



# IBM Data and Application Risk Scanner

Version: 1.1.0

Date: 01/16/2017

IBM Guardium - Property of IBM. © Copyright IBM Corp. 2017. U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, and ibm.com® are trademarks or registered 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" ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml))

**Contents**

- IBM Data and Application Risk Scanner..... 1
  - Introduction ..... 3
  - Description of the Application ..... 3
  - Target Audience ..... 3
  - Installation and Configuration ..... 4
    - Pre-Requisites ..... 4
    - Installation ..... 4
    - Configuration ..... 4
  - Un-installing the Application ..... 5
- Using the Application ..... 6
  - Types of GDPR data..... 6
  - Risk types ..... 6
  - Timeout..... 6
  - Log-in page..... 7
  - Assets Discovered tab ..... 9
  - Applications tab ..... 10
  - Databases tab..... 11
  - After clicking the GDPR scan button ..... 12
  - Results after scan has run ..... 13
- Additional information..... 14

## ***Introduction***

Use this document to install and configure the IBM Data and Application Risk Scanner for QRadar.

## ***Description of the Application***

Data privacy and security are the most pressing concerns that any organization must face. Previously within the European Union each country required different levels of compliance, the newly announced General Data Protection Regulation (GDPR) expands and standardizes data protection rules across the whole European Union.

Use the IBM Data and Application Risk Scanner application for QRadar to get a preview of the risk associated with applications and databases in your environment. For databases, this new QRadar application performs a lightweight scan of your Oracle databases searching for GDPR type of data. Only one data source will be scanned at a time. The new QRadar application also calculates an estimate of the vulnerability and risk distribution associated with applications and databases in your environment.

The application includes links for additional information on Guardium and IBM Application Security on Cloud, and how to fully protect your database and application assets.

## ***Target Audience***

- QRadar clients who do not have Guardium, or have limited deployment of Guardium.
- QRadar clients who have not used IBM's AppScan or Application Security on Cloud.
- The user of this application is a QRadar admin or Security Analyst with access to QRadar.

## ***Installation and Configuration***

### **Pre-Requisites**

A functional and licensed installation of QRadar SIEM version 7.2.7 or higher is required.

### **Installation**

1. Download the IBM Data and Application Risk Scanner from the IBM Security App Exchange Portal (<https://exchange.xforce.ibmcloud.com/hub>).
2. Login as an administrative user.
3. Go to the Admin tab and click Extensions Management in the System Configuration section.
4. Click Add, choose the application file downloaded and then click Add again.
5. Refresh the page to see IBM Data and Application Risk Scanner tab.

### **Configuration**

1. The user of IBM Data and Application Risk Scanner must provide the data source details for connecting to the Oracle database they wish to scan for GDPR type of data. The data source details involve database type, user name, password, hostname/IP, port number, service name and connection property.
2. The user of IBM Data and Application Risk Scanner should create a role and grant select any table and any dictionary to this role. Then grant this role to the user that is going to execute classification.

#### **Example:**

```
Create role g_classifier;  
grant select any table to g_classifier;  
grant select any dictionary to g_classifier;  
  
create user g_classify_user identified by guardium;  
grant connect, g_classifier to g_classify_user;  
alter user g_classify_user default role all;
```

## ***Un-installing the Application***

1. Login as an administrative user.
2. Go to the Admin tab and click the Extensions Management icon in the System Configuration Section.
3. Select the IBM Data and Application Risk Scanner and click Uninstall.

## ***Using the Application***

Use the IBM Data and Application Risk Scanner application for QRadar to get a preview of the GDPR risk associated with applications and databases in your environment. For databases, this new QRadar application performs a lightweight scan of your Oracle databases searching for GDPR type of data. Only one data source will be scanned at a time. The new QRadar application also calculates an estimate of the vulnerability and risk distribution associated with applications and databases in your environment.

### **Types of GDPR data**

The application performs a lightweight scan of the database looking for GDPR type of data using a variety of techniques including meta-data search and pre-defined regular expressions. Examples of GDPR types of data include: international and U.S. phone numbers, international passport numbers, and email addresses (@).

### **Risk types**

For databases, the Risk types are High, Medium and Unknown.

When the Risk type is High, this is indicative of GDPR data found.

When the Risk type is Medium, this is indicative of GDPR data not found or the scan has timed-out.

When the Risk type is Unknown, this is indicative of a network error or database exception interfering with the scan or the GDPR scan has not run yet.

For applications, the Risk types are High, Medium and Low.

### **Timeout**

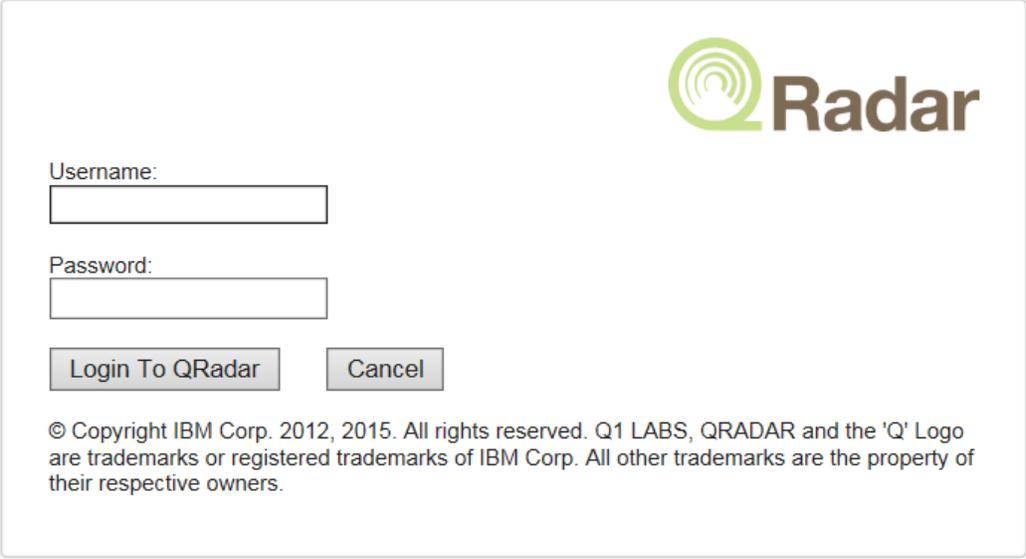
When initiating a scan of GDPR type of data for a given database, the application will only do a partial scan of that database. This means that there is an upper limit on the number of tables scanned and on the number of rows considered for each table. The scan returns immediately after the first instance of GDPR type of data has been discovered. There is also an overall upper limit of 20 minutes on the time the scan takes.

If no assets are found during the scan, a message will display: Scan completed. No asset found.

This application scans for QRadar log activities every 10 minutes looking for databases and applications that are registered with QRadar.

## Log-in page

Log-in to QRadar.



The image shows a login page for QRadar. In the top right corner, there is the QRadar logo, which consists of a green circular icon with concentric lines and the word "QRadar" in a bold, dark font. Below the logo, there are two input fields: one for "Username:" and one for "Password:". Below these fields are two buttons: "Login To QRadar" and "Cancel". At the bottom of the page, there is a copyright notice: "© Copyright IBM Corp. 2012, 2015. All rights reserved. Q1 LABS, QRADAR and the 'Q' Logo are trademarks or registered trademarks of IBM Corp. All other trademarks are the property of their respective owners."

Then select the Data and Applications Risk (Data/App Risk) tab.

If this is the first use of the IBM Data and Application Risk Scanner application, then the Service Token Setup screen below will appear. The IBM Data and Application Risk Scanner needs an admin-level service token to access REST endpoints and perform Ariel searches for this data. Print out the screen below which makes it easier to follow the steps to setup the service token. The Service Token Setup screen can also be retrieved from the Admin tab, Plug-ins, Data and Applications Risk, Token Configuration.

## Data and Application Risk



### Token Configuration



## Data and Application Risk Scanner - Service Token Setup

Current Service Token: ✓ a953dfe4-8630-43c7-b121-426e394eb400

Configure

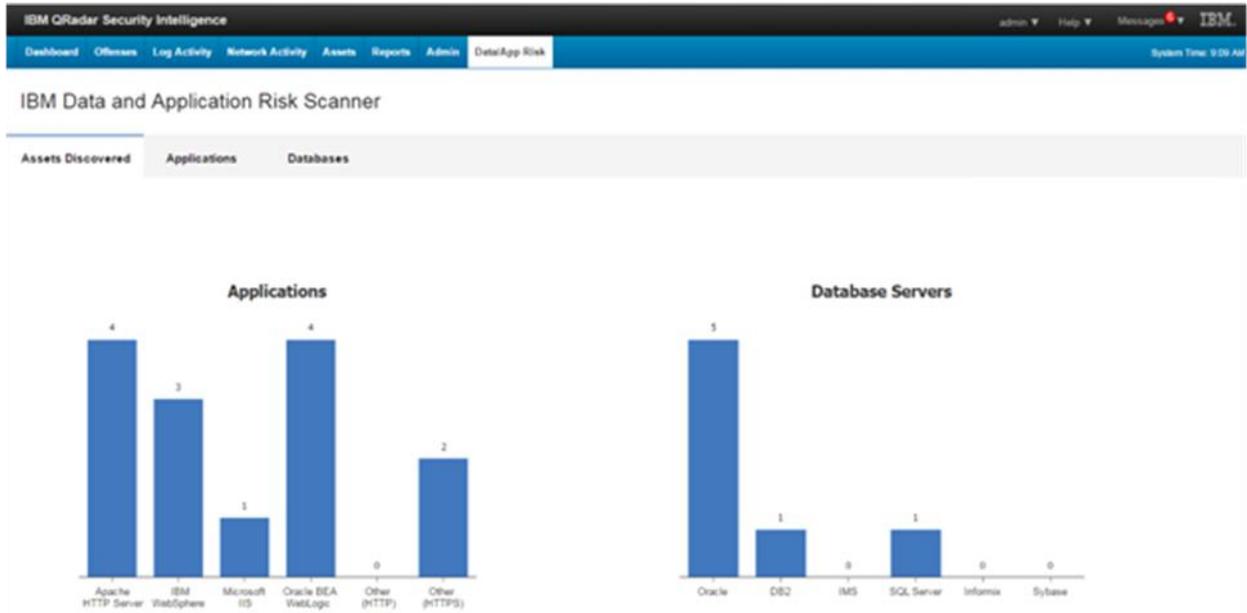
The **IBM Data and Application Risk Scanner** needs an admin-level service token to access REST endpoints and perform Ariel searches for this data.

Steps to setup the service token are:

1. Navigate to the admin tab.
2. Look for **Authorized Services** icon and open.
3. Create a token for this application. An **admin-level** token is required. Perpetual timeout is best for uninterrupted data collection.
4. Copy the token string, for example: 12345678-Dont-Use-Me-TestToken123456.
5. Navigate back to this configuration page.
6. Click configure, paste your service token in the pop-up, and click submit.
7. **Wait a few minutes.** The **IBM Data and Application Risk Scanner** sets up the initial database and host information schemas from initial API calls and Ariel searches. Daemon threads start in the background to collect information about your deployment.
8. Refresh the **IBM Data and Application Risk Scanner** page.

## Assets Discovered tab

This shows the Assets discovered - applications and database servers - in the scan.



## Applications tab

From the Applications tab, review the discovered application assets. The applications have been assigned a default risk rating that is representative of typical risk rating distributions. IBM's Application Security on Cloud can be used to scan these applications to determine their true risk rating.

The screenshot shows the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Data/App Risk'. The main content area is titled 'IBM Data and Application Risk Scanner' and has three tabs: 'Assets Discovered', 'Applications', and 'Databases'. The 'Applications' tab is active, showing a list of discovered applications. A sidebar on the left provides information about application protection and features. The main table lists applications with their risk ratings and details.

**Complete your Application Protection with Application Security on Cloud**

This demo shows basic application discovery. IBM Application Security on Cloud supports many other features including:

- ✓ Application Inventory Management
- ✓ Application Risk Management
- ✓ Static, Dynamic and Mobile Analysis
- Cross Site Scripting & SQL Injection
- OWASP Top 10
- SANS Top 25
- Many others

[Help me secure my applications](#)

[User instructions](#)

The applications below have been assigned a default risk rating that is representative of typical risk rating distributions. IBM's Application Security on Cloud can scan these applications to determine their true risk rating.

Filter   Show only high risk

Risk	Application	Application Details
High	https://thome.acme.com:443 - IT Hub	Apache HTTP Server
High	https://103.2.54.17:443	Apache HTTP Server
High	https://172.54.52.246:443	IBM WebSphere
High	https://22.80.47.145:443 - QA Resources	Oracle BEA WebLogic
High	https://66.89.131.40:999	Other(HTTPS)
High	https://77.32.81.20:4444	Other(HTTPS)
High	https://humanresources.acme.com:443 - Human Resources	Oracle BEA WebLogic

## Databases tab

Go to the Databases tab.

Select a database server and click the GDPR scan button to scan the database server.

The screenshot shows the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Data/App Risk'. The 'Data/App Risk' section is active, displaying the 'IBM Data and Application Risk Scanner' page. The 'Databases' tab is selected, showing a list of Oracle databases. A 'GDPR scan' button is visible next to the list. On the left, there is a section titled 'Complete your Data Protection with Guardium' with a list of features, some of which are checked.

IBM QRadar Security Intelligence

admin Help Messages 6 System Time: 11:51

Dashboard Offenses Log Activity Network Activity Assets Reports Admin Data/App Risk

### IBM Data and Application Risk Scanner

Assets Discovered Applications **Databases**

**Complete your Data Protection with Guardium**

This demo shows the data risk scanner, but Guardium has many other features including:

- ✓ Advanced Data Classification
- ✓ Vulnerability Assessment
- ✓ Data Protection and Compliance
- Activity Monitoring
- Real-time Alerting
- Compliance Reporting
- Blocking and Dynamic Masking
- ✓ GDPR Compliance
- ✓ and much more

[Help me protect my data](#)

[User instructions](#)

Select a database server and click the GDPR scan button

Oracle databases

Filter  Show only high risk **GDPR scan**

Risk	Database Server	Service name	Table name
Unknown	gauto-db1.guard.swg.usma.ibm.com		
Unknown	qsw2k3x64fig.guard.swg.usma.ibm.com		
Unknown	racvm12va1.guard.swg.usma.ibm.com		
Unknown	rh6x64t1-va.guard.swg.usma.ibm.com		
Unknown	su11u1x64t4-va.guard.swg.usma.ibm.com		

## After clicking the GDPR scan button

Fill in the database connection parameters: user name; password; port number; service name; and, then click GDPR scan.

The screenshot displays the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Data/App Risk'. The main content area is titled 'IBM Data and Application Risk Scanner' and shows a list of databases under the 'Databases' tab. A modal dialog box titled 'Scan database for GDPR data' is open, prompting the user to enter connection parameters. The dialog includes the following fields:

- \* Database type: Oracle (Service Name)
- \* User name: system
- \* Password: .....
- \* Host name/IP: gauto-db1.guard.swg.usma.ibm.com
- \* Port number: 1521
- \* Service name: on2pgaut
- Connection property: Connection property

Buttons for 'Scan' and 'Close' are located at the bottom of the dialog. In the background, a table lists databases with columns for 'Risk' and 'Database name'. The 'SCOTT.EMPLOYEES\_DEMO' table is highlighted. A 'GDPR scan' button is visible in the top right of the dialog area.

## Results after scan has run

When the Risk type is High, this is indicative of GDPR data found.

Click the Print button to print the scan results.

The screenshot displays the IBM QRadar Security Intelligence interface. The top navigation bar includes 'Dashboard', 'Offenses', 'Log Activity', 'Network Activity', 'Assets', 'Reports', 'Admin', and 'Data/App Risk'. The main content area is titled 'IBM Data and Application Risk Scanner' and shows a 'Databases' tab. A 'Scan Result' dialog box is open, displaying the following information:

Risk	Database Server	Table name
High	gauto-db1.guard.s	SCOTT.EMPLOYEES_DEMO
Unknown	db-win2k8qrw01.g	
Unknown	racvm12va1.guard	
Unknown	rh6x64t1-va.guard.swg.usma.ibm.com	
Unknown	su11u1x64t4-va.guard.swg.usma.ibm.com	

The dialog box also contains the text: 'Scan completed. GDPR data found. High risk is assigned. This is only a partial database scan of the GDPR data types. Use the full Guardium solution for an in-depth scan and complete analysis. The full Guardium solution, Advanced Data Classification has many more tests available with detailed recommendations, customizable options, and test-tuning features.'

The results shown are only a highly-focused sample of Data and Application Risk in the databases scanned.

The full product (see link at Advanced Data Classification) has many more tests available with detailed recommendations, customizable options, and test-tuning features.

## ***Additional information***

### Advanced Data Classification

[https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=sw-infomgt&S\\_PKG=500010163&S\\_TACT=C406001W&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US](https://www-01.ibm.com/marketing/iwm/iwm/web/signup.do?source=sw-infomgt&S_PKG=500010163&S_TACT=C406001W&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US)

### Vulnerability Assessment

<http://www-03.ibm.com/software/products/en/security-guardium-vulnerability-assessment>

### Data Protection and Compliance

<http://www-03.ibm.com/software/products/en/guardium-data-protection-for-databases>  
Activity monitoring; Real-time alerting; Compliance reporting; Blocking and dynamic masking

### GDPR compliance

<https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&referrer=&eventid=1245241&sessionid=1&key=E604B82C5D87DD5BC6293F300D87F0DD&regTag=&sourcepage=register>

<https://event.on24.com/eventRegistration/EventLobbyServlet?target=reg20.jsp&partnerref=secintel&eventid=1241814&sessionid=1&key=D96E412ACA19C50680E7684760C70FFA&regTag=&sourcepage=register>

### Data security and protection

<http://www-03.ibm.com/software/products/en/category/data-security>