

Enhanced Security Intelligence for Mainframe Applications with IBM Security zSecure suite V1.13

Glinda Cummings
WW Product Manager

Jamie Pease
zSecure Knowledge Expert



Legal

- © IBM Corporation 2011. All Rights Reserved.
- The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication 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 this presentation 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 this presentation 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. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.
- If the text contains performance statistics or references to benchmarks, insert the following language; otherwise delete:
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including 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 results similar to those stated here.
- If the text includes any customer examples, please confirm we have prior written approval from such customer and insert the following language; otherwise delete:
All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.
- Please review text for proper trademark attribution of IBM products. At first use, each product name must be the full name and include appropriate trademark symbols (e.g., IBM Lotus® Sametime® Unyte™). Subsequent references can drop "IBM" but should include the proper branding (e.g., Lotus Sametime Gateway, or WebSphere Application Server). Please refer to <http://www.ibm.com/legal/copytrade.shtml> for guidance on which trademarks require the ® or ™ symbol. Do not use abbreviations for IBM product names in your presentation. All product names must be used as adjectives rather than nouns. Please list all of the trademarks that you use in your presentation as follows; delete any not included in your presentation. IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.
- If you reference Adobe® in the text, please mark the first use and include the following; otherwise delete:
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.
- If you reference Java™ in the text, please mark the first use and include the following; otherwise delete:
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- If you reference Microsoft® and/or Windows® in the text, please mark the first use and include the following, as applicable; otherwise delete:
Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
- If you reference Intel® and/or any of the following Intel products in the text, please mark the first use and include those that you use as follows; otherwise delete:
Intel, Intel Centrino, 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.
- If you reference UNIX® in the text, please mark the first use and include the following; otherwise delete:
UNIX is a registered trademark of The Open Group in the United States and other countries.
- If you reference Linux® in your presentation, please mark the first use and include the following; otherwise delete:
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.
- If the text/graphics include screenshots, no actual IBM employee names may be used (even your own), if your screenshots include fictitious company names (e.g., Renovations, Zeta Bank, Acme) please update and insert the following; otherwise delete: All references to [insert fictitious company name] refer to a fictitious company and are used for illustration purposes only.

Please Note:



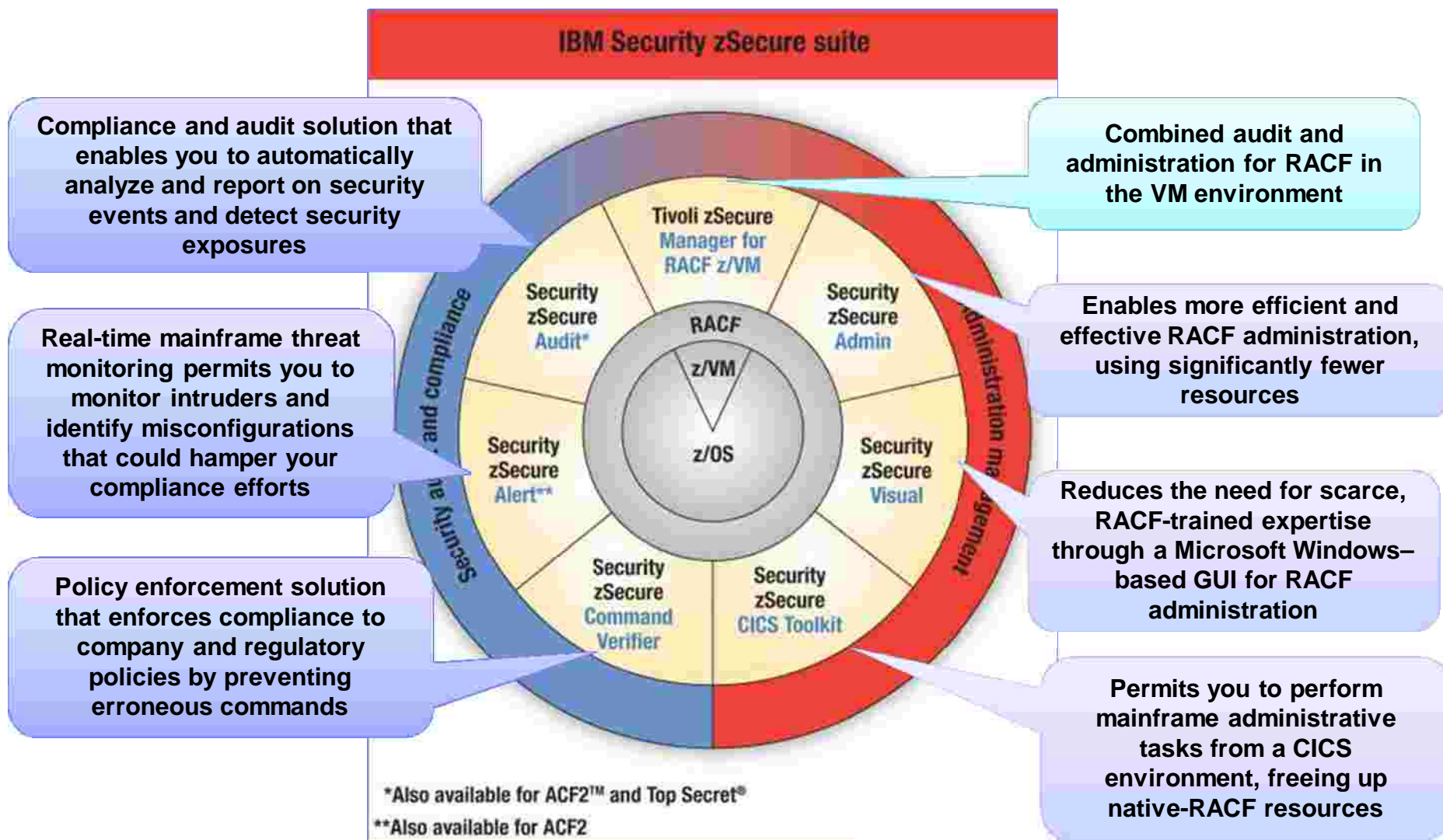
IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.

Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.

The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including 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 results similar to those stated here.

IBM Security zSecure Suite Overview



Note: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

A Short Review of zSecure Suite 1.12.0 – GA November 2010

- Multi-system support
 - RRSF support
 - Apply command to multiple profiles
 - z/OS UNIX administration
 - New support and reporting of SMF records
 - Send alerts to UNIX syslog
 - TCP/IP alerts and audit concerns
 - z/OS currency
 - Globalization
- and more...

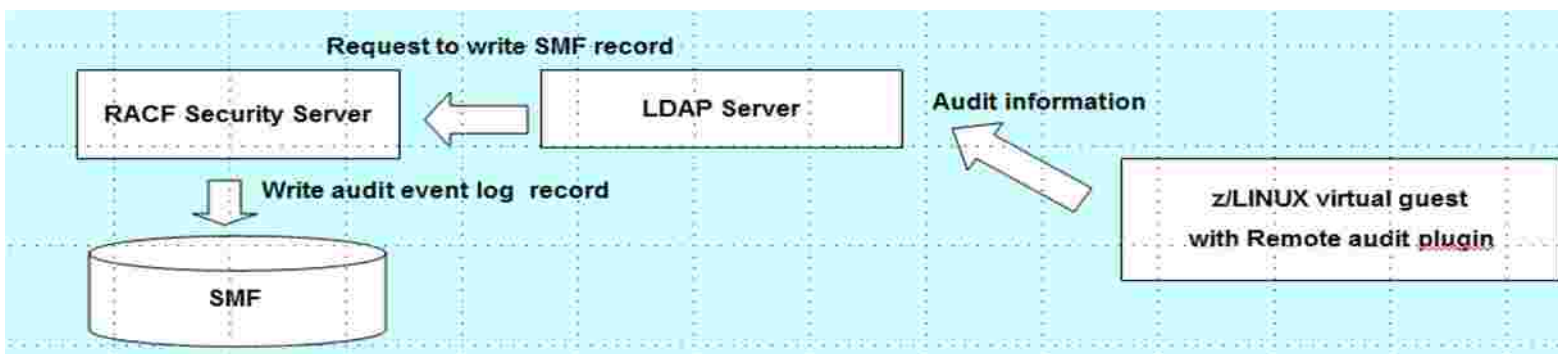
Data from multiple live systems in a single session Updates to multiple RACF databases with/out RRSF

- Multi-system support requirements
 - ü Administer multiple systems from a single application instance
 - ü Live data access
 - ü Fast data access
 - ü Allow sending the same commands to multiple systems
 - ü Use RACF Remote Sharing Facility network if present
 - Ø Support for AT and for ONLYAT keywords
 - ü Without RRSF network
 - ü Use data encryption

New SMF record types

- Communications Server NJE mail client (CSSMTP) events SMF record type 119 with subtypes 48-52
- DB2 V10R1 events SMF 102
- Linux for System z events – 4SMF record type 83 subtype
 - SMF record type 83 subtypes have shared and individual data sections
 - SMF record type 83-4 records remote audit events

New SMF record types and fields – Linux for System Z



Linux for System Z events (SMF record type 83 subtype 4)

- SMF record type 83 subtypes have shared and individual data sections
- SMF record type 83-4 records remote audit events
- One application that can write them is a Linux plug-in (daemon) **audispd**

New **R_LOGDATA** field - application-specific data from relocate section 114

- **RACF_LINK_EVENT** and **RACF_LINK_AUDIT** associate multiple records for the same event

Apply command to multiple records on a display

- zSecure 1.12 introduces **block commands** on ISPF displays:
 - **Admin:** RR..RR to Recreate multiple profiles
 - **Admin:** DD..DD to Delete multiple profiles
- Commands for all selected records are executed at once
- In addition a primary command **FORALL** is provided
 - With no selection, it applies a command to all records on the display

Writing alerts to a UNIX syslog socket

UNIX syslog added as an alert destination

- Syslog receivers are commonly used to collect messages from multiple systems, store them for log collection purposes and analyze them for alerting purposes. z/OS UNIX has a Syslog receiver that has been enhanced in z/OS V1R11, it can be used as a central point of log collection, e.g., for Linux for System Z systems. There are many cross-platform log collection solutions that zSecure Alert can now easily feed into.

∅ Also available for
zSecure 1.11.0

TCP/IP Audit concerns – IP_STACK and IP_PORT

Audit concerns pertaining to IP stacks—review required:

- ü32 By default, anyone can modify TCP/IP security parameters
- ü30 IPv[4 | 6] IP filtering support and IPSec tunnel support not active
- ü30 Denial-of-service possible without authentication
- ü28 No access control to/from foreign and local networks
- ü26 No access control required to/from foreign networks
- ü24 No access control in local network
- ü23 Ports below 1024 are not reserved - any user or program can bind to low [TCP | UDP] ports to masquerade as a legitimate service
- ü21 SMF119 subtype is not written - audit trail incomplete
- ü20 No audit trail of attacks stopped by filter rules

TCP/IP concerns – IP_STACK and IP_PORT

Audit concerns pertaining to IP stacks—worthy of attention:

- ü18 No audit trail of attacks stopped by default filter rules
- ü15 or 11 By default, anyone can read netstat [netstatoption] output that might help attackers

Audit concerns pertaining to IP ports—review required:

- ü22 Because there is no SAF parameter, any user or program can bind to a privileged [TCP | UDP] port [begin_port-end_port | port] under jobname jobname (filter) by default, thus masquerading as a legitimate service and receive passwords
- ü20 Because there is no SAF parameter, any user or program can bind to a privileged [TCP | UDP] port [begin_port-end_port | port] under jobname jobname (filter) by default, thus masquerading as a legitimate service

TCP/IP concerns – TRUSTED

Audit concerns for access to Trusted Computing Base:

- ü6 User can modify TCP/IP security parameters
- ü3 Can run attack program on a privileged protocol port between begin_port and end_port under jobname jobname (filter), thus masquerading as a legitimate service and receive passwords
- ü2 Can run attack program on a privileged protocol port between begin_port and end_port under jobname jobname (filter), thus masquerading as a legitimate service

zSecure Alert Enhancements

- TCP/IP alerts for deactivating TCP/IP security features Alerts 1609-1615 added for TCP/IP security reduction
- IBM Health Checker – Alerts 1604, 1605, and 1606 added to pass on low, medium and high severity alerts from IBM Health Checker
- SMF Record Flood detection - Alerts 1607 and 1608 are issued for z/OS V1R12 SMF record flood detection

Enhanced Security Intelligence for Mainframe Applications with IBM Security zSecure suite V1.13

IBM Security zSecure suite 1.13

*Extend auditability best practices
to the mainframe environment,
improving security posture*

- Announcement on October 4, 2011
- Availability in November 11, 2011
- Includes over 100 requests from customers
- Designed for use with z/OS 1.13
 - Also runs on z/OS release 1.10 – 1.12
 - Some functions will not work on older z/OS releases
 - zSecure V1.9 – out of support as of September 30, 2011




zSecure 1.13 New Features/Functions

- Support z/OS 1.13
- Extend the scope of zSecure to transaction and data managers
 - CICS
 - IMS
 - DB2
- Access monitor extensions
 - Performance improvements
 - High speed consolidation
- User interface improvements
- Support CICS TS V4R2
- Support IMS R12
- Support ACF2 R14 and R15
- Support TSS R12, R14 and R15



zSecure 1.13 New Features/Functions

- CARLa changes
- RACF Offline
- zSecure Visual
- zSecure Command Verifier
- Enhancements for TSIEM/TCIM Enablers
- Improved reporting capabilities for compliance reporting and monitoring
 - Communication Server
 - IMS
 - CICS



Providing ease of
use and usability

Improving Auditing and Monitoring

CICS and IMS

- New reports show:
 - Region info for - Region name, appl, default userid, SAF options, e.g., classes, attributes, etc.
- Transaction definitions
- Program definitions
- Audit concern and priority for unprotected critical transactions
- Flexibility to add your own “sensitive” transactions

Improving Auditing and Monitoring

DB2

- New reports show:
 - Region information
 - Region name, region userid, classes used, subsys id, etc.
 - zSecure Audit and Alert already process SMF records from DB2 (type 102)
 - DB2 external security events can be captured with SMF record type 80 or 230

CICS, IMS, and DB2 Resource reports

New menu options RE.C, RE.M, and RE.D

```

zSecure Suite - Main menu
Option ==> re.c_
More +
SE  Setup          Options and input data sets
RA  RACF           RACF Administration
AA  ACF2          ACF2 Administration
AU  Audit         Audit security and system resources
RE  Resource      Resource reports
  I  IP stack     TCP/IP stack reports
  U  Unix         Unix filesystem reports
  C  CICS         CICS region and resource reports
  M  IMS         IMS control region and resource reports
  D  DB2         DB2 region report
AM  Access       RACF Access Monitor
EU  Events       Event reporting from SMF and other logs
CO  Commands     Run commands from library
IN  Information  Information and documentation
LO  Local        Locally defined options
X   Exit         Exit this panel

Input complex:  IDFX
  
```

Menu RE.C:

```

zSecure Suite - Resource - CICS
Option ==>
R   Regions      CICS region reports
T   Transactions CICS transactions selection and reports
P   Programs     CICS programs selection and reports
  
```

zSecure Admin – Access Monitor

- Introduced in zSecure 1.11

- Part of zSecure Admin

What it does

- Collects information about

Access requests to datasets, transactions, files, programs, resources, etc

Consolidated into daily and (optionally) weekly, monthly or yearly files

Identifies unused profiles, members, GLOBAL entries, access list entries, groups

- Successful implementations with zSecure 1.11 and 1.12
- Value to customer -- Low cost of data collection
- Facilitates RACF database cleanup
- Helps in auditing usage
- Can assist in improving confidence of security implementation

Extended capabilities in 1.13

zSecure Admin – Access Monitor

- Enhancements for Access Monitor to assist in auditing and monitoring
 - Increased collection data for improved analysis
 - Jobname, user privileges, port of entry
 - Collect use of OPERATIONS.SPECIAL attribute
 - Collect authority granted by EXIT
 - Collect Status of OPERATIONS/SPECIAL at time of event
 - Needs RACF support – z/OS 1.13 or PTF on 1.12
- Performance enhancement for data collection
 - Have seen 40% space savings
 - Faster I/O processing
 - Very little virtual storage
- Reporting unaffected

zSecure Admin – Access Monitor

- Improve efficiency of consolidation
- Unique parts of resource names flattened
- More efficient in daily consolidation (C2PAMCOL)
- Custom data reductions
 - Improves efficiency of consolidation
 - Customer specified parts of fields values flattened
 - New CONVERSION statement
 - Defines which characters to replace
 - Specifies selection on conditions
 - Most efficient in daily consolidation but can also be used during other consolidations and for other fields

Access Monitor – Collect job name/port of entry

```

zSecure Suite - Access - Further selection
Command ==> _____
All access monitor records
Specify further selection criteria:
Jobname . . . . .  _____ (jobname or EGN mask)
Port Of Entry class . . _____ (class or EGN mask)
Port Of Entry . . . . . _____ (POE or EGN mask)

Select access records(Y/N/blank)
_ Use of commands to add/delete dataset and general resource profiles
_ Use of global access checking table
_ Use of discrete profiles           _ Access attempts undefined users
_ System special authority used      _ User has special attribute
_ Operations authority used          _ User has operations attribute
_ Installation exit used

Action against resource  Intended access  Result
_ Define                 _ _ 1. Read         _ Success
_ Delete                 _ _ 2. Update       _ No profile
_ Addvol                 _ _ 3. Control      _ Not authorized
_ Chgvol                 _ _ 4. Alter        _ Other
  
```

New in zSecure Admin for RACF Offline

✓ To ease the database clean-up or restructure efforts

New in 1.13: dynamic SPECIAL (or OPERATIONS or AUDITOR) within RACF Offline

Even when you do not have the privilege in the RACF databases

READ access on B8R.SPECIAL.database

First command to RACF Offline is

LOGON * SPECIAL

The installation can authorize a RACF analyst to test RACF commands on his "personal" copy, without giving him SPECIAL on the active RACF database

Design a RACF Cleanup or Restructure

PERMIT DELETE, CONNECT, REMOVE, add/del/change profile

Test the result using Access Monitor

Identify (production) work that would fail when the commands are put into production

A Few Other Audit Enhancements

- Extended TCP/IP reporting to include
 - New information added to TCP/IP VIPA configuration
 - Communication Server Resolver settings
- SMF record support extensions
 - Support for LDAP events written to SMF
- SMF records from CICS Transaction Server V4R2



Summary of What's new in zSecure Suite 1.13

- ✓ Automates security analysis of CICS and IMS transactions and programs
 - ✓ Provides automated determination of which System Authorization Facility (SAF) classes are being used by each active IBM DB2, IBM CICS, or IBM IMS subsystem
 - ✓ Enhances Access Monitor and allows you to improve data consolidation
 - ✓ Allows annotating userid displays with data from external human resource files such as department and employee number
 - ✓ Adds globalization enhancements to support international language support and auditing
 - ✓ Allows addition of your own sensitivity classification, audit concern, and priority to data set names and general resources
 - ✓ Supports currency with z/OS V1R13, ACF2 r14 and r15, CICS V4R2, and Top Secret R12, R14, and R15
 - ✓ Extends integration with Communications Server and provides various interface improvements
- and more...

Containing Risk and Monitoring User Activity Auditing and Monitoring Requirements Increase

Monitor RACF accounts

- Can they be mapped to users?
- Do rights match responsibilities?
- Are there any segregation of duties issues?
- Ensure compliance to policies

Monitor z/OS security configuration changes

- Who changed configuration parameters?
- When were they changed?

Monitor mainframe user activity

- Clearly see detailed information:
 - About users
 - Access granted
 - Who gave the access
- Detailed activity information for who accessed what data
- Privileged user activity reporting

Auditing and monitoring for CICS, IMS, DB2, Communication Server TCP/IP

Extend auditability best practices to the mainframe environment, improving security posture



Top Challenges zSecure Meets with Ease

Increasing Requirements

Increasing Complexity

Increasing Cost



Compliance requires structured, repeatable process

§ **zSecure Suite**

Privileged User Monitoring and Audit (PUMA)

§ **zSecure Admin, zSecure Audit & zSecure Command Verifier**

Resource access monitoring, quick and painless alternative to access reduction

§ **zSecure Admin, zSecure Audit & zSecure Alert**

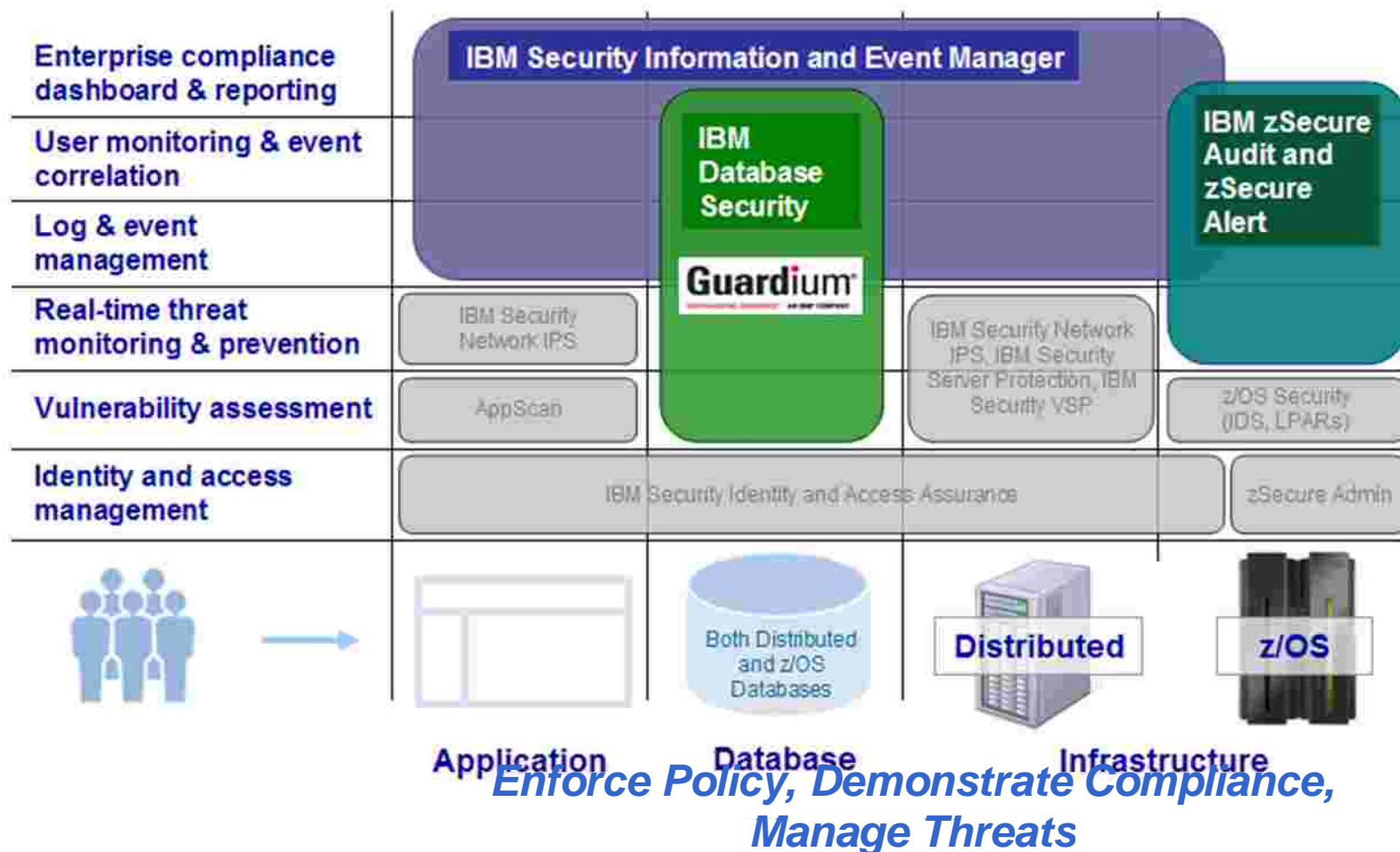
z/OS, RACF, UNIX, Linux on System z, CICS, IMS, Communication Server TCP/IP and DB2 Monitoring and Audit

§ **zSecure Audit & zSecure Alert**

Easing RACF administration and Decentralizing administration

§ **zSecure Admin, zSecure Visual, & zSecure CICS Toolkit**

Guardium and zSecure are Complementary Products



Additional zSecure Information:

Video: zSecure for Superior Mainframe Security:

<http://www.youtube.com/watch?v=tVB41OuaJ04>

White Paper: Consolidating security across platforms with IBM System z:

<http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=80003>

White Paper: Realizing Business Value with Mainframe Security Management:

<http://www.servicemanagementcenter.com/main/pages/IBMRBMS/SMRC/ShowCollateral.aspx?oid=70071>

Centralizing Security on the Mainframe (buyer's guide)

[http://www.ibm.com/common/ssi/cgi-](http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=RG&appname=SWGЕ_TI_SE_USEN&htmlfid=TIO14007USEN&attachment=TIO14007USEN.PDF)

[bin/ssialias?infotype=PM&subtype=RG&appname=SWGЕ_TI_SE_USEN&htmlfid=TIO14007USEN&attachment=TIO14007USEN.PDF](http://www.ibm.com/common/ssi/cgi-bin/ssialias?infotype=PM&subtype=RG&appname=SWGЕ_TI_SE_USEN&htmlfid=TIO14007USEN&attachment=TIO14007USEN.PDF)

Allied Irish Banks customer video:

On YouTube: http://www.youtube.com/watch?v=uv_WeSNHXdY

On IBM: https://www.ibm.com/services/forms/signup.do?source=swg-spsm-tiv-sec-dm&S_PKG=Allied-Irish-Bank

zSecure data sheets, solution sheets, and white papers

http://www-01.ibm.com/software/tivoli/products/zsecure-library.html?S_CMP=rnav

zSecure external web pages:

<http://www-01.ibm.com/software/tivoli/products/zsecure>

Redbooks [z/OS Mainframe Security and Audit Management using IBM Tivoli zSecure](#)

New! IBM Redpaper: [Empowering Security and Compliance Management for the z/OS RACF Environment using IBM Tivoli Security Management for z/OS](#)

Announced Oct 4.
NEW IBM Security
Division



For more information, please contact

Glinda@us.ibm.com

jamie_pease@uk.ibm.com