

IBM Security Guardium Analyzer Bootcamp

IBM SECURITY

Larry Lindsay, Devan Shah

October 2018



IBM®

Overview



Agenda

- Why Does Data Compliance Matter?
- Introduction to IBM Security Guardium Analyzer
- How Analyzer works?
- How Analyzer performs risk assessment?
- Hands-on Workshop To setup IBM Security Guardium Analyzer

Data Compliance



Data Compliance: GDPR



WHAT'S NEW?

THE DEFINITION OF WHAT CONSTITUTES 'PERSONAL DATA' NOW INCLUDES MUCH MORE, SUCH AS...

EMAIL ADDRESS
LOCATION
GENETIC DATA
HEALTH DATA



COOKIE STRINGS
IP ADDRESS
BIOMETRIC DATA

PENALTIES FOR NON-COMPLIANCE INCLUDE FINES OF UP TO

€20 MILLION
OR 4% OF GLOBAL TURNOVER

WIDER GEOGRAPHICAL SCOPE

GDPR applies to all companies processing the personal data of people who live in the EU



CONSENT



Consent must be freely given, specific, informed and unambiguous – with a positive opt in

AND YOU MUST BE ABLE TO PROVE IT!

NEW RIGHTS OF THE DATA SUBJECT

- ✓ the right to be informed
- ✓ the right of access
- ✓ the right to rectification
- ✓ the right to restrict processing
- ✓ the right to data portability
- ✓ the right to object
- ✓ the right not to be subject to automated decision-making

Introducing ... IBM Security Guardium Analyzer



Start fast

This software-as-a-service offering helps you get started immediately with a guided setup process.



Protect data

Specifically designed to help identify regulator data risks, this service analyzes on-premises and cloud databases to find and present users with prioritized risk information.



Next-generation data classification

A next-generation classification engine, which also powers IBM Watson offerings, searches data inside cloud and on-premises database tables, and vulnerability scanning uncovers current threats.



Reduce time to value

Pre-built functionality and dynamic dashboards surface data exposures, providing information such as: number of databases affected, severity breakdown, geographic breakdown.



Take action to minimize risk

This service combines the data classification and vulnerability scanning results to provide risk scoring and prioritization information so you can efficiently take focused steps to minimize risk.

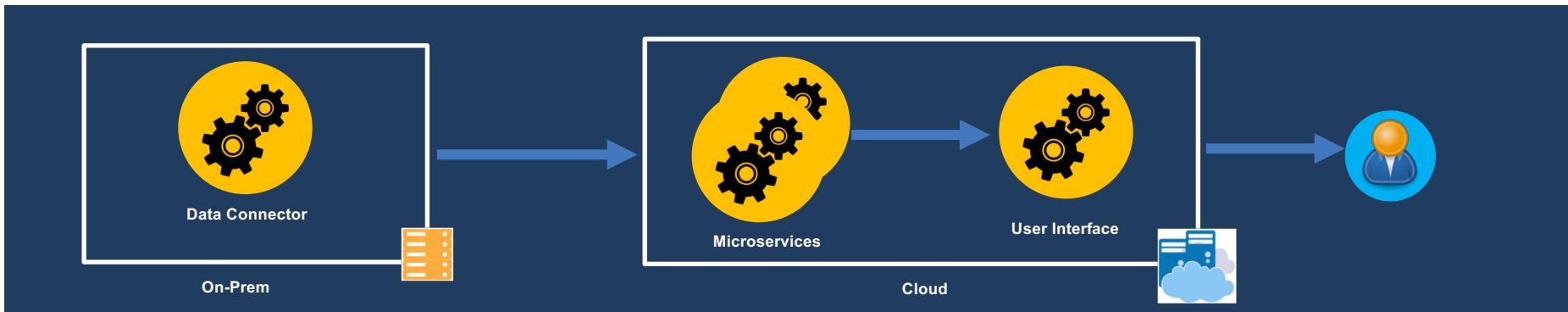


Streamline regulator activities

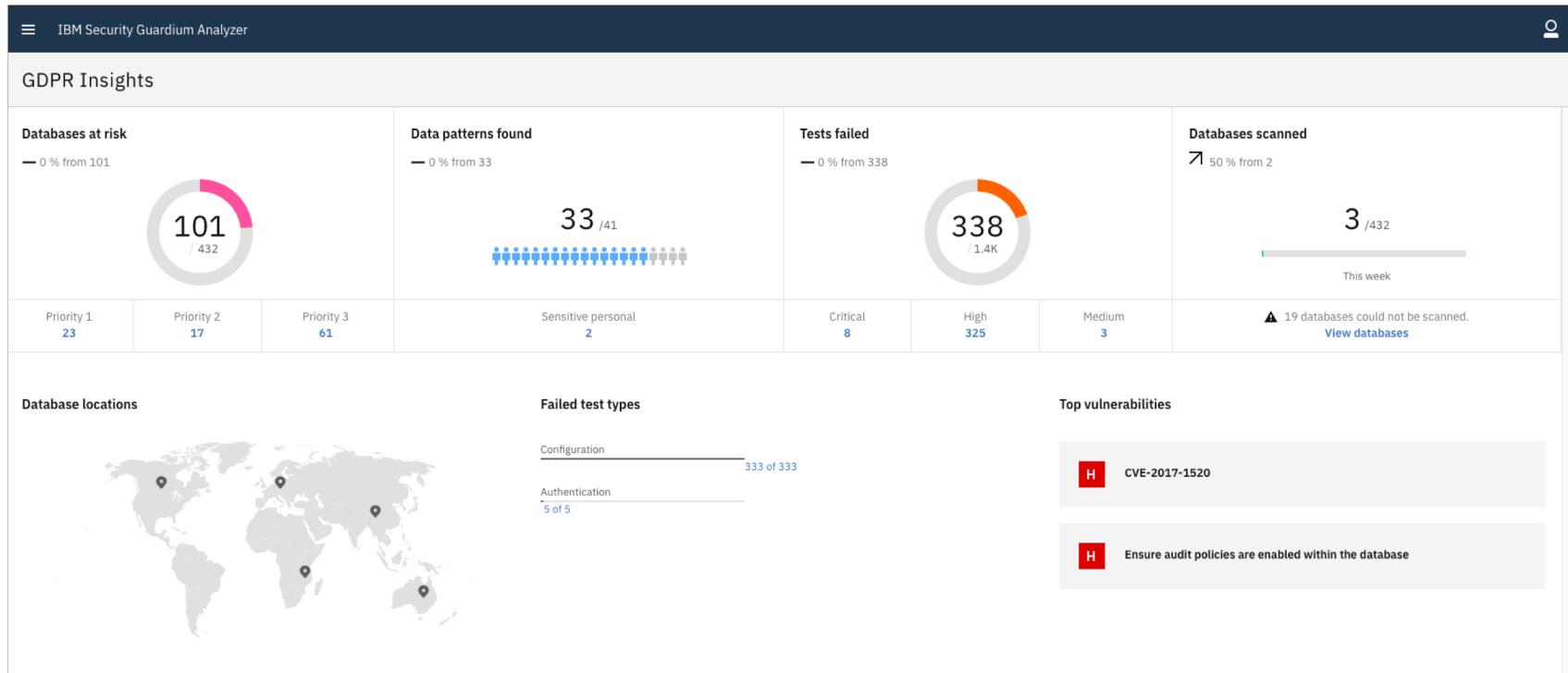
Helps compliance managers, data managers and IT managers get the information they need, at the right level of detail, to collaborate efficiently.

How it works?

- On-Prem Data Connector
 - Classification Scans
 - Vulnerability Scans
- Cloud Microservices
 - Parsers
 - Risk Engine
 - Classification Rules Management
 - Data Aggregators
- Data Visualizations
 - Provide all the data to the users



Overview: Global Dashboard



Overview: Regulator Data Insights

IBM Security Guardium Analyzer

Results Patterns ▼

3 of 432 scanned this week | scanned weekly ⟳ 🔗

Search 🔍 ✖

Found	Sensitive personal	Columns > Tables	Data subject
36/41	2	26	8

Classification	Patterns	Data subject columns	Samples matched	Tables	Databases	Personal records	Last scanned
Sensitive personal	Sexual orientation	0 of 27	79% of 106	23	15	6.57M	4 months ago
Sensitive personal	Religion/Faith	3 of 51	86% of 134	44	36	8.7M	1 week ago
Personal	Name	1 of 360	24% of 321K	239	93	20.1M	2 days ago
Personal	Address	10 of 730	1% of 1.05M	278	89	30.1M	2 days ago
Personal	UK national insurance number	0 of 125	16% of 236K	123	60	17.2M	4 months ago
Personal	Phone number	1 of 124	21% of 241K	124	60	19.4M	2 weeks ago
Personal	Email address	1 of 163	100% of 213K	160	89	18.3M	2 days ago
Personal	myregex	0 of 73	83% of 27.8K	73	25	2.37M	2 days ago
Personal	Belgium national ID	0 of 21	41% of 97	20	15	6.57M	4 months ago

Overview: Vulnerability Assessment

IBM Security Guardium Analyzer

Results / Japaora

3 of 432 scanned this week | scanned weekly

CONF

Search  

Severity	Vulnerabilities	Test type	Date found	Days open
Critical	PASSWORD_REUSE_MAX is set	Authentication	September 20, 2018	31
Critical	PASSWORD_REUSE_TIME is set	Authentication	September 20, 2018	31
High	SEC_PROTOCOL_ERROR_FURTHER_ACTION is set properly	Configuration	September 20, 2018	31
High	Check Oracle Sample Users Removed	Configuration	September 20, 2018	31
High	Check Parameter LOCAL_LISTENER Setting	Configuration	September 20, 2018	31
High	Oracle Application Express	Configuration	September 20, 2018	31
High	FIPS 140-2 for Transparent Data Encryption and DBMS_CRYPTO	Configuration	September 20, 2018	31
Medium	Oracle redo log file availability	Configuration	September 20, 2018	31
Medium	Oracle DBMS Links to External Databases	Configuration	September 20, 2018	31
Medium	Unused database components must be removed	Configuration	September 20, 2018	31

SEC_PROTOCOL_ERROR_FURTHER_ACTION is set properly 

CONF

Finding
You should set the SEC_PROTOCOL_ERROR_FURTHER_ACTION parameter to DROP or DELAY.
[Show less](#)

Description
The database is vulnerable to exhaustion of resources that could result in a Denial of Service (DoS) to other clients if not protected from a flood of bad packets submitted by a malicious or errant client connection. The SEC_PROTOCOL_ERROR_FURTHER_ACTION initialization parameter can be set to delay or drop acceptance of bad packets from a client in order to support the continued function of other non-problematic connections.
[Show less](#)

Fix recommendation
SEC_PROTOCOL_ERROR_FURTHER_ACT is not set, or is set to a value other than DROP or DELAY
[Show less](#)

• • • September 20 October 5

Mark as fixed

Comments [Add comment](#)

Database Risk

- Exposed Regulator Data
 - Sensitive Personal Information, or SPI
 - Also called "special category" data
 - Personally Identifiable Information, or PII
- Vulnerabilities
 - CVEs
 - Default Database Settings
 - Permissions

Workshop: Free Trial



Workshop: Marketplace

IBM

Marketplace  Search IBM Marketplace   

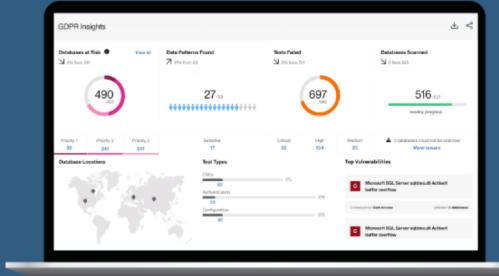
IBM Security Guardium Analyzer

Overview Details Pricing Resources FAQ Start your free trial

IBM Security Guardium Analyzer

Efficiently find regulated data, understand data and database exposures, and act to address issues and minimize risk.

[Start your free trial](#) [Watch the video \(04:39\)](#)



Data Discovery, Classification & Vulnerability Scans

This software-as-a-service offering helps you efficiently identify risk associated with personal and sensitive personal data (PII, PHI, PCI, etc.) that falls under regulations such as the E.U.'s GDPR, PCI DSS, HIPAA and other privacy mandates. The service applies next-generation data classification, as well as vulnerability scanning, to uncover privacy risks associated with such data in cloud-based and on-prem databases. It then applies risk scoring to the classification and scanning results to identify and prioritize the databases that may be most likely to fail audit, so you can act to minimize your risk.

Workshop: Ready Email

The image shows a preview of an email message. At the top right is the IBM logo. The main content starts with "Hi Analyzer," followed by a thank you message for signing up for a trial. Below this is a horizontal dashed line. Then there's a section titled "IBM Security Guardium Analyzer Trial" with instructions to use links to get started, followed by three blue links: "Launch Service," "Get Support," and "Learn About." Finally, there's a closing note from the "IBM Security Guardium Analyzer Team". A large black redaction bar is at the bottom.

IBM

Hi Analyzer,

Thank you for signing up for a subscription to **IBM Security Guardium Analyzer Trial** using the following customer account: Analyzer Workshop.

IBM Security Guardium Analyzer Trial

Use these links to get started:

→ Launch Service → Get Support → Learn About

Regards,
IBM Security Guardium Analyzer Team

Workshop: Analyzer Welcome Page

The screenshot shows a web browser window with a dark blue header bar. On the left of the header is the text "IBM Security Guardium Analyzer". On the right side of the header is a small user icon. The main content area has a white background. At the top center is a small black logo consisting of three horizontal bars. Below it, the text "[Analyzer]" is displayed in a small, gray font. In the center, the word "Welcome!" is written in a large, bold, dark blue font. Below "Welcome!" is a paragraph of text: "Getting insight into [Analyzer Workshop's] regulated personal data just got easier." At the bottom center is a blue rectangular button with the white text "Let's get started". A red rectangular box highlights this button.

IBM Security Guardium Analyzer

[Analyzer]

Welcome!

Getting insight into [Analyzer Workshop's] regulated personal data just got easier.

Let's get started

Workshop: Getting Started



[GuardAnalyzer]

Welcome!

Getting insight into [GuardAnalyzer
TechTalk's Company's] regulated
personal data just got easier.

[Let's get started](#)

Workshop: Insight Settings

The screenshot shows a configuration interface for receiving insights. At the top, there's a decorative icon of a stylized 'E' or 'F'. Below it, the section title 'Getting GDPR insight' is displayed. A descriptive text block explains that the IBM Security Guardium Analyzer helps find vulnerabilities and regulated data in databases. A question 'How often would you like to receive insights?' is followed by three radio button options: 'Weekly' (selected), 'Monthly', and 'Bi-weekly'. A large blue 'Next' button at the bottom is highlighted with a red border.

IBM Security Guardium Analyzer helps you find vulnerabilities and regulated data in your databases.

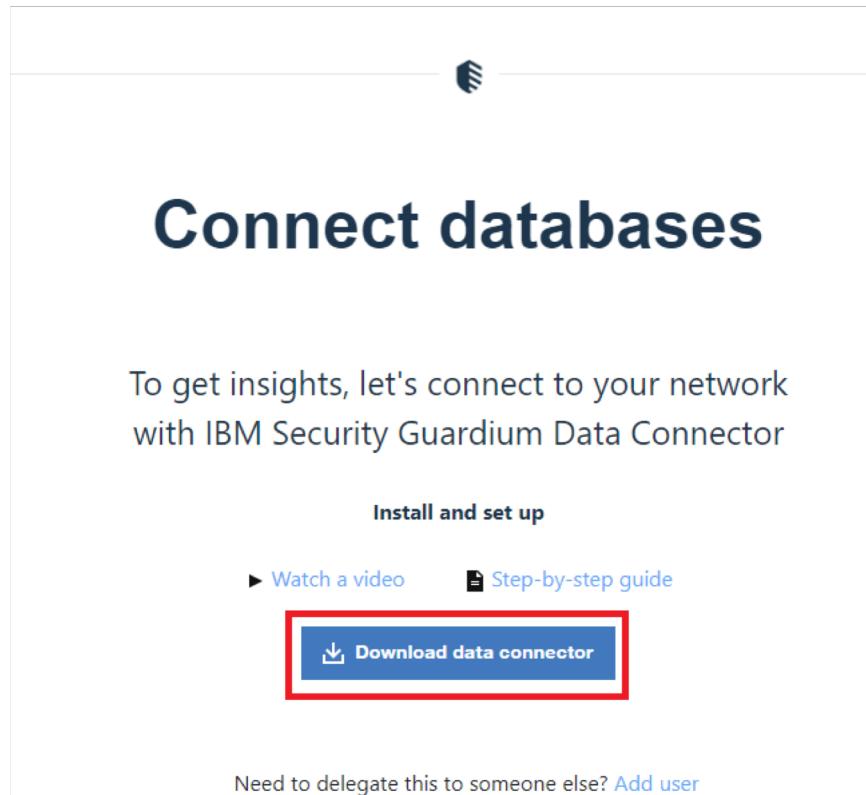
How often would you like to receive insights?

Weekly Monthly Bi-weekly

Next

- **Select how frequently Analyzer will scan your databases**

Workshop: Download Data Connector



The screenshot shows a user interface for connecting databases. At the top, there's a small icon of a shield with a checkmark. Below it, the title "Connect databases" is displayed in a large, bold, dark blue font. A sub-section title "To get insights, let's connect to your network with IBM Security Guardium Data Connector" follows. Underneath, there are several interactive elements: a blue button labeled "Install and set up", two links ("Watch a video" and "Step-by-step guide"), and a prominent blue button labeled "Download data connector" which is highlighted with a red rectangular border. At the bottom of the interface, a message reads "Need to delegate this to someone else? Add user".

Connect databases

To get insights, let's connect to your network with IBM Security Guardium Data Connector

Install and set up

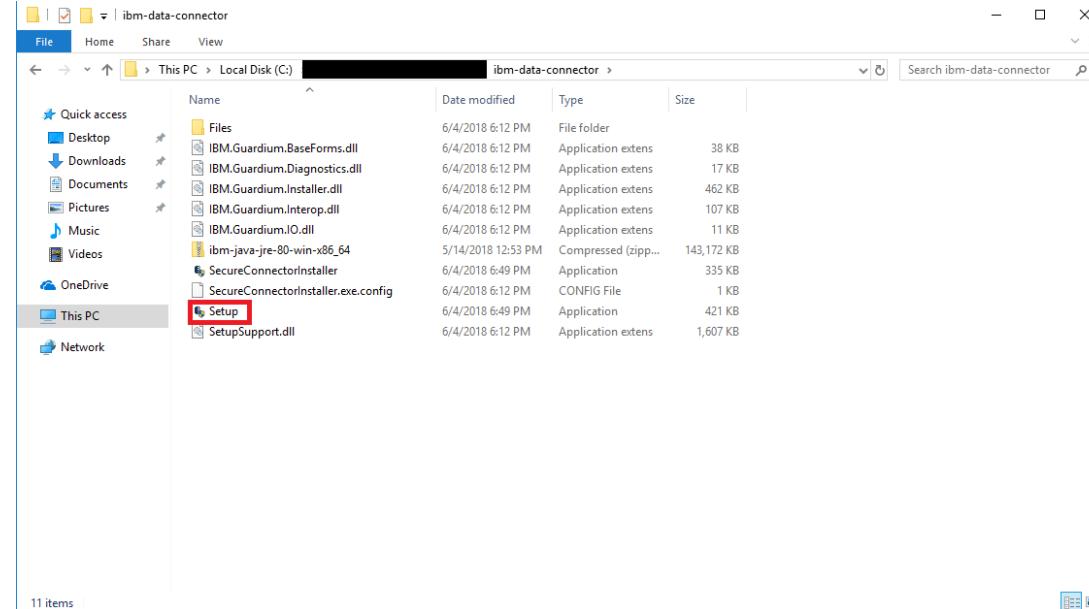
▶ Watch a video Step-by-step guide

Download data connector

Need to delegate this to someone else? [Add user](#)

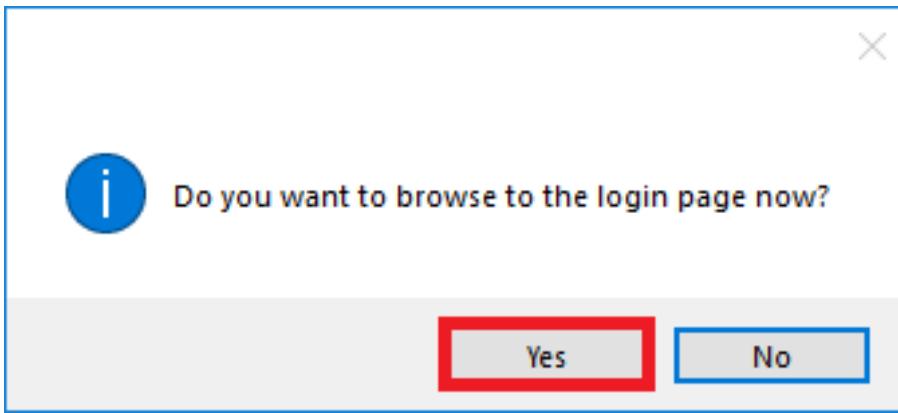
- **Video and Guide to walkthrough setting up Data Connector**
- **Download Button to get latest Data Connector Package**

Workshop: Run Setup



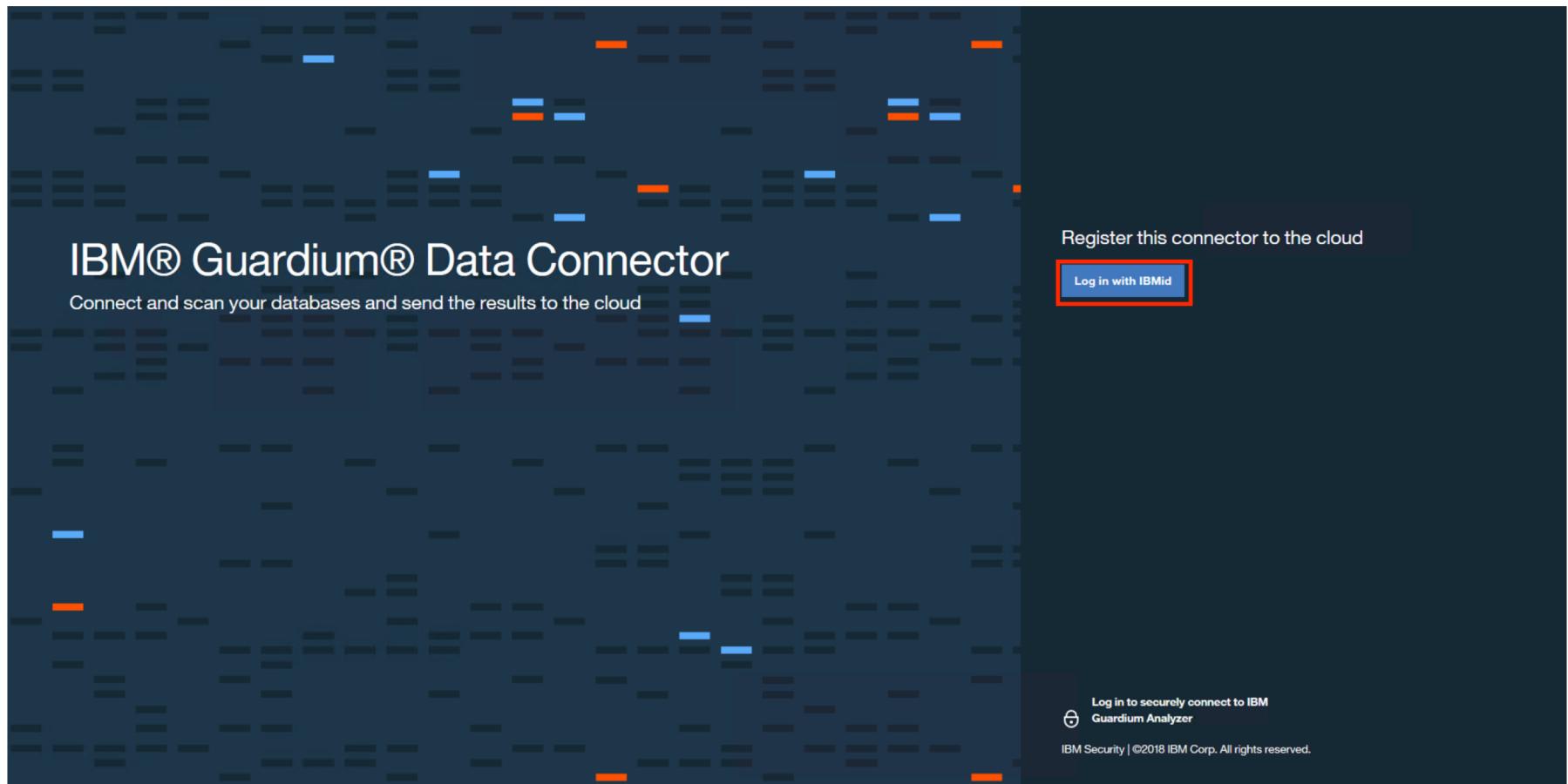
- **Unzip Data Connector package that was downloaded**
- **Run Setup.exe and run through installer**

Workshop: Navigate to Data Connector Page



- After install, popup will ask if you would like to browse to the Data Connector page

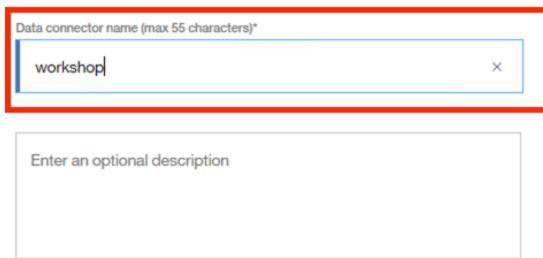
Workshop: Connector Welcome Page



Workshop: Register Connector

Register

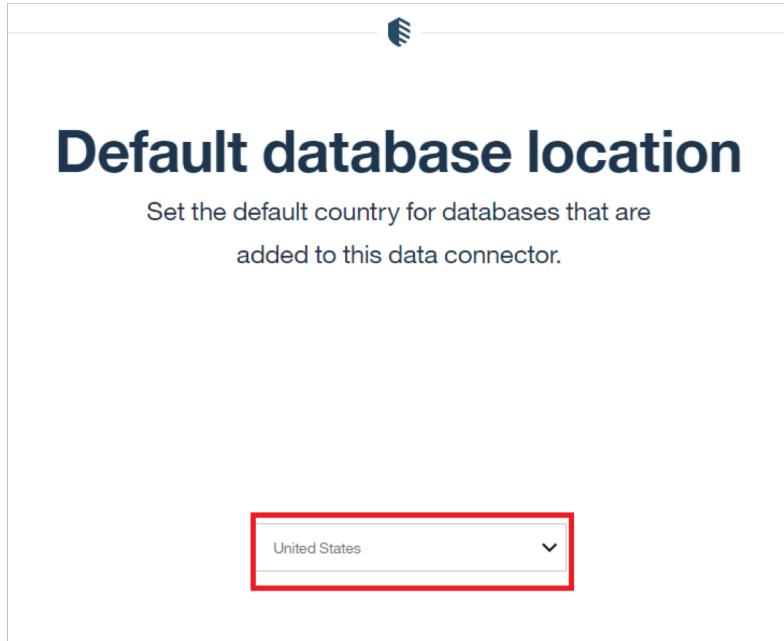
After registering your connector, you'll be ready to connect your databases to the cloud for scanning.



A screenshot of a web-based registration form. At the top, there is a label "Data connector name (max 55 characters)*" followed by a text input field containing the word "workshop". To the right of the input field is a small "x" button. Below this, there is another input field labeled "Enter an optional description" which is currently empty.

- **Fill in a unique name for this Data Connector**

Workshop: Default Location



Default database location

Set the default country for databases that are added to this data connector.

United States ▾

- Select a default Country location that scanned databases will be identified in by Analyzer (useful for Map feature on Analyzer to see where all Databases are located)

Workshop: Add Database to Scan

Add database

1 Database details

2 Scan preferences

3 Confirmation

Enter database details

First, create read-only credentials for your databases and then input them here. All displayed fields are required.

Name (max 55 characters)*
DB2 Database

Description
DB2 Database

Database type*
DB2

IP address/hostname*
[REDACTED]

Port*
50000

Database name*
SAMPLE

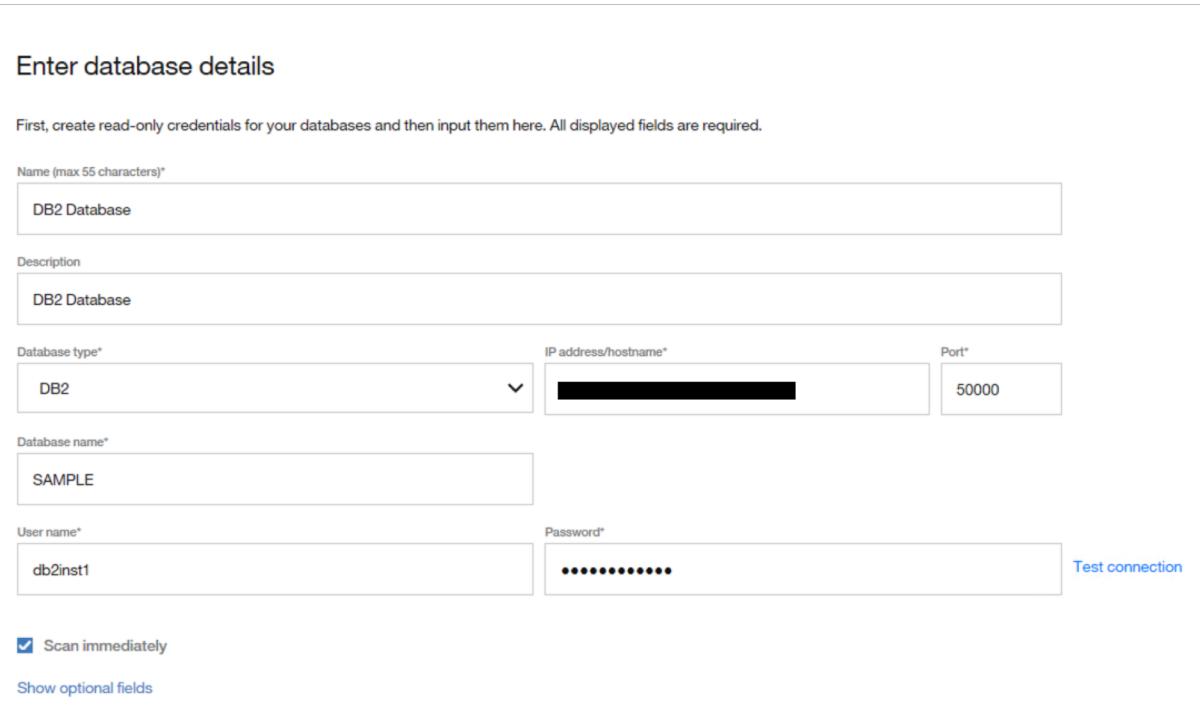
User name*
db2inst1

Password*
[REDACTED]

[Test connection](#)

Scan immediately

[Show optional fields](#)



- **Fill in Database connection information and Country (if Country is not specified, will use Default Location given on previous page)**
- **Click “Test connection” to verify Connector can connect to Database**

Workshop: Scan Time Frames

The screenshot shows the 'Scan preferences' step of a three-step wizard. On the left, a vertical navigation bar lists 'Database details' (step 1, completed with a green checkmark), 'Scan preferences' (step 2, currently selected with a blue circle and number 2), and 'Confirmation' (step 3). The main panel title is 'Scan preferences'. A descriptive text at the top says: 'Set the time frame during which scans will run. Because scans can take some time to complete, it is recommended that the time frame be at least 4 hours.' Below this are three dropdown fields: 'Database time zone' set to 'Eastern Standard Time', 'From' set to 'Wednesday 04:00', and 'To' set to 'Sunday 04:00'. Navigation buttons at the bottom include 'Step 1: Database details' with a left arrow and 'Step 3: Confirmation' with a right arrow.

Add database

Scan preferences

Set the time frame during which scans will run. Because scans can take some time to complete, it is recommended that the time frame be at least 4 hours.

Database time zone

From

To

Wednesday 04:00

Sunday 04:00

← Step 1: Database details

Step 3: Confirmation →

- Specify what time frames are allowed for Connector to scan

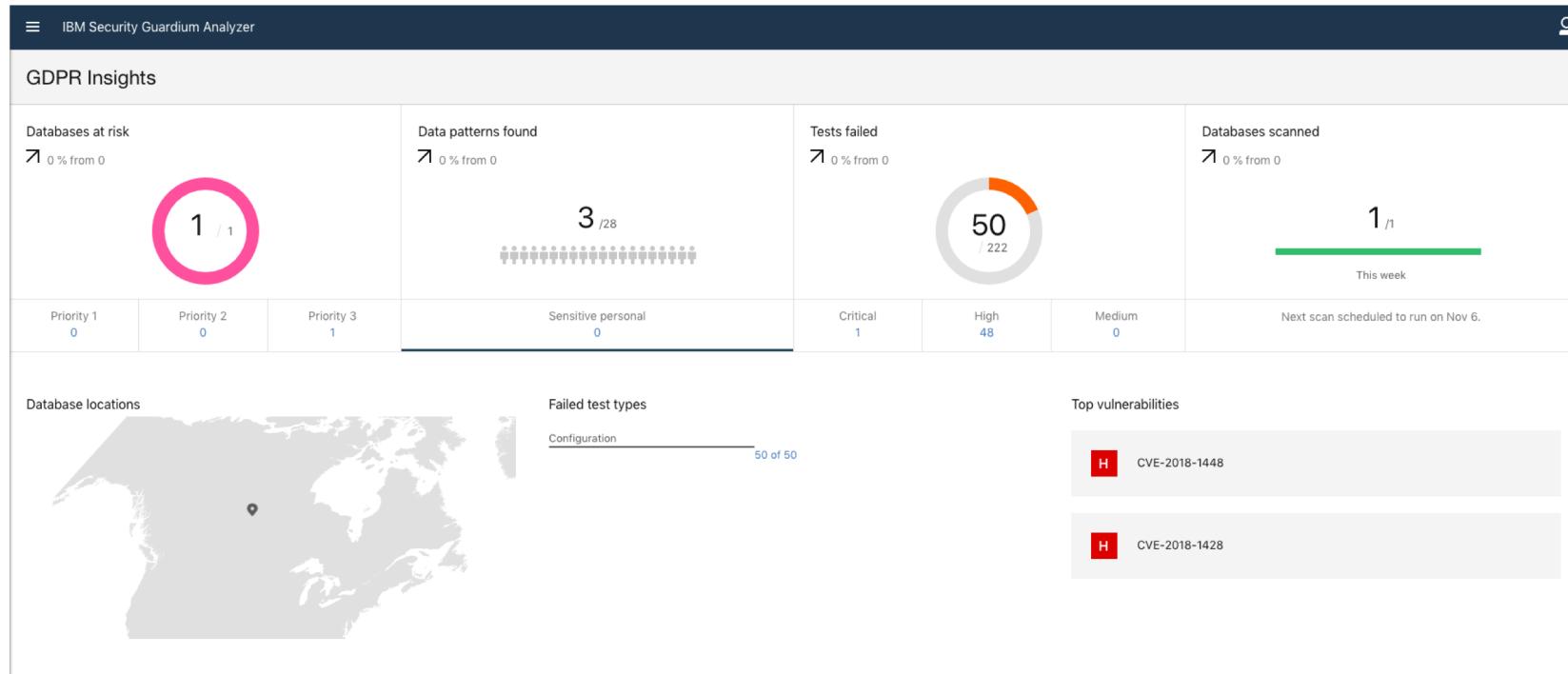
Workshop: Databases Page

The screenshot shows the 'workshop' section of the IBM Security Guardium Database Connector. At the top, there are four status indicators: 'GDPR databases' (1/1), 'Warnings' (0), 'Suspended scans' (0), and 'Average scan length' (0). Below these is a table with one row, showing a database named 'DB2 Database' located in 'Canada' with type 'DB2'. The IP address is redacted, port is 50000, service name is 'SAMPLE', and the scan status is 'Running' (highlighted with a red border). A message at the bottom states 'Risk insights from database scans will be sent to [Guardium Analyzer](#)' and a blue 'Add database' button is on the right.

Database	Line of business	Location	Type	IP address	Port	Service name	Scan status	Last scan	Next scan	
DB2 Database		Canada	DB2	[REDACTED]	50000	SAMPLE	Running	Oct 30, 2018, 7:51:09 PM	Oct 30, 2018, 7:51:01 PM	<input type="checkbox"/>

View and manage Databases on this Connector

Workshop: Back to Analyzer



- When returning to Analyzer home page, it will now show insights into the GDPR-relevant findings and risk of the added Database(s)
- Map feature will show locations of all Databases added to Connectors in your subscription

Workshop: Database Vulnerabilities

The screenshot shows the IBM Security Guardium Analyzer interface. The main left pane displays a table of vulnerabilities for a DB2 database, sorted by severity (Critical at the top). The columns include Severity, Vulnerability description, Test type, Date found, and Days open. Most entries show 'Configuration' as the test type and 'October 30, 2018' as the date found, with '0' days open. The right pane is expanded to show a detailed finding for 'Is Database Native Encryption enabled'. It includes sections for Finding (DB2 native database encryption is not enabled), Test description (This test checks if IBM DB2 database native encryption is used...), Fix recommendation (It is recommended that you enable database enc...), and a note that it was last checked on October 30. There is also a 'Mark as fixed' button and a 'Comments' section with an 'Add comment' link.

Severity	Vulnerabilities	Test type	Date found	Days open
Critical	Is Database Native Encryption enabled	Configuration	October 30, 2018	0
High	Disable database discovery DISCOVER_DB	Configuration	October 30, 2018	0
High	DISCOVER Parameter Is DISABLE Or KNOWN	Configuration	October 30, 2018	0
High	DISCOVER_INST parameter Is Disabled	Configuration	October 30, 2018	0
High	Authentication type configuration parameter	Configuration	October 30, 2018	0
High	Ensure that security plug-in support for two-part user IDs is enabled - Windows Only	Configuration	October 30, 2018	0
High	Ensure audit policies are enabled within the database	Configuration	October 30, 2018	0
High	Audit Policy CHECKING Category	Configuration	October 30, 2018	0
High	Audit Policy CONTEXT Category	Configuration	October 30, 2018	0
High	Is Audit Policy ERRORTYPE Set to A	Configuration	October 30, 2018	0
High	Audit Policy EXECUTE Category	Configuration	October 30, 2018	0
High	Audit Policy EXECUTEWITHDATA is Enabled	Configuration	October 30, 2018	0
High	Audit Policy OBJMAINT Category	Configuration	October 30, 2018	0
High	Audit Policy SECMaint Category	Configuration	October 30, 2018	0
High	Audit Policy SYSADMIN Category	Configuration	October 30, 2018	0
High	Audit Policy VALIDATE Category	Configuration	October 30, 2018	0
High	Audit On System Catalog Authority objects	Configuration	October 30, 2018	0
High	CONNECT_PROC is Defined	Configuration	October 30, 2018	0
High	Session Termination Threshold	Configuration	October 30, 2018	0
High	SSL_CIPHERSPECS is Defined	Configuration	October 30, 2018	0
High	SSL_SVR_LABEL is Defined	Configuration	October 30, 2018	0
High	SSL VERSIONS is Defined	Configuration	October 30, 2018	0

- View vulnerabilities on Databases and remediation recommendations
- Vulnerabilities are automatically sorted by highest severity

Workshop: GDPR-relevant Patterns Found

The screenshot shows the IBM Security Guardium Analyzer interface. At the top, it displays 'IBM Security Guardium Analyzer' and navigation tabs for 'Results' and 'Patterns'. A search bar is present, along with a user icon and a link to '1 of 1 scanned this week | scanned weekly'. Below the header, there are summary statistics: 'Found 3/28', 'Sensitive personal 0', 'Columns > Tables 3', and 'Data subject 0'. A detailed table follows, listing patterns categorized by classification (Personal), their details (e.g., Medical information, Name, Address), and metrics such as samples matched (e.g., 99% of 669, 83% of 1.11K), tables (e.g., 19, 17, 2), databases (e.g., 1, 1, 1), personal records (e.g., 1.39K, 1.83K, 777), and last scanned time (e.g., 7 minutes ago). The table has a light gray background with blue headers and alternating row colors.

Classification	Patterns	Data subject columns	Samples matched	Tables	Databases	Personal records	Last scanned
Personal	Medical information	0 of 27	99% of 669	19	1	1.39K	7 minutes ago
Personal	Name	0 of 36	83% of 1.11K	17	1	1.83K	7 minutes ago
Personal	Address	0 of 3	91% of 57	2	1	777	7 minutes ago

- **View regulatory Patterns identified across Databases and number of records found**
- **Drill-down into any Pattern to view specific locations**

Workshop: Ex. Name Pattern Locations

The screenshot shows the IBM Security Guardium Analyzer interface. At the top, it displays 'IBM Security Guardium Analyzer'. Below that, the title 'Patterns / Name' is shown, along with a search bar and a refresh icon. On the right, there's a message '1 of 1 scanned this week | scanned weekly' and a gear icon.

Key statistics are displayed: 'Data subject columns' (0/36), 'Samples matched' (83%), 'Databases' (1), and 'Personal records' (1.11K). To the right, it says 'Privacy: Personal' and 'Confidence level: 65%'.

The main table lists various data subjects and their details:

Data subject	Schema.Table.Column	Samples matched	Personal records	Databases	DBA name	Last scanned	Action
DB2INST1.IN_TRAY.NOTE_TEXT	100% of 3	3	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VASTRDE2.EMP1FN	100% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VPSTRDE1.RESP1FN	100% of 14	14	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.EMP.FIRSTNAME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.EMPLOYEE.FIRSTNAME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VASTRDE2.EMP2FN	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VEMP.FIRSTNAME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VPHONE.FIRSTNAME	95% of 42	42	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VSTAFAC2.FIRSTNAME	95% of 73	73	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VPROJRE1.FIRSTNAME	90% of 20	20	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VFORPLA.LASTNAME	89% of 74	74	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	
DB2INST1.VASTRDE1.FIRSTNAME	88% of 11	11	DB2 Database	Analyzer Workshop	7 minutes ago	<input type="checkbox"/>	

- Drilled down into Name Pattern, for example
- View will include Schema, Table, Database, and Database owner (User who added the database) for each regulatory record found

Workshop: Data Connectors Page

The screenshot shows the 'Data connectors' page of the IBM Security Guardium Analyzer. At the top, it displays 'Total' 1 connector and 'Warnings' 0. Below this, there's a search bar with a magnifying glass icon and a 'Download connector' button. A single connector entry is listed: 'workshop', last contacted on October 30, 2018, containing 1 Database and Version 1.0.229. The page also features a navigation bar with links like 'IBM Security Guardium Analyzer', 'Data connectors', 'Scanning weekly', and a user profile icon.

- **Connectors page to view all Connectors installed in the subscription, as well as a Download button to download Connectors in the future**

Workshop: Settings Page

IBM Security Guardium Analyzer

Settings

Account

Notifications

Manage patterns

Scan frequency

Manage users

IBMid account

Name: Analyzer Workshop

IBMid: analyzer_workshop@mailinator.com

Access your IBM account from [IBMid](#) profile

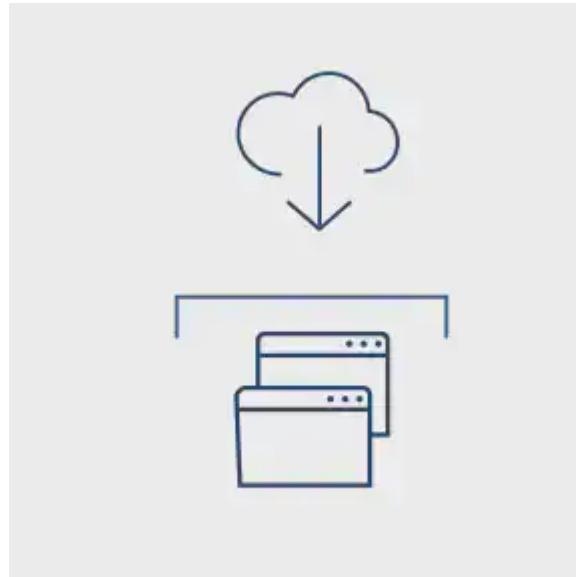
- **Change email notifications setting**
- **(Pro Accounts only) Add Patterns used to find regulatory data**
- **Adjust Scan Frequency**
- **Manage Users in Subscription**

Maintenance



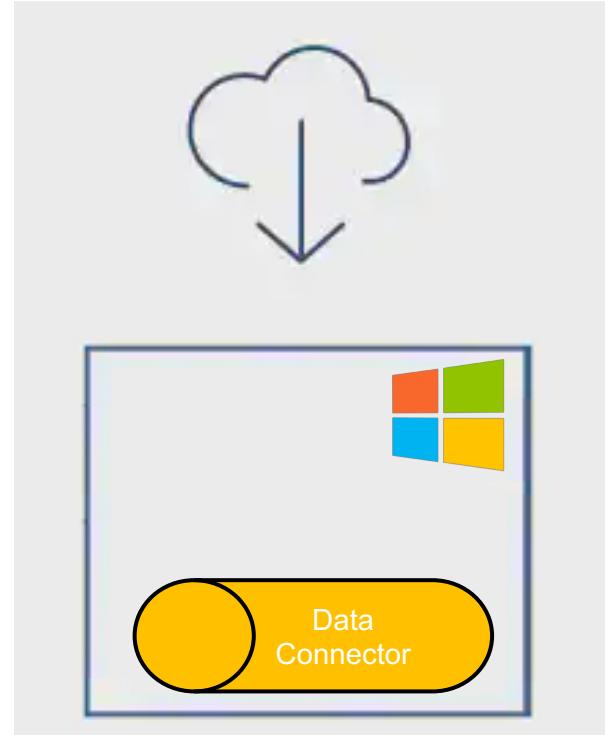
Maintenance: Cloud

- **SaaS Offering**
 - **No Patching/Updating by Users**
 - **Continuous Delivery**
 - **Always using Latest Version**



Maintenance: Data Connector

- **Windows Agent**
 - **Automatic Updates (in Background)**
 - **Regular Release of Data Connector**



Resources



Resources

- [Guardium Analyzer marketplace page](#)
 - View capabilities and subscription options
- [Free trial](#)
- [Guardium Analyzer Data sheet](#)
- [Overview Guardium Analyzer demo video](#)
- Product tutorial series:
 - [Getting started with the Data Connector](#)
 - [Adding users to Guardium Analyzer](#)
 - More to follow!
- [Getting Started Guide/FAQ](#)
- [Webcast replay:](#)
After the GDPR Enforcement Date: Myths, Realities, and What to Do Now
- Webcast: “[Analyzing Your GDPR Readiness: The Core Data Protection Capabilities You Need](#)”

IBM Security Guardium Analyzer

Overview Details Pricing Resources FAQ Start your free trial

IBM Security Guardium Analyzer

Efficiently find regulated data, understand data and database exposures, and act to address issues and minimize risk.

Start your free trial Watch the video (04:39)

Data Discovery, Classification & Vulnerability Scans

This software-as-a-service offering helps you efficiently identify risk associated with personal and sensitive personal data (PII, PHI, PCI, etc.) that falls under regulations such as the E.U.'s GDPR, PCI DSS, HIPAA and other privacy mandates. The service applies next-generation data classification, as well as vulnerability scanning, to uncover privacy risks associated with such data in cloud-based and on-prem databases. It then analyzes risk according to the classification and recommends corrective actions to mitigate the database that is much more likely to fail audit.

Let's talk



Devan Shah
Software Developer
IBM Data Security
devans@ca.ibm.com



Larry Lindsay
Senior Development Manager
IBM Security and Accessibility
llindsay@ca.ibm.com

Questions?



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.

