IBM Security Guardium Analyzer

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

Highlights

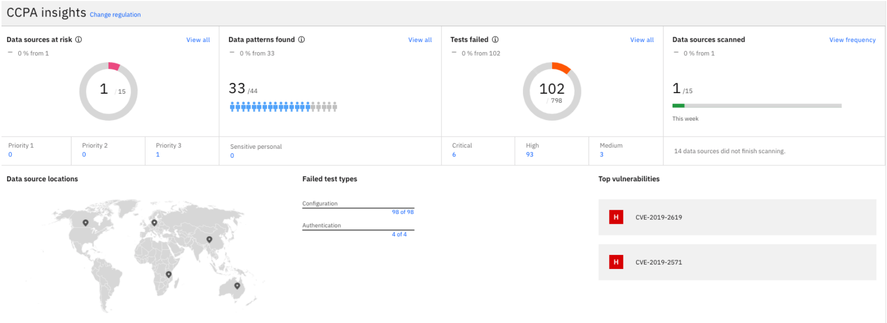
- Evaluate security and compliance risk associated with regulated data
- Find regulated personal and sensitive personal data
- Discover data across on-premises and cloud databases
- Scan for data source vulnerabilities
- Leverage next-generation data classification capabilities
- Get prioritized risk scoring and remediation recommendations

In today's digital world, data is the most complex and critical asset. It enables organizations to create greater value for its clients, making it not only crucial to the business, but also a high value target for malicious actors.

Meanwhile, the amount of data continues to grow, and in parallel, new data privacy regulations, such as the California Consumer Privacy Act, EU's General Data Protection Regulation (CCPA), Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD), and the updated New York State Cybersecurity Requirements for Financial Service Companies (23 NYCRR 500), combined with existing compliance mandates (HIPAA, PCI DSS, etc.) can create an increasingly nuanced and stringent regulatory environment.

Many different business areas inside an organization are impacted by regulatory and data privacy requirements—from Data Privacy Officers, Chief Information Security Officers, Data Risk Officers to compliance managers, data managers, IT managers, and more—and all of these groups are trying to determine how they can efficiently manage regulatory requirements, and understand their risk, while helping the business succeed.

IBM® Security Guardium® Analyzer, a software-as-a-service offering, helps users efficiently evaluate database security and compliance risk. It can support your risk assessments for GDPR, PCI, HIPAA, CCPA, LGPD and other regulations by helping identify databases most likely to be at risk of failing a regulatory audit by using next-generation data classification techniques, vulnerability scanning, and a proprietary risk-scoring algorithm. The risk scoring prioritizes the on-premises and cloud databases containing at-risk personal and sensitive personal data, helping organizations gain insights into where they may need to focus their data security and prioritize their risk remediation efforts.



CCPA insights

Data sources at risk
— 0 % from 1
1 / 15
Priority 1: 0
Priority 2: 0
Priority 3: 1

Data patterns found
— 0 % from 33
33 /44
Sensitive personal: 0

Tests failed
— 0 % from 102
102 / 798
Critical: 6
High: 93
Medium: 3

Data sources scanned
— 0 % from 1
1 /15
This week
14 data sources did not finish scanning.

Data source locations

Failed test types
Configuration: 98 of 98
Authentication: 4 of 4

Top vulnerabilities
H CVE-2019-2619
H CVE-2019-2571

The interactive Guardium Analyzer dashboard displays risk information and other insights. Users click to drill down into more detail.

Guardium Analyzer is comprised of two components: The Guardium Analyzer Data Connector and the Guardium Analyzer Dashboard. The Data Connector is deployed within the client's firewall and scans the data sources to generate classification and vulnerability insights, which are displayed in the dashboard. When using Guardium Analyzer, it is the results of the scanning that are sent to and viewed from the cloud: sensitive data is not moved and remains on-premises. The service is hosted in IBM data centers.

Find Regulated Personal and Sensitive Personal Data

Guardium Analyzer helps organizations discover and classify personal and sensitive personal data using a next-generation classification engine and pre-built data patterns. Personal information includes data such as name, address, email address, etc. Sensitive personal information includes data such as gender, sexual orientation, religion, race or ethnicity, and many others etc. (for a complete list, please see the product documentation).

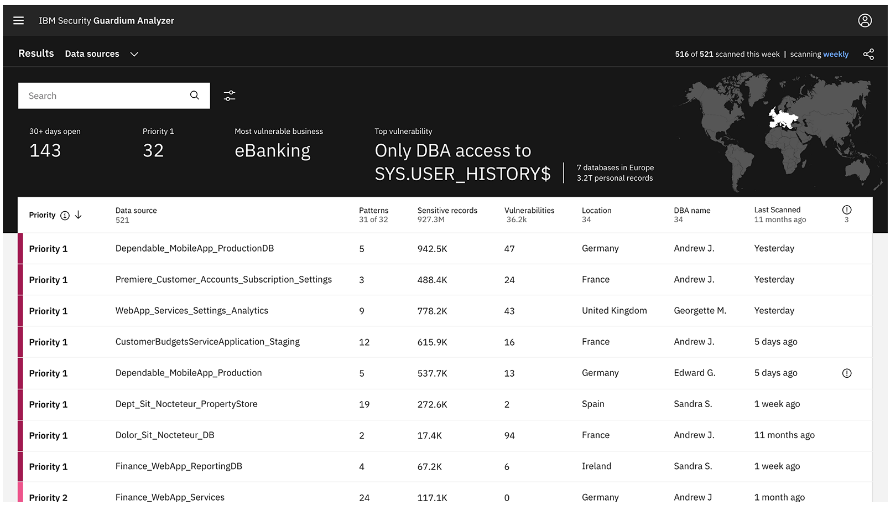
The classification engine scans and analyzes the actual text in on-premises and cloud databases to find and classify such data. Users can leverage IBM's pre-built data patterns, user-provided data patterns, or a combination of both. The Guardium Analyzer data classification engine goes beyond searching metadata and using regular expressions, randomly sampling up to 2000 rows for greater accuracy when identifying personal and sensitive personal data.

Data patterns for personal and sensitive personal data, sometimes also referred to as PII and 'special category' data, are provided it a wide variety of languages, including (but not limited to): English, French, Spanish, German, Brazilian Portuguese, Dutch, Japanese (kanji and hiragana), Danish, Finnish, and more.

Uncover Risk

Open vulnerabilities in databases can increase levels of exposure and risk—especially if those databases contain regulated data. Guardium Analyzer efficiently scans for a multitude of database vulnerabilities such as CVEs or missing patches, that might be exploited and need attention.

Specialized risk-scoring techniques are applied based on the amount of personal and sensitive personal data found in each data source, and the number of vulnerabilities found in each data source, to help users identify the level of risk associated with each database. Guardium Analyzer provides a prioritized list of database risks that users can view to help understand the urgency of their exposures, so that they can start thinking through and planning remediation steps to protect the data.


IBM Security **Guardium Analyzer**
Results **Data sources**
516 of **521** scanned this week | scanning weekly
Search

30+ days open
143

Priority 1
32

Most vulnerable business
eBanking

Top vulnerability
Only DBA access to SYS.USER_HISTORY$

7 databases in Europe
3.2T personal records

Priority ⓘ ↓	Data source 521	Patterns 31 of 32	Sensitive records 927.3M	Vulnerabilities 36.2k	Location 34	DBA name 34	Last Scanned 11 months ago	ⓘ 3
Priority 1	Dependable_MobileApp_ProductionDB	5	942.5K	47	Germany	Andrew J.	Yesterday	
Priority 1	Premiere_Customer_Accounts_Subscription_Settings	3	488.4K	24	France	Andrew J.	Yesterday	
Priority 1	WebApp_Services_Settings_Analytics	9	778.2K	43	United Kingdom	Georgette M.	Yesterday	
Priority 1	CustomerBudgetsServiceApplication_Staging	12	615.9K	16	France	Andrew J.	5 days ago	
Priority 1	Dependable_MobileApp_Production	5	537.7K	13	Germany	Edward G.	5 days ago	ⓘ
Priority 1	Dept_Sit_Nocteteur_PropertyStore	19	272.6K	2	Spain	Sandra S.	1 week ago	
Priority 1	Dolor_Sit_Nocteteur_DB	2	17.4K	94	France	Andrew J.	11 months ago	
Priority 1	Finance_WebApp_ReportingDB	4	67.2K	6	Ireland	Sandra S.	1 week ago	
Priority 2	Finance_WebApp_Services	24	117.1K	0	Germany	Andrew J	1 month ago	

Drill down from the summary dashboard to see details that show data sources that may be at risk.

Guardium Analyzer results and insights may be used to feed other applications, to enrich their risk insights and data protection activities. Users can filter the list by parameters such as risk severity (Priority 1, 2, 3), business threat, location, and data patterns.

Supports a wide variety of cloud and on-premises databases

Guardium Analyzer can scan the following data sources both on-premises and on cloud including:

- IBM Db2
- IBM Db2 for i
- IBM Db2 for zLinux
- Informix
- Microsoft SQL Server
- MySQL and MySQL Community Edition
- Oracle
- AWS RDS for Oracle
- IBM Integrated Analytics System (IIAS) (also known as Netezza Sailfish)

Supported data sources are frequently added. Please see here for a current list of data sources supported.

Clients can connect to multiple databases simultaneously, and can set up database scans on a recurring basis, or set a specific scan window for each database, allowing assessments to run at the best times for the business.

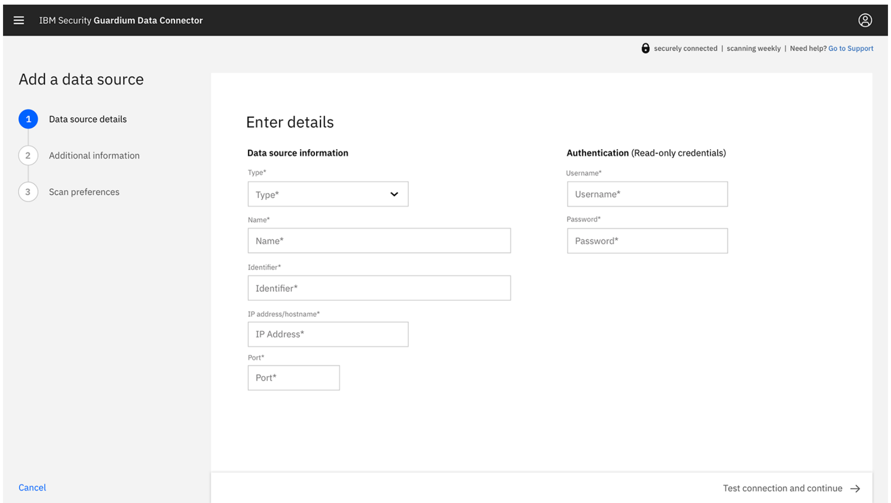
As part of the connection and scanning process, encryption techniques are applied to protect the data. No personal data is uploaded to the cloud.

Use Guardium Analyzer insights in other applications

IT Teams, SOC analysts and Guardium administrators can use Guardium Analyzer insights to enrich their applications. Guardium Analyzer’s open APIs are designed to allow other entitled applications to make calls to get database results, vulnerability results, and classification results. Alternatively, users can create a CSV file of the Guardium Analyzer classification results which may then be imported into other applications, such as IBM Security Guardium Data Protection or IBM Security Data Risk Manager.

Get reports for auditors

After scanning data sources and gaining risk insights and the details behind them, users may create an audit-ready PDF report that captures Guardium Analyzer's findings and the supporting details for a specified set of data sources, as well as descriptive information that will be needed for an auditor to understand the report.



IBM Security **Guardium Data Connector**

securely connected | scanning weekly | Need help? Go to Support

Add a data source

1 Data source details
2 Additional information
3 Scan preferences

Enter details

Data source information

Type*: Type*
Name*: Name*
Identifier*: Identifier*
IP address/hostname*: IP Address*
Port*: Port*

Authentication (Read-only credentials)

Username*: Username*
Password*: Password*

Cancel

Test connection and continue →

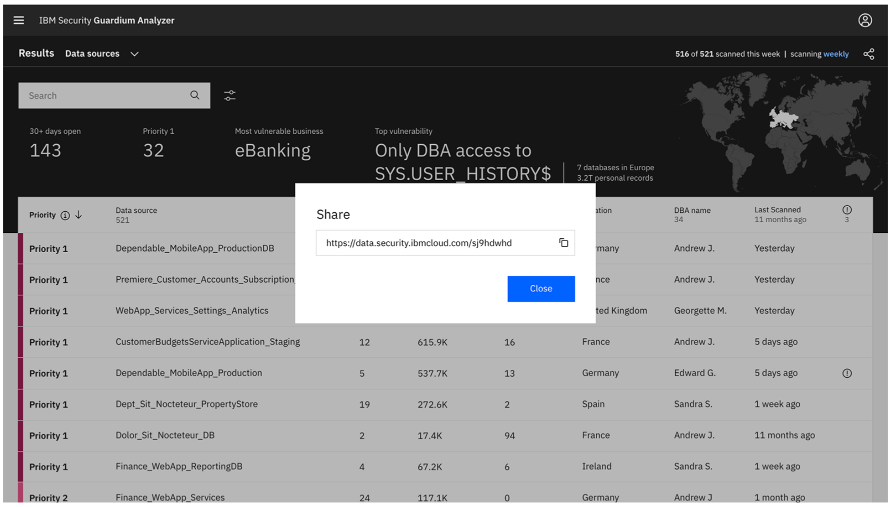
To create reports for auditors select the source or sources to report on.

For internal audit preparation, the report can be viewed online through Guardium Analyzer, shared through a link, exported into a PDF or CSV file. For external reports, users may include or exclude remediation recommendations and team comments, and can mask any personal data that appears in report.

Streamline the next steps

Guardium Analyzer helps different types of users within organizations collaborate to remediate vulnerabilities or to prepare for an audit. The technology helps compliance managers, data managers, and IT managers get the information and details they need to drive focused action around compliance and security activities.

From the screen showing the prioritized risk details and remediation recommendations, users can generate a link that can be sent to authorized data managers. Guardium Analyzer can send each data manager a prioritized list of the databases they own. Alternatively, the data manager may log in or use the link to see a list of their databases only. In this way, separation of duties is supported.



IBM Security **Guardium Analyzer**
Results **Data sources**
Search

516 of **521** scanned this week | scanning **weekly**

30+ days open
143

Priority 1
32

Most vulnerable business
eBanking

Top vulnerability
Only DBA access to SYS.USER_HISTORY$

7 databases in Europe
3.2T personal records

Share

https://data.security.ibmcloud.com/sj9hdwhd

Priority ⓘ ↓	Data source 521				ation	DBA name 34	Last Scanned 11 months ago	ⓘ 3
Priority 1	Dependable_MobileApp_ProductionDB				rmany	Andrew J.	Yesterday	
Priority 1	Premiere_Customer_Accounts_Subscription				nce	Andrew J.	Yesterday	
Priority 1	WebApp_Services_Settings_Analytics				ted Kingdom	Georgette M.	Yesterday	
Priority 1	CustomerBudgetsServiceApplication_Staging	12	615.9K	16	France	Andrew J.	5 days ago	
Priority 1	Dependable_MobileApp_Production	5	537.7K	13	Germany	Edward G.	5 days ago	ⓘ
Priority 1	Dept_Sit_Nocteteur_PropertyStore	19	272.6K	2	Spain	Sandra S.	1 week ago	
Priority 1	Dolor_Sit_Nocteteur_DB	2	17.4K	94	France	Andrew J.	11 months ago	
Priority 1	Finance_WebApp_ReportingDB	4	67.2K	6	Ireland	Sandra S.	1 week ago	
Priority 2	Finance_WebApp_Services	24	117.1K	0	Germany	Andrew J	1 month ago	

The "Share" button helps support collaboration across teams and users.

Database managers can select a specific database and view a list of the vulnerabilities found, and then click for details about the vulnerability and see suggestions for how to effectively remediate it. From there, database managers can start taking steps to reduce risk and exposure.

Why IBM?

IBM Security Guardium Analyzer is part of the IBM Security Guardium portfolio. The Guardium portfolio empowers organizations to meet critical data protection needs by delivering comprehensive visibility, actionable insights and real-time controls throughout the data protection journey. With IBM Guardium organizations have the tools to achieve smarter data protection by leveraging discovery & classification, vulnerability & risk assessments, real-time monitoring & alerting, encryption, and advanced analytics.

For more information

To learn more about this offering, contact your IBM representative or IBM Business Partner, or visit: https://www.ibm.com/marketplace/guardium-analyzer

LEGAL DISCLAIMER

Please note, clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation. Screen captures may not reflect the current released product.

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