IBM Security

Guardium External TAP Overview

Gali Diamant
Senior Software Architect - IBM Security Guardium

IBM

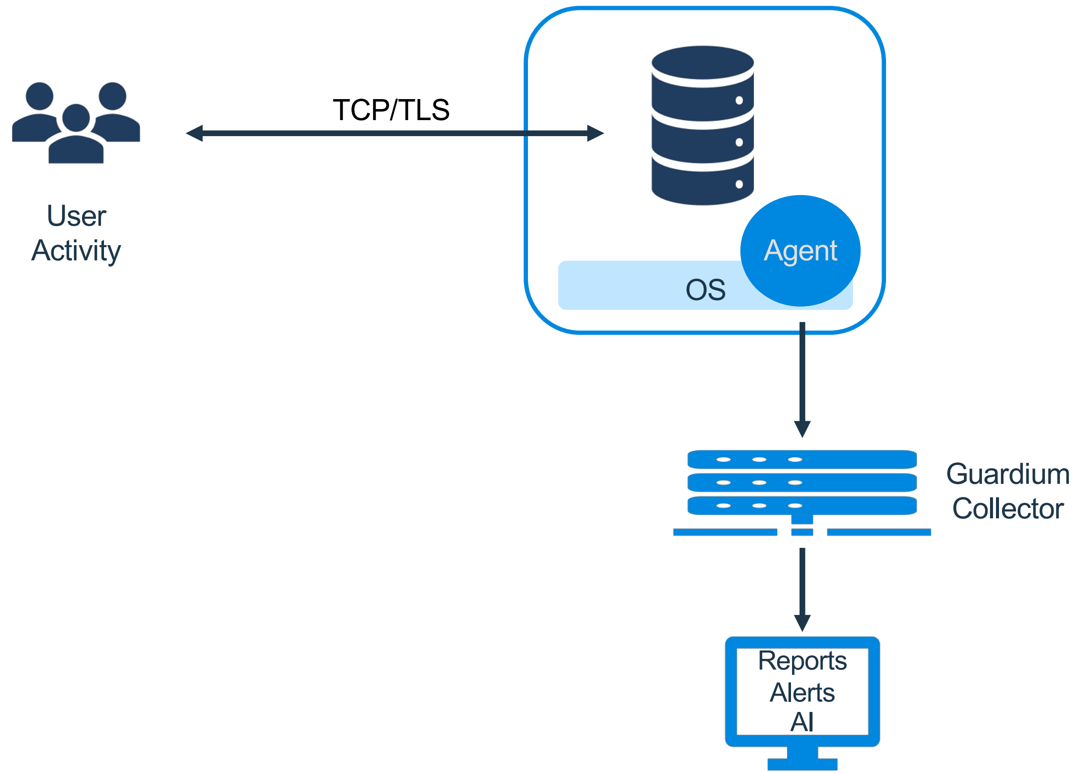
Please Note:

- IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM’s sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- 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.

Agenda

- Overview
- Challenges
- Solution
- Demo

Traditional Agent-Based Database Monitoring

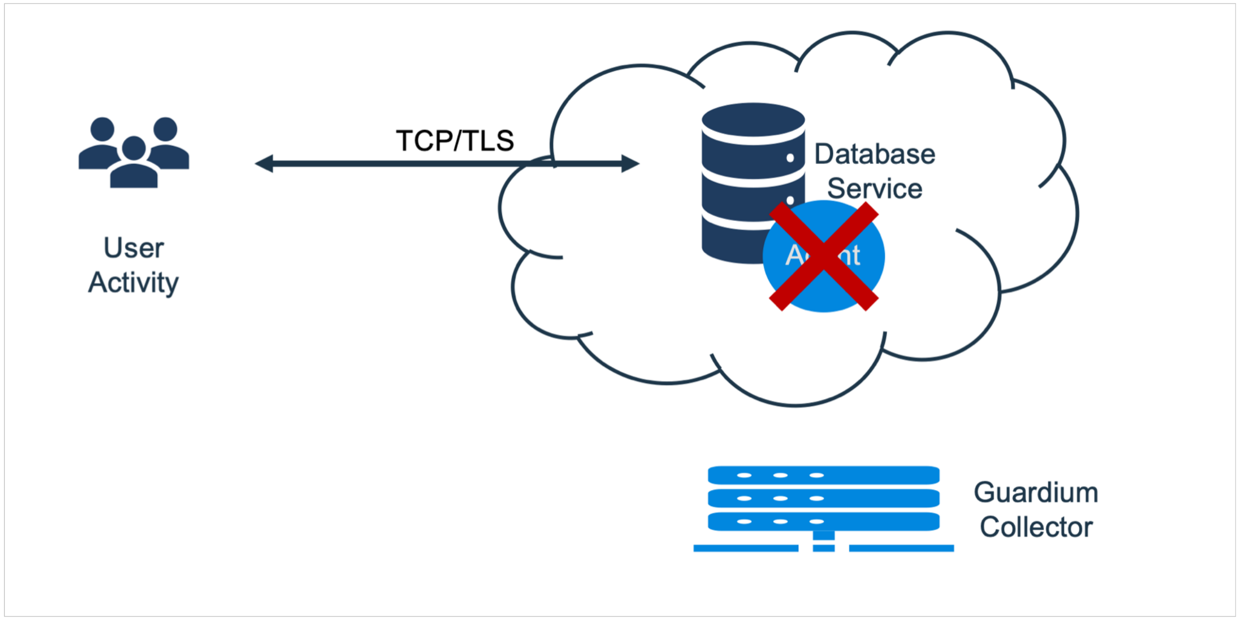


New Trends in DB usage

- **DBaaS**
- Managed Database services in the Cloud

- **Containerized Databases**
- On-premise and Cloud images

Challenges - DBaaS



User Activity

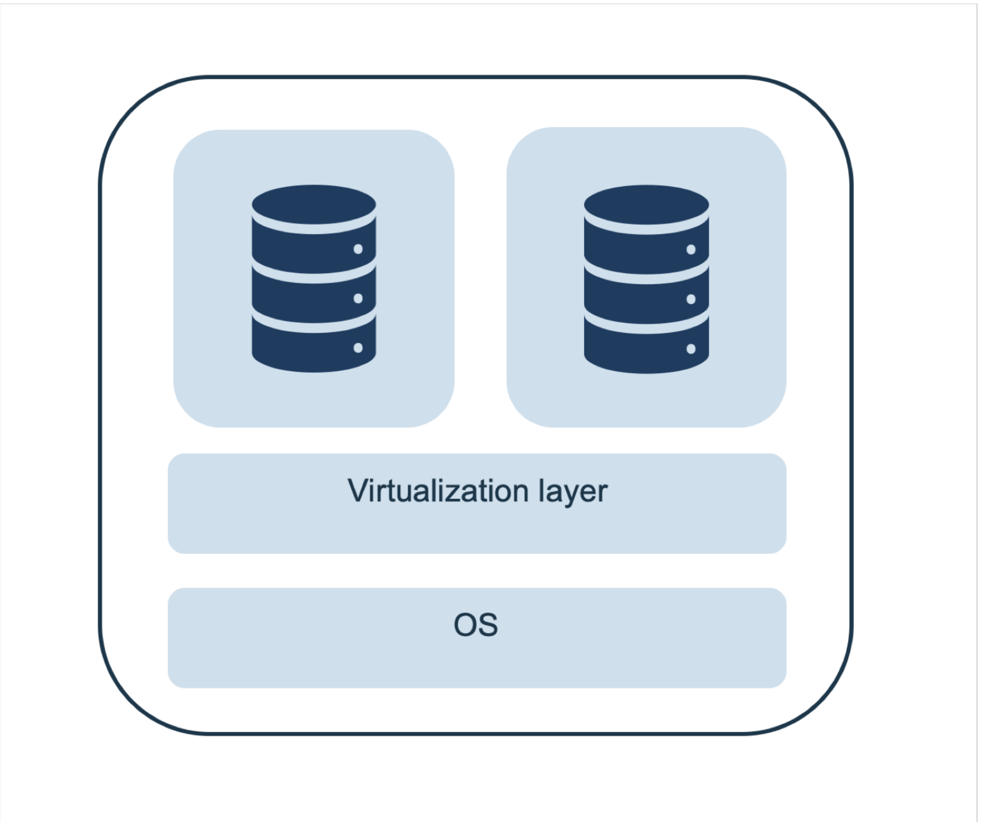
TCP/TLS

Database Service

A nt

Guardium Collector

Challenges - Containerized DBs



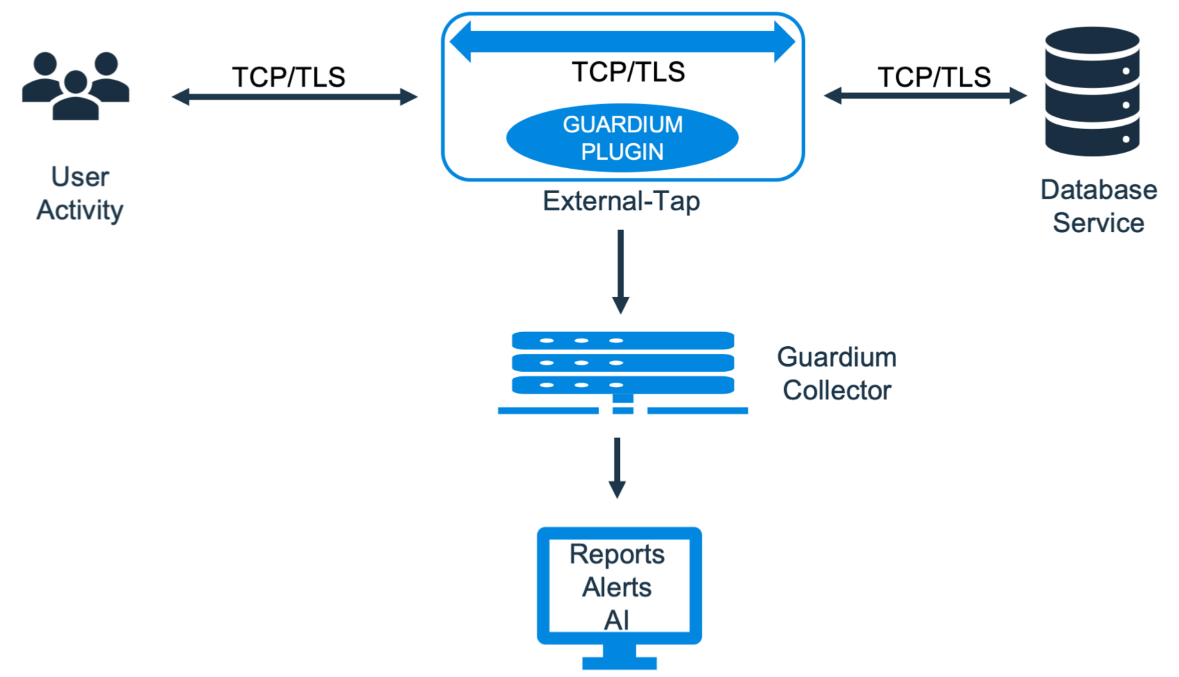
Problem

- Support monitoring capabilities for DBaaS and Containerized DBs
- Consistent approach to data protection across on-premises and cloud environments

Solution - The new Guardium External-Tap

- New and previously unavailable levels of visibility into activity
- Near real-time monitoring
- Agent capabilities (in roadmap)
  - ✓ Redaction
  - ✓ Firewall

Guardium External-Tap



User Activity

TCP/TLS

TCP/TLS

GUARDIUM PLUGIN

External-Tap

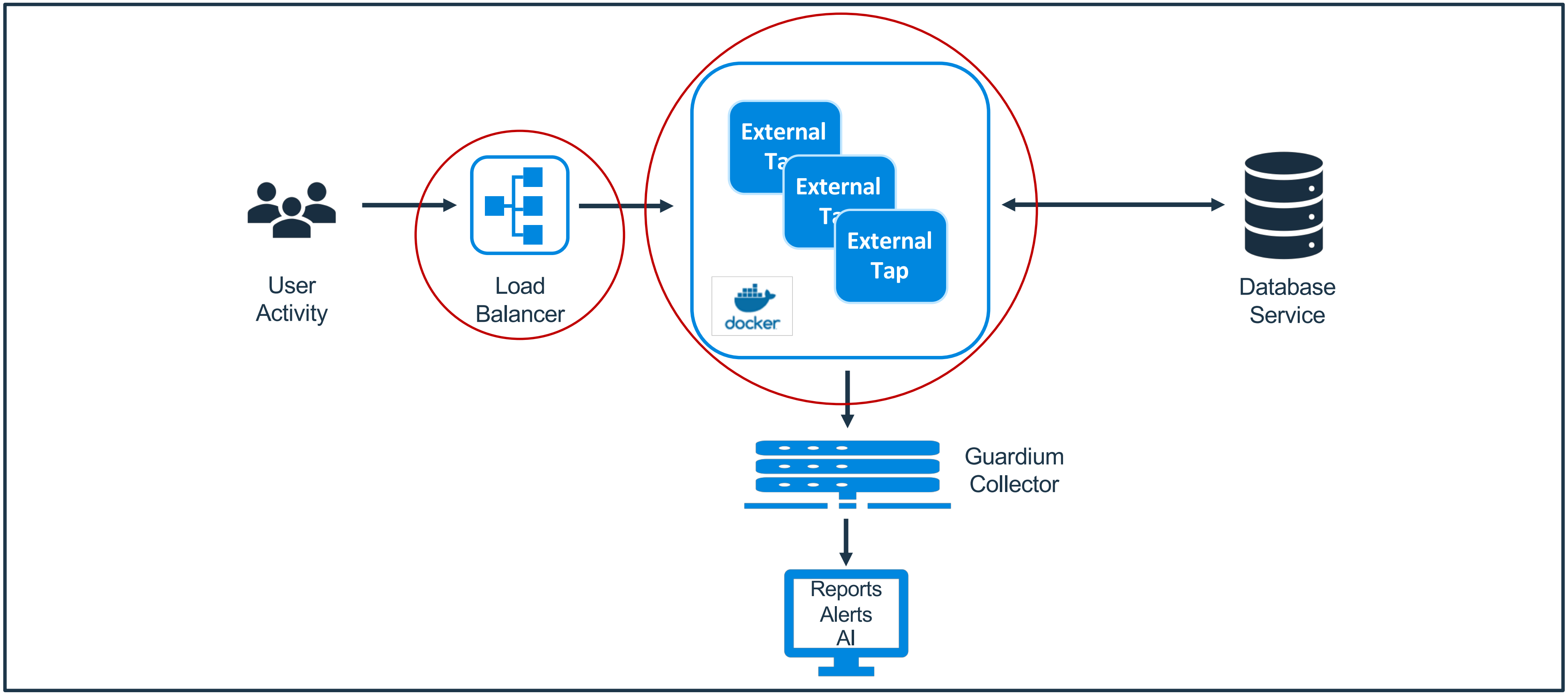
TCP/TLS

Database Service

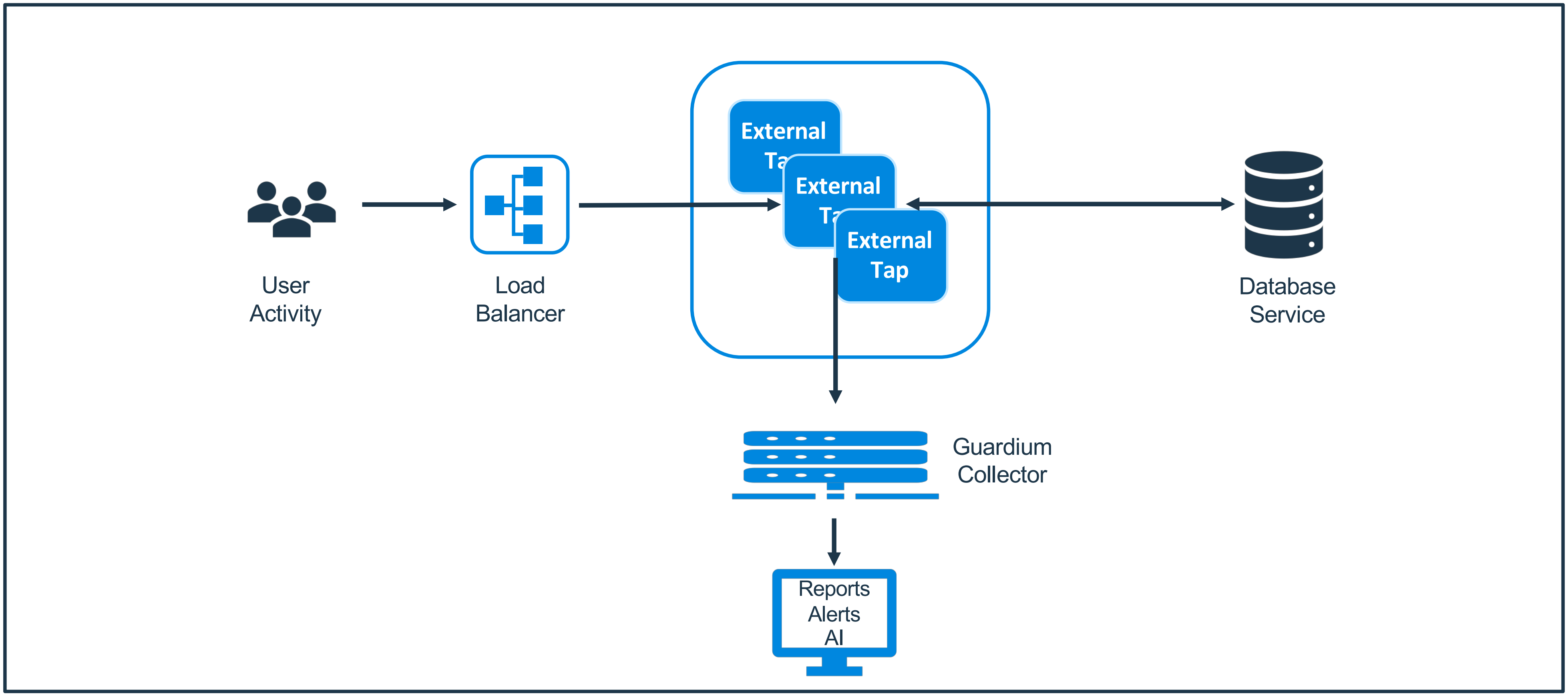
Guardium Collector

Reports
Alerts
AI

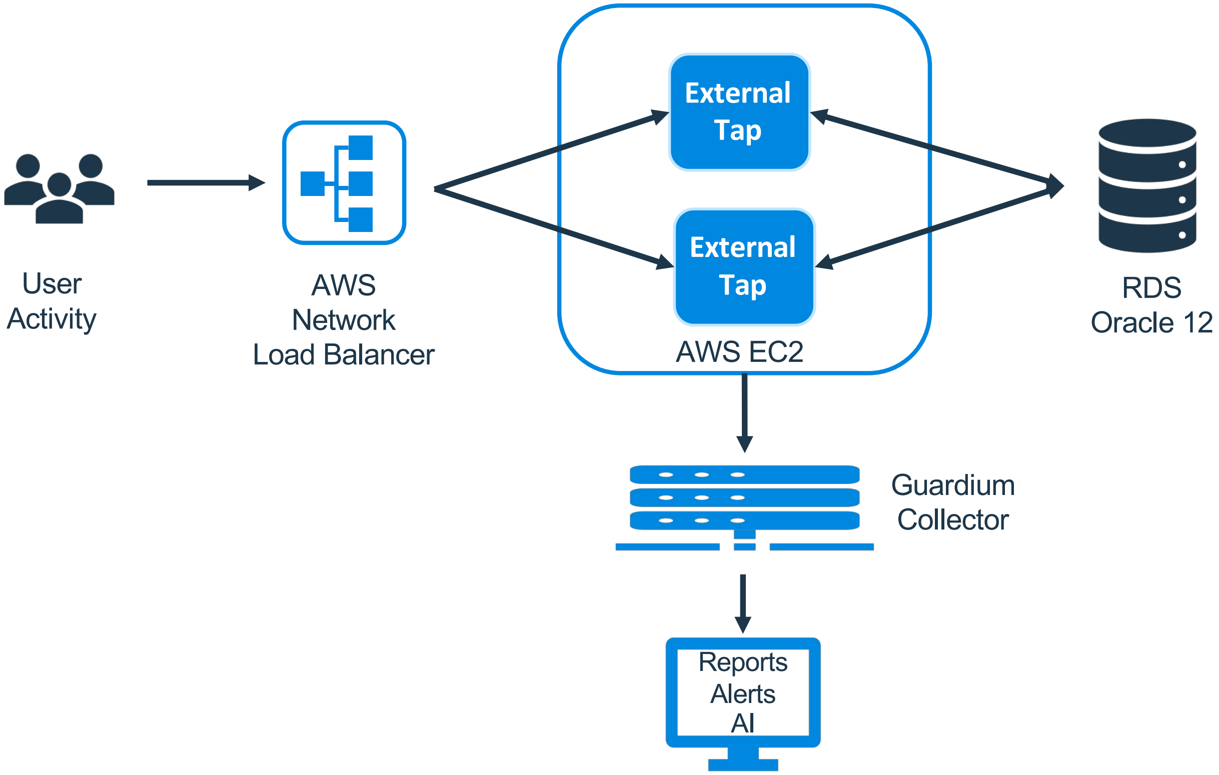
Guardium External-Tap Architecture



Guardium External-Tap Connection Set Up



Demo – AWS


User Activity
AWS Network Load Balancer
External Tap
External Tap
AWS EC2
RDS Oracle 12
Guardium Collector
Reports
Alerts
AI

External Tap - Future Plans

- Kubernetes for deploying, management and scaling

- Additional Functionality
  - ✓ S-GATE Terminate
  - ✓ Data Redaction

Supported Databases

10.6	Roadmap
✓ Oracle/RDS	✓ MySQL
✓ SQL Server/RDS	✓ Postgres SQL
✓ SQL Server/Azure	✓ MariaDB
✓ SQL Data Warehouse	✓ IBM Db2
✓ MongoDB in containers	✓ DB2 Warehouse on Cloud

IBM Security

THANK YOU

FOLLOW US ON:

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

IBM®