imperva

WHITEPAPER

Five Steps to Ensuring Secure and Compliant AWS RDS

Executive summary

Read this document to understand the security and auditing capabilities you'll need to protect your data on Amazon Relational Database Service (RDS).

If you're like other fast-paced companies, instead of building and maintaining your own databases, you're turning to database-as-a-service (DBaaS) programs that offer fast access to virtually unlimited storage capacity. In many cases, the cloud option makes more business sense as, for many, the tradeoff of agility dwarfs the nagging need for control.

However, for those of you in regulated industries or holding sensitive business secrets, security and compliance are persisting concerns that slow DBaaS programs. And that makes sense too because data protection failures are at the heart of every breach.

Data protection objectives and privacy compliance requirements don't change because your data is in the cloud, but the velocity and flexibility of the platform do require new considerations. This paper explores the areas that warrant your attention before the auditor comes knocking and demands proof.

Background note: DBaaS provides the equipment, software, and infrastructure needed for businesses to run their database on the DBaaS itself, rather than putting something together in-house. Examples of DBaaS include Amazon RDS, Microsoft Azure SQL, and Google Cloud Platform Cloud SQL.

RDS security and compliance challenges

AWS has come a long way in adding security and agility capabilities to database creation and management. At the beginning of AWS RDS adoption programs, most decision-makers go through a checklist of must-haves and conclude that AWS RDS has many of the fundamental security capabilities needed:

- Identity and Access Management (IAM)
- Encryption
- Logging (CloudTrail)

But, is that all it takes for a DBaaS program to be secure and compliant? Maybe not.

Interestingly, nearly a decade after initial publication, many elements of Gene Kim's "The Phoenix Project" storyline of security trailing the business continue today. Even now, for many organizations, security and audit teams are rarely a part of the initial cloud platform decision-making team. How prevalent the situation persists is revealed in the Cloud Security Alliance's (CSA, 2019) research.

More than three-quarters of respondents found compliance and audits to be a challenging aspect of managing the security of their public cloud resources. The implications are that, post-adoption, more accurately at product launch, there are few options besides rolling back or making mammoth changes to the programs in flight - otherwise known as crippling business delays.

More than three-quarters of respondents found compliance and audits to be a challenging aspect of managing the security of their public cloud resources, post-adoption.

Cloud Security Alliance (CSA, 2019)

AWS and other cloud providers explain away this situation as the shared responsibility model - a simple concept, but fuzzy to interpret as your responsibilities and theirs blur in platform-as-a-service (PaaS) business models and their promotional literature

Ironing out the implications of shared responsibilities or what portions of security and compliance your company owns early on in the process is best. Otherwise we relive the boxing champion's infamous declaration that, "everybody has a plan until they get punched in the mouth." In our case, that's when the auditor comes knocking.

Prevention vs. detection and response

Joe Sullivan, former CISO at Uber and Facebook, gave an interesting interview with Andreessen Horowitz (a16z Podcast, 2020). Joe said, "the role of a security leader is first to prevent something bad from happening...Job number two is to assume that you fail at that...with the ability to detect something bad going wrong as quickly as possible." Wise words. That's the difference between the old paradigms of prevention defense vs. a more realistic view of layered detection and response. Many Dev and Ops decision-makers leading the way to the cloud miss this point. The media is littered with breaches that prove prevention alone is insufficient, including the 5,185 hacking initiated data breaches reported in 2019. Attackers don't play by rules.

Although presented as an optional item referred to as "advanced monitoring" in the cloud platform documentation, detection and response are actually the other half of your security and compliance program.

Cloud visibility is a major pain point

Cloud providers are doing wonderful work. Amazon's CloudTrail logging and CloudWatch alerting added visibility into events happening within the virtual private cloud (VPC). Yet, three-quarters of CSA respondents found compliance and preparing for audits to be a challenging aspect of managing the security of their public cloud resources, postadoption. What's happening?

AWS automates the process that gives you the agility and speed of the cloud while creating mountains of information in the form of logs and configuration files. These, in turn, provide visibility into the goings-on in RDS or, at least, the raw information. The shared responsibility model says you're responsible for your data protection, which means you'll have to correlate that mountain of logs into something actionable. The critical task of inventorying fluid databases, classifying the criticality of data entries, and tracking movement and usage of the data are your responsibilities. And your ability to do all that at the speed of the cloud needs additional tooling.

Regulatory mandates increase the cost of noncompliance

British Airways was fined £183.4 million for GDPR non-compliance

The repercussion of regulatory misdeeds has taken a turn. Capital One, Uber, Facebook, and Equifax are just a few of the C-suite casualties of security failures. British Airways, for example was fined £183.4 million ($230M) for GDPR non-compliance - quite a bit less than the 2% maximum, but significant nonetheless. In this threat environment, other regulations are tightening requirements and increasing penalties.

Many elements of database management reduce your workload and improve underlying security with RDS adoption. But the attack surface is larger, and attackers want your data.

Data in cloud increases the data risk

Among the many benefits of the cloud is the is simplicity and speed it offers. RDS is an excellent example of how easy it is to accelerate design and deployment. However, one of the Achilles' heels of speed is the ease of making a mistake, and mistakes in the cloud - in most cases - have dire consequences. But data governance says you have to be able to track every bit of where it is, what the data is, and who is accessing it - regardless of where it is hosted.

> **"PCI Requirement 10: Track and monitor all access to network resources and cardholder data... A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused."**

Translated, this means you must know the existence of every DB, the classification of the columns, and who accessed it - all at the speed of the cloud. Like it or not, this isn't the responsibility of AWS.

Your role in database security and compliance in the cloud

Now we get to your part in ensuring the security and compliance of your AWS RDS-hosted data with these five essentials.

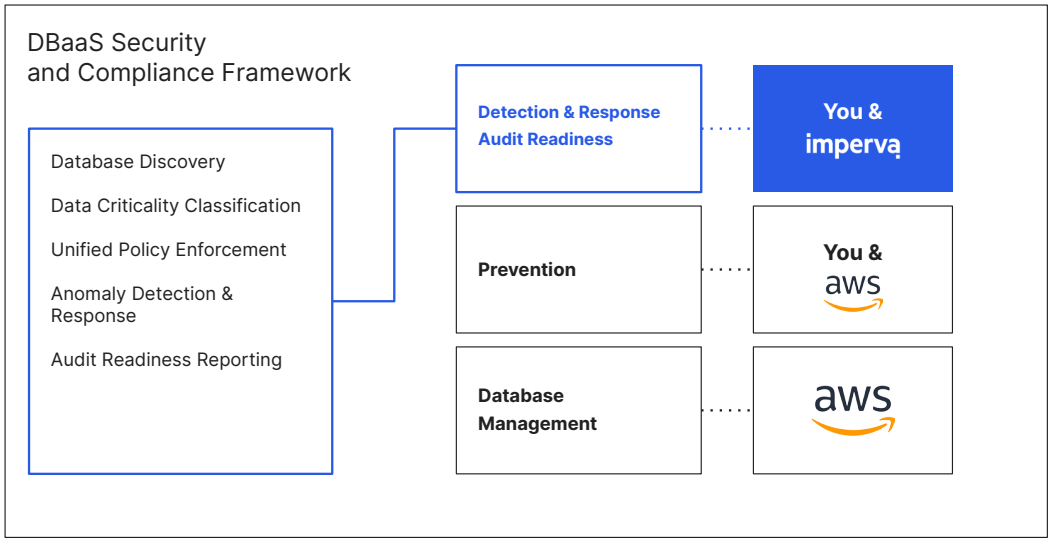

Figure 1: Your Role in database security and compliance in the cloud

DATABASE DISCOVERY - INVENTORY ALL YOUR DATABASES (CONTINUOUSLY)

The Center for Internet Security 20 (CIS 20, originally SANS 20) teaches us that the first step in security is the ability to inventory assets. The idea being that you can't protect what you don't know exists. RDS adds agility and flexibility that promotes the decentralization of data stores. There is a natural drift that occurs when databases can be created, deleted, and cloned with a few clicks by your Dev and Ops team. In this hyper- agile environment, your ability to track active, inactive, and new DBs that popup or\ disappear has to be automated.

DATA CRITICALITY CLASSIFICATION

Once you solve the database discovery challenges, you need to know what is in those databases. In particular, business secrets or privacy-regulated data, like credit cards and personal identity information (PII) has to be treated accordingly. Databases are dynamic. Predefined definitions of the data rows and columns may be obsolete moments after you think you know what is in there. Luckily, we have solutions that can keep pace with these changes.

UNIFIED POLICY ENFORCEMENT

Deploy a common security and compliance policy for consistent security controls across all of your AWS RDS database assets. Audit all types of databases across all your VPC with one lens. Protect data in AWS with alerts of unauthorized activity.

ANOMALY DETECTION & RESPONSE

Use the same rigorous monitoring used for on-premises databases with your data stored on AWS RDS. Even if you're a cloud-first company, the rigor still applies to you. Cloud database activity monitoring should use the information available from AWS infrastructures, like RDS configs, CloudTrail logs, CloudWatch alerts, and the native DB audit logs. Then layer on context-based policies and add machine learning to discover anomalies..

AUDIT READINESS REPORTING

Be ready to demonstrate compliance with data protection and privacy regulations for all of the databases. Get detailed reports for regulations such as GDPR, SOX, PCI DSS, and more.

Introduction to Imperva Cloud Data Security

Attackers are after data, and security continues to lag cloud database programs, leaving your critical data exposed to attackers. Imperva Cloud Data Security (CDS), delivered as a service, bridges the chasm between the DevOps-driven program's need for agility and security's obligation for visibility with cloud-native DBaaS security and compliance monitoring that doesn't impede the innovation pipeline.

CDS complements the cloud providers' preventive security capabilities like access management and encryption with the other half of the security and compliance programs requirement for detection, response and audit readiness:

- Continuous monitoring
- Database discovery
- Data entry classification
- Policy alerting
- Anomaly detection
- Audit readiness reporting
- SaaS agility
- Cloud-native

Unlike traditional database monitoring tools, CDS doesn't sit in front of your database as a proxy, modifying the path from user to data and creating a single point of failure, or require installing agents. Instead, CDS seamlessly collects cloud-native infrastructure and database logs to give you instant visibility into your data hosted in RDS. In fact, CDS can be onboarded in minutes to quickly ensure your security is in step with your business growth programs.

Learn more about Imperva's CDS by visiting the product information page.

Imperva is an analyst-recognized, **cybersecurity leader** championing the fight to **secure data and applications** wherever they reside.