IBM Security zSecure suite

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

Highlights

- Leverage seamless integration with an enterprise-wide view of audit and compliance efforts
- Monitor and audit incidents to help detect and prevent security exposures, as well as to assess compliance
- Automate routine administrative tasks to help reduce costs, improve productivity and enforce policy

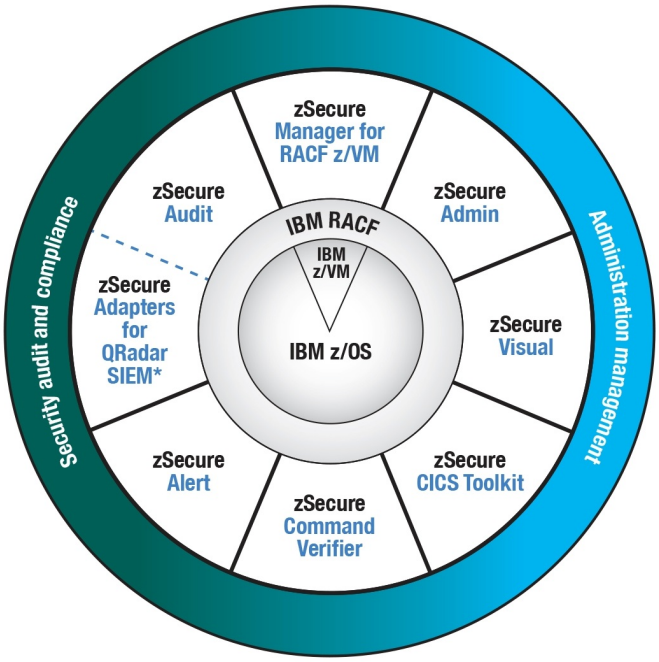
Every organization has a core set of mission-critical data that must be protected. Security lapses and failures are not simply disruptions—they can be catastrophic events, and the consequences can be felt across the entire organization. Inadvertent mistakes such as unintentional configuration errors 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 suite of solutions can help enhance the security of mainframe systems by automating administration and audit processes, while easing the burden of compliance measures along the way. IBM Security zSecure suite can help:

- Increase security and decrease complexity
- Free security administors to focus on security
- Track security events and prevent exposures to address compliance

IBM Security zSecure suite



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

Summary of products comprising the IBM Security zSecure suite

Help increase security and decrease complexity

The Security zSecure suite consists of multiple products for IBM z/OS and IBM z/VM operating systems designed to help you administer your mainframe security, monitor for threats, audit usage and configurations, and enforce policy compliance. The Security 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, enhance security intelligence and increase overall operational effectiveness. These offerings include:

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

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

- IBM Security zSecure Manager for RACF z/VM

Help reduce security administration tasks to focus on security priorities

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 Security zSecure suite offers a range of products designed to help reduce administration time, enabling valuable mainframe resources to focus on improving security quality.

Security 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 enter more quickly and process administrative commands, generate custom reports and clean up databases. And by implementing a repeatable process for security management, Security zSecure Admin can help you reduce errors 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 Security zSecure session.

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

Security 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 Security 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 Security 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. It can also help integrate mainframe security event information in with enterprise-wide security event information for end-to-end enhanced security intelligence.

Security 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. Security 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). Versions of the product support RACF, CA ACF2 and CA Top Secret.

Security zSecure Adapters for QRadar SIEM enhances security intelligence by allowing you to feed enriched mainframe security information into an enterprise audit and compliance solution, through integration with QRadar SIEM (Security Information and Event Management). zSecure provides the event source to supply the mainframe information to the enterprise dashboard, combining mainframe data with that 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.

Security zSecure Alert offers mainframe event data for threat monitoring that allows 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, Security 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. Versions of the product support RACF and CA ACF2.

Security 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, Security zSecure Command Verifier checks RACF commands against your companys' policies and procedures. When commands are entered, it verifies whether the commands comply with security policies, blocking or optionally adjusting non-compliant commands.

Security 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 Security zSecure suite is a valuable part of managing mainframe security as a business process that meets the needs of your business and its regulators and auditors. These offerings are 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 IBM z/OS and IBM z/VM, the Security zSecure suite helps you address your key challenges:

Audit and compliance:

- Report on questionable system options and dangerous settings of privileged users
- Measure and verify the effectiveness of mainframe security and security policies
- Ease compliance reporting with an interface that automates reporting about external security standards
- Enhance security intelligence by allowing you to feed mainframe security information into an enterprise audit and compliance solution for enterprise-wide audit and compliance reporting.
- Generate alerts with instant reports about security events associated with RACF, system management facilities, z/OS, IBM DB2®, CICS, IBM Information Management System (IMS™), UNIX subsystem, Linux on IBM System z®, data facility hierarchical storage manager (DFHSM), IBM Tivoli OMEGAMON®, IBM Security Key Lifecycle Manager for z/OS, IBM Communications Server, Object Access Method, PDS(E) member level auditing and IBM WebSphere® Application Server network configuration for TCP/IP

User and security administration:

- Centrally manage and provision users, profiles and resources across multiple systems
- Constantly monitor privileged users and critical information for misuse
- Help reduce operational costs and achieve fast incident detection

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:
ibm.com/software/security/products/zsecure/index.html

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 13 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 Corporation

Software Group

Route 100

Somers, NY 10589

Produced in the United States of America

July 2014