IBM Security

IBM Security Guardium Data Protection

Simple, Scalable and Relevant

Benazeer Daruwalla
IBM Data Security

April 2020

Legal Disclaimer

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.

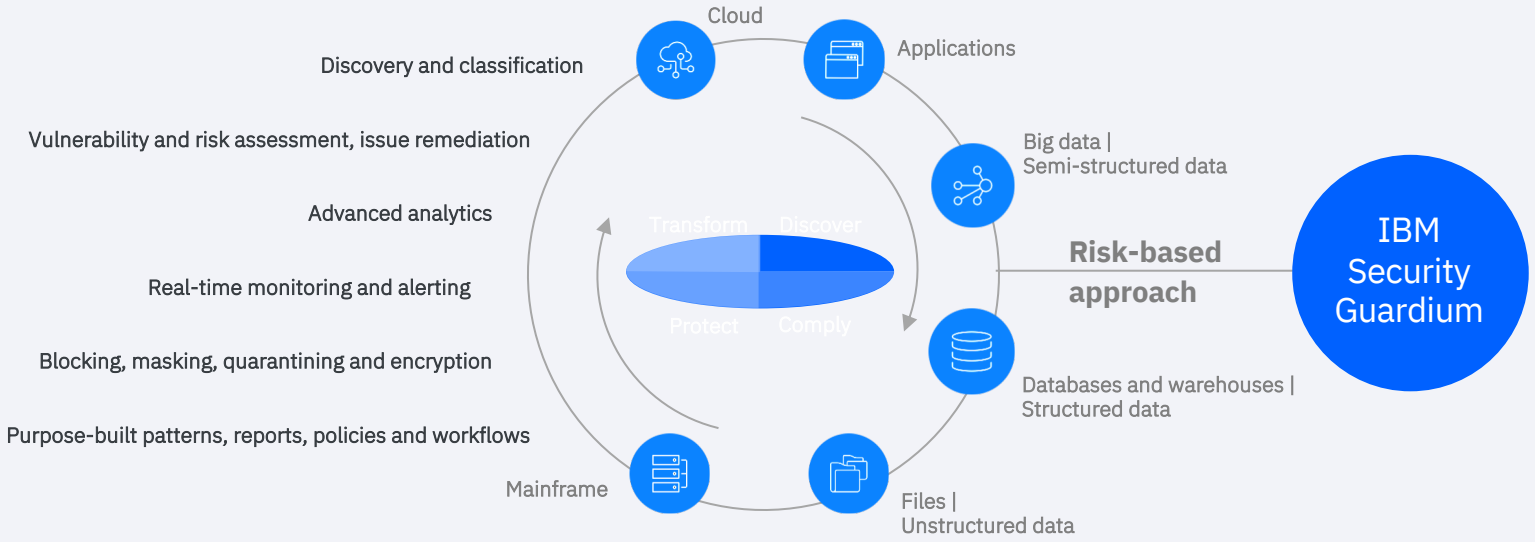
Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, 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	Cloud provider data security	Legacy and cloud native architectures will co-exist	94% utilize multiple clouds
• Ability to protect database workloads deployed in cloud-native architectures	• Lack of comprehensive visibility to spot and protect against risks across environments	• Need to bridge technology, process and skills gap between modern and traditional IT architectures	• Scalability and availability between multiple clouds
Business Agility	**Visibility and control**	**Simplification**	**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*

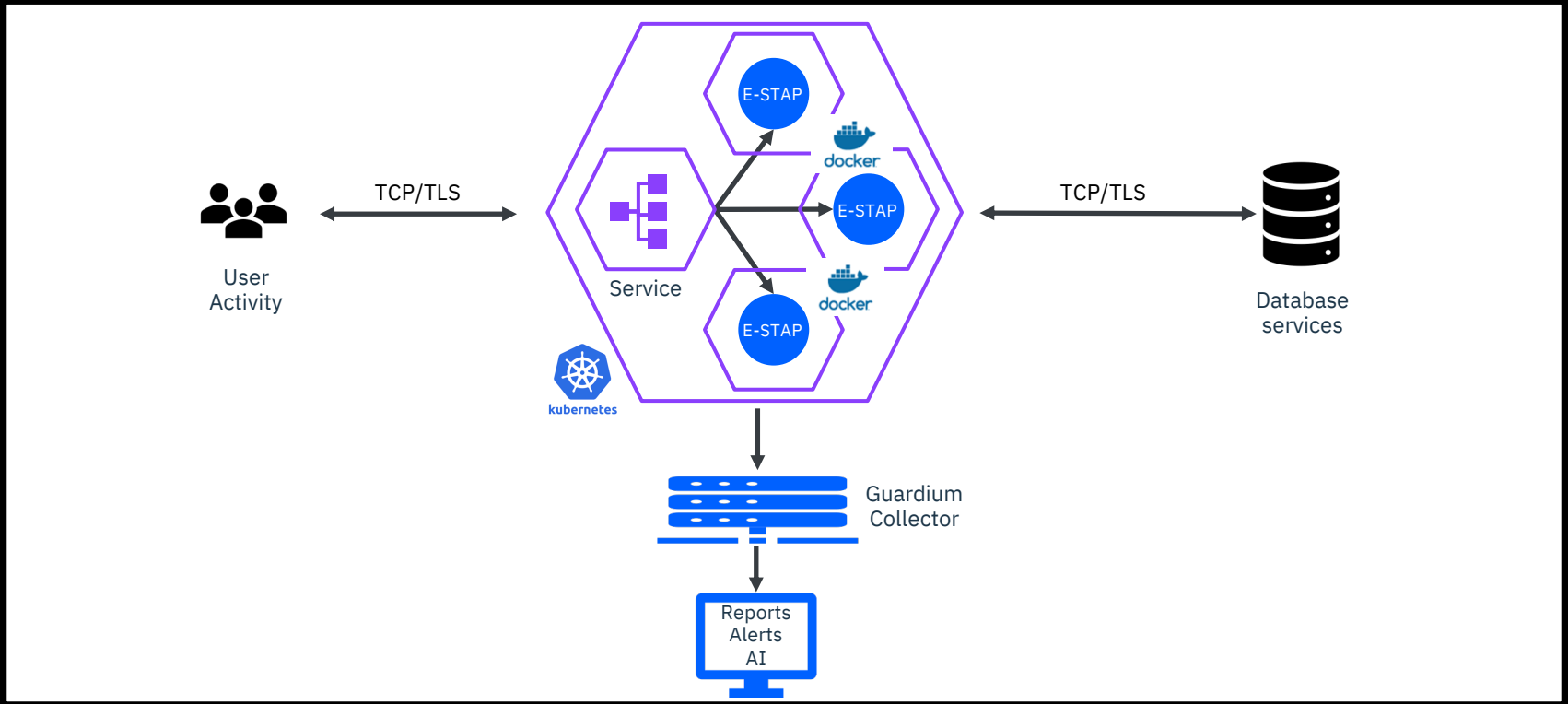
* Only available with External-TAP

Technical Details

Guardium External-TAP
AWS/Azure Data Streaming
Native Logging

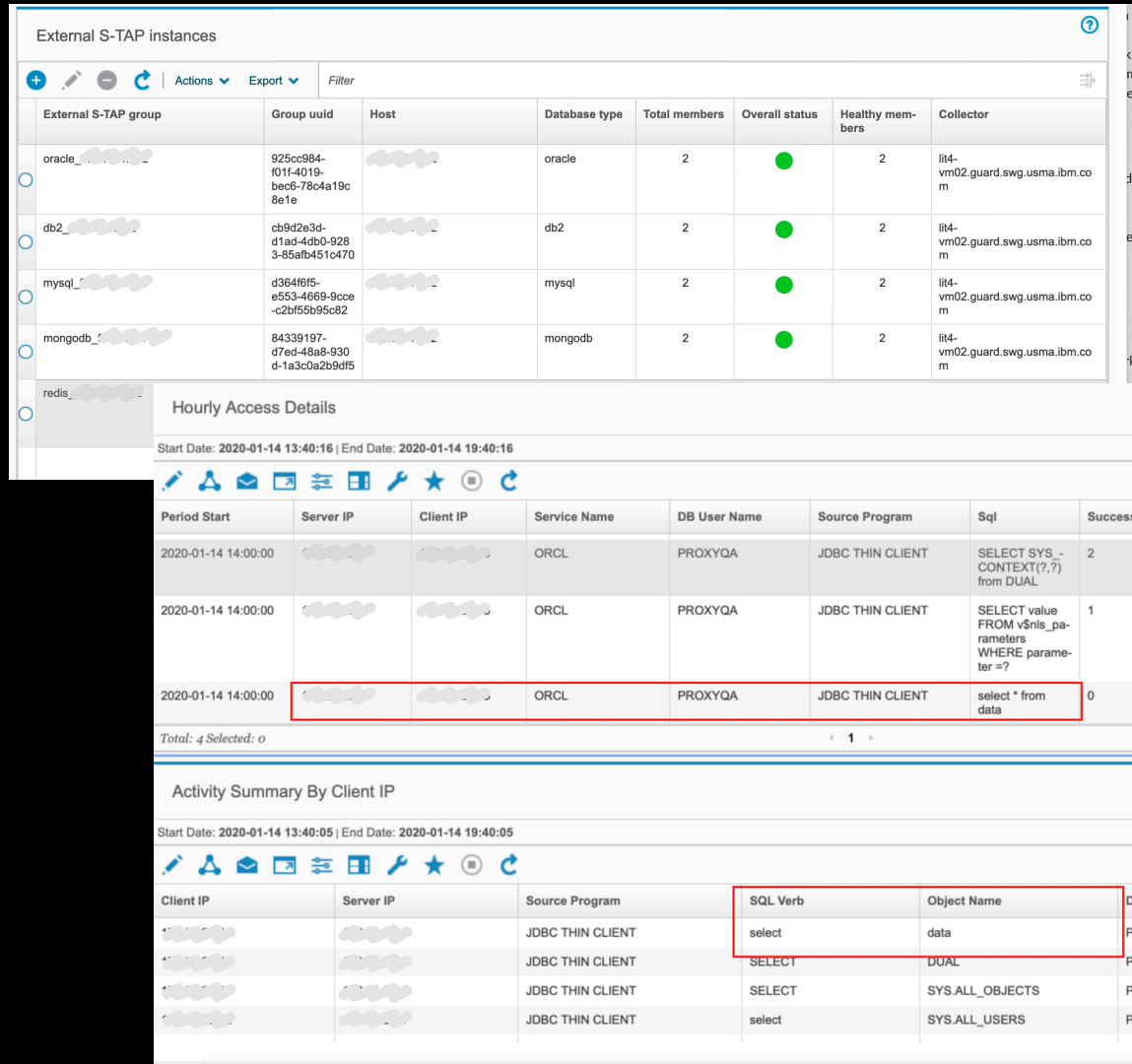
Guardium External-TAP

Guardium External-TAP V11.x deployment



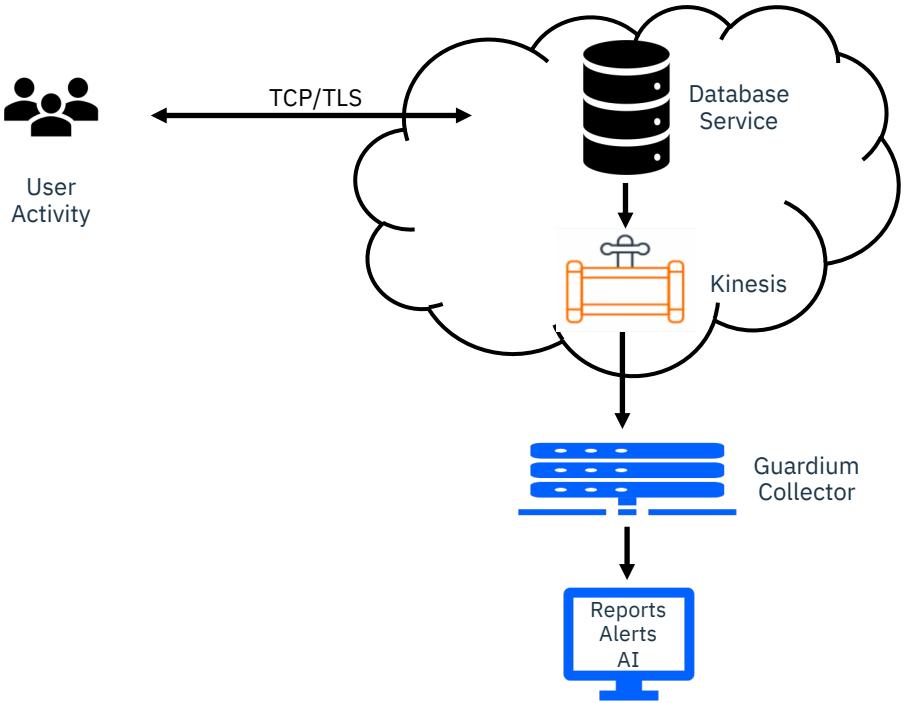
Guardium External-TAP

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)



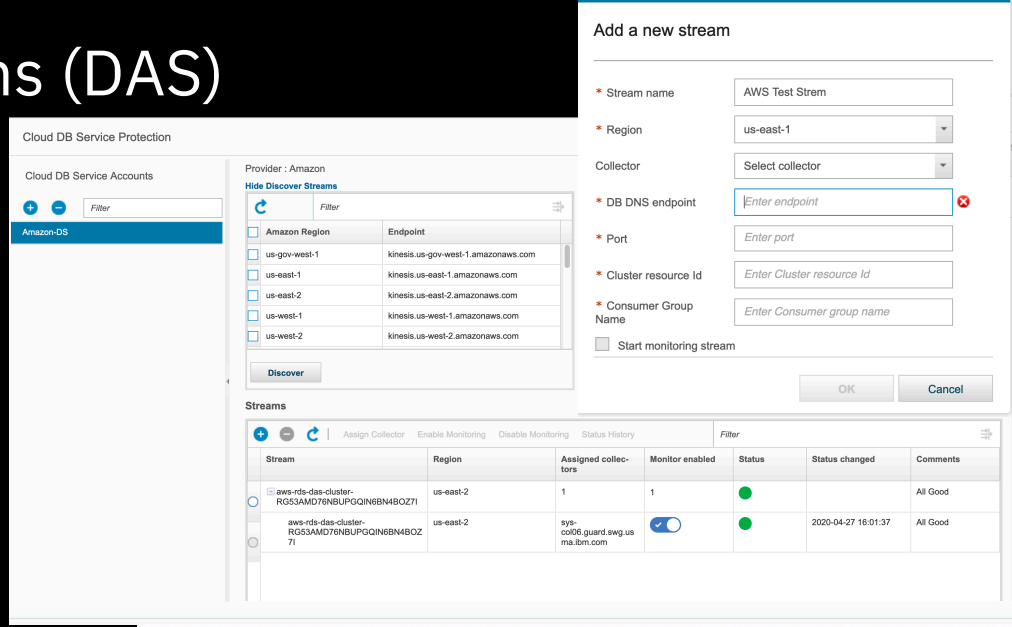
Data Streaming

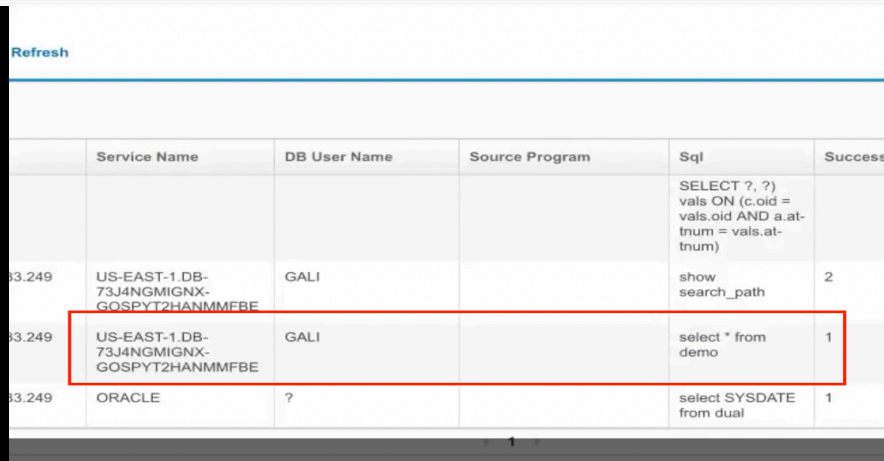
Monitoring using AWS Database Activity Streams



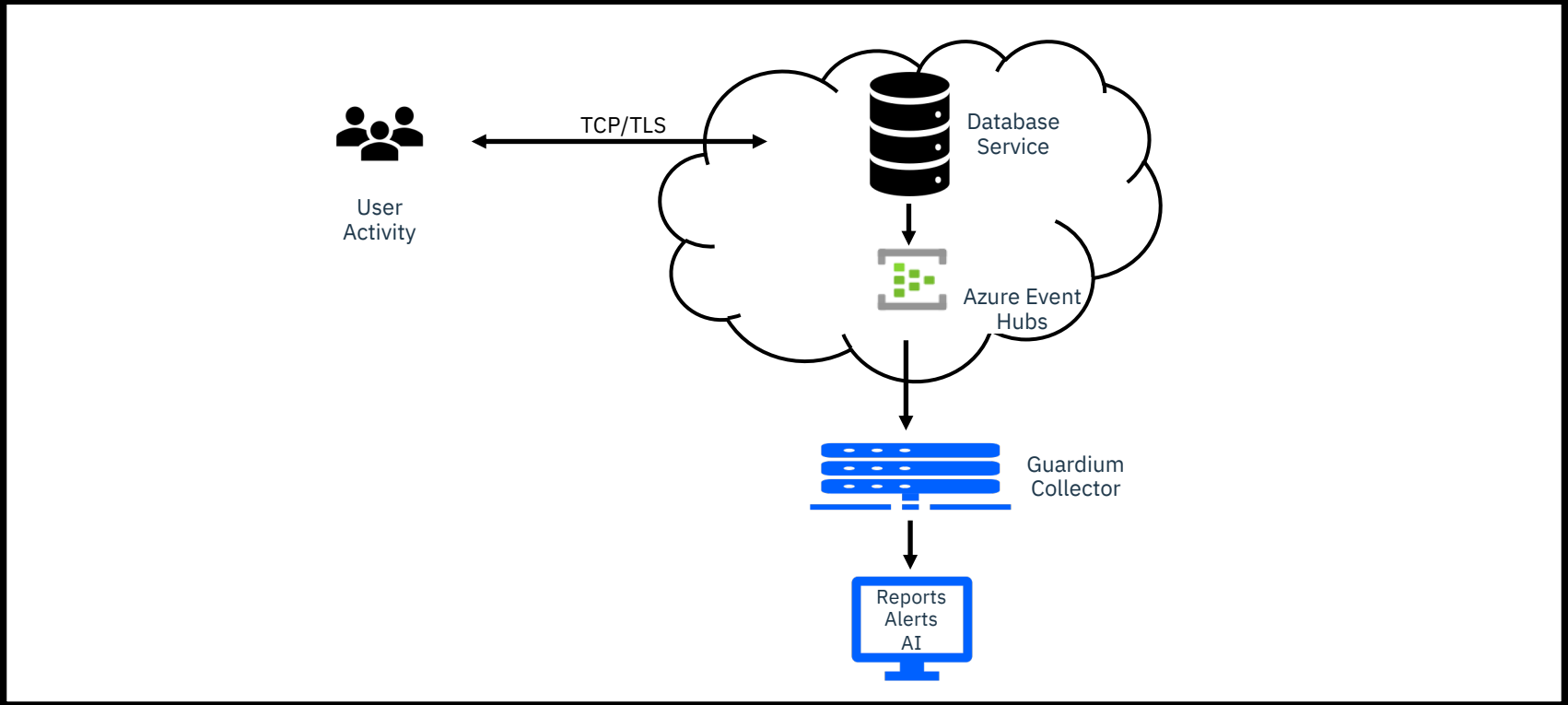
AWS Database Activity Streams (DAS)

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)



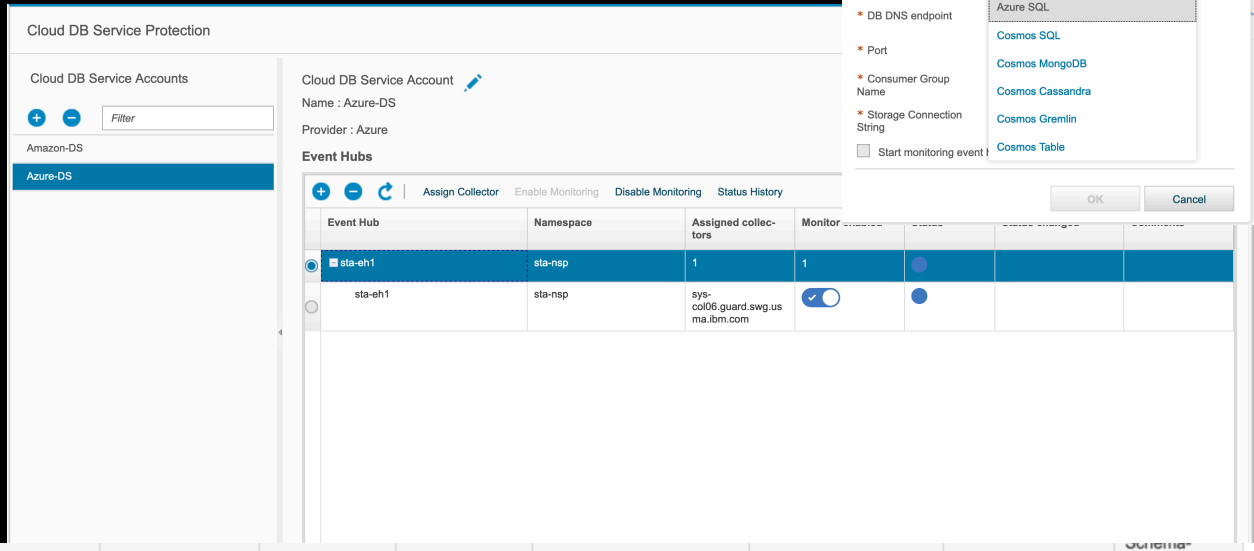


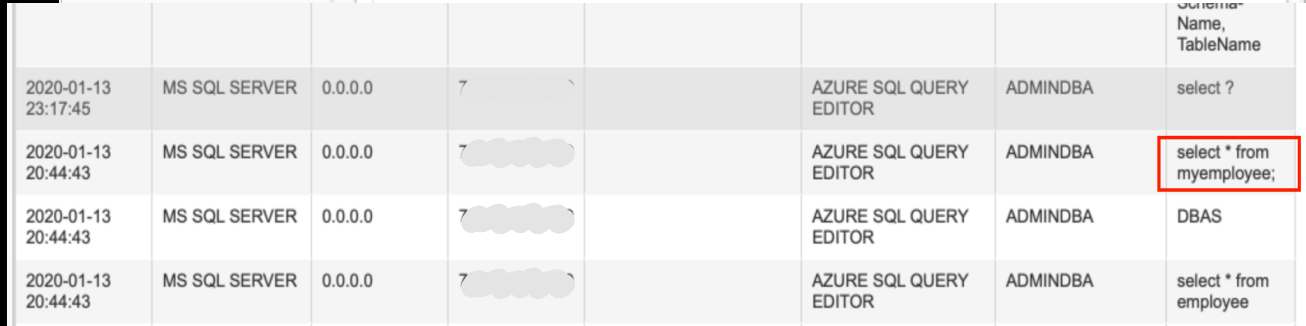
Monitoring using Azure Event Hubs



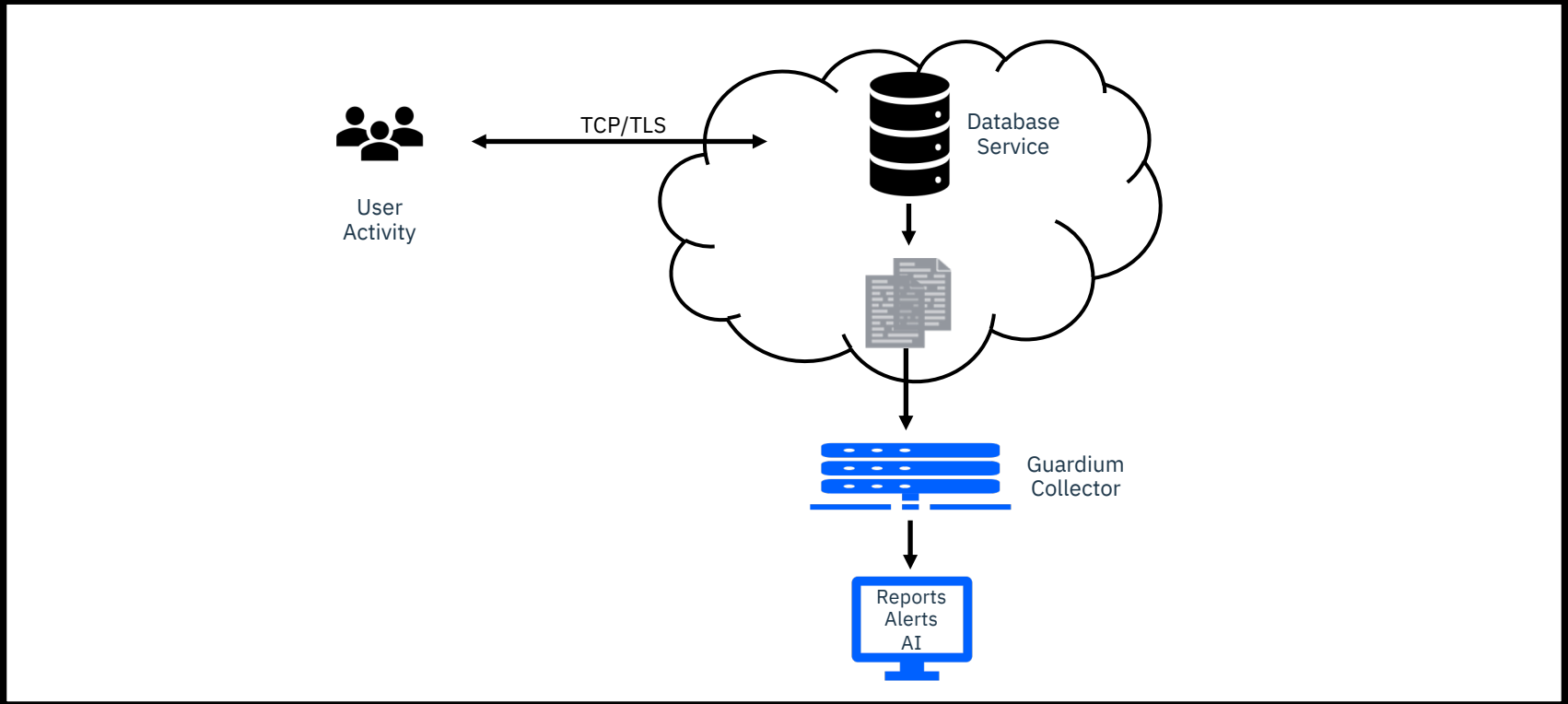
Azure Event Hubs

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)



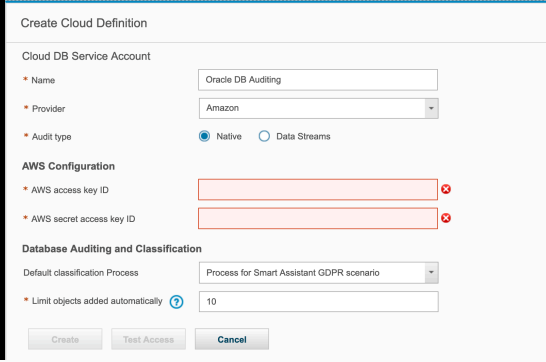


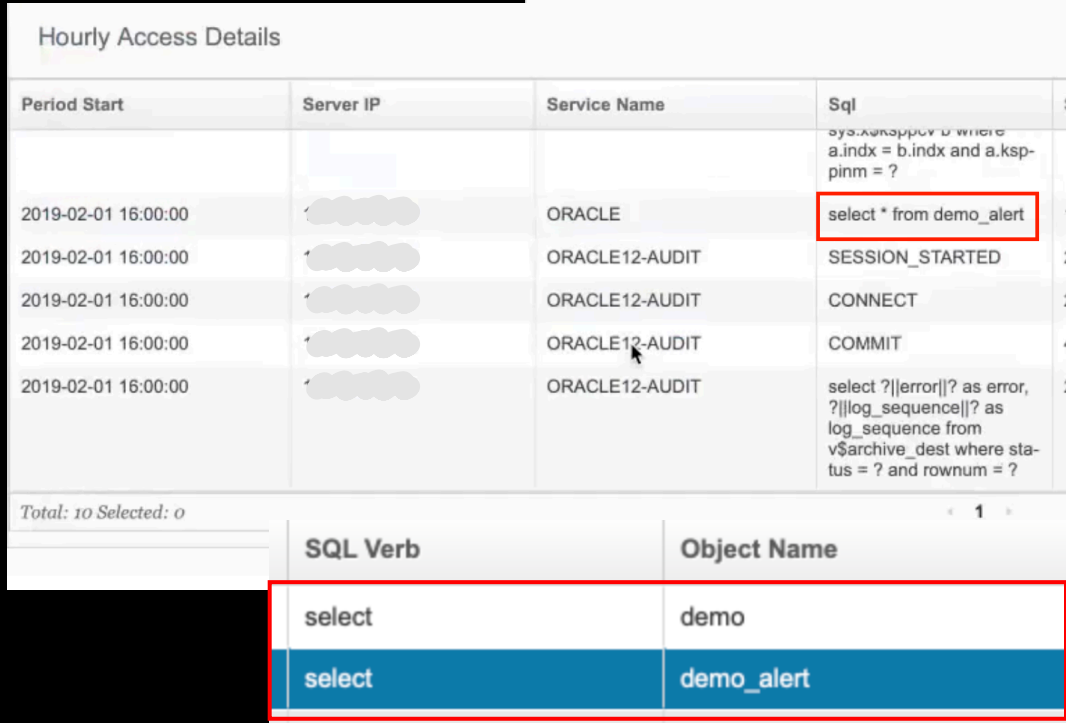
Monitoring using Native Logs



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)





Facilitate Secure Hybrid Cloud Adoption

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

Collection Mechanism	Sources
External-TAP	• **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	• AWS Aurora PostgreSQL • AWS Aurora MySQL (planned)
Azure Event Hubs	• Azure SQL Server • Azure SQL DW • Azure Cosmos DB (Mongo, Cassandra, SQL, Gremlin, Table)
Native Logs (Connectors)	• AWS Oracle RDS. Amazon Redshift (BP provided on Guardium AppX). More in plans
S-TAPs	• 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)

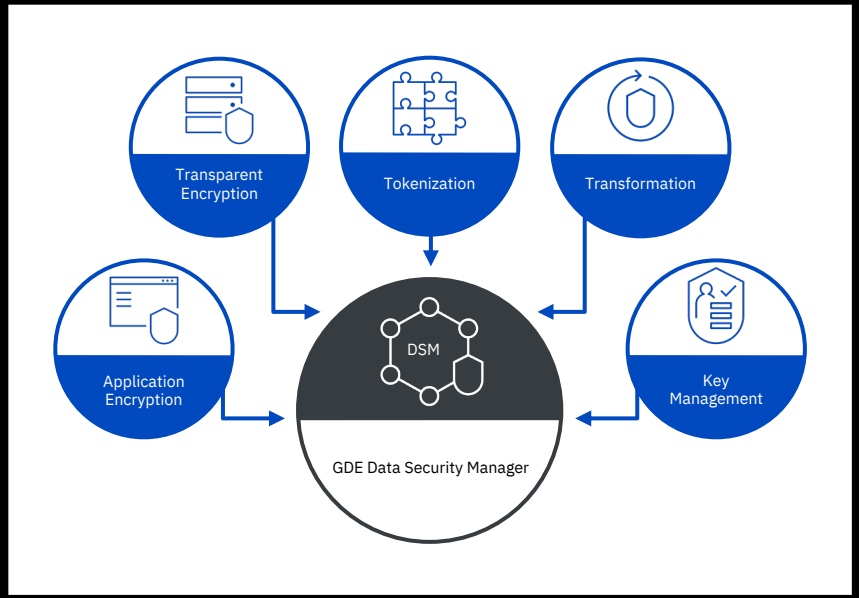
Core Highlights

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/

IBM **Security**

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions