imperva

# Imperva Snapshot™

Assessment of data security posture of cloud databases

**24 Oct 2021**

# Table of Contents

## Technology Brief

## Report Analysis

## Imperva Products

## Security Risks Appendix

# Technology Brief

A patent-pending approach for cloud database scanning

**In this section you will learn about:**

- Patent-pending cloud data security posture technology explained
- How does isolated inspection work?

PATENT PENDING

# Imperva Snapshot ™

A patent pending cloud-native technology that analyzes cloud databases, in a secured and production-safe technique

## 1-Click Deployment

Easily deployed through a Cloud Formation Template

## 100% serverless

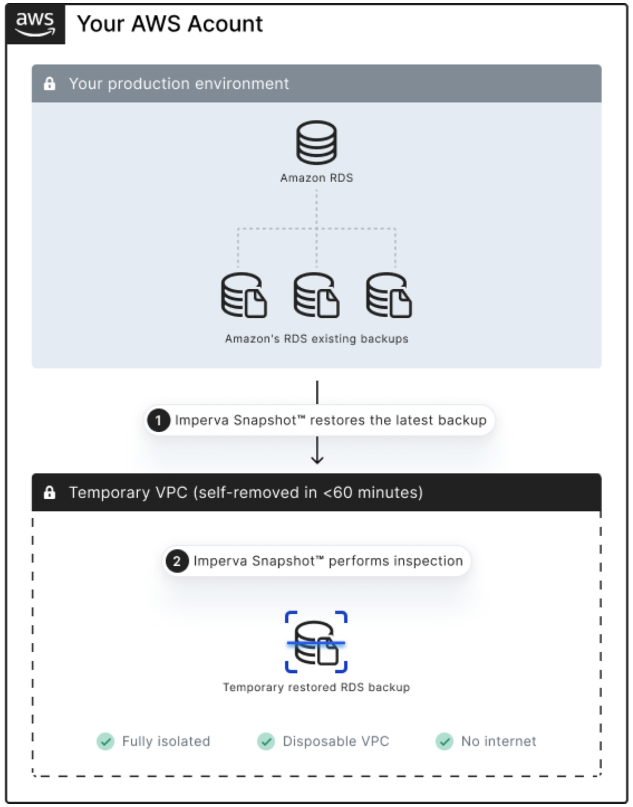
Cloud-native rapid inspection without a single agent

## Isolated, one-time inspection

Runs in an isolated network and disposes when done

## Production-safe

Zero access to production databases


aws
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

# Report Overview

**Imperva Snapshot ™ data security posture methodology**

1. A new, isolated Virtual Private Cloud (VPC) is created in your account to perform a short period, disposable assessment
2. A temporary database is restored from your existing RDS snapshot within an isolated VPC, detached from your production
3. Multiple inspection engines are triggered through the inspection process, all within the isolated snapshot
4. Upon completion, the report is sent while the isolated VPC is removed, including its restored RDS from the snapshot

## Data risk categories in this report:

### Misconfigurations & Posture

We check for risky configurations and bad hygiene

- No password expiration policy
- SSL not enabled
- Excessive permissions
- Too many DBAs

### Known Vulnerabilities

We scan for any exploits, known vulnerabilities, which can cause:

- Remote code execution
- Authentication bypass
- Privilege escalation
- Full database control

### Privacy & Compliance

We scan all content to identify sensitive data and display it by data types:

- Email, Credit card, ID, etc.
- Personal Data, PCI
- GDPR, CCPA, etc.
- CIS, Disa

* More about this subject check here

# Report Analysis

RDS Vulnerability & Classification Tool

**In this section you will learn about:**

- Overall security risk assessment
- Misconfigurations & Posture findings
- Security vulnerabilities findings
- Database privacy-related assessment

# Cloud Data Security Posture

Report highlights and main issues found

## Your database security risk level

### Risk Level: High

39 potential security risks were found within this database classified as HIGH or CRITICAL.

## High Level Findings

### Misconfigurations & Bad Practices

**57** • 48 non-compliant

Some misconfigurations and posture issues were found which require revision of your cloud environment

### Vulnerabilities

**30** • 12 with high CVSS

This database include component which are not fully updated to address security risks

### Sensitive data records

**52K** • 6 categories

This database holds sensitive data records. Certain regulations may apply

## Top Insights

- The database is not with the latest security update and is vulnerable to known exploits
- Misconfigured privileges result in too excessive permissions
- Sensitive personal data & identifiable data must not be accessed by unauthorized entities

Want to know more about Database Security?

Check Imperva Recommendations and learn from the world leading companies.

Learn more

# Misconfigurations & Bad Practices

This page details issues related to misconfiguration and posture which may impose security risks if exploited

## Total Assessments

125

### Distribution of the assessments

- ⚠ 34 Misconfigurations
- 🔔 23 Issues Require Attention
- 🔒 68 No Issues

## Security Risks

57

### Severity Distribution

| | |
|---|---|
| Critical | 1 |
| Major | 31 |
| Minor | 25 |

## Non-compliance assessments

48

### Tested Regulations

DISA

CIS Center for Internet Security Confidence in the Connected World

## Misconfigurations by Category

| Category | No. of assessments |
|---|---|
| Auditing | 23 |
| Misconfiguration | 9 |
| Authentication and User Management | 8 |
| Access Control | 8 |
| General Database Info | 6 |
| Resource Control | 3 |

## Top Misconfigurations

| Security Risk | Category | Severity |
|---|---|---|
| EXECUTE ANY PROCEDURE Granted to User OUTLN | Access Control | Critical |
| Oracle GLOBAL_NAMES Parameter is Disabled (CIS v3.0.0 Oracle 12c) | General Database Info | Major |
| Oracle 'CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' Action Audit Not Enabled (RDS) | Auditing | Major |
| Audit is not Enabled for GRANT ANY OBJECT PRIVILEGE activities/requests | Auditing | Major |
| Audit is not Enabled on SYS.AUD$ Table | Auditing | Major |

* More about this subject check here

# Known Vulnerabilities

This page details known vulnerabilities (CVEs) related to database security.
These issues should be resolved with the relevant updates to avoid putting your data in high risk.

### Total Vulnerabilities Found

**30** • 12 with high CVSS

### Vulnerabilities by severity

5 Critical

19 Major

6 Minor

### Vulnerabilities by Year

| Year | Number of Vulnerabilities |
|---|---|
| 2021 | 5 |
| 2020 | 17 |
| 2019 | 7 |
| 2016 | 1 |

### Top Vulnerabilities by Severity

| Vulnerability | Severity | Description |
|---|---|---|
| CVE-2019-12900 | Critical | Vulnerability in the Core RDBMS (bzip2) component of Oracle Database Server |
| CVE-2021-2035 | Critical | Vulnerability in the RDBMS Scheduler component of Oracle Database Server |
| CVE-2020-14735 | Critical | Vulnerability in the Scheduler component of Oracle Database Server |
| CVE-2020-14734 | Critical | Vulnerability in the Oracle Text component of Oracle Database Server |
| CVE-2016-10251 | Critical | Vulnerability in the Oracle Multimedia component of Oracle Database Server |

* More about this subject check here

# Privacy & Compliance

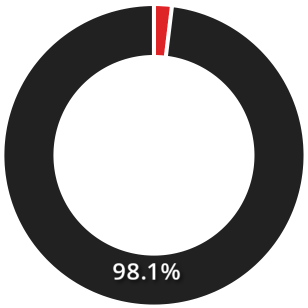
This page shows all the sensitive data we found in your database by categories

### Total Data Records

**14M**

Number of records found with privacy related data which have compliance impact.

### Data Ratio



| | | |
|---|---|---|
| 🟥 | Tables with sensitive Data | 9 |
| ⬛ | Tables unclassified with sensitive data | 462 |

### Sensitive Data Records

**52K**

Number of sensitive personal data records found and classified by privacy categories.

## Sensitive Data Distribution

| Category | Columns | Items |
|---|---|---|
| City | 6 | 24K |
| Email Address | 4 | 7K |
| Mailing Address | 4 | 7K |
| Postal Code | 4 | 7K |
| Credit Card | 2 | 6K |
| Person Contact Data | 3 | 1.1K |

### Columns with Personal Data

**23** out of 4862

🟨 **15** PCI related data ⬜ **8** Other Personal data

### Personal Data was found

There are world standards that may be applied to you:

**GDPR may apply**

If this data represents EU citizens

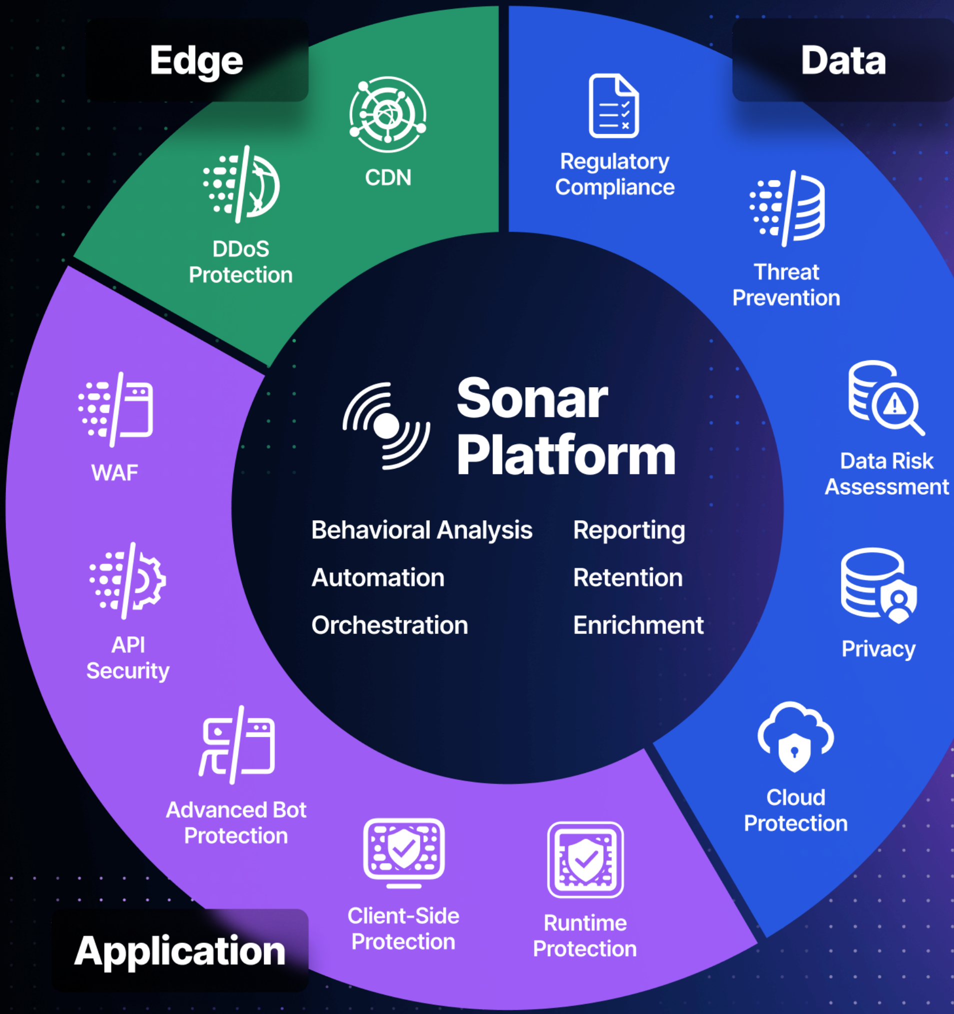
**CCPA may apply**

If this data represents US citizens

* More about this subject [check here]()

# Imperva Products

We protect what drives today's digital economy



**In this section you will learn about:**

- Imperva Data Security
- About Imperva

# Imperva Data Security

## Secure data everywhere it lives

Data is the target in every cyberattack. Imperva goes beyond compliance to malicious access to your data disturbed across on-premises and multi clouds infrastructure.

### Go beyond compliance

Secure access from insider threats and misuse

### Discover critical data

In hybrid, distributed environments.

### Centralized analysis

To automatically enforce everywhere.

## Cloud Data Security

Protects managed databases

## Database Security

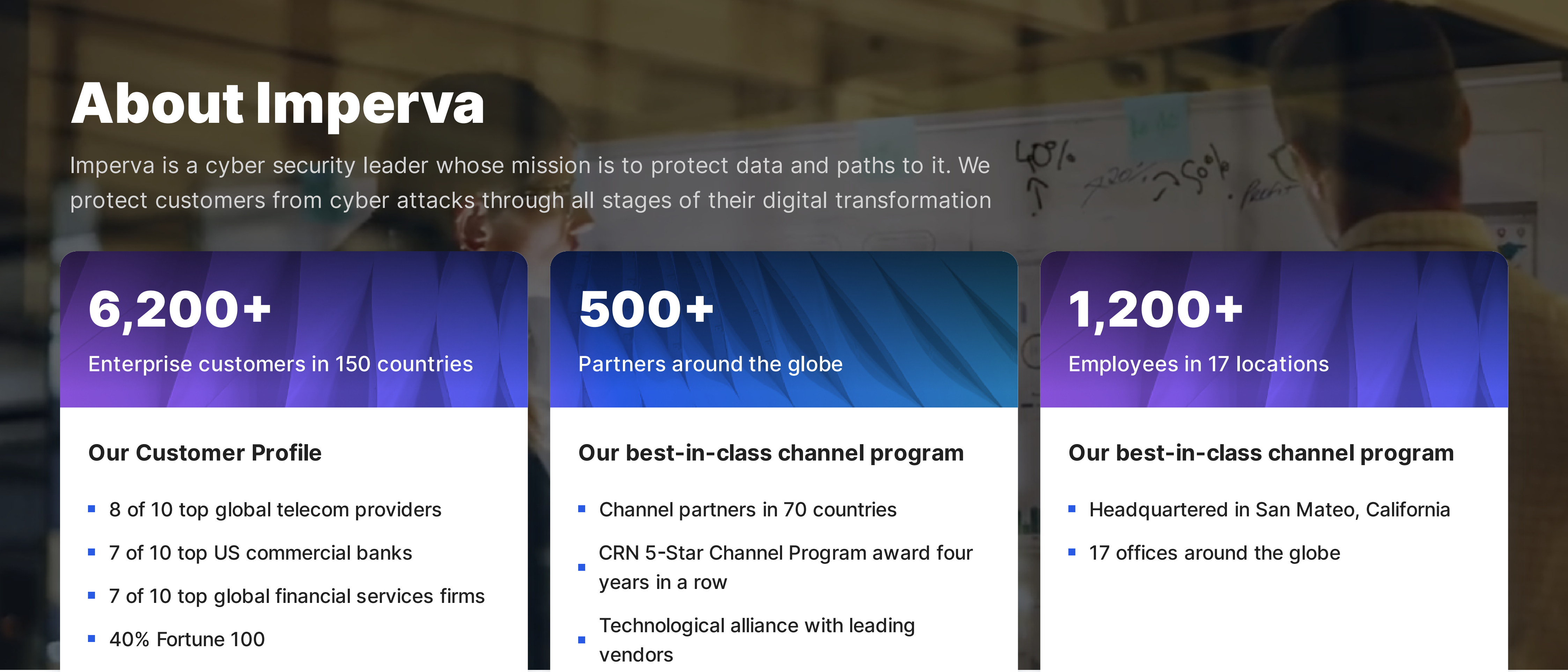
Prevents data extortion

## Data Privacy

Increase DSAR efectiveness

## Data risks Analytics

Identifies insider threats



# About Imperva

Imperva is a cyber security leader whose mission is to protect data and paths to it. We protect customers from cyber attacks through all stages of their digital transformation

## 6,200+

Enterprise customers in 150 countries

### Our Customer Profile

- 8 of 10 top global telecom providers
- 7 of 10 top US commercial banks
- 7 of 10 top global financial services firms
- 40% Fortune 100

## 500+

Partners around the globe

### Our best-in-class channel program

- Channel partners in 70 countries
- CRN 5-Star Channel Program award four years in a row
- Technological alliance with leading vendors

## 1,200+

Employees in 17 locations

### Our best-in-class channel program

- Headquartered in San Mateo, California
- 17 offices around the globe

### Contact Sales

+1 866 926 4678

Contact us →

### Technical Support

+1 (855) 574-9831

Support Email →

### Other links

Website

Youtube

Linkedin

Twitter

# Security Risks Appendix

A patent-pending approach for cloud database scanning

**In this section you will learn about:**

- A detailed list of all risks and issues we found

# Misconfiguration & Bad Practices

Detailed list of issues found

## We’re here to help you resolve these issues

Imperva’s Cloud Data Security products are designed to provide the best data security protection to fit your budget

Get in touch

| Assessments | Description | Category | Severity |
|---|---|---|---|
| EXECUTE ANY PROCEDURE Granted to User OUTLN | Checks if the user OUTLN has been granted the "EXECUTE ANY PROCEDURE" privilege. | Access Control | Critical |
| Oracle GLOBAL_NAMES Parameter is Disabled (CIS v3.0.0 Oracle 12c) | Checks if the Oracle GLOBAL_NAMES parameter is disabled. | General Database Info | High |
| Oracle 'CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' Action Audit Not Enabled (RDS) | Checks that 'CREATE PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' action audit is enabled. | Auditing | High |
| Audit is not Enabled for GRANT ANY OBJECT PRIVILEGE activities/requests | Check that all access grants of database objects are audited. | Auditing | High |
| Audit is not Enabled on SYS.AUD$ Table | Checks if the table "SYS.AUD$" is audited. | Auditing | High |
| Audit is not Enabled for USER activities/requests | Checks that all create, drop, alter user statements are audited. | Auditing | High |
| Audit is not Enabled for TRIGGER activities/requests | Checks that all TRIGGER statements are audited. | Auditing | High |
| Audit is not Enabled for DIRECTORY activities/requests | Checks that all DIRECTORY statements are audited. | Auditing | High |
| Oracle 'AUDSYS.AUD$UNIFIED' Audit Option Not Enabled (RDS) | Checks that 'AUDSYS.AUD$UNIFIED' audit option is enabled. | Auditing | High |
| Oracle 'DROP PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' Action Audit Not Enabled (RDS) | Checks that 'DROP PROCEDURE/FUNCTION/PACKAGE/PACKAGE BODY' action audit is enabled. | Auditing | High |

| Assessments | Description | Category | Severity |
|---|---|---|---|
| Oracle SQL92_SECURITY Parameter is Disabled (CIS v3.0.0 Oracle 12c) | Checks if the Oracle SQL92_SECURITY parameter is disabled or does not exist. | Access Control | High |
| Audit is not Enabled for ROLE activities/requests | Checks that all create, update, delete or setting of roles statements are audited. | Auditing | High |
| Audit is not Enabled for PROCEDURE activities/requests | Checks that all PROCEDURE statements are audited. | Auditing | High |
| Audit is not Enabled for PROFILE activities/requests | Checks that all PROFILE statements are audited. | Auditing | High |
| Users Assigned Default Application Administration Roles (RDS) | Checks if users are assigned Application Administration Roles which are assigned system or elevated application object privileges. | Access Control | High |
| DBFIPS_140 parameter is not configured | Checks if the parameter 'DBFIPS_140' is configured and his value is set to 'TRUE'. If encryption is not required for the database and data derived from it, this is not a finding. Review DBMS settings to determine whether data stored on the database is encrypted according to organizational requirements. If not, this is a finding. NOTE: This initialization parameter is available starting with Oracle Database 12c Release 1 (12.1.0.2). | General Database Info | High |
| Audit is not Enabled for ALTER SYSTEM activities/requests | Checks that all ALTER SYSTEM statements are audited. | Auditing | High |
| Audit is not Enabled for SYSTEM GRANTS activities/requests | Checks that all GRANT ROLE and REVOKE ROLE operations are audited. | Auditing | High |
| Audit is not Enabled for PUBLIC SYNONYM activities/requests | Checks that all PUBLIC SYNONYM statements are audited. | Auditing | High |
| Audit is not Enabled for DATABASE LINK activities/requests | Checks that all DATABASE LINK statements (DROP and CREATE) are audited. | Auditing | High |
| Auto minor version upgrade is disabled | If the database engine used by your application supports it, ensure that the RDS Instances have Auto Minor Version Upgrade Enabled. | Misconfiguration | High |
| RDS backup retention is not set | Thre is a managed backup function of the RDS Database. It is possible to define the backup window and retention period of the backup. You should have a retention policy set for each type of data being stored. You should set this to at least 7 days. Possible values are from 0 to 35 days. | Misconfiguration | High |
| Encryption at rest is disabled | Amazon RDS instances and snapshots can be encrypted at rest by enabling the encryption option on the Amazon RDS DB instance. Data that is encrypted at rest includes the underlying storage for a DB instance, its automated backups, read replicas, and snapshots. It is recommended that encryption at rest be enabled. | Misconfiguration | High |
| DB snapshots are not encrypted | Ensure that your RDS snapshots are encrypted in order to achieve compliance for data-at-rest encryption within your organization. | Misconfiguration | High |

| Assessments | Description | Category | Severity |
|---|---|---|---|
| Subscriptions are disabled for DB security groups | RDS event subscriptions provide notification of selected event changes at a DB security group level. Event subscriptions are designed to provide incident notification of events which may affect the network availability of the RDS instance. | Misconfiguration | High |
| Multi-Availability zone is disabled | Provides AWS managed high availability of the Database Tier across 2 availability zones within a region through asynchronous replication at the data layer. | Misconfiguration | High |
| RDS is publicly accessible | Customers can deploy RDS databases within a VPC through the configuration of: 1. Subnet Group for RDS, this group will be used for deployment of single or Multi-AZ RDS instances. 2. Network access through configuration of Security Groups for RDS. 3. Access from outside the VPC hosting the DB instance by enabling/disabling a Public IP address. Network access to the managed Data-Tier must be tightly controlled using Security Groups for RDS and non local accessibility of the DB instance. | Misconfiguration | High |
| Assignment of direct privilege to users (RDS) | List all database privilege assigned directly to users and not through roles. | Access Control | Medium |
| Subscriptions are not enabled for instance level events | RDS event subscriptions provide notification of selected event changes at Data Base engine level such as Deletion, Failure, Failover, Low Storage and Maintentance. Event subscriptions are designed to provide incident notification of events which may affect the availability of a RDS database instance. | Misconfiguration | Medium |
| No SNS topic was created for sending out notifications | For the RDS event subscriptions to be able to send out notifications, an SNS topic should be created. Amazon Simple Notification Service (Amazon SNS) is a web service that coordinates and manages the delivery or sending of messages to subscribing endpoints or clients. When using Amazon SNS, you (as the owner) create a topic and control access to it by defining policies that determine which publishers and subscribers can communicate with the topic. RDS events generated through defined RDS event subscriptions need to be sent out to administrators in order to be acted upon. | Misconfiguration | Medium |
| Users with DEFAULT profile | Users which haven't been explicitly associated with a profile, assume the DEFAULT profile, which is unlimited. In order to fix this, create a profile and assign it to the user: ALTER USER {user} PROFILE {profile} | Access Control | Medium |
| Profiles with too long PASSWORD_LIFE_TIME (RDS) | Checks the length of the PASSWORD_LIFE_TIME parameter for profiles. | Authentication and User Management | Medium |
| Profiles with too long PASSWORD_GRACE_TIME (RDS) | Checks that the number of days that can pass after the user's password is expired is maximum 5 | Access Control | Low |
| Oracle AUDIT_TRAIL Parameter is Disabled (CIS v3.0.0 Oracle 12c) | Checks if the Oracle AUDIT_TRAIL parameter is disabled. | Auditing | Low |

# Known Vulnerabilities

Detailed list of issues found

## We're here to help you resolve these issues

Imperva's Cloud Data Security products are designed to provide the best data security protection to fit your budget

Get in touch

| Assessments | Description | Category | Severity |
|---|---|---|---|
| CVE-2019-12900: Vulnerability in the Core RDBMS (bzip2) component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-12900 according to the affected versions list published by Oracle. | Known Attacks | Critical |
| CVE-2021-2035: Vulnerability in the RDBMS Scheduler component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2021 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2021-2035 according to the affected versions list published by Oracle. | Known Attacks | Critical |
| CVE-2020-14735: Vulnerability in the Scheduler component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-14735 according to the affected versions list published by Oracle. | Known Attacks | Critical |
| CVE-2020-14734: Vulnerability in the Oracle Text component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2020 is not applied on the database server and if the oracle text component is installed and VALID. If patch is not apply and component is valid, checks if the server is vulnerable to CVE-2020-14734 according to the affected versions list published by Oracle. | Known Attacks | Critical |
| CVE-2016-10251: Vulnerability in the Oracle Multimedia component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2016-10251 according to the affected versions list published by Oracle. | Known Attacks | Critical |
| CVE-2020-2511: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2511 according to the affected versions list published by Oracle. | Known Attacks | High |
| CVE-2020-5360: Vulnerability in the Oracle Database - Enterprise Edition Security (Dell BSAFE Micro Edition Suite) component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2021 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-5360 according to the affected versions list published by Oracle. | Known Attacks | High |
| CVE-2020-2510: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2510 according to the affected versions list published by Oracle. | Known Attacks | High |
| CVE-2020-2969: Vulnerability in the Data Pump component of Oracle Database Server | Checks if the Oracle Critical Patch Update from July 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2969 according to the affected versions list published by Oracle. | Known Attacks | High |
| CVE-2019-3740: Vulnerability in the Oracle Database - Enterprise Edition (Dell BSAFE Crypto-J) component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2021 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-3740 according to the affected versions list published by Oracle. | Known Attacks | High |

| Assessments | Description | Category | Severity |
|---|---|---|---|
| CVE-2020-2737: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2737 according to the affected versions list published by Oracle. | Known Attacks | High |
| CVE-2019-2853: Vulnerability in the Oracle Text component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-2853 according to the affected versions list published by Oracle. | Known Attacks | High |
| CVE-2020-2512: Vulnerability in the Database Gateway for ODBC component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2512 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2019-2956: Vulnerability in the Core RDBMS (jackson-databind) component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2019 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-2956 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2020-2515: Vulnerability in the Database Gateway for ODBC component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2515 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2020-14741: Vulnerability in the Database Filesystem component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-14741 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2020-2527: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2527 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2020-2978: Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server | Checks if the Oracle Critical Patch Update from July 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2978 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2021-2173: Vulnerability in the Recovery component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2021 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2021-2173 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2020-2731: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2731 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2019-2955: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2019 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-2955 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2020-2568: Vulnerability in the Oracle Applications DBA component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2568 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2019-2954: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2019 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-2954 according to the affected versions list published by Oracle. | Known Attacks | Medium |
| CVE-2021-2045: Vulnerability in the Oracle Text component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2021 is not applied on the database server and if the oracle text component is installed and VALID. If patch is not apply and component is valid, checks if the server is vulnerable to CVE-2021-2045 according to the affected versions list published by Oracle. | Known Attacks | Medium |

| Assessments | Description | Category | Severity |
|---|---|---|---|
| CVE-2020-14742: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-14742 according to the affected versions list published by Oracle. | Known Attacks | Low |
| CVE-2020-2734: Vulnerability in the RDBMS/Optimizer component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2734 according to the affected versions list published by Oracle. | Known Attacks | Low |
| CVE-2021-2000: Vulnerability in the Unified Audit component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2021 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2021-2000 according to the affected versions list published by Oracle. | Known Attacks | Low |
| CVE-2020-2516: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from January 2020 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2020-2516 according to the affected versions list published by Oracle. | Known Attacks | Low |
| CVE-2019-2940: Vulnerability in the Core RDBMS component of Oracle Database Server | Checks if the Oracle Critical Patch Update from October 2019 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2019-2940 according to the affected versions list published by Oracle. | Known Attacks | Low |
| CVE-2021-2207: Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server | Checks if the Oracle Critical Patch Update from April 2021 is not applied on the database server. If not, checks if the server is vulnerable to CVE-2021-2207 according to the affected versions list published by Oracle. | Known Attacks | Low |

imperva

Protecting data and all paths to it