IBM Security zSecure suite

Deploy next-generation mainframe security administration, compliance and audit solutions

Every organization has a core set of mission-critical data that must be protected. Security lapses and failures are not simply disruptions—they can be catastrophic events, and the consequences can be felt across the entire organization. Mistakes such as unintentional configuration errors and careless security commands by privileged users alone can result in millions of dollars in damages. Malicious users with authorized access can cause even greater damage.

As a result, security management faces serious challenges in protecting the company’s sensitive data. IT staffs are challenged to provide detailed audit and controls documentation at a time when they’re already facing increasing demands on their time due to events such as mergers, reorganizations and other changes. Many organizations do not have enough experienced mainframe security personnel to meet demand, and expanding employee skill sets with low-level mainframe security technologies can be time consuming.

One way to offset these challenges is to establish effective processes to manage user administration, audit configurations and settings and monitor changes and events. That’s where the IBM® Security zSecure™ suite comes in. This comprehensive suite can help enhance the security
of mainframe systems by automating administration and audit processes, while easing the burden of compliance measures along the way. The zSecure suite can:

- Help increase security and decrease complexity
- Help free security administrators to focus on security
- Monitor and audit incidents to help detect security exposures and assess compliance

**Help increase security and decrease complexity**

The zSecure suite consists of multiple products for IBM z/OS® and IBM z/VM® designed to help you administer your mainframe security, monitor for threats, audit usage and configurations, and enforce policy compliance. The zSecure suite helps improve the efficiency and manageability of the mainframe security environment.

**Administration, provisioning and management products** can significantly reduce administration overhead, contributing to improved productivity, faster response time and reduced training time needed for new security personnel. These offerings include:

- IBM Security zSecure Admin
- IBM Security zSecure Visual
- IBM Security zSecure CICS® Toolkit

**Audit, monitoring and compliance products** help ease the burden of compliance audits, improve security and incident handling, and increase overall operational effectiveness. Offerings include:

- IBM Security zSecure Audit
- IBM Security zSecure Alert
- IBM Security zSecure Command Verifier
- IBM Security zSecure Adapters for SIEM

**Combined audit and administration** functions for the IBM Resource Access Control Facility (IBM RACF®) feature on z/VM are provided by:

- IBM Security zSecure Manager for RACF z/VM

---

**Summary of products that comprise the IBM Security zSecure suite**

* Product offers a subset of the capabilities provided by zSecure Audit
Help free security administrators to focus on security

Although preventing security breaches is paramount, administrators are frequently bogged down with tedious, time-consuming, day-to-day tasks that can divert their attention from security issues. The zSecure suite offers a range of products designed to help reduce administration time, enabling valuable mainframe resources to focus on improving security quality.

zSecure Admin is a leading security software product that enables efficient and effective RACF administration to help improve productivity. By putting a user-friendly layer over your RACF databases, you can quickly and easily process administrative commands, generate custom reports and clean up databases. And by implementing a repeatable process for security management, zSecure Admin can help you reduce errors, enhance identity governance and improve the overall quality of services. The Access Monitor function allows you to clean up unused permissions. To help reduce errors and the time required to administer multiple RACF databases, you can manage multiple systems from a single zSecure session.

zSecure Visual provides a Microsoft Windows-based graphical user interface for RACF administration that can reduce the need for expensive, RACF-trained staff. With the ability to establish a secure connection directly with RACF, zSecure Visual is ideal for decentralizing RACF administration without requiring users to have green screen (3270) or IBM Interactive System Productivity Facility (ISPF) and Time Sharing Option (TSO) skills for security administration.

zSecure CICS Toolkit allows you to perform mainframe administrative tasks from an IBM Customer Information Control System (CICS) environment, helping free scarce native-RACF resources from basic administrative routines and enabling decentralized administration. Using the zSecure CICS Toolkit application programming interface (API), you can use the RACF database to centralize the security for applications custom-built for CICS.

Track security events and prevent exposures to address compliance

Simultaneously keeping up with the demands for audit and controls documentation and trying to prevent security breaches can be overwhelming. The zSecure suite delivers auditing, monitoring and compliance solutions designed to help reduce security exposures while helping minimize the time needed to comply with auditors’ requests.

zSecure Audit delivers a comprehensive mainframe compliance and audit solution to quickly analyze and report on mainframe events and automatically detect changes and security exposures through extensive status auditing. The technology lets you create standard and customized reports that can be viewed under ISPF/TSO or in Extensible Markup Language (XML) format for use in databases and reporting tools. zSecure Audit also allows you to send Simple Network Management Protocol (SNMP) or UNIX syslog messages to an enterprise management console for policy exceptions or violations that indicate a possible security breach or weakness. The compliance framework testing capability offers easy compliance audit reporting for the Security Technical Implementation Guide (STIG) from the Defense Information Systems Agency (DISA) and Payment Card Industry Data Security Standard (PCI-DSS).

zSecure Adapters for SIEM enhances security intelligence by allowing you to feed real-time, enriched mainframe security information into an enterprise audit and compliance solution, based on integration with products including IBM QRadar® SIEM and IBM Common Data Provider for z Systems®.
zSecure provides the event source to supply mainframe information to the enterprise dashboard, combining mainframe data with data from other operating systems, applications and databases. QRadar SIEM provides the unique ability to capture comprehensive log data, interpret that data through sophisticated log analysis, and communicate results in an efficient, streamlined manner for full, enterprise-wide audit and compliance reporting. It can also feed IBM QRadar Advisor with Watson™ for cognitive analytics.

**zSecure Alert** offers mainframe event data for threat monitoring solutions that allow you to efficiently monitor for intruders and identify configuration changes that could hamper your compliance efforts. It goes beyond conventional intrusion detection solutions to support intrusion prevention, by taking countermeasures via automatically generated commands. In addition, zSecure Alert enables you to quickly detect unauthorized logons and attempts, user behavior that violates security policy and instances where your core systems may be at risk. Having this information readily in hand can help you identify dangerous configuration changes before they can be exploited, while staying one step ahead of the auditors.

**zSecure Command Verifier** is a robust policy enforcement solution that adds granular controls for keywords and parameters in RACF commands, and can help enforce mainframe compliance to company and regulatory policies by helping prevent erroneous commands from being run on the system. As a result, it helps increase control and decrease security risks and cleanup costs. Running in the background, zSecure Command Verifier checks RACF commands against your company's policies and procedures. When commands are entered, it verifies whether the commands comply with security policies, blocking or optionally adjusting noncompliant commands.

**zSecure Manager for RACF z/VM** provides combined audit and administration capabilities for the z/VM environment. It 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. As a result, it helps you maximize IT resources, reduce errors, improve quality of services and demonstrate compliance. The technology lets you create standard and customized reports.

**Why IBM?**

The zSecure suite is a valuable part of managing mainframe security as a business process that is designed to meet the needs of your business and its regulators and auditors. These offerings are the product of more than 25 years committed to innovation on the mainframe and to enabling you to improve and simplify mainframe security audit and administration. Through a broad range of offerings for z/OS and z/VM, the zSecure suite helps you address your key challenges:

- **Audit and compliance:**
  - Report on questionable system options and dangerous settings of privileged users to support segregation of duties
  - Measure and verify the effectiveness of mainframe security and security policies such as DISA STIG and PCI-DSS
  - Ease compliance reporting with an interface that automates reporting about external security standards
  - Enhance security intelligence by allowing you to feed real-time mainframe security information into an enterprise audit and compliance solution for enterprise-wide audit and compliance reporting, and into cognitive analytics solutions including IBM QRadar and IBM Operation Analytics for z Systems
- Generate alerts with instant reports about security events associated with RACF, IBM System Management Facilities (SMF), z/OS, IBM DB2®, CICS, IBM Information Management System (IMS™), UNIX subsystem, Linux on IBM z Systems, data facility hierarchical storage manager (DFHSM), IBM OMEGAMON®, IBM Security Key Lifecycle Manager, IBM Communications Server, Object Access Method, PDSE member-level auditing, IBM WebSphere® Application Server network configuration for TCP/IP, IBM Multi-Factor Authentication for z/OS (IBM MFA), and pervasive encryption

- User provisioning and security administration:
  - Centrally manage and provision users, profiles and resources across multiple systems
  - Constantly monitor privileged users and critical information for misuse, and improve identity governance
  - Help reduce operational costs and achieve fast incident detection

**IBM Security zSecure suite at a glance**

**Optional system support:**

- IBM RACF
- CA ACF2 R14 through R16
- CA Top Secret R14 through R16
- IBM DB2 V10 through V12
- IBM IMS V12R1 through V14R1
- IBM CICS TS v3R1 through v5R4
- IBM MQ V7.01 through V9.0

**Operating systems:**

- IBM z/OS V2R3, V2R2, V2R1 or V1R13

**Browsers:**

- For zSecure Visual: Microsoft Windows 7, Microsoft Windows 8 or Microsoft Windows 10

**For more information**

To learn more about the IBM Security zSecure suite, please contact your IBM representative or IBM Business Partner, or visit the following website:


**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
Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

© Copyright IBM Corporation 2017

IBM Security
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
July 2017

IBM, the IBM logo, ibm.com, CICS, DB2, OMEGAMON, QRadar, RACE, WebSphere, X-Force, z/OS, z Systems, zSecure, IMS, and z/VM are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.