IBM Security Guardium Analyzer

Highlights

- Assess security & compliance risk associated with GDPR data
- Find GDPR data across on-premises and cloud databases
- Scan for database vulnerabilities
- Leverage next-generation data classification to find GDPR data
- Use prioritized risk scores & remediation recommendations to address risks

The European Union's General Data Protection Regulation (GDPR) is a pivotal and sweeping regulation that reflects the growing importance of data privacy. The GDPR will likely transform the relationships of data holders or processors and the people associated with that data (known as data subjects). As of May 25, 2018, enterprises worldwide that process personal data concerning E.U. data subjects will need to comply with the provisions of the GDPR, regardless of where that data is held or processed. The potential penalties for noncompliance can be substantial, with non-compliance fines up to 20 million Euros, or 4% of global annual revenue, as further described in the regulation.

Many different business areas inside an organization are impacted by GDPR 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 GDPR requirements while helping the business succeed.

IBM® Security Guardium® Analyzer, a software-as-a-service offering, can help compliance managers, data managers, and IT managers get started on the GDPR journey by locating GDPR-relevant personal data in on-premises and cloud databases; classifying it; identifying vulnerabilities; and helping users understand where to get started to try and minimize risk.

When using Guardium Analyzer, the *results* of the risk analysis are sent to and viewed from the cloud, but the personal and sensitive personal data itself is not moved and remains on-premises. The service is hosted in IBM data centers.

GDPR COMPLIANCE ANALYSIS AS-A-SERVICE

Guardium Analyzer helps users efficiently assess security and compliance risk associated with GDPR-relevant personal data. It helps identify databases most at risk of failing a GDPR-oriented audit and then helps minimize risk using next-generation classification techniques and vulnerability scanning. This can prioritize the on-premises and cloud databases containing at-risk personal and sensitive personal data which requires further attention.

Users can set up database scans on a reoccurring basis: Select a scan window for each database, allowing assessments to run at the best times for the business, and then select the database scan frequency (scan weekly or monthly, for example). After the scans occur, results and risk information are sent to the cloud for viewing in a summary dashboard.

The interactive Guardium Analyzer dashboard displays potential GDPR-related risk information. Users click to drill down into more detail.

Find GDPR-Relevant Personal Data

Guardium Analyzer helps organizations find GDPR personal data using a next-generation classification engine and pre-built GDPR-oriented data patterns that help efficiently find and classify types of personal and sensitive personal data. When it comes to classification, the service goes beyond searching top-level data, and can analyze the actual text in on-premises and cloud-based database tables to find and classify GDPR-relevant personal data, such as personal identification numbers, gender, etc.

Uncover Risk

Open vulnerabilities in databases can increase levels of exposure and risk—especially if those databases contain GDPR-regulated data. Guardium Analyzer applies vulnerability scanning and assessment capabilities and efficiently scans for a multitude of database vulnerabilities. It then can identify vulnerability issues, such as CVEs or missing patches, that might be exploited and need attention.

Specialized risk-scoring techniques are applied to the GDPR classification results and the vulnerability scans results. The offering helps identify the level of risk associated with each database and provides specific details for what is at risk in the database and why, and it provides specific recommendations for remediation.

Take Action

The risk scoring information is used to present entitled users with a prioritized list of risks, and provides users with information they can use to understand what steps might need to be taken to address the vulnerability risks and help protect GDPR-relevant personal data.

Guardium Analyzer also includes a progress dashboard. Based on repeated scans of the cloud and the on-premises database environment, as well as the risk scores and prioritized remediation recommendations, the dashboard shows how your risk levels are trending, as well as the progress that's been made to address those risks over time.

IBM SECURITY GUARDIUM ANALYZER KEY FEATURES

Key features delivered as part of Guardium Analyzer v1.0 include:

Connectivity to cloud and on-premises databases. Helps clients connect to their databases to uncover personal data and vulnerabilities related to GDPR-regulated data. Clients can connect to multiple databases simultaneously. As part of the connection and scanning process, encryption techniques are applied to protect the data, and no personal data is uploaded to the cloud.

Guardium Analyzer supports Oracle, db2, and MS SQL Server databases that are on-premises or on cloud.

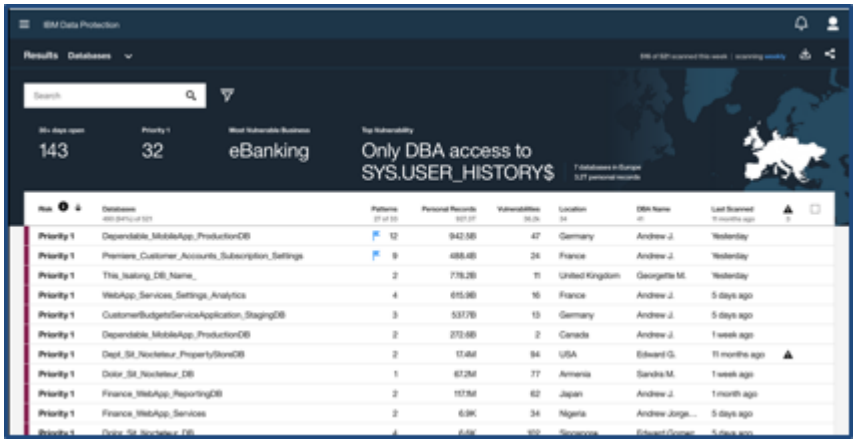
Next-generation data classification. Provides a next-generation classification engine, which also powers IBM Watson offerings, and pre-built GDPR-oriented data patterns to help you efficiently identify and classify types of GDPR-regulated data. The classification engine scans and analyzes the actual text in on-premises and cloud databases to find and classify such data. Users can leverage IBM's pre-built GDPR data patterns, user-provided data patterns, or a combination of both.

Vulnerability scans. Open vulnerabilities in your databases can increase your level of exposure and your risk. This offering applies vulnerability scanning and assessment capabilities and efficiently scans for a multitude of database vulnerabilities. It then can identify pressing vulnerability issues, such as CVEs, that might be exploited and need attention.

Risk scores. Based on the information from the data classification and vulnerability scans, risk scoring techniques are applied to deliver prioritized risk information. The risk scoring is based on the amount of personal data found, the type of personal data found (sensitive personal vs regular personal), and the number of vulnerabilities found. The databases with the greatest amount of identified risk are tagged as Priority 1, and the databases with the least amount of risk are assigned Priority 3.

The offering helps identify the level of risk associated with each database, provides specific details for what is at risk in the database and why, helps organizations understand what type of GDPR-relevant personal data is in their databases and what the level of risk is to the business.

Prioritized remediation recommendations. The risk scoring information is used to present you and your compliance or security team(s) with a prioritized list of risks.



Drill down from the summary dashboard to get the prioritized details that show databases that may be at risk.

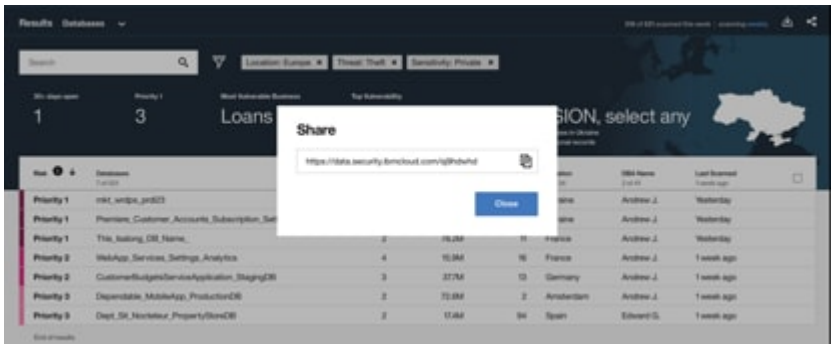
The prioritized risks help users understand what steps could be taken to address the vulnerability risks and help secure GDPR-relevant personal data. These recommendations help organizations prioritize their focus and mitigate GDPR-related risks.

Users can filter the list by factors such as risk severity (Priority 1, 2, 3), business threat, location, and data patterns.

STREAMLINE GDPR-RELATED ACTIVITIES

Guardium Analyzer helps different types of users within organizations collaborate on GDPR-related data activities. The technology helps compliance managers, data managers, and IT managers get the information and details they need to drive focused action around GDPR compliance activities.

From the screen showing the prioritized risk details and remediation recommendations, users may click a “Share” button to generate a link that may be sent to authorized data managers. Guardium Analyzer can send each data manager a prioritized list of the databases they own. In turn, 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.



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 this GDPR-related risk and exposure.

Why IBM?

The IBM Security Guardium Analyzer platform provides a comprehensive approach to data security – for on-premises, on-cloud, and hybrid environments. The broader Guardium data security and protection platform leverages intelligence and automation to provide a centralized, strategic approach to securing types of sensitive data. Robust real-time and right-time analytics help security teams analyze the risk landscape and quickly uncover internal and external threats. The solution provides a broad range of data protection capabilities, including:

- Automated discovery and classification of types of sensitive data
- Entitlement reporting
- Vulnerability assessment and remediation
- Data and file activity monitoring for NAS, SharePoint, Windows, and Unix repositories
- Masking, encryption, blocking, alerting and quarantining
- Automated compliance support

Guardium helps security teams protect sensitive data in today's heterogeneous environments, across databases, data warehouses, Hadoop, NoSQL, in-memory systems, files, cloud environments, and more. The solution can adapt to changes in the IT environment—whether that includes adding new users, expanding capacity, or integrating new technologies.

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