Oracle Data Safe

Oracle Data Safe is a unified control center for managing database security in the Oracle Cloud. Data Safe provides an integrated set of features enabling users to understand the sensitivity of their data, evaluate risks to data, mask sensitive data, implement and monitor security controls, assess user security, monitor user activity, and address data security compliance requirements.

FREQUENTLY ASKED QUESTIONS

ABOUT ORACLE DATA SAFE

Why is this cloud service important to customers?

Oracle Data Safe supports all Oracle Cloud Database offerings. Oracle Database Cloud Service provides different sets of security features based on database type and edition. Oracle Autonomous Database takes care of a number of security concerns for customers automatically, including:

- Network security and monitoring
- OS and platform security
- Database patches and upgrades
- Administrative separation of duties
- Data encryption enabled by default

However, in the cloud, security is a shared responsibility between the provider and the user, and users still have to manage some things such as:

- Additional database and data security controls
- User accounts and the associated risk
- Identifying and understanding sensitive data
- Implementing controls to protect data at the appropriate level
- Auditing user activities, and more

Oracle Data Safe addresses this with integrated data security functionalities accessible to any Oracle Cloud customer through a cloud-based control center. Oracle Data Safe combines information about users, data and data infrastructure to enable users to manage risks to their sensitive data.

What customer problems are addressed with Data Safe?

Whether working with on-premises or cloud databases, DBAs need to take measures to protect the enterprise data under their care. This requires being able to answer a number of questions such as:

- Security assessment
  - Are my databases securely configured?
  - Do I have gaps in my configuration strategy?
  - How can I best remediate these gaps?
- Sensitive data discovery
  - What types of sensitive data do I have?
  - How much sensitive data is stored in this database?
  - Where is my sensitive data located?
- Data protection
  - How can I efficiently support test/dev and analytics without exposing sensitive data?
- Audit
  - How can I manage the audit data collected from individual servers?
  - How can I centralize audit data to simplify reporting and event correlation?
  - How can I be alerted to inappropriate user activity?

What features does Oracle Data Safe include?

Data Safe allows customers to perform security assessments of their database and their database users

- Security assessments allow customers to create and maintain security baselines. This enables rapid identification of configuration risks and facilitates consistent use of security controls across the enterprise.
- User assessments help customers understand their user risk profile. Over-privileged users are frequently targeted by cyber attackers to leverage their extensive set of privileges to mount data attacks.

Data Safe manages database server audit policies and securely collects, removes and retains audit data from database servers

- Database audit policies can be centrally managed and configured
- If an attacker compromises a privileged user account, the attacker may also be able to alter or destroy the audit records for the database. Moving the audit data as quickly as possible to a secure centralized repository makes it difficult for attackers to hide their tracks.
- Audit data can be retained for forensic and compliance purposes

Data Safe discovers sensitive data in databases

- Common categories of sensitive data can be discovered by Data Safe so customers don't accidentally overlook some columns of sensitive data
- Sensitive data can then be masked by Data Safe to protect information in test databases

Data Safe masks sensitive data in development and test databases

- Development and test databases need production-like data to modify and test applications. However, development and test databases aren't protected to the same level as production and the sensitive data needs to be replaced in the database.
- Masking needs to account for foreign/primary key mappings so that sensitive data used for linking data needs to remain consistent

Data Safe dashboard allows customers to quickly assess and then drill down to review risk

- When alerts are received, the dashboard provides a quick overview of the data security status for the target databases
- Unusual dashboard activity can be drilled down to find specific issues

What is the Oracle Data Safe user experience like?

The Oracle Data Safe control center provides users with an overview of risks associated with their users, sensitive data and platform. Users select from various features exposed in the control center to assess users and security, search for sensitive data, manage audit policies and mask data for use in test, development and analysis.

We've worked hard to remove the complexity from database security, while at the same time giving you the flexibility to meet your security control objectives. The Data Safe user interface is intuitive and uses intelligent defaults. For example, it automatically recommends data masking techniques for the discovered sensitive data if you want to remove that sensitive data from a non-production copy of the database. If the defaults are adequate for your needs, you can complete the entire masking process without typing a single line of code!

Can customers use this to meet compliance regulations like GDPR?

Compliance laws such as the European Union (EU) General Data Protection Regulation (GDPR) and the upcoming California Consumer Privacy Act (CCPA) levy requirements on companies to safeguard the privacy of their customers. Data Safe helps customers with their various compliance requirements such as identifying where sensitive data is located, masking sensitive data for non-production use, securely capturing audit data and so forth.

What is the benefit of Data Safe for cloud database customers?

Cloud requires a shared responsibility model for security. Oracle has highly automated tools to provide the Oracle portion of the shared security model which include: network security and monitoring, OS and platform security, database patches and upgrades, administrative separation of duties, and data encryption by default. Customers are responsible for managing the security of data such as user permissions, protecting sensitive data and setting up appropriate audit policies. Data Safe provides tools to help customers with their portion of security management. Data Safe is a unique capability in the industry. By making these essential data security functionalities available to all Oracle Cloud customers, it sets a new standard for cloud database security.

AVAILABILITY

Which types of Oracle Databases in the Oracle Cloud will be supported?

Data Safe works with all Oracle Cloud Database Services (like Autonomous Database, Exadata, VM, Baremetal) provided they are addressable (public IP) and there is a network connection to the database being secured. In many cases such as Autonomous Database Serverless, Data Safe connects using the public IP. In some cases, you would have to allow access to the Data Safe Service IP address range by changing the network ACL rules. Please read here for more details.

Is Data Safe available for on-premises customers?

Not for this release.

Does Data Safe support Cloud at Customer database deployments?

Not for this release.

In which regions is Data Safe available?

Data Safe is available in all regions where Autonomous Database is supported today.

GETTING STARTED

How do I get started?

If you are using a cloud database on Oracle Cloud, getting started is as easy as 1-2-3.
1. Enable Data Safe with the click of a button in the Oracle Cloud Infrastructure.
2. Register your target databases.
3. Log on to the Oracle Data Safe console and start leveraging all Data Safe capabilities.

What type of training is needed for my administrators to use Data safe?

No prior specialized security expertise is needed. We've worked hard in Data Safe to remove the complexity from database security, while at the same time giving you the flexibility to meet your security

control objectives. The Data Safe user interface is intuitive and uses intelligent defaults. If the defaults are adequate for your needs, you can run through all the features of Data Safe without typing. Having said that, there is a comprehensive online help to guide you through the different features.

USING ORACLE DATA SAFE

What are the some of the security considerations with using Data Safe?

- Data Safe is built upon Next generation security offered by Oracle Cloud Infrastructure (OCI).
- For isolation, each customer's data is kept in a separate database. All access to customer's databases and Data Safe data is audited.
- A Data Safe account has to be created in target databases with appropriate privileges. For Autonomous Database Serverless customers, this can be done automatically in the near future.
- Only your authorized users can access the Oracle Data Safe console. Depending upon the extent of their access, they can be limited to certain features in Data Safe and to only one or few databases, or they can get access to security data for all of your databases.
- The security data about your databases remains private to you at all times.

What does it mean that Data Safe is included with subscription to Oracle cloud databases? What are the usage limits?

If you are a paid subscriber to any cloud database on Oracle Cloud, you can use Data Safe at no additional cost. You can store up to 1 Million audit records per month per target database. If you exceed this limit, you may incur additional costs. In addition, we built in some limits to prevent abuse.

What is your audit data retention policy?

By default, we keep audit data for 6 months, but you can extend it up to one year.

How do I get support for Data Safe?

Full support is included like with all other services on Oracle Cloud Infrastructure. You may submit your support requests through the Oracle Support portal using your Oracle Customer Support Identifier (CSI).

MORE INFORMATION

I'd like to learn more about Data Safe – how can I keep up-to-date with the latest?

For more information, please see the Oracle Data Safe page on Oracle Technology Network (OTN). A variety of helpful information is available online including data sheet, white paper and videos.

https://www.oracle.com/database/technologies/security/data-safe.html

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

 blogs.oracle.com/oracle

 facebook.com/oracle

 twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE