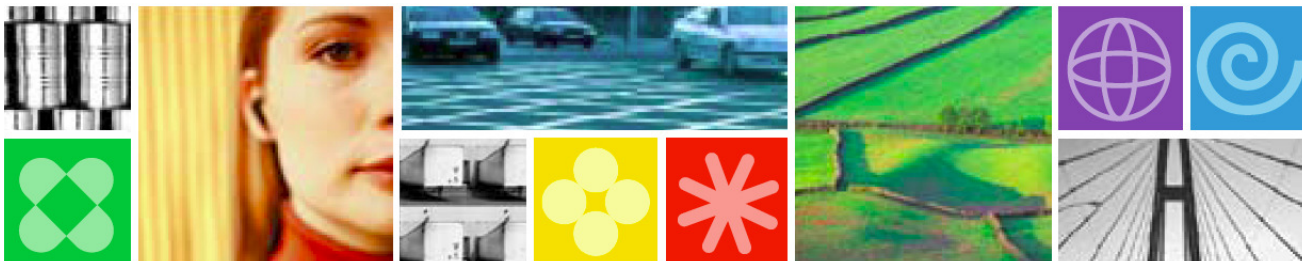




Leveraging your mainframe for cost-effective security and compliance

Glinda Cummings
WW Sr. Product Manager
glinda@us.ibm.com





Trademarks and disclaimers

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. IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce. 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 are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others. Information is provided "AS IS" without warranty of any kind.

The 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.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list prices and performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

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 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 or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

© IBM Corporation 1994-2009. All rights reserved.

References in this document to IBM products or services do not imply that IBM intends to make them available in every country.

Trademarks of International Business Machines Corporation in the United States, other countries, or both can be found on the World Wide Web at <http://www.ibm.com/legal/copytrade.shtml>.



System z Solution Edition for Security

■ A NEW Offering Packaging Concept:

This specially priced offering includes:

- 5 packages of hardware and software
- Up to 5 years of hardware maintenance
- Installation / implementation services
- Each suite of functionality is competitively priced
- An ability to address System z and a variety of distributed system security needs, making System z the Enterprise Hub for security.

OFFERING DETAILS

- z/OS® and Linux for System z security functionality priced competitively in a suite of solutions.
- A single physical server to solve a variety of enterprise security needs



Solution Edition for Security

- **5 offering security solutions that contain hardware, software, and services**
 - Each includes a recommended comprehensive set of non-integrated Security products
 - Each is available on one of the following: **z10 EC, z10 BC, z9 EC, z9 BC, or an LPAR on an existing z9[®] or z10 System z[®] processor**
 - Each includes 400 hours of STG lab services for implementation/configuration

- Enterprise Fraud Analysis

- ▶ Record and playback insider actions, forensic analysis to discover relationships, real time prevention workflow applied to operations (Tivoli zSecure Manager for RACF z/VM)

- Enterprise Encryption and Key Management

- ▶ Protecting personally identifiable data; enterprise encryption: Discover, audit and monitor and serve encryption keys (TKLM for z/OS)

- Centralized Identity & Access Management

- ▶ Cross platform user provisioning and management; cross platform authentication services (Tivoli Security Management for z/OS, TIM, TFIM, TIAA, Tivoli zSecure Manager for RACF z/VM)

- Securing Virtualization: z/VM[®], Linux for System z

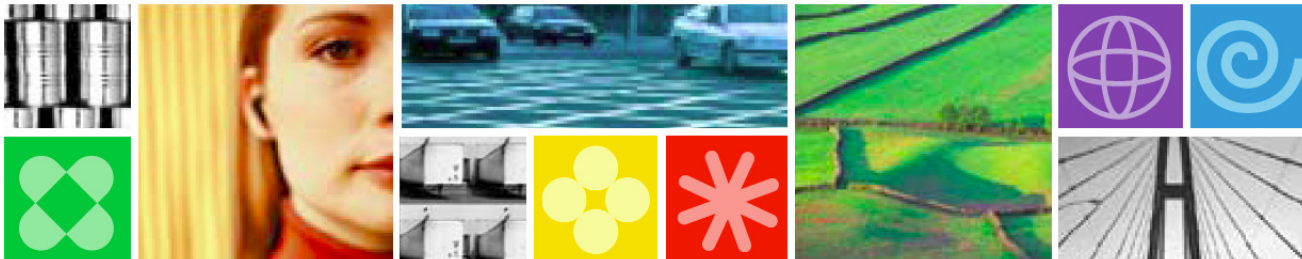
- ▶ Easily secure new virtualized workloads; security lifecycle management of server images running in Linux for System z, improved readiness for private cloud (Tivoli zSecure Manager for RACF z/VM, TIAA)

- Compliance / Risk Mitigation / Secure Infrastructure: z/OS[®]

- ▶ Audit and Alert processing, Simplified management operations, Data anonymization for development and test (Tivoli Security Management for z/OS, TKLM for z/OS)



What else is new



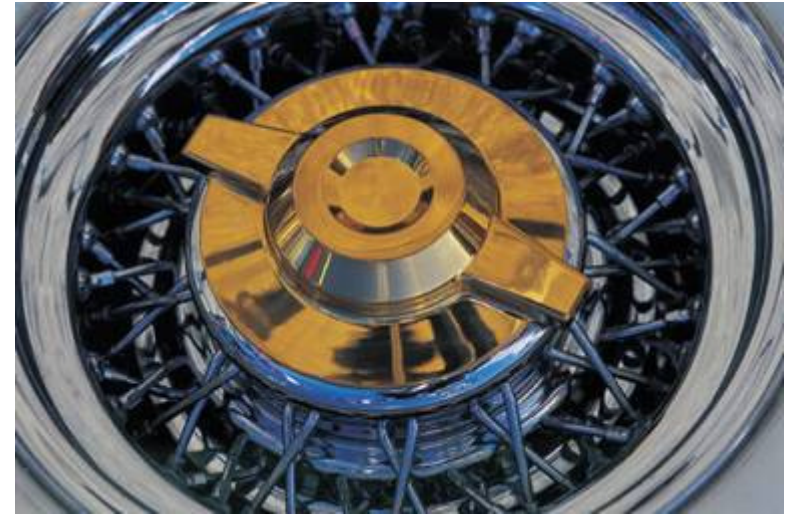


Why Tivoli Security Management for z/OS?

- **Improve service**
 - Leverage the most secure platform in the enterprise

- **Reduce cost**
 - Datacenter consolidation
 - Imbedded best practices
 - Reduce “cost of compliance”

- **Manage risk**
 - Data disclosure / privacy regulations
 - Failed audits, breach in industry





The Tivoli Security Management for z/OS

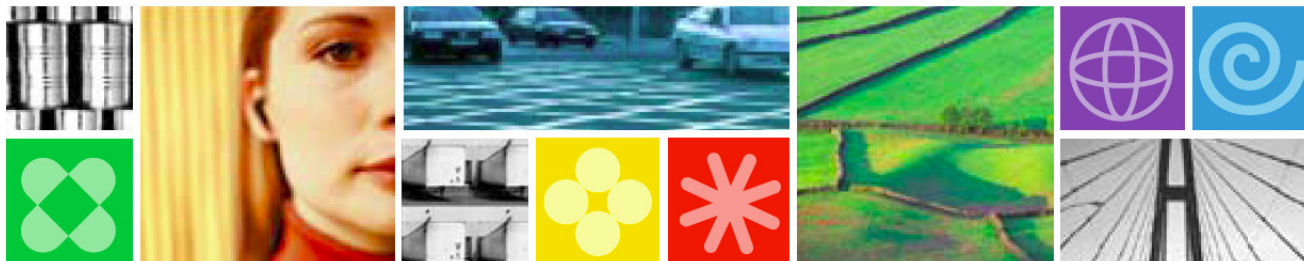
- Offers the capability to:
 - Administer your mainframe security while helping reduce administration time, effort, and costs
 - Monitor for threats by auditing security changes that affect z/OS, RACF, and DB2
 - Audit usage of resources
 - Monitor and audit security configurations
 - Enforce policy compliance
 - Capture comprehensive log data
 - Increase capabilities in analyzing data from the mainframe for z/OS, RACF and DB2
 - Interpret log data through sophisticated log analysis
 - Provide auditing results in an efficient, streamlined manner for full enterprise-wide audit and compliance reporting

- Components:
 - IBM Tivoli zSecure Admin
 - IBM Tivoli zSecure Audit
 - IBM Tivoli zSecure Command Verifier
 - IBM Tivoli Compliance Insight Manager





Announcing zSecure v1.11





Availability

- **Announcement November 3, 2009**
- **GA November 6, 2009**
 - Order via Shop zSeries
 - <https://www14.software.ibm.com/webapp/ShopzSeries/ShopzSeries.jsp>
 - <http://www.ibm.com/systems/z/os/zos/buy.html>



Supported platforms

- **Supports z/OS 1.11**
 - Also runs on (some) older z/OS releases
 - Formal support for z/OS 1.4 and newer
 - zSecure Visual server requires z/OS 1.6 and newer
- **CICS TS 2.1 through 4.1**
- **CA ACF2 and CA TSS release 8 through 12**
- **DB2 up to release 9.1**
- **zSecure Visual**
 - Tested with Windows XP SP2 and SP3, Vista
 - Testing with Windows 7 as I speak



What's New

- **Currency for z/OS v1.11**
 - Format and analyze live Communication Server (TCP/IP) stack configuration information for auditing and alerting
 - Support for new RACF and SMF fields for identity propagation
 - Support Load Module Signature Verification regulation requirements



What's New

- zSecure Admin – RACF Database Cleanup
 - **Address the problem of:**
 - obsolete authorizations with RACF database clean-up function
 - including
 - unused user,
 - group authorizations,
 - unused connects



What's New

- Extended monitoring of status changes in z/OS and RACF
- Integration with CICS to deal with multiple events contained in a single CICS SMF 110 Record, plus
- New CICS event information provided to Tivoli Compliance Insight Manager
- Report on IBM Data Facility Storage Management Subsystem (DFSMS) Re-movable Media Manager (RMM) new dynamic variants
- Using MVS System Management Facilities (SMF) format administrative commands from OMEGAMON for regulatory compliance



What's New

- Support Partitioned Data Set Extended (PDSE) and PDS member level auditing
- Audit and Alert on Internet Protocol Security (IPSEC) configuration information
- Ability to integrate with IBM Tivoli Key Lifecycle Manager for security events
- Report on IBM WebSphere Application Server V7 security events



What's New

- Audit and report for security events from Object Access Method (OAM) by using SMF
- Administration enhancements to the user interface (UI) for multiple permits and connects
- Multiple administration enhancements to ease and simplify reporting and administration tasks
- Ability to exploit new functionality for CA ACF2
- Ability to deliver globalization enhancements for Double Byte Character Set (DBCS)



zSecure 1.11 new functions and features

■ **New functions**

- Access Monitor for RACF
- Finding RACF profiles with values in segment fields
- TCPIP stack configuration
- Support and Reporting of SMF records extended
- Extended monitoring
- z/OS and ACF2 currency
- Globalization
- and more



zSecure Administration Suite Value Points

Improved mainframe security	There is always a chance of a breach, but with zSecure Admin your cleaner, safer administration will reduce this chance. Avoiding expensive breaches saves costs.
Reduce admin time	With zSecure Admin, the time taken to execute tasks is typically reduced, allowing scarce mainframe resources to focus on increasing security quality, compliance, monitoring and auditing.
Quicken response time	Idle end-users waiting for the creation of userids and other administrative tasks are serviced more quickly with zSecure Admin, thus reducing idle time.
Remove in-house efforts	Many companies have in house development efforts. These often cost more time to build and maintain than companies realize. zSecure Admin eliminates these costs.
Enable decentral resources	Helpdesk worker and distributed (non-RACF) administrators are typically cheaper. Tivoli zSecure eliminates the needs for decentralized TSO roll-out.



zSecure Security Audit and Compliance Suite Value Points

Pass audits, improve security	Have the reports that auditors and regulators require. Reduce the chance of costly security breaches through more secure mainframe administration.
Save time and costs	zSecure Audit can cut the man-hours needed to audit, report and then clean-up administrative databases. One customer claimed to have spent one month with a Big Five firm to generate the reports standard in zSecure Audit. Realize significant CPU savings due to zSecure Audit's efficient reporting engine.
Increase operational effectiveness	zSecure Audit show what JCL, parameters or load modules were changed, thus reducing downtime of applications caused by unexpected or improper modifications.
Improve speed of incident reaction	Because e-mail alerts contain the relevant details, administrators can move more quickly to diagnose and remediate failures or exposures with zSecure Alert.
Eliminate in-house software efforts	Reduces or eliminates need for internal applications and fixes to enforce compliance.



A Few Resources

- **Read: ["Enhance the security of your enterprise with IBM System z and IBM Tivoli security solutions"](#)**
- **Read: ["Enhance and accelerate audit and compliance activities for the mainframe environment"](#)**
- **Visit the Web page for [IBM Tivoli Security Management for z/OS](#).**
- **Visit the Web page for [IBM Tivoli zSecure Suite](#).**



Resource Center

Redbooks

- <http://www.redbooks.ibm.com/>
- CCR2 Newsletter Article
- <http://www.ibm.com/software/tivoli/features/ccr2/ccr2-2007-09/innovative-mainframe.html>