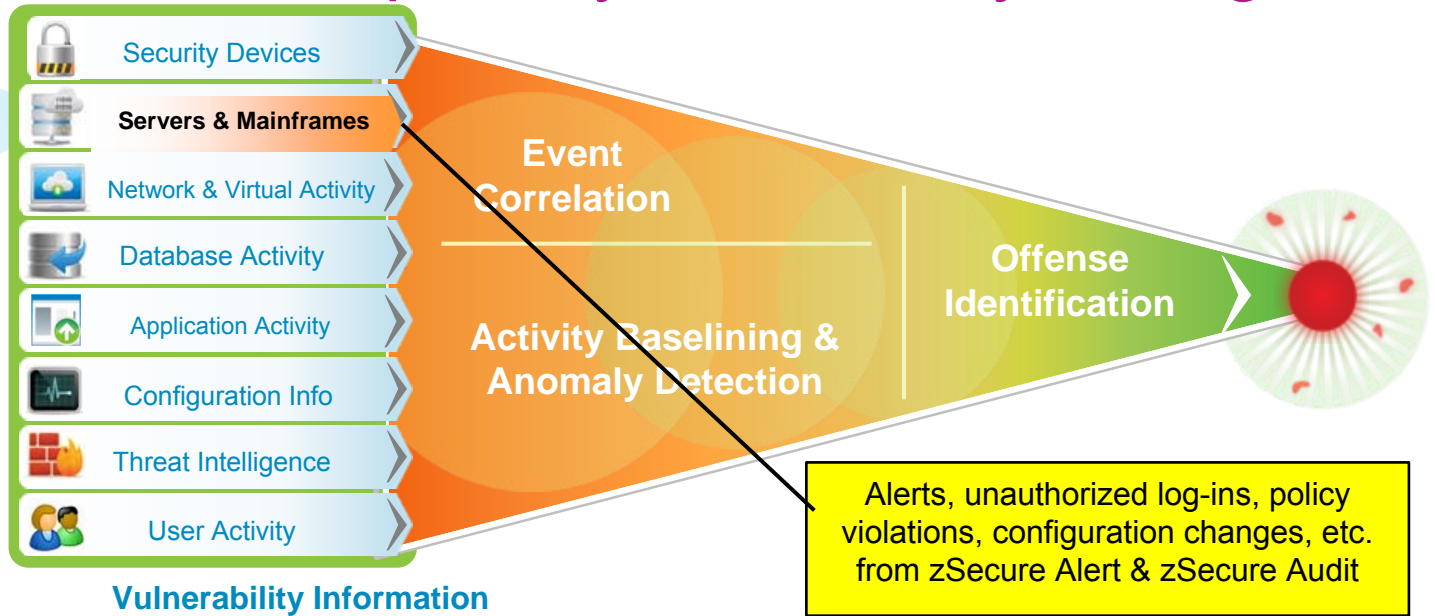
Identity and User Context

Real-time Network Visualization and Application Statistics

Inbound Security Events

zSecure & QRadar improve your Security Intelligence

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



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

zOS and RACF – System Changes by Resource Sensitivity

Dashboard Offenses Log Activity Network Activity Assets Reports Admin System Time: 20:40

Search... Quick Searches Add Filter Save Criteria Save Results Cancel False Positive Rules Actions Quick Filter...

Viewing events from 2012-10-19 20:00:00 to 2012-10-19 20:15:00 View: Select An Option: Display: Custom

Grouping By:

Resource sensitivity (custom)



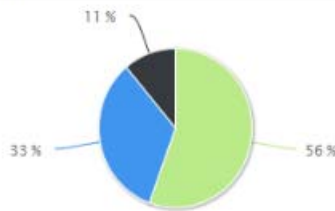
Current Filters:

Event Name is any of [RACHECK Successful access or RACHECK Su... (Clear Filter), Resource sensitivity is not N/A (Clear Filter), Resource sensitivity is not any of [Catalog or SMF dataset] (Clear Filter), Log Source is any of [R IBM RACF or R IBM zOS] (Clear Filter), Access intent is any of [UPDATE or CONTROL or ALTER] (Clear Filter), SAF Class is DATASET (Clear Filter)

Current Statistics

Total Results: 9
 Data Files Searched: 2 (21.1 MB Total)
 Compressed Data Files Searched: 2 (1.2 MB Total)
 Index File Count: 16 (932.7 KB Total)
 Duration: 17ms

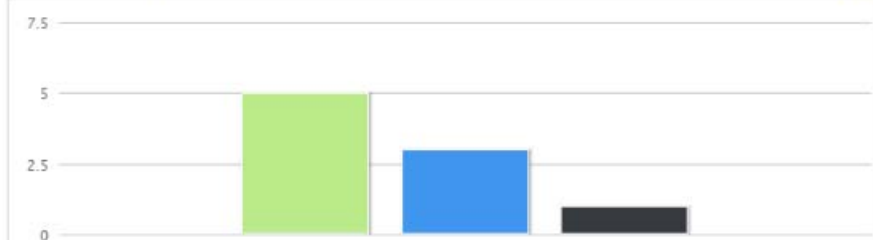
Top 10 Resource sensitivity (custom) Results By Count



Legend

STC proclib MSTR STClb MSTR prmlb

Top 10 Resource sensitivity (custom) Results By Count



Legend

STC proclib MSTR STClb MSTR prmlb

(Hide Charts)

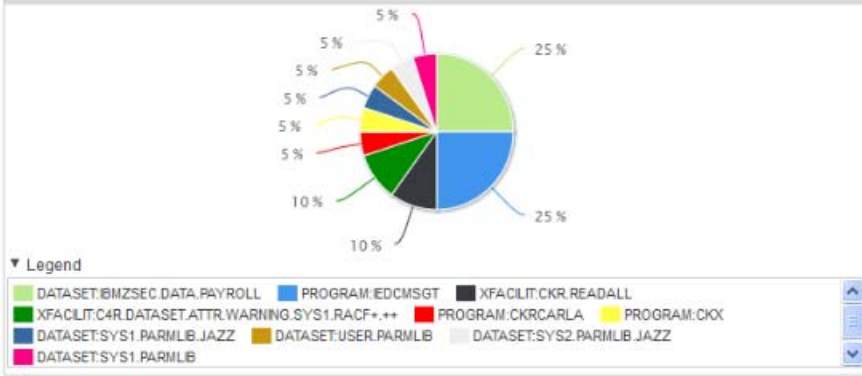
Resource sensitivity (custom)	Username (Unique Count)	Person name (custom) (Unique Count)	Data set name (custom) (Unique Count)	Access intent (custom) (Unique Count)	Access allowed (custom) (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Job name (custom) (Unique Count)	Count
STC proclib	PEASEJ	JAMIE PEASE GB TIV	USER.PROCLIB	UPDATE	ALTER	2012-08-21 14:37:45	R IBM RACF	PEASEJ	5
MSTR STClb	PEASEJ	JAMIE PEASE GB TIV	SYS1.PROCLIB.ZT00...	UPDATE	ALTER	2012-08-21 14:41:48	R IBM RACF	PEASEJ	3
MSTR prmlb	PEASEJ	JAMIE PEASE GB TIV	USER.PARMLIB	UPDATE	ALTER	2012-08-21 15:52:22	R IBM RACF	PEASEJ	1

RACF – Access Violations by Resource

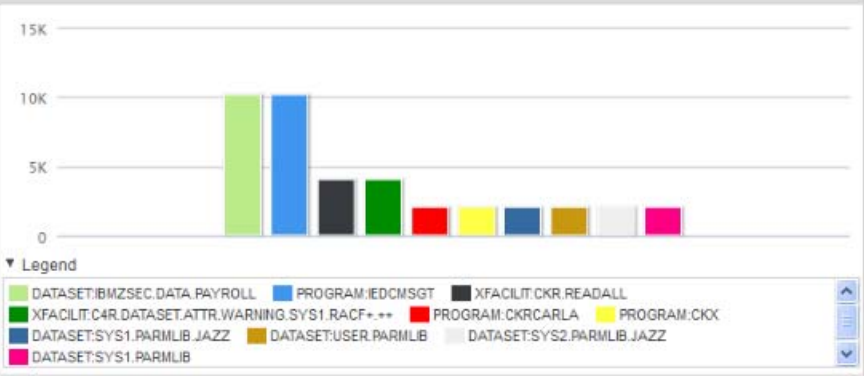
Search... ▾ Quick Searches ▾ Add Filter Save Criteria Save Results Cancel False Positive Rules ▾ Actions ▾ Quick Filter...

Total Results: 40 988 Compressed Data Files Searched: 2 152 (1.2 GB Total) Duration: /m 15s 354ms
 Data Files Searched: 2 152 (21.5 GB Total) Index File Count: 32 505 (1.3 GB Total)

Top 10 SAF Class (custom):SAF resource name (custom) Results By Count



Top 10 SAF Class (custom):SAF resource name (custom) Results By Count



(Hide Charts)

SAF Class (custom)	SAF resource name (custom)	Username (Unique Count)	Person name (custom) (Unique Count)	Event Name (Unique Count)	Log Source Time (Minimum)	Log Source (Unique Count)	Event Count (Sum)	Access intent (custom) (Unique Count)	Access allowed (custom) (Unique Count)	Resource sensitivity (custom) (Unique Count)	Count
DATASET	IBMZSEC.DATAP...	U866ABC	DEX DEXTER	RACHECK Insuffi...	2012-08-22 15:4...	R IBM RACF 3	10,200	READ	NONE	N/A	10,200
PROGRAM	IEDCMSGT	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	10,200	READ	NONE	APF lib+Lnk	10,200
XFACILIT	CKR.READALL	C2ECQRLF	N/A	RACHECK Insuffi...	2012-08-21 14:5...	Multiple (2)	4,084	READ	NONE	N/A	4,084
XFACILIT	C4R.DATASET.AT...	U866KYU	FALLON CARRINGTON	RACHECK Insuffi...	2012-08-22 16:3...	R IBM RACF 3	4,080	UPDATE	NONE	N/A	4,080
PROGRAM	CKRCARLA	C2ECQRLF	N/A	RACHECK Insuffi...	2012-08-21 14:5...	Multiple (2)	2,042	READ	NONE	APF lib+Lnk	2,042
PROGRAM	CKX	C2ECQRLF	N/A	RACHECK Insuffi...	2012-08-21 14:5...	Multiple (2)	2,042	READ	NONE	APF lib+Lnk	2,042
DATASET	SYS1.PARMLIB.J...	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	USER.PARMLIB	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	SYS2.PARMLIB.J...	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	SYS1.PARMLIB	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
DATASET	SYS1.PARMLIB.Z...	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	2,040	READ	NONE	MSTR prmlib	2,040
PROGRAM	IEWBODEF	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020
PROGRAM	CEEMENU3	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020
XFACILIT	C4R.RACF.AUDIT...	U866KYU	FALLON CARRINGTON	RACHECK Insuffi...	2012-08-22 16:1...	R IBM RACF 3	1,020	UPDATE	NONE	N/A	1,020
DATASET	U866KYU.C2R2F...	U866ABC	DEX DEXTER	RACHECK Insuffi...	2012-08-22 16:4...	R IBM RACF 3	1,020	READ	NONE	N/A	1,020
PROGRAM	FTPDNS	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020
PROGRAM	CEEBINSS	QRADFTP	QRADAR FTP USERID	RACHECK Insuffi...	2012-08-21 18:1...	R IBM RACF 3	1,020	READ	NONE	APF lib+Lnk	1,020

Integrated SMF log data and supporting details

Viewing events from 2012-07-05 18:51:00 to 2012-07-05 19:06:00 View: Display:

Current Filters:
Log Source is z/OS [\(Clear Filter\)](#)

Current Statistics











View Data

Event Name	Log Source	Event Count	Time	Line Level Category	Source IP	Source Port	Destination IP	Dest Port	Username	Magnitude
Non-VSAM data set input	z/OS	4	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
PGD member address replace	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set output	z/OS	4	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
VSAM data set open	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set input	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Job start	z/OS	1	18:58	Service Started	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set input	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
VSAM data set close	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Delete from catalog	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Scratch data set	z/OS	1	18:58	File Deleted	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set input	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
UDPF Socket Close	z/OS	1	18:58	Session Terminated	172.16.30.157	0	172.16.30.157	28644	OMVS	Minor
PGD member address replace	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
PGD member address replace	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set output	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set output	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Define in catalog	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
UDPF Socket Close	z/OS	1	18:58	Session Terminated	172.16.30.157	0	172.16.30.157	28643	OMVS	Minor
PGD member address replace	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Non-VSAM data set output	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
UDPF Socket Close	z/OS	1	18:58	Session Terminated	172.16.30.157	0	172.16.30.157	28642	OMVS	Minor
Job end	z/OS	1	18:58	Service Stopped	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
Job step result	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor
VSAM data set close	z/OS	1	18:58	Information	172.16.30.157	0	172.16.30.157	0	CRMBPA2	Minor

Showing 1 to 24 items (Elapsed time: 0:00:00.076)
Copyright © 2012 Q1 Lexis Inc. All rights reserved.

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

Complementary capabilities by use case scenarios

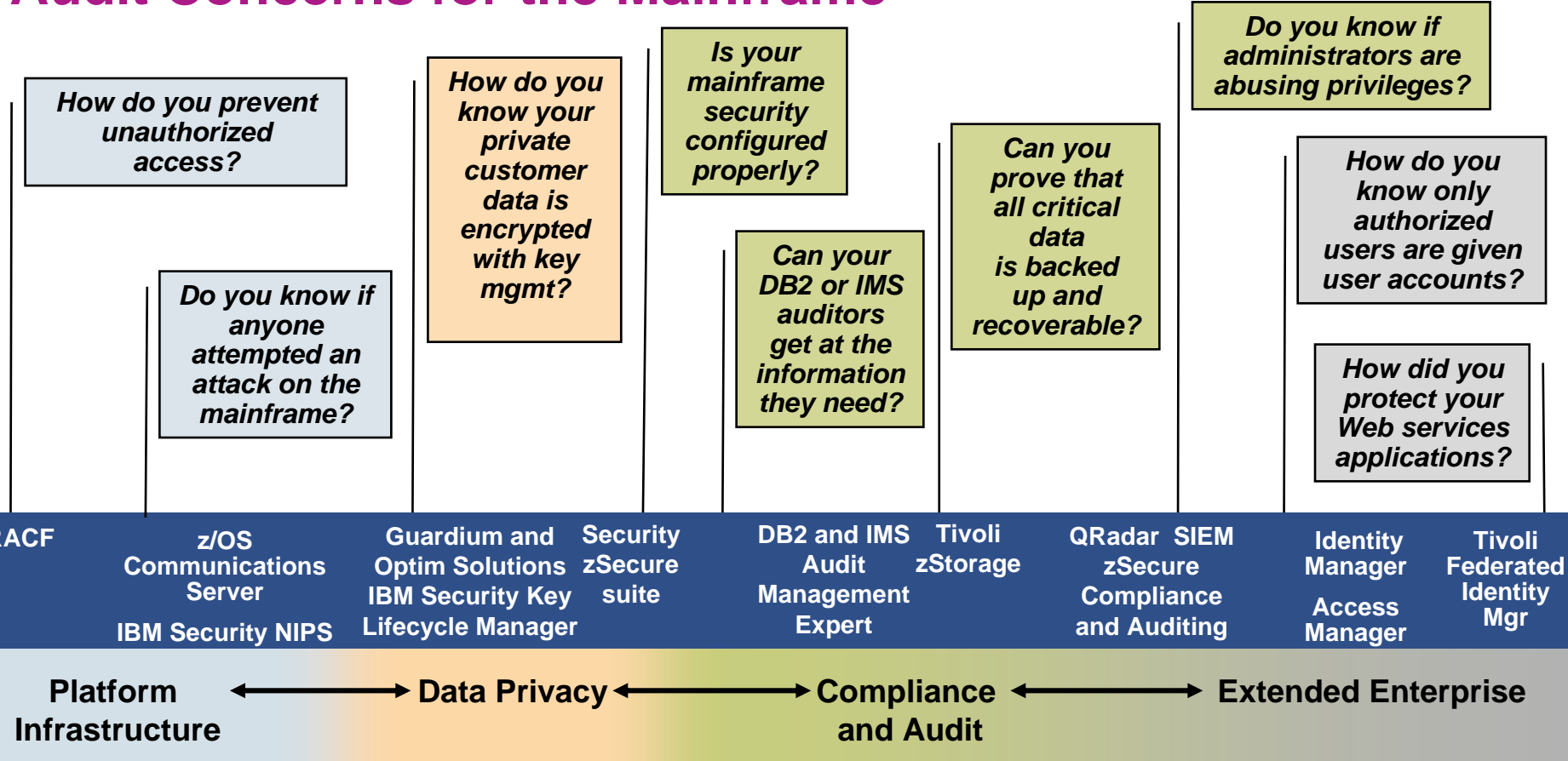
QRadar target use case	zSecure Suite complementary capabilities
 Complex threat detection	 zSecure Alert detects unauthorized logons and attempts, user behavior in violation of security policy, and instances where your core systems may be at risk
 Malicious activity identification	 Identify dangerous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



Value of zSecure and QRadar Security Intelligence integration

- **Strengthen mainframe security operations and help improve protection for critical mainframe environment**
- **Improve compliance visibility real-time with standards and regulations by simplifying audit and management efforts**
- **Consolidate enterprise security view allowing the identification and remediation of excess mainframe access, threats and concerns.**
- **Store event data in forensically secure database to address regulation mandates.**
- **Trigger complex correlation of threats, insider fraud and business risk as easy to understand “offenses” for further investigation and follow-ups**

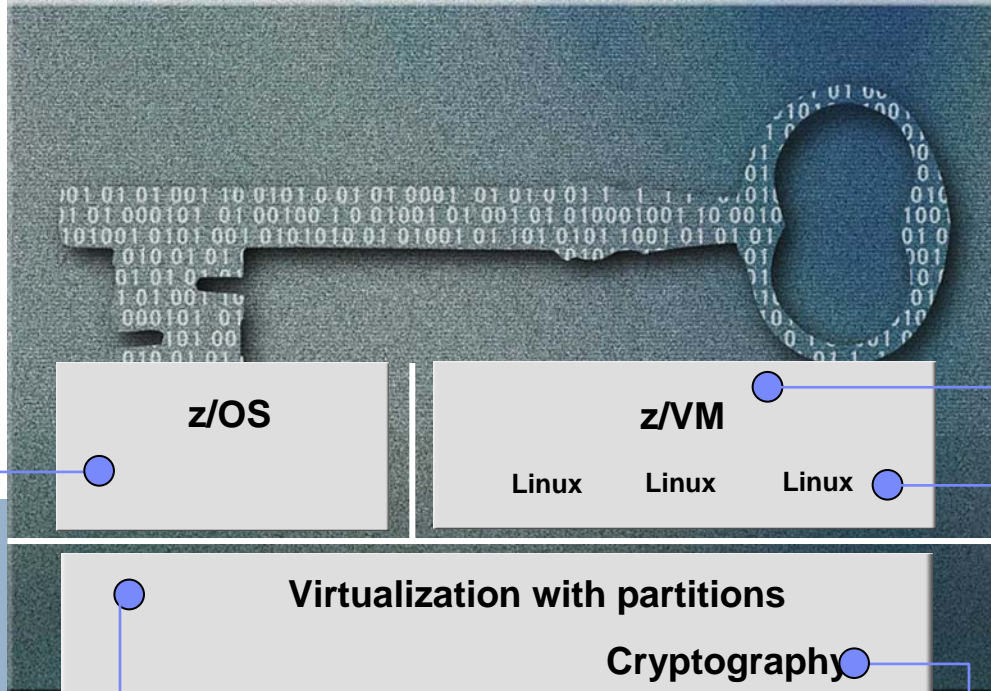
IBM Solutions Help to Address Potential Security and Audit Concerns for the Mainframe



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

System z Evaluations & Certifications

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



z/OS

- Common Criteria EAL4+
 - with CAPP and LSPP
 - z/OS 1.7 → 1.10 + RACF
 - z/OS 1.11 + RACF (OSPP)
 - z/OS 1.12 + RACF (OSPP)
- Common Criteria EAL5
 - z/OS RACF 1.12 (OSPP)
- z/OS 1.10 IPv6 Certification by JITC
- IdenTrust™ certification for z/OS PKI Services
 - FIPS 140-2
 - System SSL z/OS 1.10 → 1.12
 - z/OS ICSF PKCS#11 Services – z/OS 1.11
- Statement of Integrity

z/VM

- Common Criteria
 - z/VM 5.3
- EAL 5+ for CAPP and LSPP
- System Integrity Statement

Linux on System z

- Common Criteria
- SUSE SLES10 certified at EAL4+ with CAPP
- Red Hat EL5 EAL4+ with CAPP and LSPP
- OpenSSL - FIPS 140-2 Level 1 Validated
- CP Assist - SHA-1 validated for FIPS 180-1 - DES & TDES validated for FIPS 46-3

Virtualization with partitions

Cryptography

- System z9 EC and z9 BC System z10 EC and z10 BC
 - Common Criteria EAL5 with specific target of evaluation -- LPAR: Logical partitions
 - zEnterprise 196 & zEnterprise 114
 - Common Criteria EAL5+ with specific target of Evaluation – LPAR: Logical partitions
- Crypto Express2 & Crypto Express3 Coprocessors
 - FIPS 140-2 level 4 Hardware Evaluation
 - Approved by German ZKA
- CP Assist
 - FIPS 197 (AES)
 - FIPS 46-3 (TDES)
 - FIPS 180-3 (Secure Hash)

Mainframe is the Ultimate Security Platform

Resource Access Control Facility

Security Key Lifecycle Manager for z/OS

InfoSphere Guardium Family

InfoSphere Guardium Data Encryption for DB2 and IMS Databases

QRadar Security Information and Event Management

IBM Security Network Intrusion Prevention System

Communications Server & Netview for z/OS/

Security zSecure Suite

Security Identity Manager

Security Access Manager

Security Federated Identity Manager

Security Directory Integrator

Security Directory Server

WebSphere Application Server

WebSphere DataPower Server

AppScan



Solution Edition for Security

Security Identity & Access Assurance

Protect Your Business Assets with Ultimate Security with zEnterprise

- ✓ Designed for the highest level of security for commercial platforms
- ✓ Consistent policy based security management
- ✓ Protects critical data with encryption and key management
- ✓ Delivers a secure foundation for enterprise cloud
- ✓ Helps meet compliance and audit requests
- ✓ Monitors potential threats with vigilance



IBM zEnterprise® is the foundation for a secure enterprise

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



IBM Security

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



Intelligence

Integration

Expertise



ibm.com/security

© **Copyright IBM Corporation 2012. 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.