



# Guardium External TAP Overview



**Gali Diamant**  
**Senior Software Architect - IBM Security Guardium**





## Please Note:

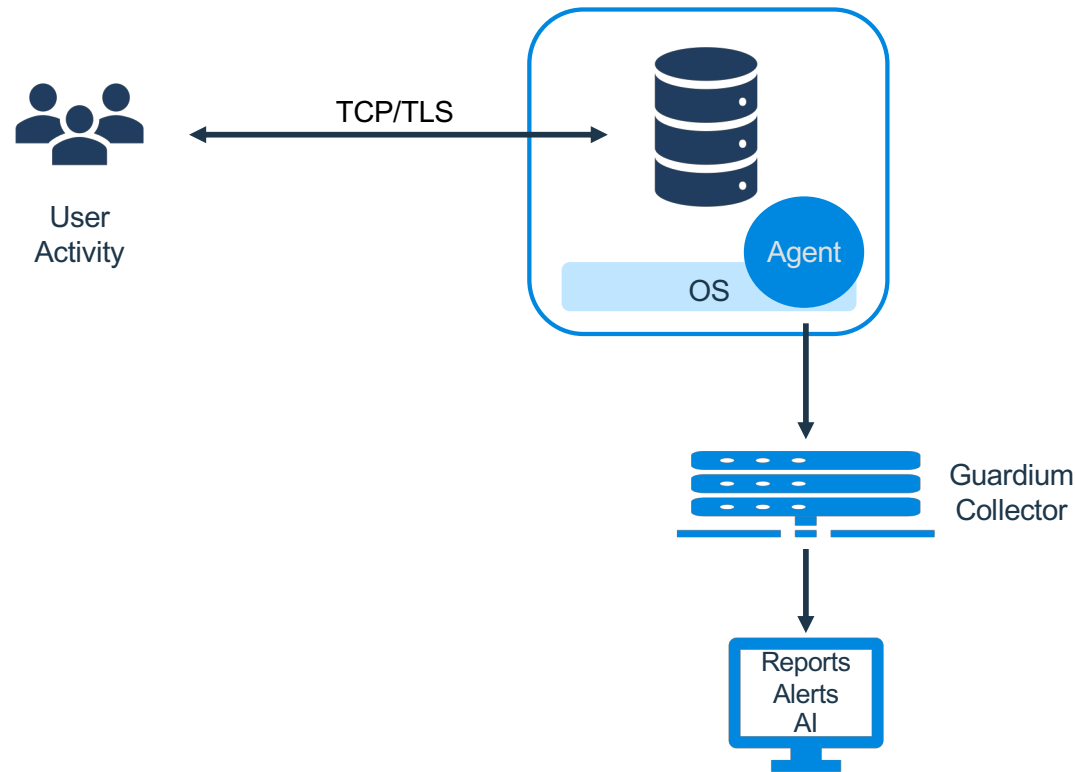
- IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- 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

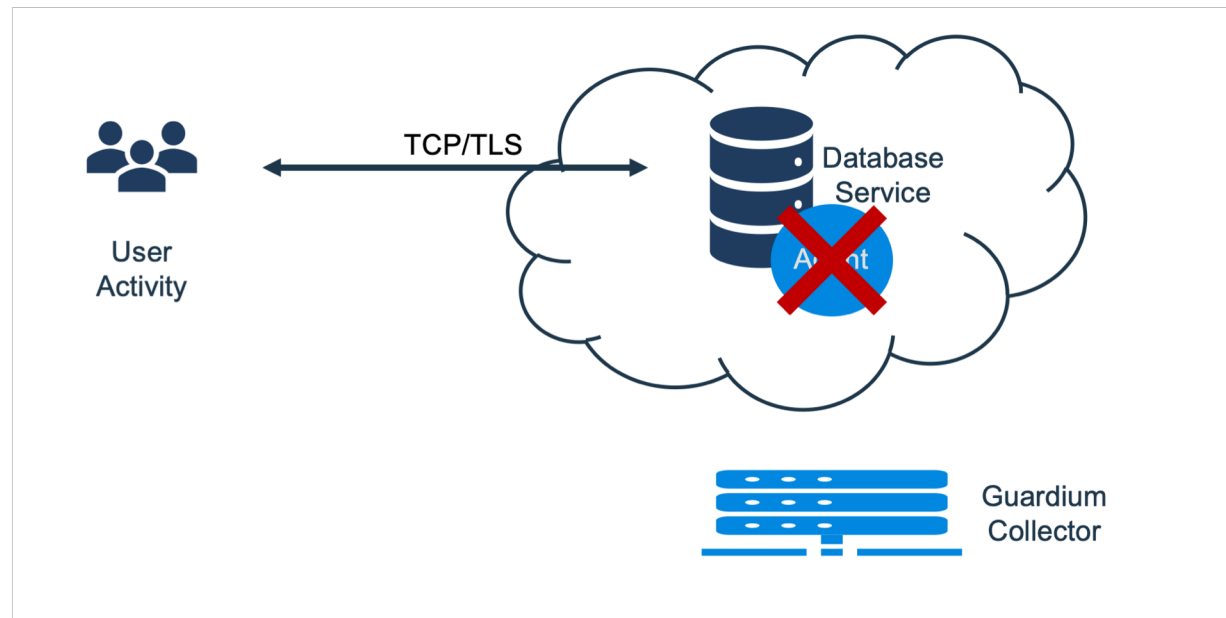




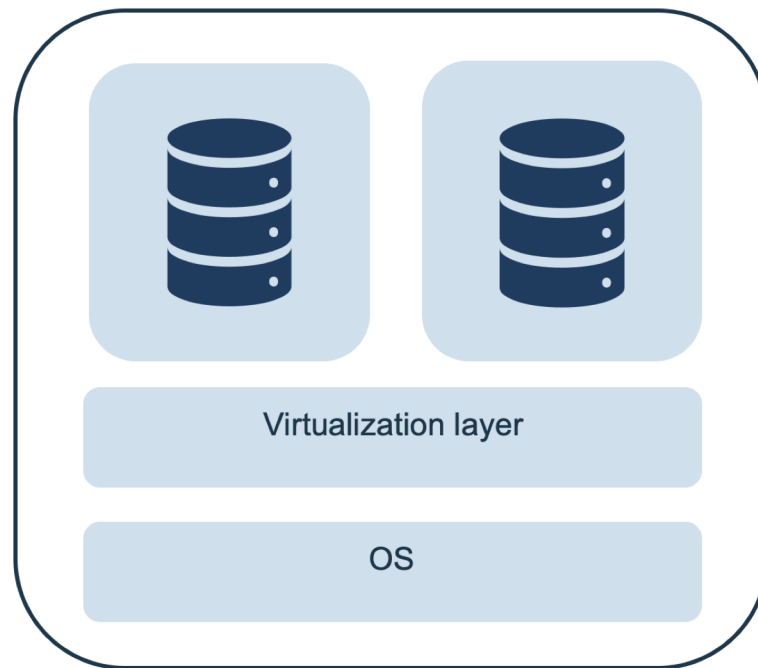
## New Trends in DB usage

- **DBaaS**
  - Managed Database services in the Cloud
- **Containerized Databases**
  - On-premise and Cloud images

# Challenges - DBaaS



## Challenges - Containerized DBs





# Problem

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

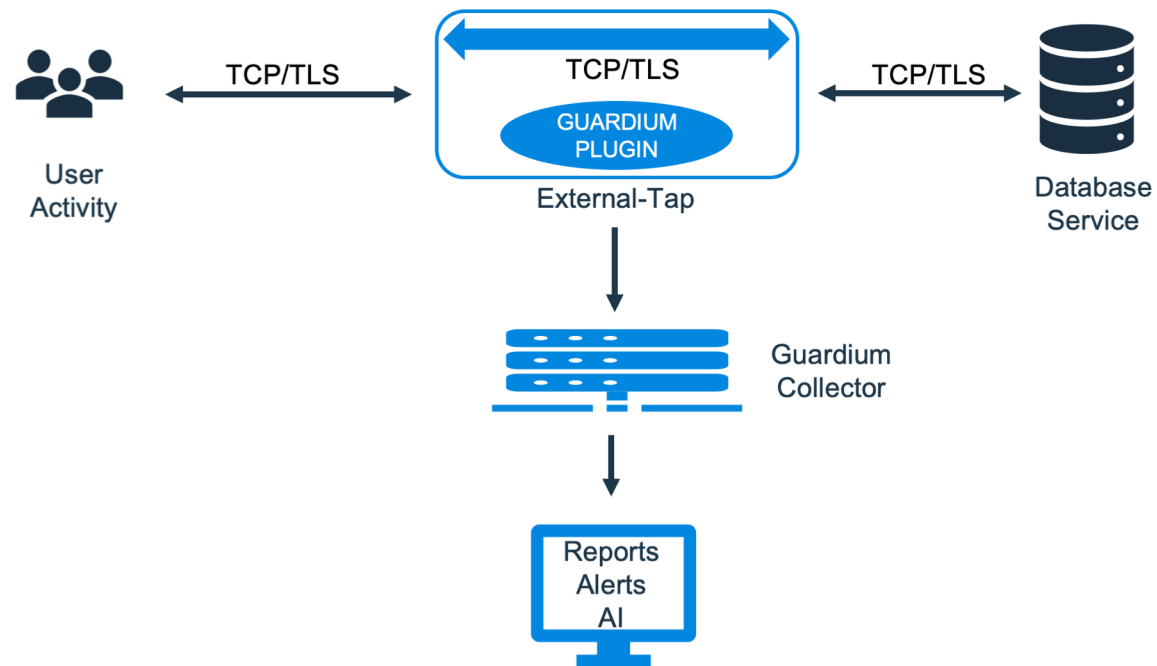




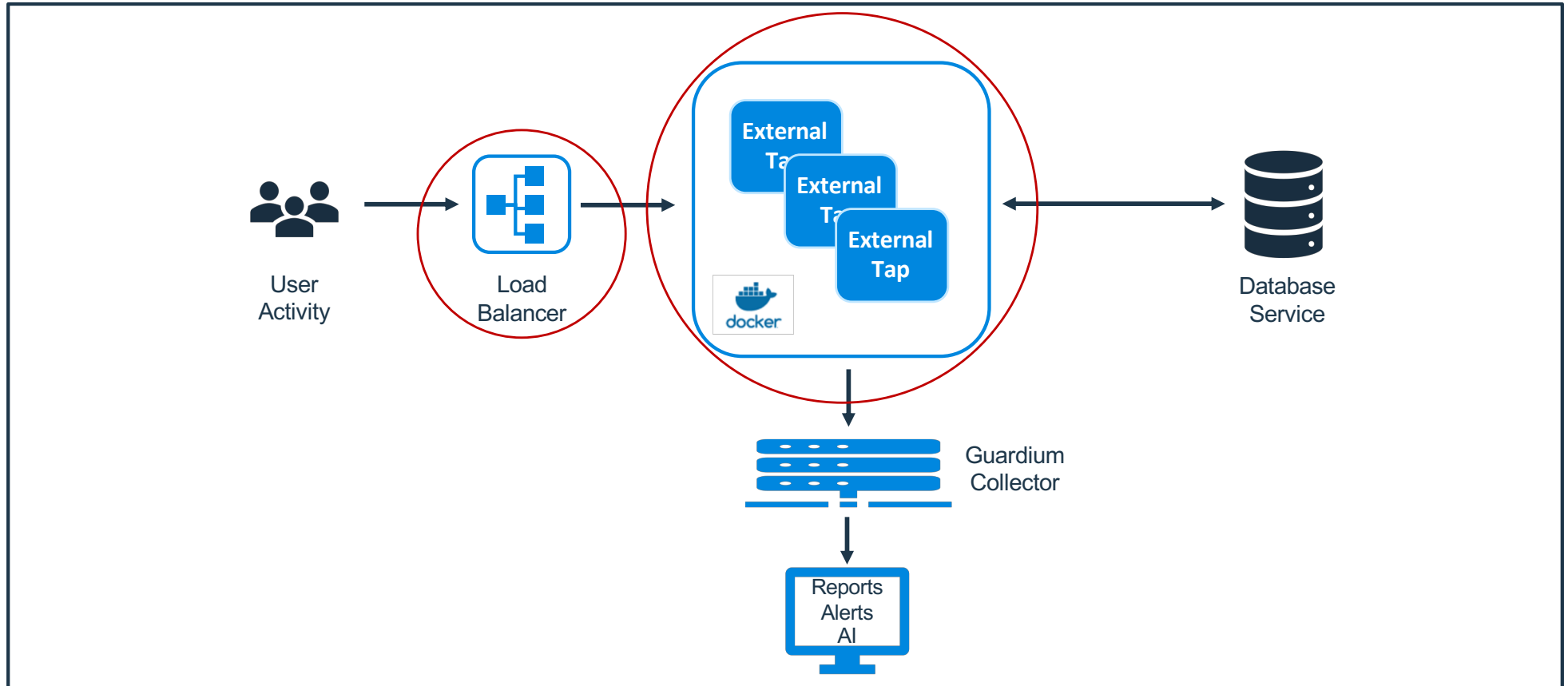
## Solution - The new Guardium External-Tap

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

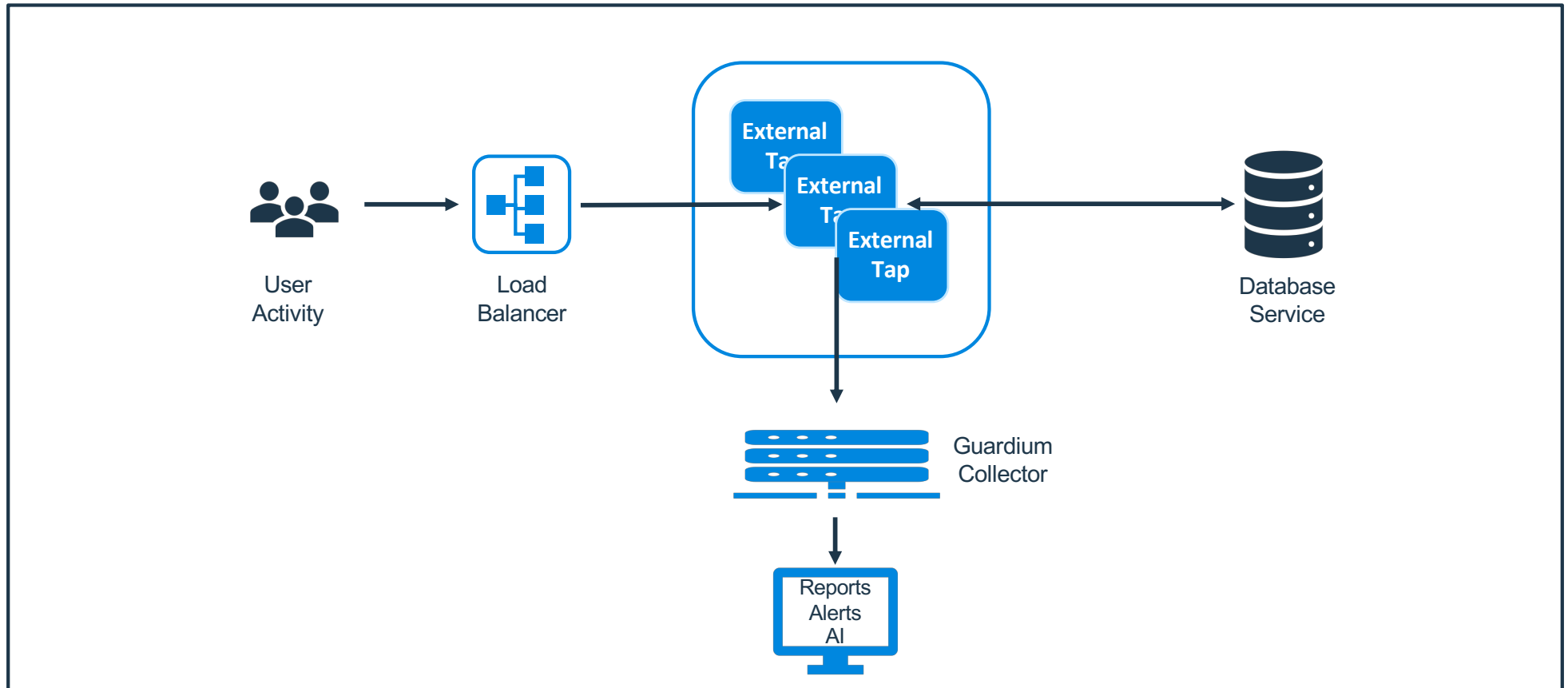
# Guardium External-Tap



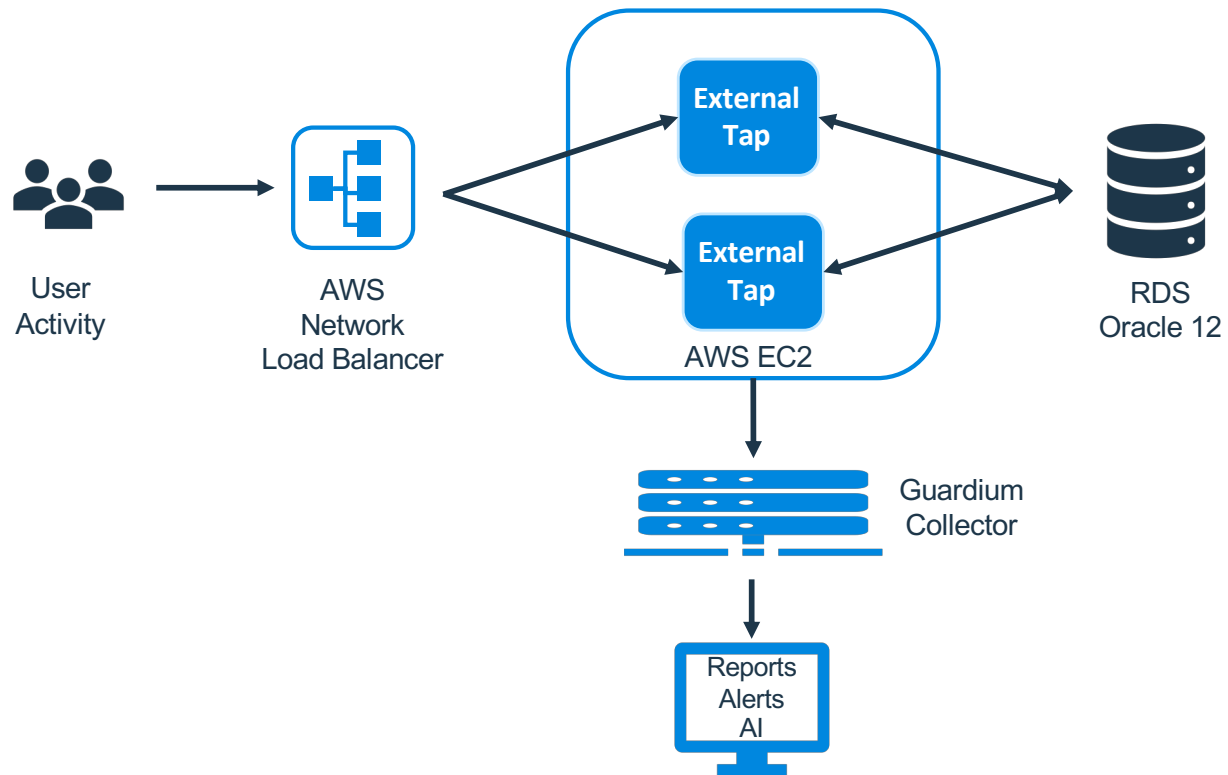
# Guardium External-Tap Architecture



# Guardium External-Tap Connection Set Up



## Demo – AWS





## External Tap - Future Plans

- Kubernetes for deploying, management and scaling
- Additional Functionality
  - ✓ S-GATE Terminate
  - ✓ Data Redaction



## Supported Databases

10.6	Roadmap
<ul style="list-style-type: none"><li>✓ Oracle/RDS</li><li>✓ SQL Server/RDS</li><li>✓ SQL Server/Azure</li><li>✓ SQL Data Warehouse</li><li>✓ MongoDB in containers</li></ul>	<ul style="list-style-type: none"><li>✓ MySQL</li><li>✓ Postgres SQL</li><li>✓ MariaDB</li><li>✓ IBM Db2</li><li>✓ DB2 Warehouse on Cloud</li></ul>



# THANK YOU

FOLLOW US ON:

-  [ibm.com/security](https://ibm.com/security)
-  [securityintelligence.com](https://securityintelligence.com)
-  [xforce.ibmcloud.com](https://xforce.ibmcloud.com)
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  [youtube/user/ibmsecuritysolutions](https://youtube/user/ibmsecuritysolutions)

© Copyright IBM Corporation 2016. 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.

