IBM Security Guardium Analyzer

Highlights

- *Efficiently assess security and compliance risk associated with regulated data, such as PCI, PII, and PHI*
- *Find regulated data across on-premises and cloud databases; scan for database vulnerabilities*
- *Leverage next-generation data classification capabilities with out of the box data pattern recognition for global privacy mandates and regulations – or customize your own data patterns to extend these capabilities*
- *Use prioritized risk scoring results and remediation recommendations to start addressing risks*

In today's digital world, data is our most complex and critical asset. It runs our businesses and enables organizations to create greater value for clients – making it not only crucial to the organizations that store and manage it, but also a high value target to malicious actors. Meanwhile, the amount of data continues to grow: 2.5 quintillion bytes of data are created daily[1]. In parallel, new data privacy regulations such as the California Consumer Privacy Act, the General Data Protection Regulation, Brazil's Lei Geral de Proteção de Dados Pessoais (LGPD), and updated New York State Cybersecurity Requirements for Financial Service Companies (23 NYCRR 500) combine with existing compliance mandates (SOX, HIPAA, PCI DSS, etc.) to create an increasingly nuanced and stringent regulatory environment.

All of these elements combine to make data security, privacy and compliance increasingly challenging. As more and more data is created, new compliance requirements are added, and data privacy in general reaches new levels of influence in consumer purchasing decisions, how can technology leaders ensure they keep close tabs on this data and the associated security and compliance risk?

Many different business areas inside an organization are impacted by these considerations – 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 data security and compliance requirements while helping the business succeed.

[1] Forbes, "How Much Data Do We Create Every Day? The Mindblowing Stats Everyone Should Read" May 21, 2018

IBM® Security Guardium® Analyzer, a software-as-a-service offering, can help compliance managers, data managers, and IT managers get started on their data security and compliance journeys by locating regulated 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 regulated data itself is not moved and remains on-premises. The service is hosted in IBM data centers.

DATA CLASSIFICATION & RISK ANALYSIS AS-A-SERVICE

Guardium Analyzer helps users efficiently assess security and compliance risk associated with regulated data. It helps identify databases containing regulated data, such as PHI, PII, or PCI, and then helps minimize risk using next-generation classification techniques and vulnerability scanning. This can prioritize on-premises and cloud databases containing at-risk 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 data risk information. Users click to drill down into more detail.

Find Data Relevant To Your Business

Guardium Analyzer can help organizations find all types of data, such as customer or regulated data, using a next-generation classification engine and pre-built data patterns that help efficiently find and classify types of personal and sensitive regulated data. Out of the box, Guardium Analyzer provides data patterns for PII and Special Category (GDPR-relevant) data, with additional data patterns being added on a continuing basis. Users can easily add additional classification patterns to extend Guardium Analyzer's capabilities in support of additional regulations such as PCI DSS, HIPAA, the California Consumer Privacy Act, and others by uploading their own keyword or regular expression pattern rules. When it comes to classification, for any pre-existing or user-provided pattern, 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 regulated data, such as personal identification numbers, gender, address, etc.

Uncover Risk

Open vulnerabilities in databases can increase levels of exposure and risk—especially if those databases contain regulated or 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 both the classification results and the vulnerability scan 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 personal or customer 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 regulated data and vulnerabilities related to the databases where the data is stored. 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 regulated data is uploaded to the cloud.

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

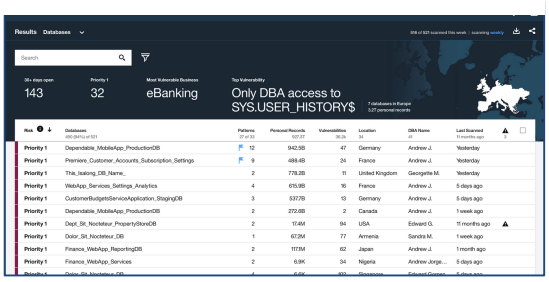
Next-generation data classification. Provides a next-generation classification engine, which also powers IBM Watson offerings, and pre-built data patterns to help you efficiently identify and classify PII and Special Category data. The classification engine scans and analyzes the actual text in on-premises and cloud databases to find and classify such data.

In addition, users can leverage IBM's pre-built data patterns, user-provided data patterns, or a combination of both to support data privacy needs.

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 regulated data found, the type of regulated data found, 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 regulated 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.

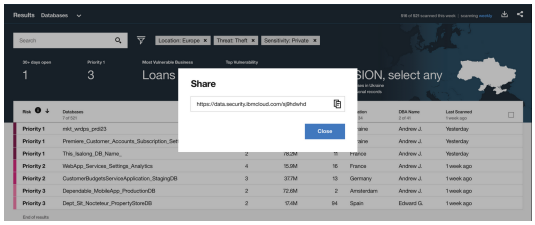
The prioritized risks help users understand what steps could be taken to address the vulnerability risks and help secure relevant regulated data. These recommendations help organizations prioritize their focus and mitigate security and compliance risks.

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

STREAMLINE DATA SECURITY AND COMPLIANCE ACTIVITIES

Guardium Analyzer helps different types of users within organizations collaborate on data security and compliance activities. The technology helps compliance managers, data managers, and IT managers get the information and details they need to drive focused action around compliance, privacy, and broader data protection 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 risk and exposure.

WHY IBM SECURITY GUARDIUM?

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 regulated 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 regulated 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 regulated 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

GDPR 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.

Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings to support your compliance journey.

IBM Security
75 Binney St
Cambridge, MA 02142

Produced in the United States of AmericaSeptember 2018