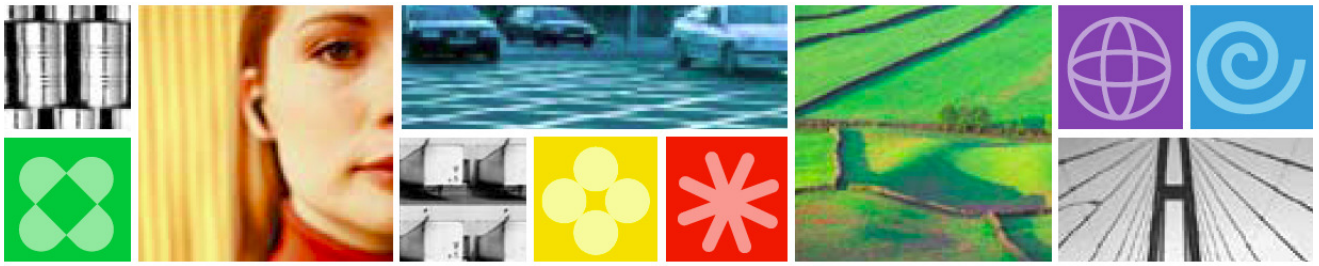
Leveraging the Mainframe as your Cost Effective Enterprise Security Hub



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.

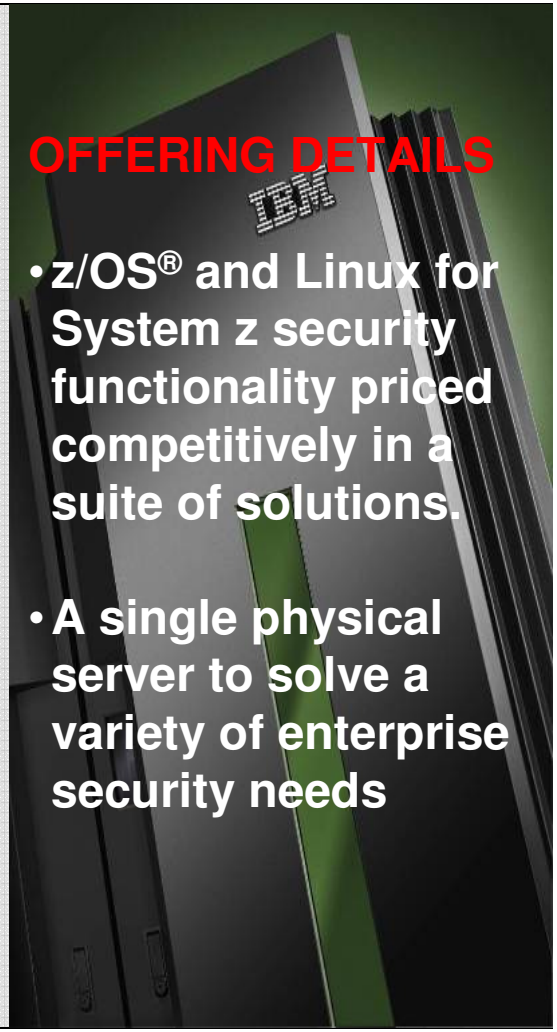
Photographs shown may be engineering prototypes. Changes may be incorporated in production models.

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.**

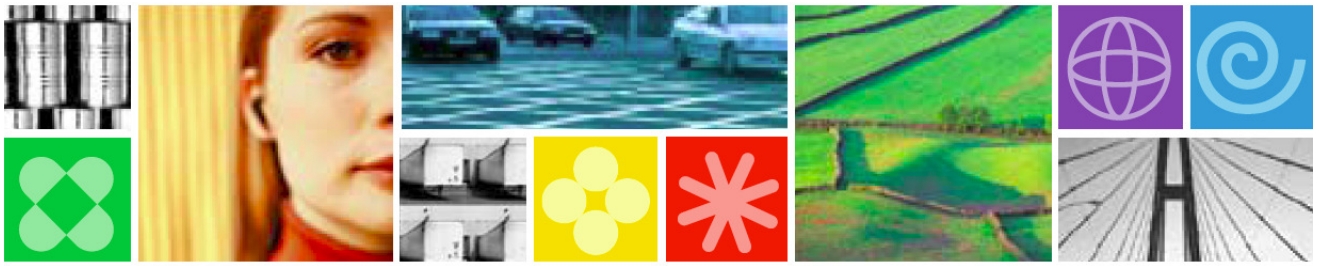


Solution Edition for Security

- **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

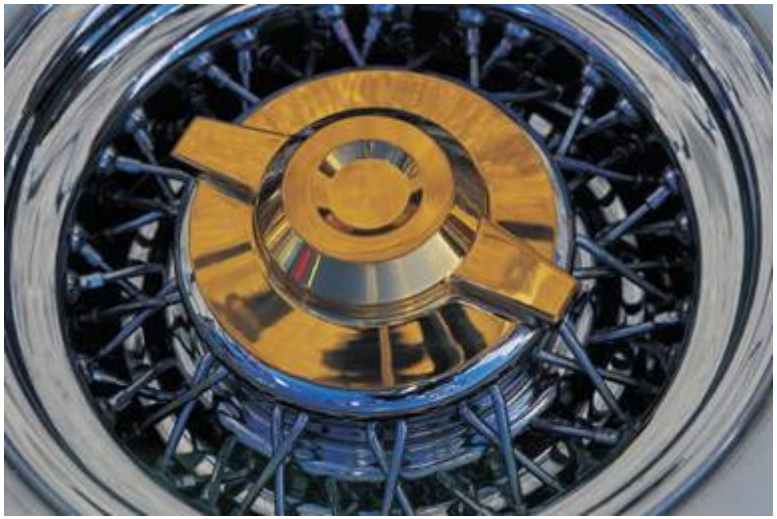
- Enterprise Fraud Analysis
  - Record and playback insider actions, forensic analysis to discover relationships, real time prevention workflow applied to operations (Tivoli zSecure Manager for RACF z/VM)
- Enterprise Encryption and Key Management
  - Protecting personally identifiable data; enterprise 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)

Tivoli Security Management for z/OS



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”

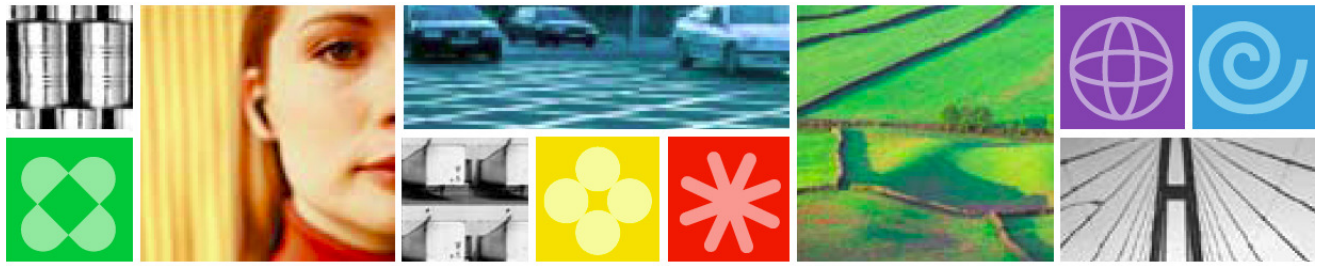
- **Manage risk**
  - Data disclosure / privacy regulations
  - Failed audits, breach in industry

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**

Tivoli zSecure suite

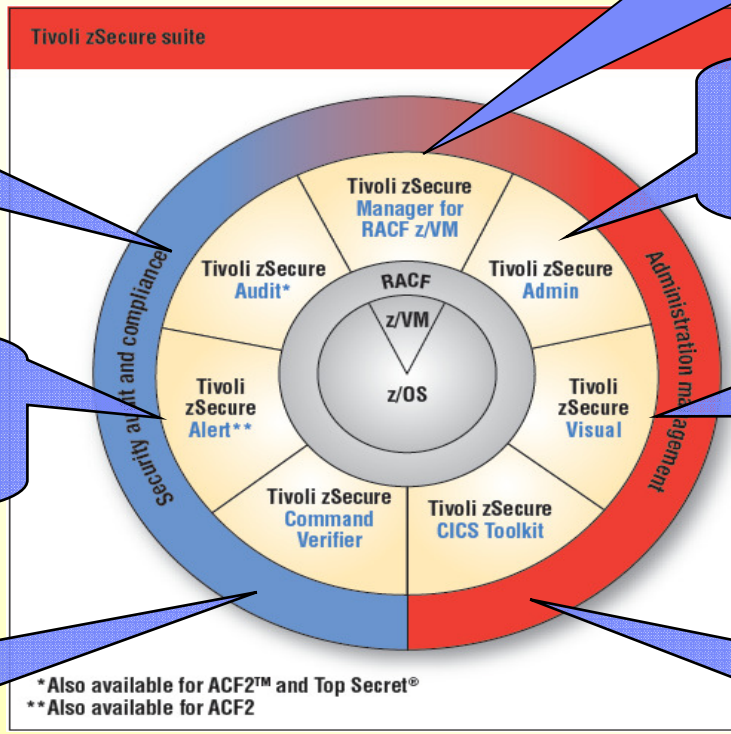


Introducing the IBM Tivoli zSecure Suite

Adds a user-friendly layer that enables superior administration coupled with audit capabilities for the z/VM RACF feature

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

Enables more efficient and effective RACF administration, using significantly less resources



Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts

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

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

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

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

Security administration is not easy

- **Situation:**
  - Technical users perform administration
  - User administration by non-technical users
  - Technical aspects of security by technical teams

- **Best Solution Available?:**
  - Use RACF commands via ISPF
    - Output is not easy to interpret
  - Use unloaded RACF database in DB2
    - Information not up to date

zSecure Solution

- Easy RACF administration – zSecure Admin
  - Overview of profiles, show context of security
  - Overtype fields to make corrections
  - Reports showing differences and effective security
- Actual information from active RACF database
- Simulate RACF reorganizations with RACF Offline

zSecure Admin – Improved RACF Provisioning of Users, Resources, and Control Options

- **Significant cost reduction**
  - Intuitive screens
  - Easier search capabilities
  - Simplification of complicated tasks
  - Self Help to assist in RACF knowledge
- **Comprehensive**
  - Intelligent cross-referencing
  - Automation of RACF administration
  - Use Live RACF, Historical RACF, Offline RACF, or compare one to another
  - Verify options to clean up and find RACF profile anomalies

zSecure Audit Assessment and Compliance Monitoring

z-Series + RACF +
Other entities

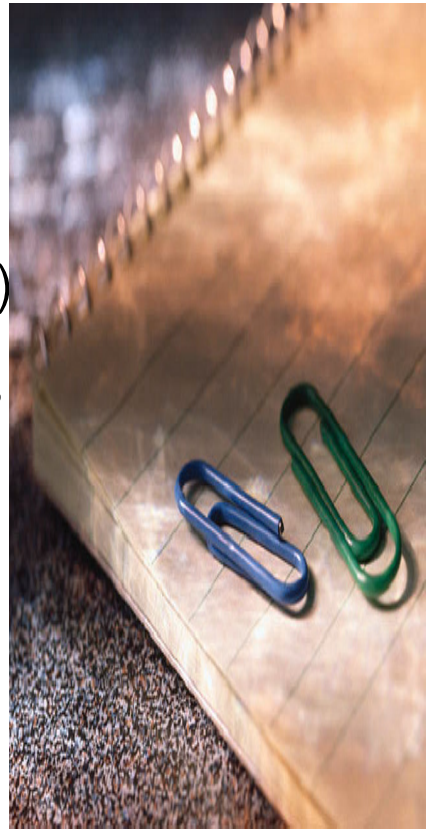
Knowledge base includes parameters from your system configurations compared to known security threats

Analyze, detect, and report on security settings, trusted users, critical resources, and security exposures

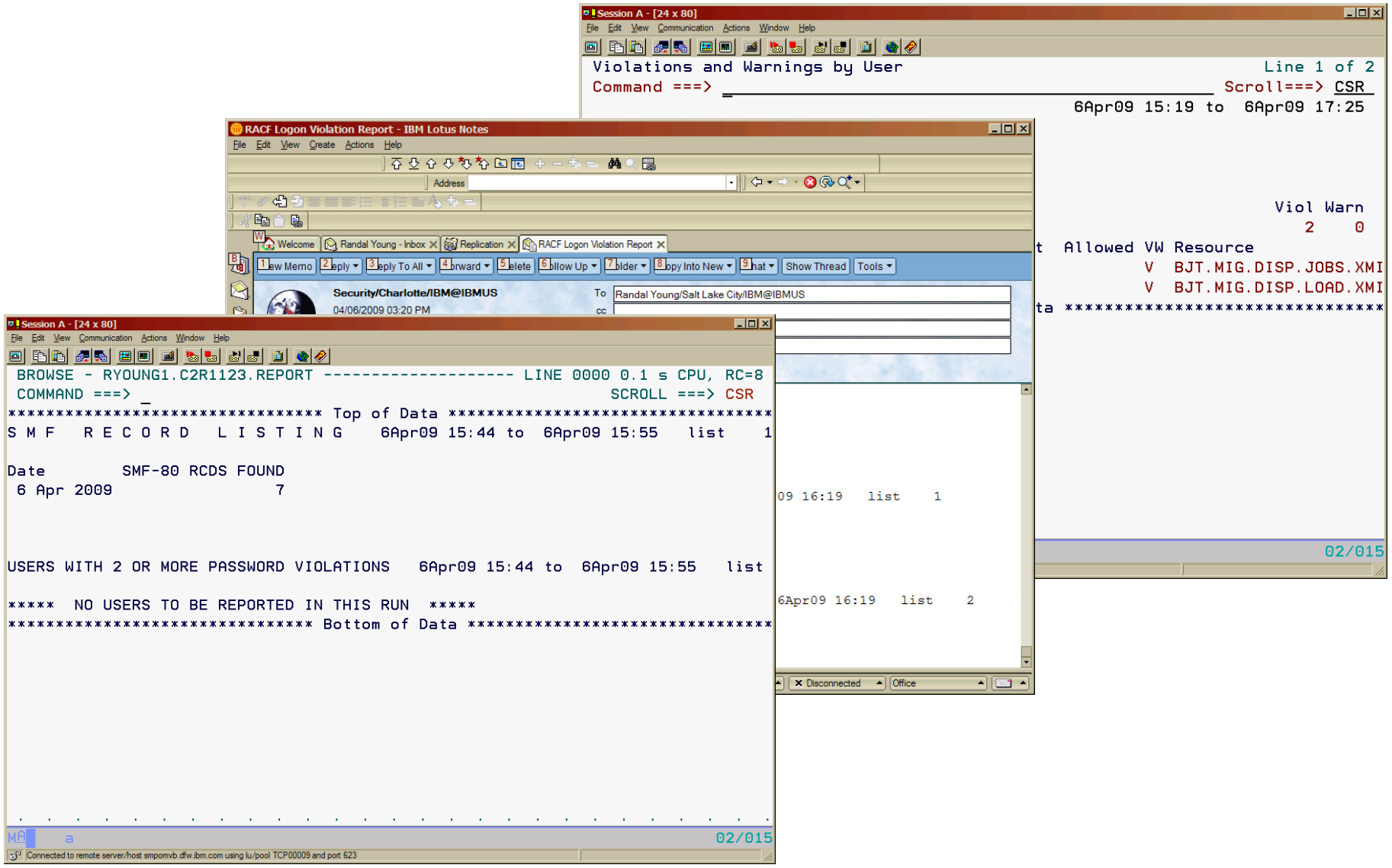
Comprehensive event analysis for compliance monitoring and forensic reviews

zSecure Audit – RACF and z/OS SMF Event Auditing

- **Easy to use without requiring SMF technical knowledge**
- **Filter events using thresholds, filters, and masking**
- **Goes well beyond RACF-DSMON**
  - More than 60 record types (DSMON limited to type 80,81)
  - Cross reference to system information and RACF profiles
  - Monitor datasets even if RACF Auditing is turned off
  - Monitor “Special” and “Operations”
  - Includes DB2 and CICS Record types
  - Define your own record types



Any Report to Print, ISPF, and/or E-mail



The CARLa language allows you to….

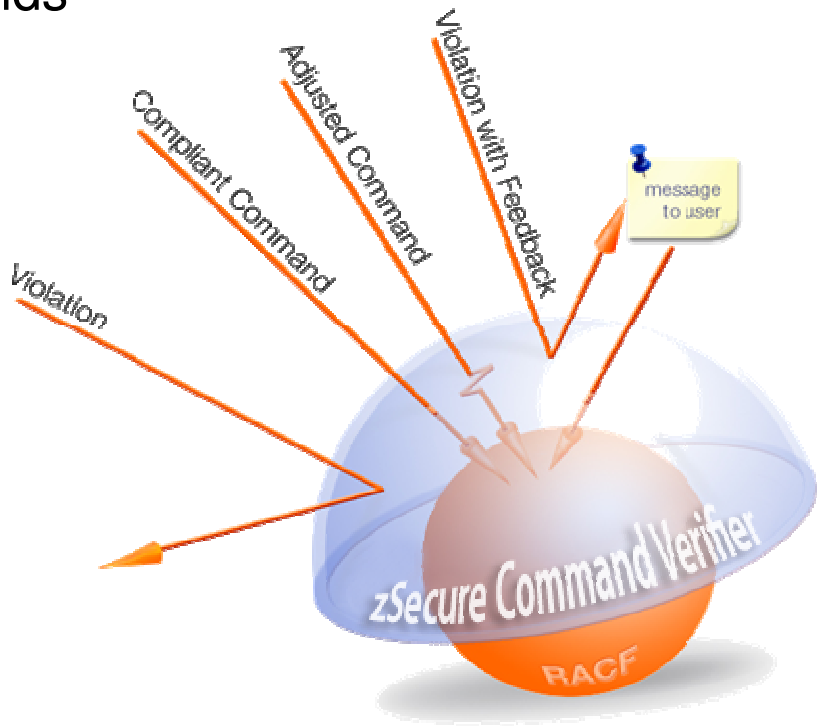
- **Customize existing reports or create new reports**
- **Additional interpreted RACF and SMF field names**
- **Compare today's report with yesterday's**
- **Determine and show exceptions to policy**
- **Automatically generate security reports**
- **Generate RACF commands**
- **Send output (via Email) to …**
  - Administrator(s),
  - Auditor(s),
  - Management

zSecure Alert – Real Time Monitoring

- Report changes that create policy exceptions or require compliance monitoring in real time
  - Addition or removal of security authority and privileges
  - Revoking of production userids
  - Excessive Universal Access granted
  - Modification of security options
  - Audit trail disabled
  - Update to a critical dataset
  - Dynamic addition of APF dataset
- Fully Configurable and Customizable

zSecure Command Verifier

- **Control points for RACF commands**
  - Refuse or Change RACF commands
  - Protect SETROPTS commands
- **Enforces standards**
  - Enforce Naming Standards
  - Limit System / Group Special
  - Separation of authority
- **Uses rules stored in RACF**
  - Standard resource profiles
  - ACL values determine authorization
  - Full documentation on setup

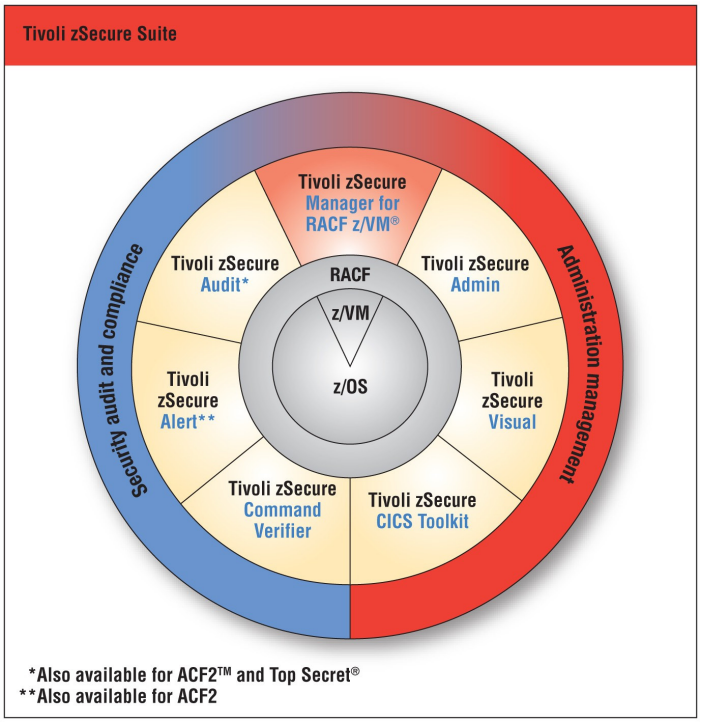


Tivoli zSecure Manager for RACF z/VM

The Tivoli zSecure Manager for RACF z/VM adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit capabilities for the z/VM RACF feature

Key Features

- **Enhances user management and provisioning for the VM environment**
- **Automates complex, time-consuming z/VM security management tasks with simple, one-step actions that can be performed without detailed knowledge of RACF command syntax**
- **Extends auditing capability by reading the RACF database, analyzing SMF records generated by RACF z/VM, and providing user privileges from both RACF and the VM directory**
- **Supports ease of management and auditing of the Linux guests if they use RACF for authentication while running in the VM environment**
- **Allows users to generate and view customized audit reports with flexible schedule and event selections**



Benefits Summary

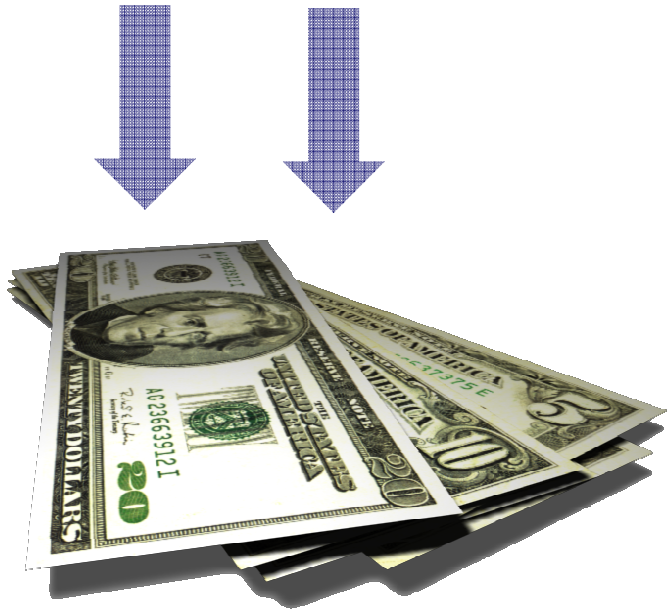
- **Improves the functionality of the mainframe's security system while helping reduce administration time, effort and cost**
- **Save time and costs through improved security and incident handling**
- **Helps to pass audits more easily**

Driving ROI with Tivoli zSecure suite

- **Achieve savings with simplified security administration**
- **Reduce administrative overhead with automated security auditing and reporting**
- **Reduce audit time and costs with consistent compliance reporting**
- **Reduce human error and increase integrity of mainframe security**
- **Produce repeatable and sustainable monitoring and auditing processes**

Reduce costs through repeatable and sustainable tasks

- **Reduce mainframe security administration costs**
  - Through simplified RACF administration
- **Improve user productivity**
  - Through faster access to information
  - Through compliance with SLAs
- **Enhance z/OS security**
  - Through automation of security policy enforcement
  - Through stronger z/OS and RACF security change monitoring
- **Improve z/OS audit and tracking**
  - Through central security event analysis
  - Through efficient user access tracking
- **Develop operational efficiencies to enable a dynamic infrastructure**



- **The problem:**
- **3 of the Top 10 Threats to Enterprise Security are insider related:**
  - Employee error
  - Data stolen by partner/employee
  - Insider Sabotage
- **Insider driven fraud costs US enterprises over $600 Billion annually**

Contain risk and failed audits with user activity monitoring, audit and reporting

- **Monitor RACF accounts**
  - Can they be mapped to users?
  - Do rights match responsibilities?
  - Are there any segregation of duties issues?
- **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
- **RACF policy enforcement**

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

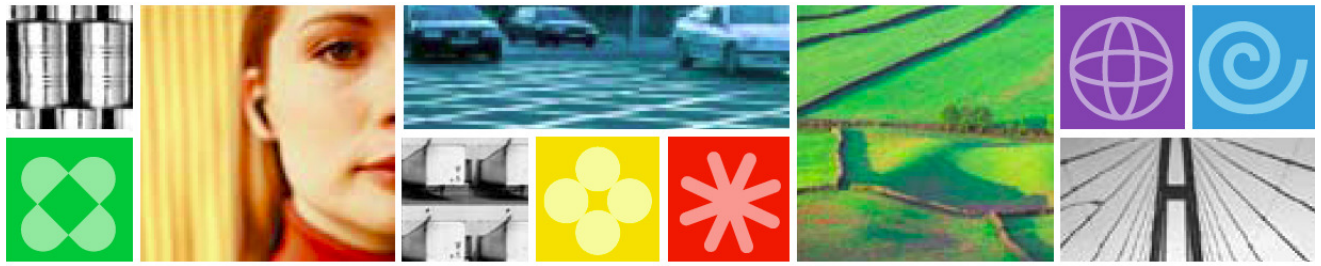
zSecure Administration Suite Value Points

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.**

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)

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

Questions anyone?