IBM Security zSecure Command Verifier

Enforce RACF policies and protect the security of your mainframe environment

Highlights

- Proactively enforce policy compliance on IBM® Resource Access Control Facility (IBM RACF®), prevent noncompliant RACF commands, reduce database cleanup time and audit concerns
- Reduce the risk of security breaches, failed audits and system outages caused by internal errors and noncompliant commands
- Raise alerts when risky commands are executed to help reduce chances of outages or decreased integrity of security

Central security personnel of RACF for mainframes often find themselves plagued with problems caused when technical specialists, field administrators, help desk users, application security administrators and other decentralized administrators issue commands that are not compliant with security policies and administration standards. Mistakes and ignored procedures, such as naming standards and policies for granting authorities, result in a "polluted" mainframe security environment that can require countless hours to clean. Worse, they can leave your infrastructure open to vulnerabilities and serious audit concerns.

Left unattended, a database that is inconsistent and poorly maintained as a result of noncompliant commands being run on the RACF system can lead to:

- Violations of your naming standards and installation policies
- Security exposures, such as abuse of privileged user IDs and segregation-of-duties conflicts
- System or application outages
- Audit concern findings and failed audits

Central mainframe security personnel need a way to prevent security changes that can reduce the availability and compliance of their systems, cause security database pollution or increase policy violations and security

vulnerabilities. IBM Security zSecure™ Command Verifier takes control of RACF commands so you can ensure the continuous security and compliance of your RACF environment.

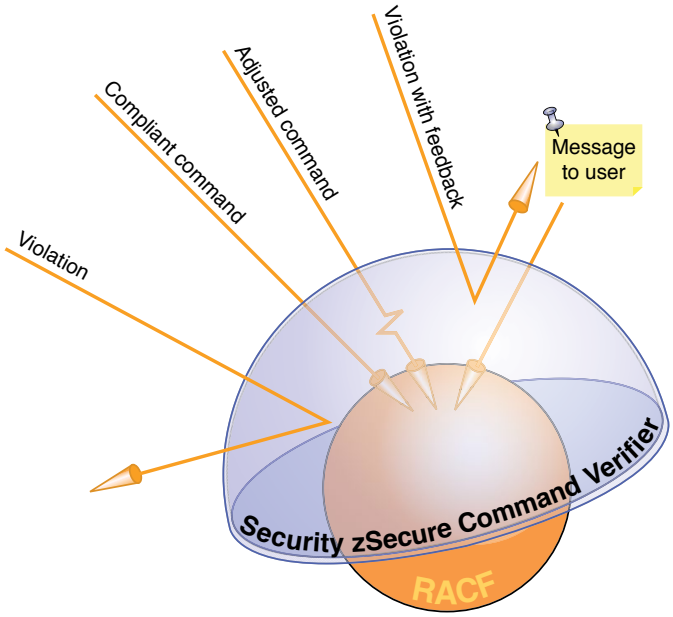
zSecure Command Verifier provides an additional security layer that enables you to compare each RACF command to your security policies, prior to processing. Commands are intercepted as they are entered and compared to your security policy to determine whether or not they should be run. Because the zSecure Command Verifier policy rules are defined through normal RACF profiles, security specialists do not require programming skills or assembler coding knowledge to configure zSecure Command Verifier—this also means that new policies can be added dynamically for immediate policy enforcement. zSecure Command Verifier enables you to:

- Conserve resources by eliminating RACF cleanup time
- Reduce the risk of security breaches and failed audits
- Increase security control, even when decentralizing administration
- Audit policy definitions with normal RACF reporting procedures

Verify commands before processing to proactively monitor policy compliance

zSecure Command Verifier helps prevent noncompliant administrative commands from being run. For example, in a RACF environment, privileged users might have permissions that enable them to change or delete all profiles within their scope—or run commands that violate installation policies for applications and devices.

To help prevent these kinds of administrative errors, zSecure Command Verifier automatically verifies command keywords against your specified policies as soon as an RACF command is issued—regardless of whether the command is initiated from



IBM Security zSecure Command Verifier acts as a protective shield against noncompliant commands issued in the RACF mainframe environment.

Time Sharing Option (TSO), Interactive System Productivity Facility (ISPF), a batch job or the operator console. Among other capabilities, zSecure Command Verifier lets you:

- Limit authorities on select profiles to READ
- Require the use of GROUPs on the PERMIT command
- Enforce naming conventions
- Prevent changes to RACF SETROPTS options
- Enforce application installation policies
- Enforce format of installation data fields
- Control whether userids can be added to access list for resources with a userid or groupid as high-level qualifier
- Maintain segregation-of-duties policies
- Monitor for multi-factor authentication and policy violations for the pervasive encryption feature in IBM Z®

Retrieve command information effortlessly with Command Audit Trail

A special Command Audit Trail feature in zSecure Command Verifier stores changes to profiles in the RACF database, so you can easily discover when a change to a profile was made and which administrator issued a particular command. With the Command Audit Trail feature, you can retrieve information on these changes in seconds, saving countless hours of log file research and reducing the risks associated with accidental or malicious actions performed by privileged users.

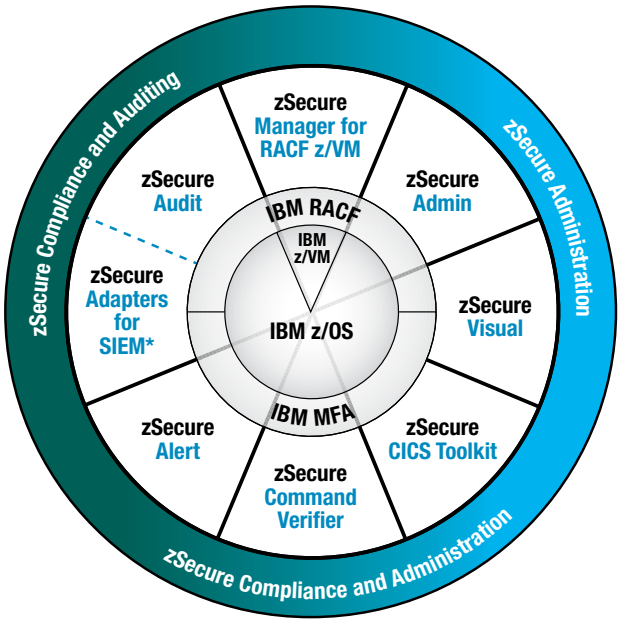
Take control by setting policies, alerts and default values

To help you stay ahead of—and prevent—potential security breaches, system administrators can easily use zSecure Command Verifier to specify policies using RACF profiles, to determine the type of verification to be performed and to define the action to take when a noncompliant command is detected, including prevention of command execution.

In addition, zSecure Command Verifier can generate immediate, real-time alerts if certain RACF commands are issued, helping to prevent system outages caused when administrators issue incorrect RACF commands. Notification controls offer processing options with appropriate messages when commands are changed.

You can also establish policy definitions to provide mandatory and default values for commands where RACF does not provide defaults. In addition, zSecure Command Verifier enables you to grant users access to specific commands that those users would not normally be authorized to use. This capability is typically used to authorize service desk and help desk personnel to display users, groups and resource definitions. By using these convenient, automated control features, zSecure Command Verifier helps central security personnel to assure the quality and consistency of RACF security.

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

Summary of products that comprise the IBM Security zSecure suite, including IBM Security zSecure Command Verifier

Easy, independent installation helps speed time to value

zSecure Command Verifier is implemented as part of the RACF Common Command Exit, a standard RACF application programming interface (API), which eliminates the need to design, code and maintain assembler routines that handle parsing of hundreds of keywords. Because the software runs as a command exit, it should be installed on all systems for which your installation policies must be enforced. zSecure Command Verifier works independently of other solutions in the zSecure suite and can serve as an important add-on to other third-party RACF tools that lack this vital functionality.

Why IBM?

zSecure Command Verifier is part of the family of zSecure products designed to provide comprehensive audit and administration process automation for the mainframe. The robust security features in the zSecure product family represent the IBM commitment to delivering the industry's best security interface for your mainframe.

For more information

To learn more about IBM Security zSecure Command Verifier, please contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/us-en/marketplace/command-verifier

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 15 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

For more information on IBM Security, please visit: **ibm.com**/security

IBM Security
New Orchard Rd
Armonk, NY 10504

Produced in the United States of America
September 2017

WGD03083-USEN-01