

# IBM Guardium–Database Activity Monitoring

Bille Akhil<sup>1</sup>, Balu Ashik<sup>2</sup>, Jinka Chandu<sup>3</sup>, Dr S.Vimala<sup>4</sup>, Mr. N. Darwin<sup>5</sup>, Mr. N. Darwin<sup>6</sup>

<sup>1</sup>UG - Electronics and Communication, Prathyusha Engineering College, Chennai, Tamil Nadu.

<sup>2</sup>UG - Electronics and Communication, Prathyusha Engineering College, Chennai, Tamil Nadu.

<sup>3</sup>UG - Electronics and Communication, Prathyusha Engineering College, Chennai, Tamil Nadu.

<sup>4</sup>Assistant Professor, Electronics and Communication Engineering, Prathyusha Engineering College, Chennai, Tamilnadu.

<sup>5,6</sup>Associate Professor, Electronics and Communication Engineering, Prathyusha Engineering College, Chennai, Tamil Nadu.

## ABSTRACT

In earlier days all data was stored in files in the written format it is difficult to maintain and access the data. But nowadays due to the digital era data enlarged more. Guardium helps in maintaining, accessing, and protecting data. IBM Guardium tool for protecting sensitive data of a customer's like Debit Card, Credit Card, CVV, Expiry Date, Aadhar, PAN, Passport, Insurance Id's To restrict the permissions to the level1 and level2 employees of the company. To mask data with the special characters like \$,&,\* and we will make visible the last four digits to recognize the data. To restrict the commands entered by the employees and ensure the restriction of DDL, DML commands in a database.

**Keywords—IBM Guardium, Masking, Redaction, Tokenization, Encryption**

## 1. Introduction

The IBM Guardium item give a straightforward, vigorous psolution for forestalling information spills from Databases archives, assisting with guaranteeing the honesty of data in the server farm and robotizing consistence controls. The Guardium arrangement is intended for usability and adaptability. It will in general be set up for a lone Database or extraordinary numerous heterogeneous Databases arranged across the undertaking.

These are the key functional areas of Guardium Database Security solution:

- **Vulnerability Assessment:** This remembers finding known weaknesses for Database items, yet also providing complete visibility into complex Database infrastructures, detecting misconfigurations, assessing and mitigating risks.
- **Data Discovery and Classification:** Despite the fact that grouping alone doesn't give any assurance, it serves as a crucial first step towards defining proper security policies for different data depending on its criticality and compliance requirements.
- **Data Protection:** Guardium tends to Data encryption very still and on the way, Dynamic information concealing, and different advancements for safeguarding information uprightness and secrecy.
- **Monitoring and Analytics:** this incorporates observing of database execution attributes and complete.monitoring is the process of observing system testing whether they functions correctly. Analytics is the process of turning data (usually behavioral data) into insight. Perceivability in all entrance and regulatory activities for each occurrence. Additionally, extraordinary continuous assessment, peculiarity distinguishing proof and security information and event the board (SIEM) joining can be given.
- **Audit and Compliance:** This incorporates progressed evaluating instruments past local abilities, concentrated examining and revealing across different Database conditions, implementing detachment of obligations, and instruments supporting measurable investigation and consistence

reviews.

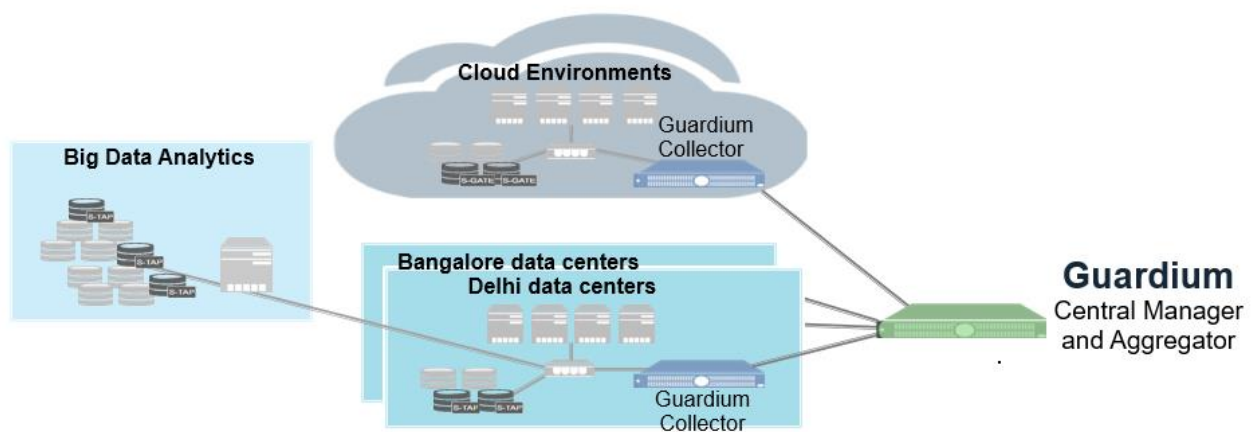
- Performance and scalability: It's a significant prerequisite for all Database security answers for be ready to endure high loads, limit execution upward and support organizations in high-accessibility designs.

IBM Security Guardium gives the least complex, most IBM Security Guardium gives the least complex, most strong answer for guaranteeing the protection and honesty of believed data in your server farm and decreasing expenses via robotizing the whole consistence examining process in heterogeneous conditions.

IBM's Security Guardium gives a basic method for mechanizing and bringing together consistence controls, even in topographically scattered multi-merchant conditions. It decreases consistence costs by giving:

- Granular real-time policies that automatically detect suspicious actions, even those of insiders.
- A protected incorporated data set vault containing a fine- grained review trail of all data set exercises across the endeavor, as well as significant record sharing exercises.
- Adaptable work process computerization to produce consistence gives an account of a planned premise, appropriate them to oversight bunches for electronic sign-offs and speed increase and store the eventual outcomes of remediation practices in the document.
- Automated instruments find and gathering data covered by consistence arranges so consistent plans and consistence work process by and large encompass required data.
- Forensically solidified IBM Guardium Collector (apparatus) stores all information in the Audit Repository Database in scrambled and packed design for filing.

## 2. Experimental Methods or Methodology



**Fig 1. Block Diagram**

The Guardium solution combines an appliance-based solution with light-weight software probes that are installed on database servers combined with an application code base that considers a profoundly thorough and adjustable arrangement of strategies to control and get corporate information bases.

These combined mechanisms allow the Guardium solution to see not only traditional client server and web-based application communications, yet in addition dangers that could begin on data set servers- - empowering Guardium to make a move on all unapproved access endeavors.

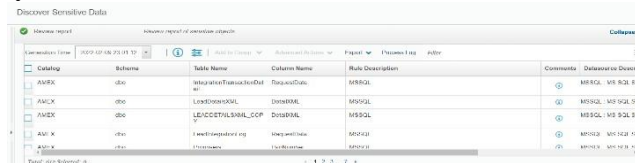
The Guardium arrangement can get and restrict assaults to an information base through checking of all data set passageways (nearby and remote).

The Guardium engineering is both organization based and have based through machines and programming tests individually. It consistently screens organization and servers for information base messages. The Guardium arrangement can be sent in an assortment of functional modes to give adaptability and complete inclusion to all information base traffic.

VERIZON will have multiple Guardium collectors. Collectors send data to Guardium Aggregator on a scheduled basis. Aggregator allows Collectors to be dedicated to monitoring and policy enforcement tasks.

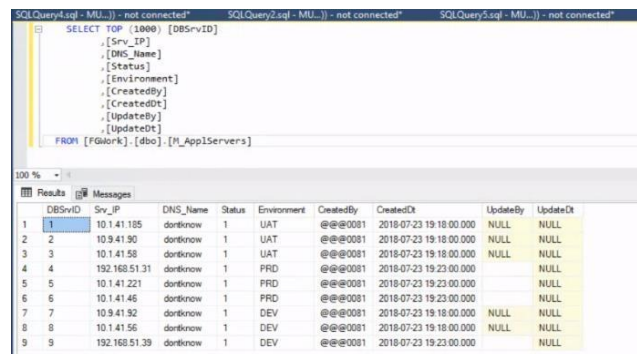
### 3. Results and Discussion

IBM Guardium protects our data and monetizes databases and it will help to count the number of queries and restrict the DDL and DML commands of the database. Sensitive data can be discovered using IBM, Masking policy, DDL and DML commands can be monetized.



Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Database	Owner
ANEX	dbo	uspAdminTransactionOut	TransActOut	MSSQL		MSSQL_MSI SQL SE	
ANEX	dbo	uspAdminSQL	DBINTERNAL	MSSQL		MSSQL_MSI SQL SE	
ANEX	dbo	uspAdminSQL_COP	DBINTERNAL	MSSQL		MSSQL_MSI SQL SE	
ANEX	dbo	uspAdminSQL	DBINTERNAL	MSSQL		MSSQL_MSI SQL SE	
ANEX	dbo	uspAdminSQL	DBINTERNAL	MSSQL		MSSQL_MSI SQL SE	

Fig. 2. Sensitive Discovery



```
SELECT TOP (1000) [DBSrvID]
, [Srv_IP]
, [DNS_Name]
, [Status]
, [Environment]
, [CreatedBy]
, [CreatedDt]
, [UpdateBy]
, [UpdateDt]
FROM [FG@ork].[dbo].[H_AppIServers]
```

DBSrvID	Srv_IP	DNS_Name	Status	Environment	CreatedBy	CreatedDt	UpdateBy	UpdateDt
1	10.1.41.185	dotknow	1	UAT	@@0081	2018-07-23 19:18:00.000	NULL	NULL
2	10.9.41.90	dotknow	1	UAT	@@0081	2018-07-23 19:18:00.000	NULL	NULL
3	10.1.41.58	dotknow	1	UAT	@@0081	2018-07-23 19:18:00.000	NULL	NULL
4	192.168.51.31	dotknow	1	PRD	@@0081	2018-07-23 19:23:00.000	NULL	NULL
5	10.1.41.221	dotknow	1	PRD	@@0081	2018-07-23 19:23:00.000	NULL	NULL
6	10.1.41.46	dotknow	1	PRD	@@0081	2018-07-23 19:23:00.000	NULL	NULL
7	10.9.41.92	dotknow	1	DEV	@@0081	2018-07-23 19:18:00.000	NULL	NULL
8	10.1.41.56	dotknow	1	DEV	@@0081	2018-07-23 19:18:00.000	NULL	NULL
9	192.168.51.39	dotknow	1	DEV	@@0081	2018-07-23 19:23:00.000	NULL	NULL

Fig. 3. Masking Policy

### CONCLUSION

IBM Guardium tool for protecting sensitive data's of a customer's like Debit Card, Credit Card, CVV, Expiry Date, Aadhar, PAN, Passport, Insurance Id's .To restrict the permissions to the level1 and level2 employees of the company. To mask data with the special characters like \$,&,\* and we will make visible the last four digits to recognize the data. To restrict the commands entered by the employees and ensuring the restriction of DDL, DML commands in a database.

### References

- [1] S.Mazumder,S.Yu,S.Guo,"BigDataToolsandPlatforms",2016
- [2] NIST.FoundationsforInnovationinCyber-PhysicalSystems–WorkshopReport.January 2013.
- [3] Y. Liu, P. Ning, M. K. Reiter: False datainjectionattacksagainststateestimationinelectric power grids. ACM TISSEC 14(1): 13(2011)
- [4] E.Bertino,G.Ghinita:Towardsmechanismsfor detection and prevention of data



exfiltrationbyinsiders. ASIACCS2011:10-19.

- [5] E.Bertino: Data Protection from Insider Threats. Synthesis Lectures on DataManagement, Morgan&Claypool Publishers2012
- [6] Mandiant. The Advanced Persistent Threat,2010
- [7]Mandiant.ExposingOneofChina’sCyberEspionageUnit.February,2013,<http://intelreport.mandiant.com/>
- [8] The Tallinn Manual on the InternationalLawApplicabletoCyber Warfare.CambridgeUniversity Press, 2013, available at<http://www.ccdcoe.org/249.html>
- [9] D.Liu, S.Wang: Query encrypted databasespractically.ACMCCCS2012:1049-1051
- [10] J.Szefer, R. B. Lee: Architectural supportfor hypervisor-secure virtualization. ASPLOS2012:**437-450**
- [11] Dr.S.Vimala, N.R. Gladiss Merlin, L.Ramanathan, R.Cristin, “Optional routing and deep regression neural network for rice leafdisease prediction in IOT”,International Journal of Computational Methods, Dec 2020, SCI Journal.
- [12] Vimala, S. and Srivatsa, S.K, “Live Bandwidth Allotment LBA-MAC Protocol for MANETS,” ARPN Journal of Engineering and Applied Sciences (SJR Rating: 0.21, SCOPUS-H Index-7), Vol.11, N0.9, pp.5616-5622,2016.