imperva
Snapshot

SOLUTION BRIEF

Imperva Snapshot™

DBaaS Vulnerability & Classification Tool

Introduction

Database-as-a-Service (DBaaS) is one of the fastest growing cloud services being used to support transformation and advanced DevOps efforts, offering flexibility and significant operational efficiencies. It also brings agility, enabling businesses to develop and deploy new services and applications more quickly, thereby aligning with the overall transformation effort. However, due to the dynamic nature of the cloud environment, security teams are very concerned with the lack of visibility they have on their data in the cloud, including who has access to what data, and how this poses exposure risks.

Click-of-a-button experience to view current cloud data risks

Imperva snapshot™ Cloud Database security risk assessment tool provides a free and easy way to intermittently assess security and compliance status of your database. Delivered as an easy-to-deploy Serverless application deployed in your environments, our tool empowers security teams with a cloud-native solution tailored to review the current status of data living in each of your databases as well as the security and compliance status of the database itself.

It offers you real-time visibility into the type of data stored and what regulations and frameworks may apply . With this tool you can evaluate the database security status without being a database expert. **Imperva snapshot™** helps you build a plan to secure your cloud database and comply with data privacy and protection regulations.

The tool analyses the following elements:

1. Data classification - Process stored data to identify content that may have privacy impact.
2. Database posture - Sessions, Configurations, environment settings
3. Database configuration - System tables, DB Roles, User info
4. Vulnerabilities - Identify, define, and catalog cybersecurity vulnerabilities according to publicly disclosed CVEs.

How to start **Imperva snapshot™** assessment?

1. Begin by registering to **Imperva snapshot™**
2. You will receive a Welcome email, open it and click **'Get Started**'
3. **You must be logged in to AWS before starting a scan** (through your SSO login if available, or through the AWS console)
4. Copy your database ID (RDS page), please note the AWS region
5. Click check boxes to allow AWS resources capabilities to run.
6. Click **Create stack** to run the tool or **Create change stack** to preview how the stack will be configured before creating the stack.

Notes:

- **Report data and some metadata for troubleshooting and analysis is kept for 30 days. Other raw metadata is being anonymized and kept for future statistical and research purposes**
- **Upon completion,PDF Report is sent to the email account provided during registration**

Understanding compliance risks

Privacy regulations and consumer expectations around the secure storage of their data continue to evolve. The tool provides the means to quickly assess your Database status in regards to security vulnerabilities, privacy regulations (GDPR, CCPA) and compliance requirements for the cloud data stores (DISA & CIS).

imperva Snapshot

Safe & secure Database scan

The tool provides CISO, InfoSec, SRE and Security Teams a quick and ultra safe way to assess cloud data risks related to database security vulnerability and privacy compliance without the need to perform complicated registrations or signup into SaaS products, just a-click-of-a-button experience..
The entire database evaluation process is performed on your own account.

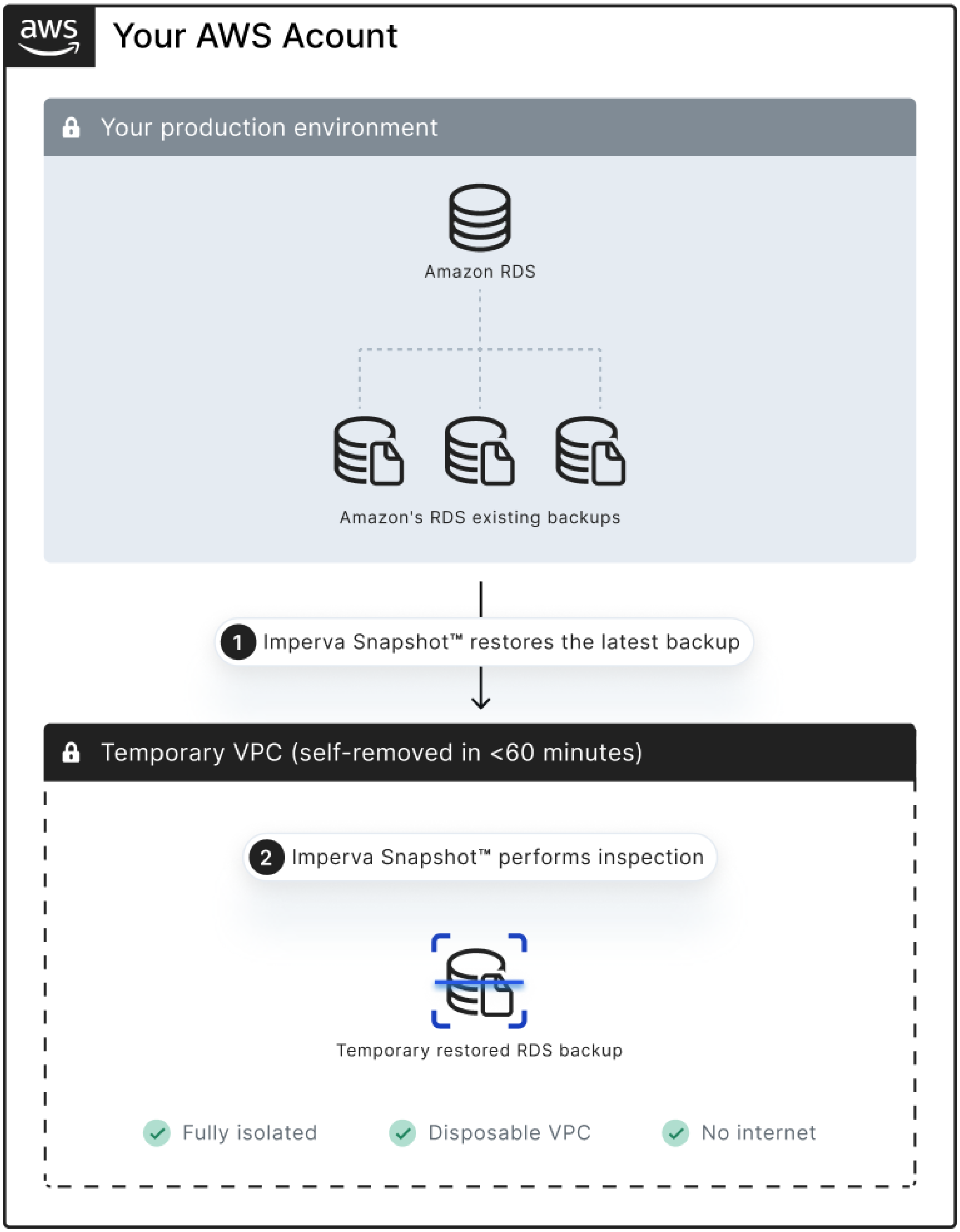
Privacy

The tool is designed to maintain customer and users privacy

- Data is processed at customer VPC (virtual private cloud) environment
- No actual data is leaving customer VPC
- The service collects security evaluation test results and Imperva Snapshot related operational data
  - Data is categorized according to the privacy assessment categories
  - No sensitive data is collected or identified
- The meta data is sent to Imperva to support
  - Sending report to the user who requested the report (Run the tool)
  - Operational support in case of malfunction
- Data sent to Imperva service is encrypted at rest

imperva

Snapshot



Your AWS Acount

Your production environment

Amazon RDS

Amazon's RDS existing backups

1 Imperva Snapshot™ restores the latest backup

Temporary VPC (self-removed in <60 minutes)

2 Imperva Snapshot™ performs inspection

Temporary restored RDS backup

✓ Fully isolated ✓ Disposable VPC ✓ No internet

Imperva Snapshot™ Operation flow diagram

Method

The tool is designed to operate with confidentiality, The collected data is maintained within your account until the report data is completed. Once the report data is sent for report creation, the tool and all of its components are erased from your account.

The entire tool operation does not have any impact on your production databases.

The tool's operation flow is as follows:

1. The user is logged to the AWS account
2. The user is directed
3. The User enters the Database name to be inspected
4. The tool deploys an isolated sandbox environment created by us...
5. The sandbox environment restores a temporary database from a snapshot, your snapshot.
6. A temporary database is created from a previously saved DB snapshot within the tool's isolated environment at your own account
7. The tool runs the following checks:
    a. Cloud database posture misconfigurations
    b. Database Security vulnerability assessment according to known issues and CVEs
    c. Classify sensitive data according to personal data categories
8. The raw data is processed and a statistical analysis is performed.
9. The statistical results are sent in secured, machine readable format to Imperva.
10. Imperva service creates a user readable PDF report
11. **Upon completion, PDF Report is sent to the email account provided during registration**

Key findings

Security risks

The following are some of the security risks and vulnerabilities that are mapped according to known CVEs and Imperva's database risk prevention practices:

1. Audit trail issues - some audit features may be turned off and may prevent your SOC teams from performing proper security investigations. This may refer to User and Entities activities monitoring within the Database, adding or removing data as well as access activities from the outside.
2. Records with insufficient information - some records may be wrongly configured to collect partial data which prevent from conducting adequate security investigations.
3. Configuration drifts - Some processes may create task specific credentials which are not removed when the tasks are completed
4. Database encryption - Database may not be encrypted properly to avoid data breaches and compliance to standards as well as compliance to privacy regulations.
5. Logging of various unsuccessful attempts to perform actions that may incorporate security risks like retrieval of use privileges, passwords, etc. (Maybe by hostile elements).
6. Unused database components that need to be removed.

Posture issues & risks

The following are some of the posture issues that may be found, both controllers and operators need to be aware of so proper mitigation may be applied:

1. Subscription to enable monitoring of events.
2. Use of default AWS usernames & credentials.
3. Misconfiguration of DB instance to environment
4. Publicly exposed DB instances or DB elements
5. DB snapshots Issues
6. Configuration data for newly created databases is not properly displayed.

7. Database high availability issues across regions & zones (May not confide to single zone)
8. Encryption at rest is not properly enabled
9. Database backups issues related to its retention periods
10. Configuration issues related to security groups and VPCs
11. Definition of database topics to be able to send outbound notifications
12. Auto upgrades proper configuration to maintain database resiliency to 3rd party vulnerabilities.
13. Event subscription enabled for security groups to ensure awareness and response in case of any relevant database affecting events.

Compliance to privacy

The tool scans the data within the database and signals sensitive private data that may require special attention. The database content is scanned, according to the data found the tool provides information of which data types are populated within it.

Personal data groups

Personalization Data: Political Affiliation, Religion, Biometrics, Ethnicity, Sexuality

Person Contact Data: Business/Person Name, Person First Name, email, Mobile, etc.

Personal Identifiers: Person ID, Citizenship ID, National ID

Person ID - Student ID, Health ID, Local ID

Supported categories

1. Access Codes
2. Password
3. Person Name
4. Person ID
5. Personal Data
6. Username

7. National ID
8. Credit Card
9. Email Address
10. Account Number
11. Financial Number
12. GPS
13. City
14. Mailing Address
15. Postal Code
16. Mailing Address
17. Network Address
18. Organization Name
19. Payroll
20. Gender
21. National ID
22. Vehicle Number
23. Phone Number

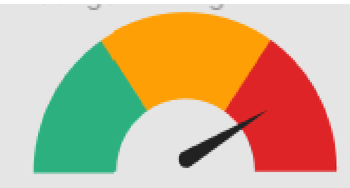
Report structure

Key findings

Risk levels

Overall risk level is determined as follows:

Risk level: HIGH



- **Posture -Any findings (1 or more) with CRITICAL and list this finding first**

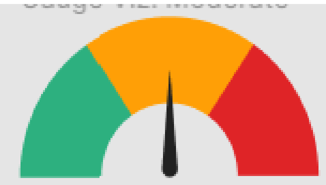
OR

- **Any number of CVEs with Severity: High**

OR

- **Any finding of private data without any encryption (RDS encryption or Any other type of encryption)**
  - **Person Name**
  - **Email Address**
  - **Phone number**
  - **Credit Card**

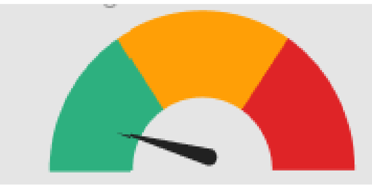
Risk level: MEDIUM



- **No CRITICAL or HIGH severity issues found**

  AND
- **40% or more with severity MEDIUM or MAJOR**

Risk level: Not HIGH, not Medium, but at least 1 finding



- **No CRITICAL or HIGH severity issues found**
  AND
- **61% or more issues with severity LOW or MINOR**

Risk level: No Risk Found

High Level Findings

Details the count of the following findings:

1. Cloud database misconfigurations
2. Cloud database vulnerabilities
3. Sensitive data misconfigurations

Possible remediation

Provide details for recommendation of risks found and possible mitigation or resolution.

Assessment summary

Provide statistics of issues found as follows:

1. Total assessment which identified issues
2. Number of security risks by risk level
3. Non-compliant assessments based on CIS & DISA frameworks
4. Security risks by categories
5. Top security risks

Data classification

Details statistics of privacy related data found in the cloud database

1. Total Data Records- Pie Chart Footnote, if needed
2. Sensitive Data by categories
3. Number of DB columns with privacy related data
4. Geo distribution of frameworks, standards & regulations that may apply

Security Risks

List of security risks found, the list may be limited by size in cases of large numbers of risks found.