



# Assure Db2 Data Monitor

## Complete control over the visibility of confidential IBM i data

Regulations like PCI DSS and HIPAA have long suggested the benefits of tracking access to confidential data. More recently, regulations like GDPR have begun to require it, and new regulations are likely to follow that lead.

It's imperative that your organization monitor and control the list of people allowed to access your most sensitive databases, and exactly what data they can read. Hoping that unauthorized users are not viewing corporate financial data, executive compensation, medical data and customer lists is not enough. You need tools to prevent accidental data disclosure and intentional breaches of confidentiality.

Assure Db2 Data Monitor, a feature of Assure Security and part of its Assure Compliance Monitoring feature bundle, is an innovative solution that gives you complete control over the visibility of confidential IBM i data. It monitors and alerts you to users who have viewed sensitive records in Db2 databases, as well as how and when the data was viewed. It even blocks records from view by unauthorized users.

With Assure Db2 Data Monitor, you can monitor the security of your most valuable corporate data while meeting the most stringent regulatory requirements for data confidentiality.

### Benefits

- Monitors and controls the access of all users, even administrators, to highly sensitive information
- Prevents theft and accidental exposure of confidential data
- Meets the most stringent regulatory requirements for monitoring access to critical information
- Satisfies auditors by logging views of confidential data



## How It Works

Assure Db2 Data Monitor goes beyond the normal auditing of IBM i database changes to offer total read access control for sensitive data at the record level, without requiring application changes.

Administrators configure Assure Db2 Data Monitor to identify:

- The owner(s) of the file who can see all records
- The field or fields that identify a record as containing sensitive data
- A field or fields that uniquely identify each record

*For example, in the diagram below, a database of financial transactions with trading partners might specify that the partner's company ID field defines the sensitivity of each record, and that transfer IDs uniquely identify each record.*

The Assure Db2 Data Monitor administrator then configures rules that define who can access records in the file. A variety of criteria are available to define the context in which users can view records, such as IP address, day of week, time of day, program stack and more. Without configuring user access, only the owners can see the records.

*In our example, the administrator has configured criteria that allow a user to only see financial transfer records for a specific company ID.*

When a user views confidential data, Assure Db2 Data Monitor logs the access in a journal entry, and can alert on the read access. The logged information identifies the file and record that was read, the user that read it, the program they were using, and more.

Before Assure Db2 Data Monitor, the user could see all the financial data in the file for all companies in the database

BEFORE Shows all the transactions

TRANSFER_ID	COMPANY_ID	CLIENT_ID	TRANSFER_DATE	TRANSFER_TIME	TRANSFER_AMOUNT	TRANSFER_CURRENCY
200098570	405	1070	2019-03-12	09:56:02	983400.00000	USD
200098575	405	1070	2019-03-12	09:56:02	67820400.00000	GBP
200098580	405	1070	2019-03-12	09:56:02	1000000.00000	USD
200098585	226	1071	2019-03-12	09:56:02	150712000.00000	USD
200098590	226	1071	2019-03-12	09:56:02	2000000.00000	USD
200098595	621	1072	2019-03-12	09:56:02	75356000.00000	EUR
200098600	226	1071	2019-03-12	09:56:02	2000000.00000	EUR
200098605	621	1072	2019-03-12	09:56:02	75356000.00000	USD
200098610	621	1072	2019-03-12	09:56:02	1000000.00000	USD
200098615	621	1072	2019-03-12	09:56:02	75356000.00000	USD
200098620	654	1073	2019-03-12	09:56:02		
200098625	621	1072	2019-03-12	09:56:02		
200098630	654	1073	2019-03-12	09:56:02		
200098635	654	1073	2019-03-12	09:56:02		
200098640	405	1074	2019-03-12	09:56:02		
200098645	405	1074	2019-03-12	09:56:02		
200098650	405	1074	2019-03-12	09:56:02		
200098655	621	1075	2019-03-12	09:56:02		
200098660	621	1075	2019-03-12	09:56:02		
200098665	123	1076	2019-03-12	09:56:02		
200098670	123	1076	2019-03-12	09:56:02		
200098675	123	1076	2019-03-12	09:56:02		
200098680	123	1076	2019-03-12	09:56:02		

AFTER

TRANSFER_ID	COMPANY_ID	CLIENT_ID	TRANSFER_DATE	TRANSFER_TIME	TRANSFER_AMOUNT	TRANSFER_CURRENCY
200098570	405	1070	2019-03-12	09:56:02	983400.00000	USD
200098575	405	1070	2019-03-12	09:56:02	67820400.00000	GBP
200098580	405	1070	2019-03-12	09:56:02	1000000.00000	USD
200098640	405	1074	2019-03-12	09:56:02	14567640.00000	ZAR
200098645	405	1074	2019-03-12	09:56:02	19955862.00000	ZAR
200098650	405	1074	2019-03-12	09:56:02	7901958.00000	ZAR
200098725	405	1078	2019-03-12	09:56:02	983400.00000	EUR
200098730	405	1078	2019-03-12	09:56:02	983400.00000	EUR
200098735	405	1078	2019-03-12	09:56:02	75356000.00000	EUR
200098740	405	1074	2019-03-12	09:56:02	68607068.00000	ZAR
200098755	405	1078	2019-03-12	09:56:02	75356000.00000	USD
200098795	405	1078	2019-03-12	09:56:02	1000000.00000	USD
200098800	405	1079	2019-03-12	09:56:02	75356000.00000	RUB
200098810	405	1079	2019-03-12	09:56:02	128504.00000	RUB
200098820	405	1079	2019-03-12	09:56:02	1452653.23000	RUB

Allows to show the transactions for Company ID 405 only

After Assure Db2 Data Monitor, the user only sees the financial transaction information for company 405, the only company they are authorized to see

## Key Features

### Control of Db2 data visibility

- Confidential records are identified by the content of a specified field(s)
- Users can only view the confidential records they are configured to see
- Even administrative users can be blocked from viewing sensitive records
- The file's owners always have full visibility

### Configurable read access criteria

- Powerful criteria allow you to fine tune read access
- Extensive criteria are available, including IP address, job information, day of week, time of day, program stack and more
- Simulation mode allows for testing configurations without impact to daily operations

### Logging and alerts on read access

- Views of confidential data rows are logged
- The information logged identifies the file and record that was read, the user who read it and more
- Alerts are sent via popup, email or your specific program

### Requires IBM i OS version 7.2 or greater