IBM Security Guardium for z/OS

Protect data in your z/OS database environments with scalable monitoring, analytics, and automation

Organizations that deploy IBM Z Systems™ mainframes have protection built in—including pervasive encryption, security in the processor, operating system, storage, and applications. But even mainframe environments need additional protection against growing threats and new levels of sophistication. They also need to meet an increasing number of regulations from industry and government, as well as address concerns from the public about whether data is sufficiently protected.

As a result, organizations are deploying new controls to help protect sensitive mainframe data—in DB2, IMS and Data Sets—from unauthorized access. At the same time, these controls need to be supported by detailed audit trails that help demonstrate compliance. Relying on database administrators and manual, homegrown processes to generate audit trails is not only inefficient, it inherently violates separation-of-duties (SOD) requirements in various rules for compliance. There is no way to prevent unauthorized database access, and database auditing can create high overhead, causing some organizations to eliminate auditing altogether.

IBM Security Guardium® provides an optimized, integrated, comprehensive means of securing sensitive data enterprise-wide, across mainframe as well as distributed environments. It empowers security teams to protect against threats and data loss by: (1)

Highlights

- Help ensure IBM® DB2®, IBM IMS™ and Data Sets security in IBM z/OS® shops
- Protect sensitive data via alerts and blocking unauthorized database activities
- Granular visibility of privileged users, mainframe-resident applications, and network clients
- Integrate with z/OS security for end-to-end access management
- Support separation of duties (SOD) preventing unauthorized changes
- Automate compliance workflow
- Utilize security intelligence, analytics, and automated forensics

automatically finding and classifying sensitive data; (2) analyzing data access patterns and alerting if there's anomalous behavior; (3) detecting threats; (4) preventing unauthorized database access; and (5) protecting sensitive data through real-time blocking and quarantining.

Guardium also includes automated compliance workflows and pre-packaged templates to support security mandates, such as the Sarbanes-Oxley Act (SOX), Payment Card Industry Data Security Standard (PCI-DSS), other data privacy laws like General Data Protection Regulations (GDPR), California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA).

Organizations can also customize these templates or create their own custom monitoring policies and reports. By leveraging the solution's automated compliance workflows, you can help ensure that the right reports get to the right people in time for sign-off.

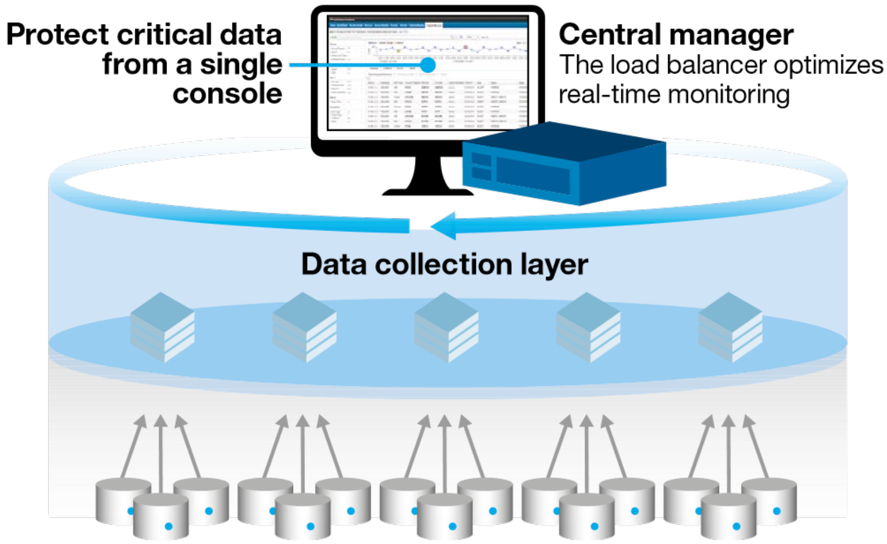
IBM Security Guardium for z/OS provides comprehensive data security and compliance capabilities for DB2, IMS and Data Sets on z/OS. The solution can be used for the mainframe environment only; or it can be integrated with other Guardium data security and monitoring components on distributed systems throughout the enterprise—providing a robust, centralized data security solution.

Avoid the costs and response delays of traditional security solutions

Historically, organizations seeking to monitor and secure their sensitive data on z/OS have used purpose-built solutions based on logging utilities, such as trace or transaction logs. These solutions, and others built upon them, suffer from a variety of limitations, including:

- Reliance on costly database administrators for compliance reporting, which also fails to provide the segregation of duties required by auditors
- Failure to capture all critical activities required by auditors (such as read operations when using logging, or SQL statements when using traces)
- Lack of granular analysis and real-time alerting capability, eliminating the possibility of immediately detecting and preventing unauthorized activities
- The need to apply significant amounts of skilled labor to analyze log data to identify breaches and prepare audit reports

Guardium for z/OS eliminates these limitations, while providing important additional capabilities, such as compliance automation, reporting, and an enterprise-wide view of the data security and compliance posture. Unlike traditional logging and trace approaches, Guardium is scalable and flexible, using lightweight software sensors called S-TAPs to capture DB2, IMS and Data Set activities by privileged users; mainframe-resident applications; and network clients, including those connecting through services such as Java Database Connectivity (JDBC), DB2 or IMS. Proven IBM event-capture technologies are used for each environment to ensure that all critical operations are captured, without the use of expensive audit traces.


Protect critical data from a single console
Central manager
The load balancer optimizes real-time monitoring
Data collection layer

IBM Security Guardium S-TAP probes

Guardium for z/ OS features a multi-tier architecture that offloads mainframe events for low overhead and improved security analysis.

Each S-TAP on z/OS is optimized for the unique monitoring requirements of a particular data environment. Some key capabilities include:

- IBM Security Guardium S-TAP for DB2 on z/O S monitors all DB2 activities, including SELECTs, UPDATEs, Data Manipulation Language (DML), data definition language (DDL) and changes in access privileges. To enhance performance, the underlying DB2 event-capture technology can be shared with IBM Query Monitor in systems that use both offerings.

- IBM Security Guardium S-TAP for Data Sets on z/O S supports IBM Customer Information Control System (IBM CICS®) transactions and a comprehensive range of file types, including entry-sequenced data set (ESDS), key-sequenced data set (KSDS), relative record data set

(RRDS), virtual relative record data set (VRRDS) and linear data set (LDS), monitoring OPENs, READs, UPDATEs, DELETEs, CREATEs and ALTERs. In addition, the STAP can monitor Virtual Storage Access Method (VSAM) files and Linear Data Sets (LDS) from DB2 and IMS.

- IBM Security Guardium S-TAP for IMS on z/OS monitors both online and batch tasks, providing auditing and policy management for a wide range of commands.

Each S-TAP sends information specified by user-defined audit policies to an IBM Security Guardium Collector for z/O S appliance. This ensures that the mainframe is not burdened with incremental storage or processing requirements, network traffic is limited, and a full audit trail is stored securely.

Spanning database platforms, applications, and locations, the Guardium multi-tier architecture aggregates and normalizes audit information into a single centralized repository. This provides comprehensive enterprise-wide compliance reporting, correlation, forensics, and database-focused analytics for security intelligence. Organizations starting with a mainframe implementation can scale up to support any mix of databases and systems—simply by adding appropriate S-TAPs, Collector appliances (virtual or physical) and Aggregator appliances (virtual or physical) Or Guardium Insights for z/OS, configured to work together in a federated model.

In addition, Guardium supports multi-stream load-balancing to enable the distribution of event monitoring in a round-robin fashion across multiple Guardium collectors. This helps increase the scalability of the overall solution by offloading events quickly from z/OS and reducing the load on individual collectors.

User interface helps you analyze and protect to reduce risks to sensitive data

The Guardium user interface helps enable the centralized management of security policies, alerts, report definitions, compliance processes and settings without involving system administrators or database administrators. This structure enables the segregation of duties that is required by auditors and helps streamline compliance activities. Guardium enables organizations to:

- Analyze threats to sensitive data by automatically discovering and classifying sensitive data and uncovering compliance risks; determine who is accessing data, using analytics and machine learning to analyze data usage patterns to uncover risks; and identify anomalies to help prevent data breaches

- Help protect data by allowing users to define granular access policies and the type of response to take for policy violations; policies can be based on a specific data object, type of command, user ID, client IP address, operating system (OS) user name, source application, or time of day

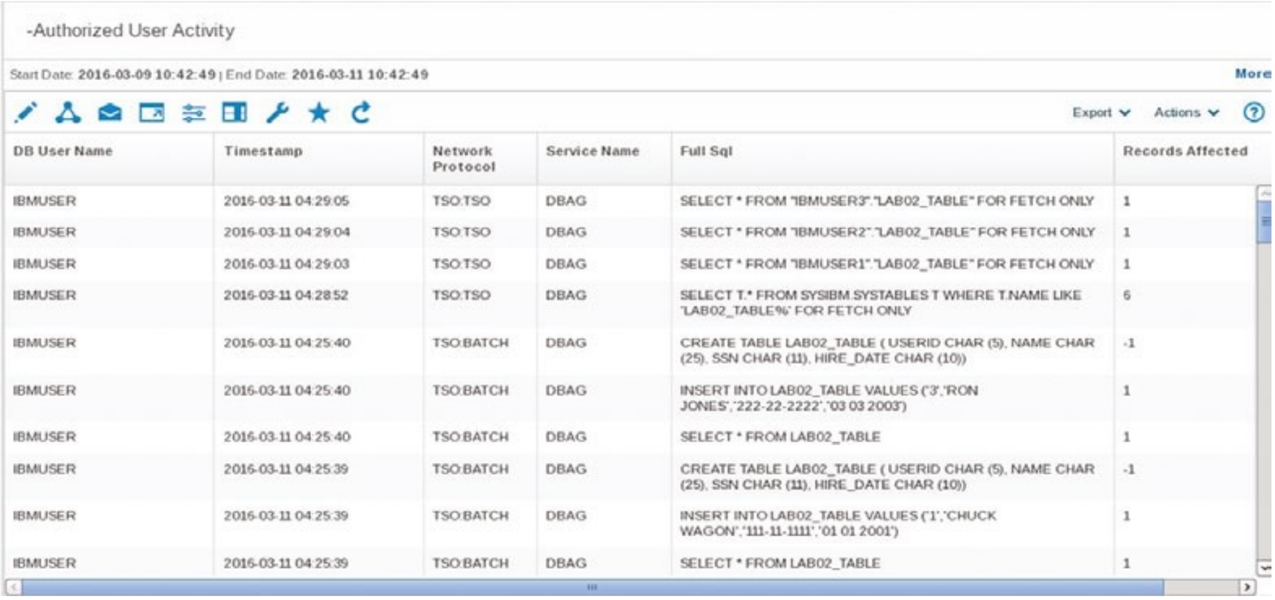
- Use predefined entitlement reports to help ensure that users only have the privileges required to perform their duties— and track changes in privileges over time, using Guardium workflow to require approval of any changes

- Analyze OS and database risks, privileges and authorities using automated database vulnerability assessment tests and recommend steps for remediation

- Support the z/OS environment by using integrated solutions, such as the IBM Security zSecure™ suite and IBM

Resource Access Control Facility (IBM RACF®), for end-to-end access management and control

- Leverage out of the box integration with SIEM solutions like IBM Security QRadar®, Splunk or ArcSight, etc. for real-time security intelligence, which can alert Guardium to risks (such as rogue users and IP addresses), thus allowing Guardium to react quickly and proactively to defend against emerging threats


-Authorized User Activity

Start Date: 2016-03-09 10:42:49 | End Date: 2016-03-11 10:42:49

DB User Name	Timestamp	Network Protocol	Service Name	Full Sql	Records Affected
IBMUSER	2016-03-11 04:29:05	TSO:TSO	DBAG	SELECT * FROM "IBMUSER3"."LAB02_TABLE" FOR FETCH ONLY	1
IBMUSER	2016-03-11 04:29:04	TSO:TSO	DBAG	SELECT * FROM "IBMUSER2"."LAB02_TABLE" FOR FETCH ONLY	1
IBMUSER	2016-03-11 04:29:03	TSO:TSO	DBAG	SELECT * FROM "IBMUSER1"."LAB02_TABLE" FOR FETCH ONLY	1
IBMUSER	2016-03-11 04:28:52	TSO:TSO	DBAG	SELECT T.* FROM SYSIBM.SYSTABLES T WHERE T.NAME LIKE 'LAB02_TABLE%' FOR FETCH ONLY	6
IBMUSER	2016-03-11 04:25:40	TSO:BATCH	DBAG	CREATE TABLE LAB02_TABLE (USERID CHAR (5), NAME CHAR (25), SSN CHAR (11), HIRE_DATE CHAR (10))	-1
IBMUSER	2016-03-11 04:25:40	TSO:BATCH	DBAG	INSERT INTO LAB02_TABLE VALUES ('3','RON JONES','222-22-2222','03 03 2003')	1
IBMUSER	2016-03-11 04:25:40	TSO:BATCH	DBAG	SELECT * FROM LAB02_TABLE	1
IBMUSER	2016-03-11 04:25:39	TSO:BATCH	DBAG	CREATE TABLE LAB02_TABLE (USERID CHAR (5), NAME CHAR (25), SSN CHAR (11), HIRE_DATE CHAR (10))	-1
IBMUSER	2016-03-11 04:25:39	TSO:BATCH	DBAG	INSERT INTO LAB02_TABLE VALUES ('1','CHUCK WAGON','111-11-1111','01 01 2001')	1
IBMUSER	2016-03-11 04:25:39	TSO:BATCH	DBAG	SELECT * FROM LAB02_TABLE	1

With an intuitive user interface, Guardium for z/OS makes it easier to monitor privileged user activities—including the “who, what, when, where and how” details of user access.

With Guardium, security teams gain real-time visibility into the z/OS data environment, enabling earlier detection and prevention of unauthorized database activities. They can quickly see the “who, what, where, when and how” details of data access. The lightweight Guardium S-TAPs are optimized to reduce the monitoring overhead. By automating the entire security and compliance lifecycle, Guardium helps reduce labor costs, facilitate communication throughout the organization and streamline audit preparation.

How Guardium complements IBM Security zSecure Suite

1. Guardium understands DB2-controlled security; by integrating it with IBM Security zSecure Audit, organizations can get insights into RACF-controlled security for DB2 resources and privileges.

2. zSecure Audit reconciles duplicate security definitions stored in both DB2 Catalog tables and RACF databases, thereby providing a “single version of truth” from a database entitlements perspective.

3. The zSecure platform provides audit collection and reporting of the z/OS environment and, when combined with Guardium, it gives a consistent view of the database management system (DBMS) and OS configuration and access controls.

4. When combining alert feeds from Guardium and zSecure into QRadar solutions, customers can have a single, consolidated view of security events across the complete z Systems environment, from a single point of control.

Why Guardium for z/OS?

Guardium for z/OS provides a comprehensive, proactive approach to safeguarding sensitive data, helping reduce cost and risk. Customers choose Guardium for z/OS because it:

- Has the support of IBM experts, who have a deep understanding of the z Systems environment.

- Optimizes security for the z/OS environment, with lightweight S-TAP agents that monitor all activities for authorized access before execution
- Delivers real-time alerts using low- latency, real-time streaming via TCP/IP
- Enables users to reduce overhead by using IBM Z Systems Integrated Information Processors (zIIP) for TCP/IP message processing and some server-s ide filtering capabilities
- Includes automated functionality, intelligence, and pre-built reports to help reduce security risks, protect sensitive data, and simplify compliance
- Supports commercial and proprietary multi-vendor data sources across a wide range of platforms, as well as applications, big- data environments, file systems and file shares
- Delivers a simple and effective architecture for operational efficiency—for example, allocating one address space per DB2 subsystem
- Enables audit data to be aggregated enterprise-wide for reporting and analysis
- Provides built-in tools, templates, and mechanisms for assessing vulnerabilities, reporting, security, compliance, audit, and automation
- In addition to z/OS, Guardium supports a wide range of platforms and data sources. To see the complete list of platforms currently supported by Guardium, please visit: www.ibm.com/support/docview.wss?uid=swg2704597

Why IBM?

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, provides security solutions to help organizations drive security into the fabric of their business so they can thrive in the face of uncertainty.

IBM operates one of the broadest and deepest security research, development and delivery organizations. Monitoring more than one trillion events per month in more than 130 countries, IBM holds over 3,000 security patents. To learn more, visit ibm.com/security.

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

For more information

To learn more about IBM Security Guardium for z/OS, please contact your IBM representative or IBM Business Partner, or visit the following website: https://www.ibm.com/products/ibm-guardium-data-protection/mainframes