

IBM Security Guardium Data Protection

Simple, Scalable and Relevant

Benazeer Daruwalla
IBM Data Security

April 2020

Legal Disclaimer

© IBM Corporation 2020. All Rights Reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

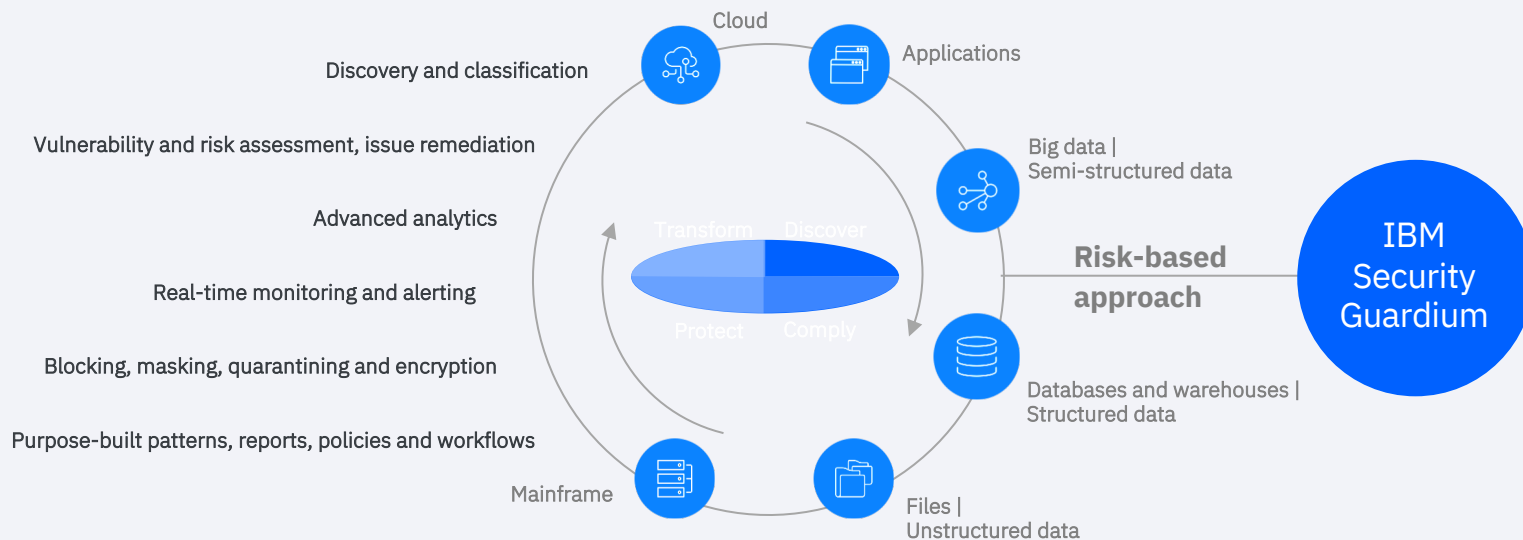
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

IBM Security Guardium empowers you to meet your most important data protection needs

With smarter capabilities throughout your entire data protection journey

- **Complete visibility**
- **Actionable insights**
- **Real-time controls**
- **Automated compliance**



Today, businesses
need increased
agility to remain
competitive...



and they're incorporating cloud-based technologies to drive their
organizations forward

Top 4 data protection trends in the era of digital transformation

Cloud accelerates business transformation

- Ability to protect database workloads deployed in cloud-native architectures

Business Agility

Cloud provider data security

- Lack of comprehensive visibility to spot and protect against risks across environments

Visibility and control

Legacy and cloud native architectures will co-exist

- Need to bridge technology, process and skills gap between modern and traditional IT architectures

Simplification

94% utilize multiple clouds

- Scalability and availability between multiple clouds

Coverage

Key success factors for securing hybrid multi-cloud environments

Dynamic

- Flexible data collection mechanisms allow you to monitor and protect thoroughly
- Support compliance monitoring and **proactive** protection in real time with separation of duties
- **Minimize vendor risks and reliance** on cloud providers for auditing

Orchestrated

- Risk-based data security analytics find the anomalies-in-the-haystack that need attention
- Centralized policy enforcement to increase efficiency and reduce costs
- Workflow automation and orchestrated response

Modern

- Seamless upgrades with built-in resiliency
- Deploy and run anywhere with cloud-native, containerized technology
- Reduced operational costs – enable IT, Dev and SecOps



Private cloud /
Service Provider cloud

Guardium capabilities for securing hybrid multi-cloud environments

Dynamic

- Active & passive monitoring for 20+ cloud data sources using:
 - **External-TAP**
 - **Cloud Provider APIs**
 - **Native Logs**
- Discover, classify, assess & monitor with out-of-the-box support for compliance & privacy regulations
- Advance reporting
 - 800+ customizable reports
- Minimize security blind spots & take real-time action with blocking and redaction*
- Store data security & audit data to meet retention requirements & uncover unknown threats

Orchestrated

- Centralized policy enforcement & management across hybrid multi clouds
- Automate compliance workflows for audit reviews & approvals
- Orchestrate remediation & response with IT & SecOps tools
 - ServiceNow, Splunk, QRadar, Resilient, etc.

Modern

- Uses cloud-native & containerized technology (deploy-anywhere)
- Simplify & streamline deployment with cloud management frameworks, such as Kubernetes & OpenShift
- Elastic, scalable & fail-proof*

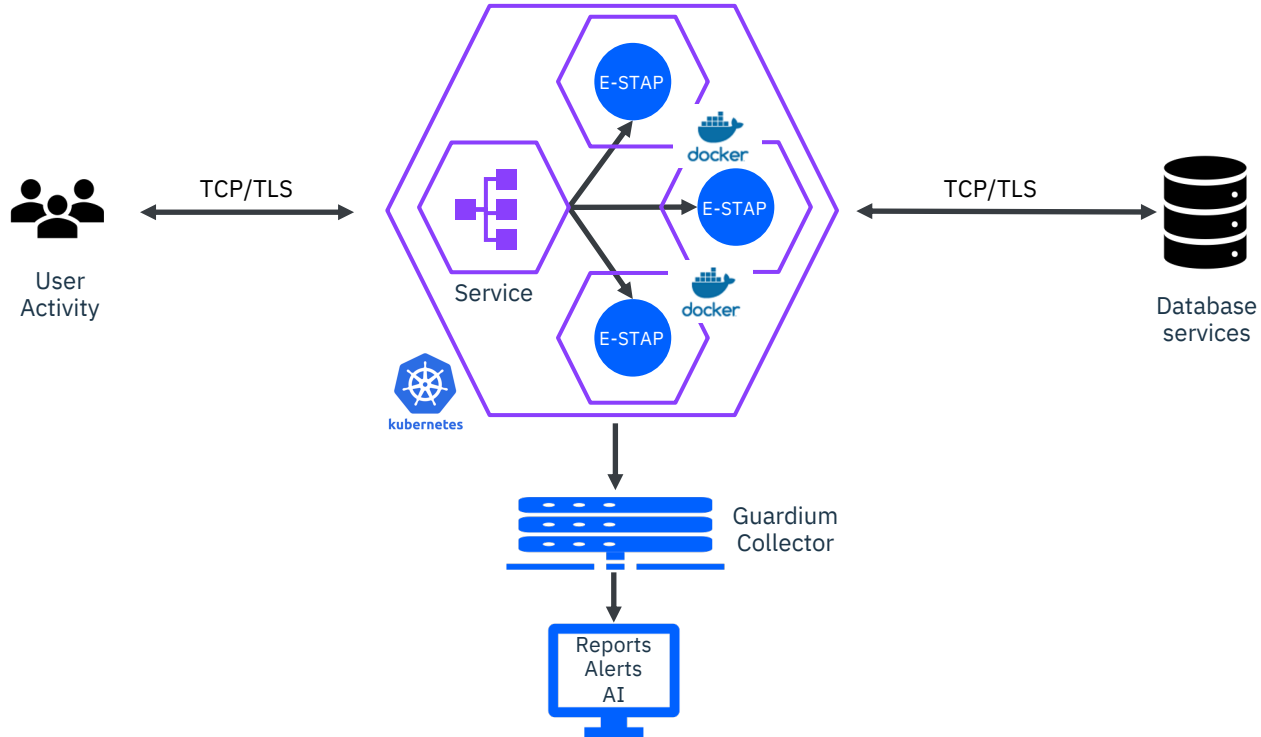
* Only available with External-TAP

Technical Details

Guardium External-TAP
AWS/Azure Data Streaming
Native Logging

Guardium External-TAP

Guardium External-TAP V11.x deployment



Guardium External-TAP

1. Organic solution based on S-TAP technology
2. Supports containerized databases + databases consumed as a service
3. Real-time interception of SSL and plain text TCP/IP Traffic
4. Redaction, Blocking and Alerting
5. Local traffic can be monitored by configuring DNS rules/ingress rules
6. Auto-deploy & Auto-scale with Kubernetes
7. Easy to integrate with SecDevOps pipeline
8. Certified on Docker and RHOS. Available on Docker Hub, and IBM Cloud Registry (planned)

The screenshot displays the Guardium External-TAP management interface. The top section, titled "External S-TAP instances", contains a table with columns: External S-TAP group, Group uuid, Host, Database type, Total members, Overall status, Healthy members, and Collector. Below this table is a "Hourly Access Details" section for the period 2020-01-14 13:40:16 to 2020-01-14 19:40:16. This section includes a table with columns: Period Start, Server IP, Client IP, Service Name, DB User Name, Source Program, Sql, and Success. A red box highlights a row in this table. Below the hourly details is an "Activity Summary By Client IP" section for the period 2020-01-14 13:40:05 to 2020-01-14 19:40:05, which includes a table with columns: Client IP, Server IP, Source Program, SQL Verb, and Object Name. A red box highlights a row in this table.

External S-TAP group	Group uuid	Host	Database type	Total members	Overall status	Healthy members	Collector
oracle_...	925cc984-f01f-4019-bec6-78c4a19c8e1e	...	oracle	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
db2_...	cb9d2e3d-d1ad-4db0-9283-85afb451c470	...	db2	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
mysql_...	d364f6f5-e553-4669-9cce-c2b55b95c82	...	mysql	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
mongodb_...	84339197-d7ed-48a8-930d-1a3ca2b9df5	...	mongodb	2	●	2	lit4-vm02.guard.swg.usma.ibm.com
redis_...							

Period Start	Server IP	Client IP	Service Name	DB User Name	Source Program	Sql	Success
2020-01-14 14:00:00	ORCL	PROXYQA	JDBC THIN CLIENT	SELECT SYS_CONTEXT(?,?) from DUAL	2
2020-01-14 14:00:00	ORCL	PROXYQA	JDBC THIN CLIENT	SELECT value FROM v\$nis_parameters WHERE parameter =?	1
2020-01-14 14:00:00	ORCL	PROXYQA	JDBC THIN CLIENT	select * from data	0

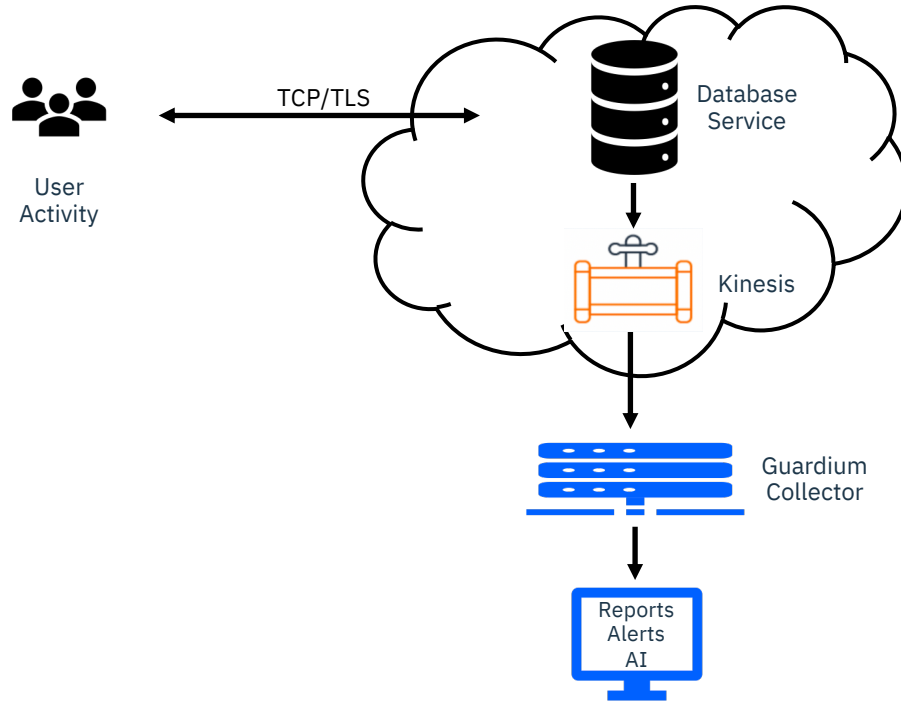
Total: 4 Selected: 0

Client IP	Server IP	Source Program	SQL Verb	Object Name
...	...	JDBC THIN CLIENT	select	data
...	...	JDBC THIN CLIENT	SELECT	DUAL
...	...	JDBC THIN CLIENT	SELECT	SYS.ALL_OBJECTS
...	...	JDBC THIN CLIENT	select	SYS.ALL_USERS



Data Streaming

Monitoring using AWS Database Activity Streams



AWS Database Activity Streams (DAS)

1. Easy to use
2. Dependency on cloud provider's roadmap
3. Limited DB support
4. Passive, not real-time
5. Limited data (No failed SQL or Result set)

Cloud DB Service Protection

Cloud DB Service Accounts

Amazon-DB

Provider: Amazon

Hide Discover Streams

Discover

Streams

Assign Collector Enable Monitoring Disable Monitoring Status History Filter

Stream	Region	Assigned collectors	Monitor enabled	Status	Status changed	Comments
aws-rds-das-cluster-RG53AMD7ENBUPGQIN6BN4BOZ71	us-east-2	1	1	●		All Good
aws-rds-das-cluster-RG53AMD7ENBUPGQIN6BN4BOZ71	us-east-2	sys-col06.guard.aws.usma.fdm.com	●	●	2020-04-27 16:01:37	All Good

Add a new stream

* Stream name AWS Test Strem

* Region us-east-1

Collector Select collector

* DB DNS endpoint Enter endpoint

* Port Enter port

* Cluster resource Id Enter Cluster resource Id

* Consumer Group Name Enter Consumer group name

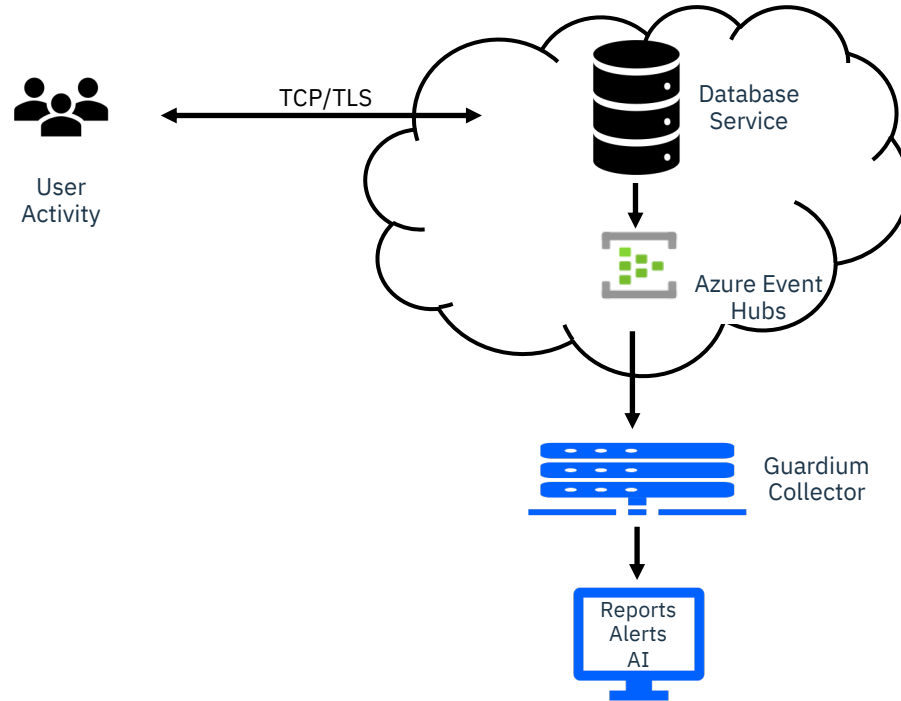
☐ Start monitoring stream

OK Cancel

Refresh

	Service Name	DB User Name	Source Program	Sql	Success
3.249	US-EAST-1.DB-73J4NGMIGNX-GOSPYT2HANMMFBE	GALI		SELECT ?, ?) vals ON (c.oid = vals.oid AND a.atnum = vals.atnum)	2
3.249	US-EAST-1.DB-73J4NGMIGNX-GOSPYT2HANMMFBE	GALI		show search_path	1
3.249	ORACLE	?		select * from demo	1
3.249				select SYSDATE from dual	1

Monitoring using Azure Event Hubs



Azure Event Hubs

- 1. Easy to use
- 2. Dependency on cloud providers roadmap
- 3. Add-on subscription to Event Hubs may be required
- 4. Passive, not real-time
- 5. Limited data (No result set)

Cloud DB Service Protection

Cloud DB Service Accounts

+ - Filter

Amazon-DS

Azure-DS

Cloud DB Service Account

Name : Azure-DS

Provider : Azure

Event Hubs

+ - ↺

Assign Collector Enable Monitoring Disable Monitoring Status History

Event Hub	Namespace	Assigned collectors	Monitor
sta-eh1	sta-nsp	1	1			
sta-eh1	sta-nsp	sys-col06.guard.swg.us ma.ibm.com	<input checked="" type="checkbox"/>	<input type="checkbox"/>		

Add a new event hub

* Event Hub Name

STA-EH2

Collector

Select collector

* Namespace

Enter Namespace

* DB Type

Azure SQL

* DB DNS endpoint

Azure SQL

* Port

Cosmos SQL

* Consumer Group Name

Cosmos MongoDB

* Storage Connection String

Cosmos Cassandra

* Start monitoring event

Cosmos Gremlin

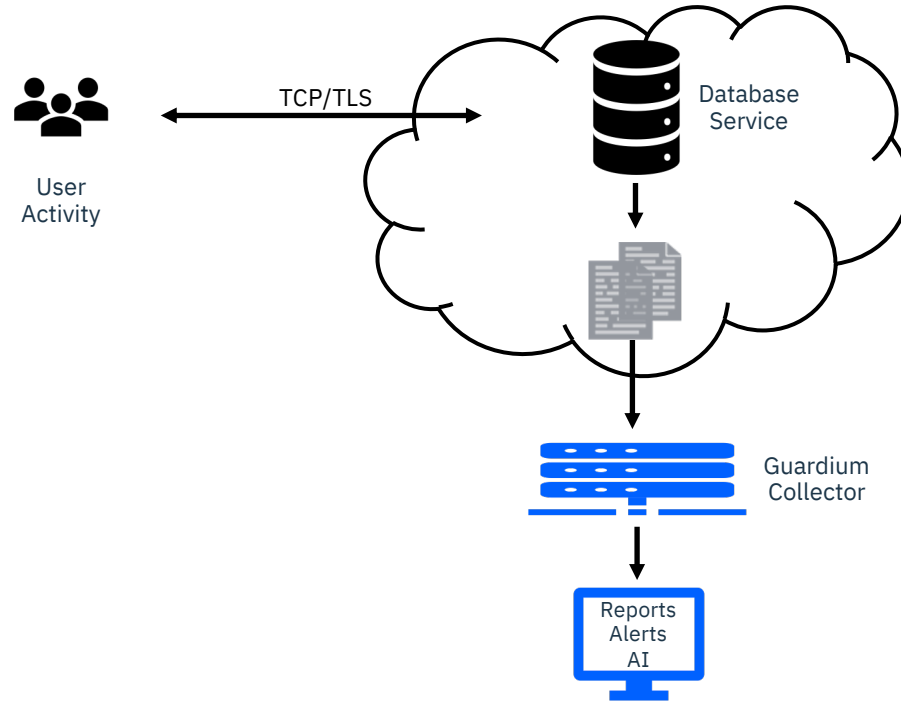
Cosmos Table

OK

Cancel

							Original Name, TableName
2020-01-13 23:17:45	MS SQL SERVER	0.0.0.0	7		AZURE SQL QUERY EDITOR	ADMINDBA	select ?
2020-01-13 20:44:43	MS SQL SERVER	0.0.0.0	7		AZURE SQL QUERY EDITOR	ADMINDBA	select * from myemployee;
2020-01-13 20:44:43	MS SQL SERVER	0.0.0.0	7		AZURE SQL QUERY EDITOR	ADMINDBA	DBAS
2020-01-13 20:44:43	MS SQL SERVER	0.0.0.0	7		AZURE SQL QUERY EDITOR	ADMINDBA	select * from employee

Monitoring using Native Logs



Native logging

1. Easy to use
2. Extra costs for log storage
3. Passive, not real-time
4. Limited data (No failed SQL or No result set)

Create Cloud Definition

Cloud DB Service Account

* Name

* Provider

* Audit type ☒ Native ☐ Data Streams

AWS Configuration

* AWS access key ID

* AWS secret access key ID

Database Auditing and Classification

Default classification Process

* Limit objects added automatically

Hourly Access Details			
Period Start	Server IP	Service Name	Sql
2019-02-01 16:00:00		ORACLE	select * from demo_alert
2019-02-01 16:00:00		ORACLE12-AUDIT	SESSION_STARTED
2019-02-01 16:00:00		ORACLE12-AUDIT	CONNECT
2019-02-01 16:00:00		ORACLE12-AUDIT	COMMIT
2019-02-01 16:00:00		ORACLE12-AUDIT	select ? error ? as error, ? log_sequence ? as log_sequence from v\$archive_dest where statu s = ? and rownum = ?
Total: 10 Selected: 0			
		SQL Verb	Object Name
		select	demo
		select	demo_alert

Facilitate Secure Hybrid Cloud Adoption

1. [Support Matrix](#) (not exhaustive) for Database Activity Monitoring

Collection Mechanism	Sources
External-TAP	<ul style="list-style-type: none">• AWS : Aurora, MySQL, PostgreSQL, Oracle, Mongo Atlas, Redshift, MariaDB, S3 (v11.2), DynamoDB (v11.2)• Azure : SQL Server, SQL DW, Mongo Atlas• IBM Cloud : DB2 DW, DB2, MongoDB (v11.2), PostgreSQL(v11.2), MySQL (v11.2)• IBM Cloud Pak for Data(planned): IPS, DB2 DW, DB2• Google Cloud (planned): Google Cloud SQL• Containers: MongoDB, PostgreSQL, MySQL• Others: Redis, Sybase ASE, Sybase IQ
AWS Database Activity Streams	<ul style="list-style-type: none">• AWS Aurora PostgreSQL• AWS Aurora MySQL (planned)
Azure Event Hubs	<ul style="list-style-type: none">• Azure SQL Server• Azure SQL DW• Azure Cosmos DB (Mongo, Cassandra, SQL, Gremlin, Table)
Native Logs (Connectors)	<ul style="list-style-type: none">• AWS Oracle RDS. Amazon Redshift (BP provided on Guardium AppX). More in plans
S-TAPs	<ul style="list-style-type: none">• Supports all DBMS IaaS Deployment as documented in the Support Matrix

2. Support for Vulnerability Assessment

- AWS RDS: Oracle, SQL Server, MySQL, PostgreSQL
- Azure SQL DB (planned)

New Packaging: Guardium Data Protection for Database Services (GA: March 2020)

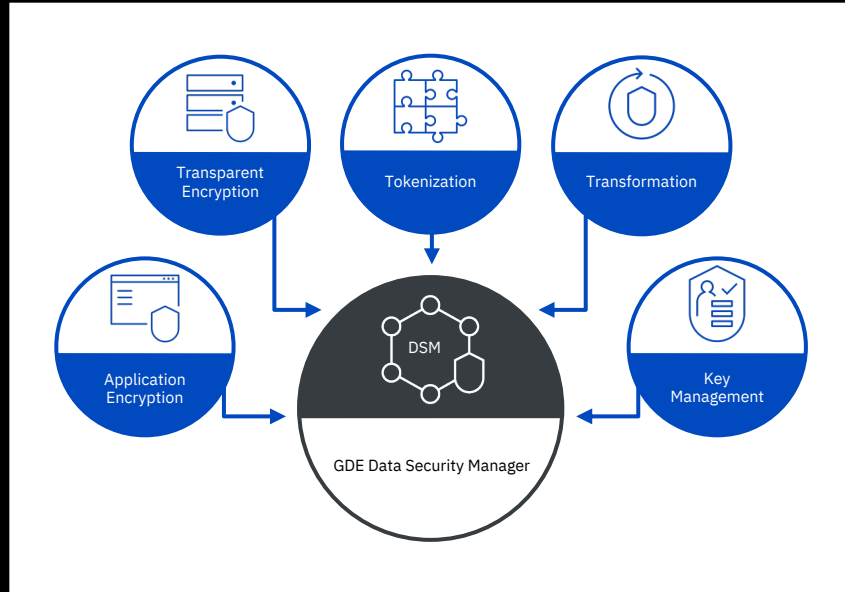
Core Highlights

1. Metric: Managed Activated Processor Cores (MAPC) that scales multiple cloud providers
2. Same functions and features of Guardium Data Protection for Databases
3. You don't pay for collection mechanism. Flexible.
4. Unlimited and not-event based
5. No hidden costs for storage or need for premium or add-on subscription services
6. Available on cloud marketplaces under "IBM Security Guardium Data Protection"

Please note:

- For non-Guardium client or current clients that require additional entitlements: Use Data Protection for Database services
- For existing clients with entitlements (PVU or MVS): Talk to your Guardium sales rep for conversion.

Guardium Data Encryption – Across Entire Enterprise



Data Encryption - Structured / Unstructured Data
– *ANYWHERE* [GDE]

Application Encryption – Structured data with
Format Preserving Encryption [GAE]

Oracle and KMIP Key Management –
Centralized storage, management and security for
encryption keys [GDKM]

Cloud Key Mgmt – Encryption key mgmt. options
for Public Clouds (AWS, Azure, Salesforce) [GCKM]

Tokenization / Data Masking – Secure
applications at the field level using fully encapsulated
solution using Format Preserving Encryption anywhere
[GTO]

Reference Material

External S-TAP:

<https://ibm.biz/BdqyqH>

Deploying External S-TAP on AWS:

<https://ibm.biz/BdqyqX>

Configuring AWS Database Activity Stream with Guardium

<https://ibm.biz/Bdqyq4>

Configuring Azure Event Hubs with Guardium

https://www.ibm.com/support/knowledgecenter/SSMPHH_11.1.0/com.ibm.guardium.doc/discover/cloud_db_discover_azure.html

Guardium Lab at THINK 2020:

Monitoring Next-Gen Data Sources in a Multicloud World with External TAP and Cloud Connectors [2177]

<https://www.ibm.com/events/think/>

THANK YOU

FOLLOW US ON:



ibm.com/security



securityintelligence.com



ibm.com/security/community



xforce.ibmcloud.com



[@ibmsecurity](https://twitter.com/ibmsecurity)



youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2019. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

