ORACLE

Secure Critical Data with Oracle Data Safe

Extend Database Security with a Unified Control Center for Managing Sensitive Data

August, 2020, Version 2.0

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

The Growing Need to Protect Sensitive Data in the Cloud

Many organizations now consider data to be one of their most valuable organizational assets. However, if that data is not well protected, it can quickly become a liability. Practically every day we hear stories about high-profile data breaches, as well as attacks on individual systems and databases (see sidebar). Growing privacy concerns have increased the regulations that dictate how organizations treat user data, including the European Union's General Data Protection Regulation (GDPR), the United States' Health Insurance Portability and Accountability Act (HIPAA), the new California Consumer Protection Act (CCPA), and other governing bodies. It's an expensive problem, and the associated fines for non-compliance have made it even more so. For example, Marriott was forced to pay more than £99 million in fines; and British Airways faces £183 million in fines for recent GDPR breaches.

Attackers may be full-time employees of a nation-state, members of an organized crime syndicate, or just curiosity seekers, but they all have one thing in common: a propensity to leverage gaps in your security strategy. While some of these attacks are designed to wreak havoc on business operations, others are motivated by a more explicit goal: to steal your data. And since this data typically resides in a database, the latter becomes the prime target for hackers.

In addition to this constant barrage of external threats, companies also face threats from internal users — sometimes intentional, and other times through inadvertent errors, omissions, and oversights involving security software configurations and the associated data.

The distributed nature of today's work teams only exacerbates the problem. Organizations must commonly manage many types of users in many different geographies — including internal DevTest teams and external partner organizations — all of which require differing levels of access to corporate data.

To mitigate both intentional and unintentional breaches, enterprises need to identify sensitive data, protect it with appropriate controls, and routinely audit usage of that data in database management systems. Some business leaders are concerned about moving databases to the cloud because of these security issues — compounded by a shortage of in-house expertise protecting sensitive data.

This paper describes Oracle Data Safe, an integrated and comprehensive cloud service that ensures data security for Oracle Databases, in Oracle Cloud and on-premises. Data Safe helps secure your databases via *security* and *user risk assessments*, *user activity auditing*, *sensitive data discovery*, and *data masking*. With this well-integrated and easy-to-use solution, Oracle Database customers of all sizes and in all verticals can address their database security requirements easily.

Data Breaches in the News

- In 2019, Capital One reported one of the top 10 largest data breaches ever. The breach was discovered after details of the hack were posted on the code sharing website, GitHub.
- In April 2019, vpnMentor discovered an unsecured database hosted on Microsoft Azure that contained personal information on nearly 80 million U.S. households.
- In February 2018, FedEx realized that they had inadvertently exposed the personal information from 119,000 of their customers in a database on an unsecured Amazon Web Services (AWS) cloud storage server. The discovery was made by Kromtech Security and it is estimated this information went unsecured for four years before being discovered.

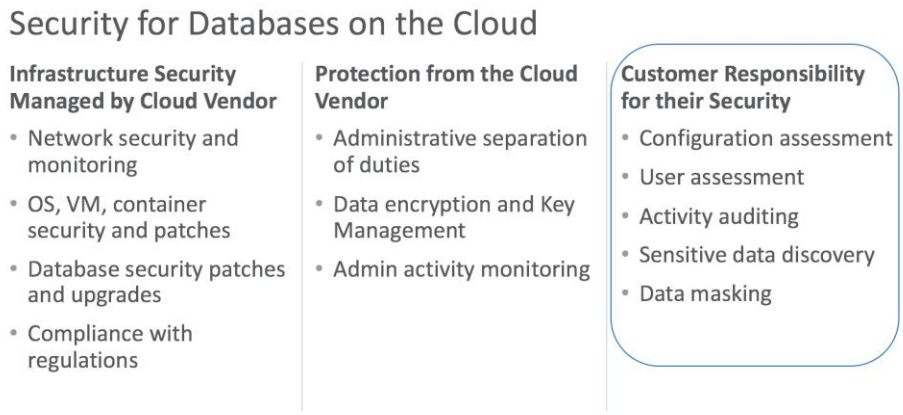
The Cost of Compliance

- GDPR fines can be as high as four percent of annual revenue
- HIPAA fines can be US$1.5 million per violation
- CCPA fines will be as high as $700 per individual — plus litigation costs

Democratizing Security with Oracle Data Safe

As data and applications move to the cloud, the responsibility for securing an organization's assets becomes progressively more complex. While cloud service providers are responsible for securing their global infrastructure and protecting

client databases from access by their own personnel, each cloud customer must implement its own measures to secure its users and data.



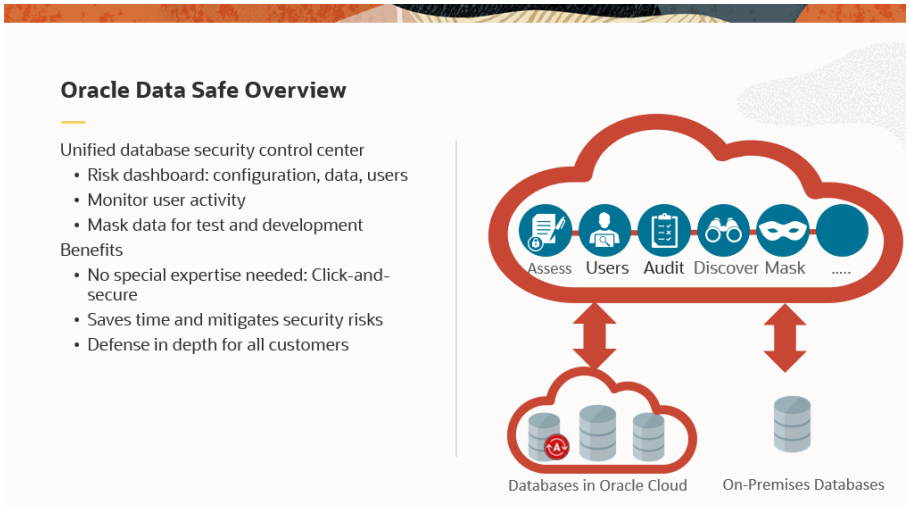
For example, in an Infrastructure as a service (IaaS) environment, a cloud provider may secure cloud infrastructure, operating systems, and network services, but not the applications and users that access the data. Organizations are responsible for deciding what sensitive data goes into the database and which users can access it. This isn't something that a cloud vendor can decide, as it is specific to each company's industry, operations, customer base, and business goals.

To properly protect organizational data, it is necessary to first know how it's configured, who is using it, and what types of sensitive data each database contains. It also means keeping track of who needs to access production data (versus sample, masked, or aggregate data), and putting a process in place for removing that data when it is no longer needed.

Oracle Data Safe is an important part of this multifaceted security strategy. It provides an integrated set of capabilities that will help you secure your users and configurations as well as meet data security compliance requirements. Oracle Data Safe is your single point of control for managing database security, both in the cloud and on-premises.

Raise the Bar on Database Security with Data Safe

- Gain a complete view of database security from one cohesive environment
- No special expertise needed, and no need to stitch together many different tools
- Nothing to install and nothing to maintain



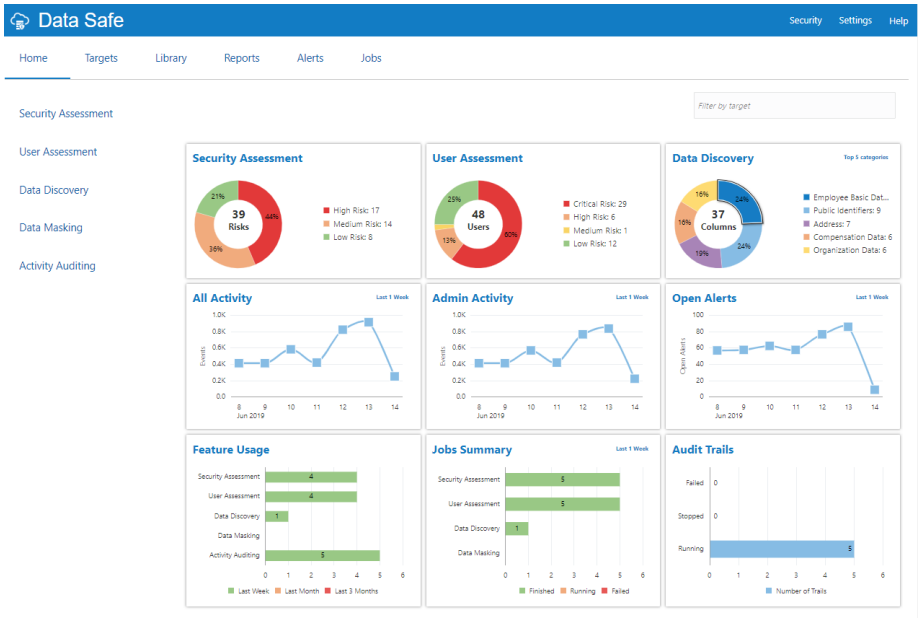
Oracle Data Safe provides a unified security control center for Oracle Databases

Controlling Access to Sensitive Data in Five Easy Steps

Enterprise databases frequently include large quantities of personal information, making them attractive targets for hackers who want to steal data and disrupt business practices. To mount a strong defense you need to know precisely *where* your sensitive data is located and *who* is accessing that data. In addition, knowing what risks are associated with your users and having the ability to audit activities are critical to a good security posture. Oracle Data Safe makes it easy to systematically complete these tasks with five inter-related components:

- Security Assessment
- User Assessment
- Activity Auditing
- Data Discovery
- Data Masking

Oracle Data Safe puts these five components together into a unified, user-friendly environment, so you don't need multiple tools — and highly skilled database security experts — to protect your data. This popular service is available today for databases on Oracle Cloud Infrastructure, on-premises databases, as well as databases running in Oracle Cloud@Customer.

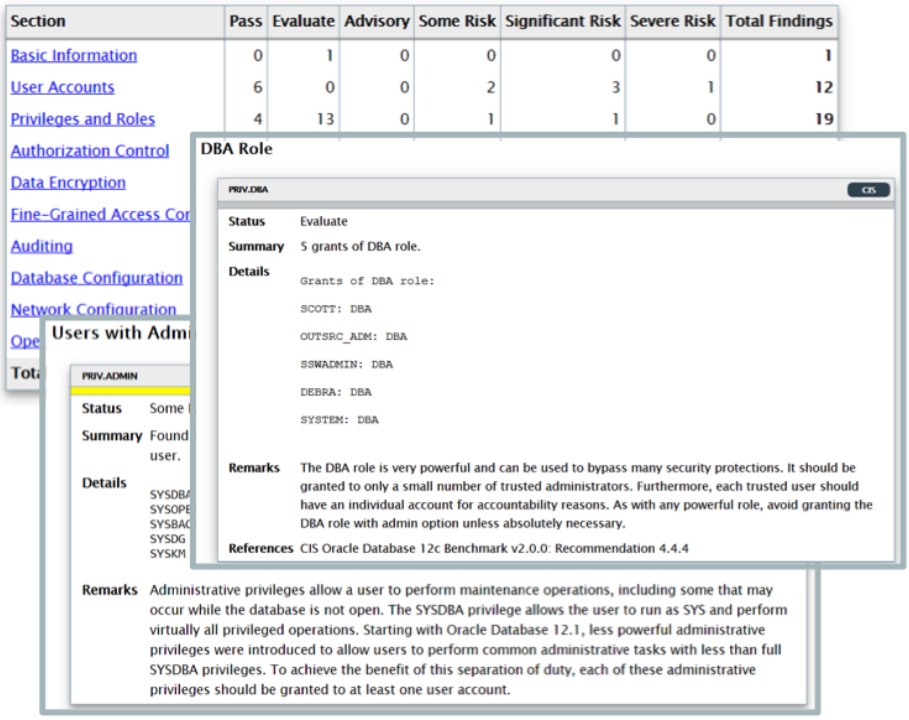


A unified security control center for Oracle Databases

Step 1: Security Assessment

A security assessment helps you determine if there are gaps in your configuration strategy and offers guidance on how to remediate those gaps. The Security Assessment feature enables you to identify security vulnerabilities and to verify that encryption, auditing, and access controls have been implemented.

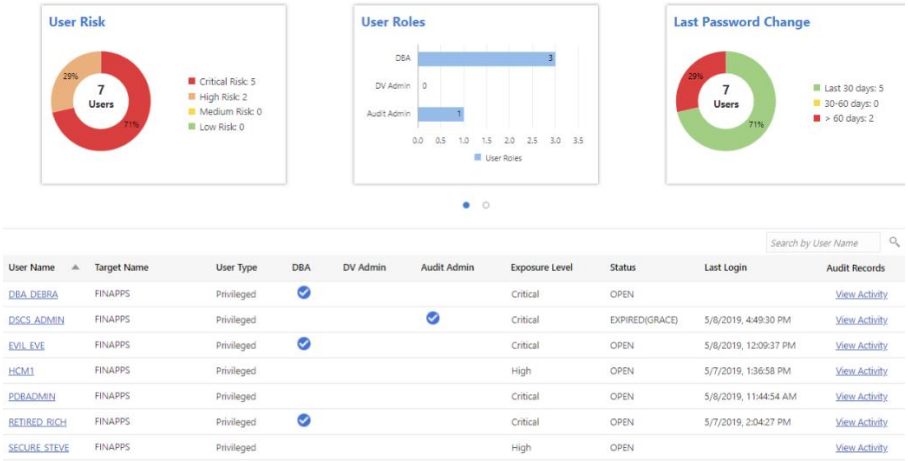
Oracle Database allows flexibility in how customers configure users, privileges, and security controls to meet different requirements. For example, the user and security controls implemented for a production system containing sensitive customer data might differ from those for a development system with synthetic test data. The Security Assessment feature of Oracle Data Safe enables you to examine security configuration parameters so you can implement the correct level of security and controls for each application. This might include, for example, identifying when default passwords are being used or when users have more privileges than they should. The findings and recommendations support both the European Union General Data Protection Regulation (EU GDPR) and the Center for Internet Security (CIS) benchmark.



Use the Security Assessment to examine security parameters and implement application controls

Step 2: User Assessment

Oracle Data Safe includes user assessment and monitoring capabilities that help you pinpoint risks, especially those associated with privileged users and accounts. You can now identify the database users who pose the highest risk if their accounts were to be compromised or if they were to go rogue and become bad actors. These accounts might require a higher level of monitoring or a possible reduction in privileges within the context of their roles. User Assessment reports help you quickly identify dormant accounts for locking or removal. Links from the User Assessment reports to the Activity Auditing function show the audited activities performed by the users.



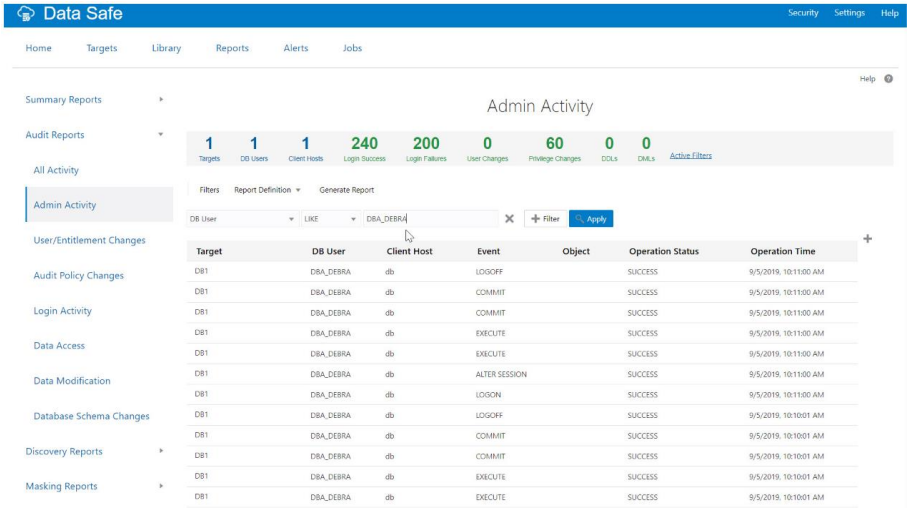
The User Assessment feature allows administrators to identify and evaluate privileged accounts

There are several activity auditing reports provided by Data Safe. These include summary of events collected and alerts, all audited activities, audit policy changes, admin activity, login activity, database query operations, DDLs, DMLs, and user and entitlement changes. You can view the generated alerts and filter and search for them. Both alerts and audit data reports can be customized and saved or downloaded in PDF or XLS format.

Step 3: Activity Auditing

With Data Safe Activity Auditing, you can monitor user activities on Oracle Databases, collect and retain audit records per industry and regulatory compliance requirements, and trigger alerts for unusual activity. You can audit sensitive data changes, administrator and user activities, and other activities recommended by the Center for Internet Security (CIS). You can set up alerts when a database parameter or audit policy changes, a failed login by an admin occurs, user entitlements change, and when a user is created or deleted. The Oracle Database includes a number of pre-defined polices and any of these can be enabled through Data Safe with just a few clicks.

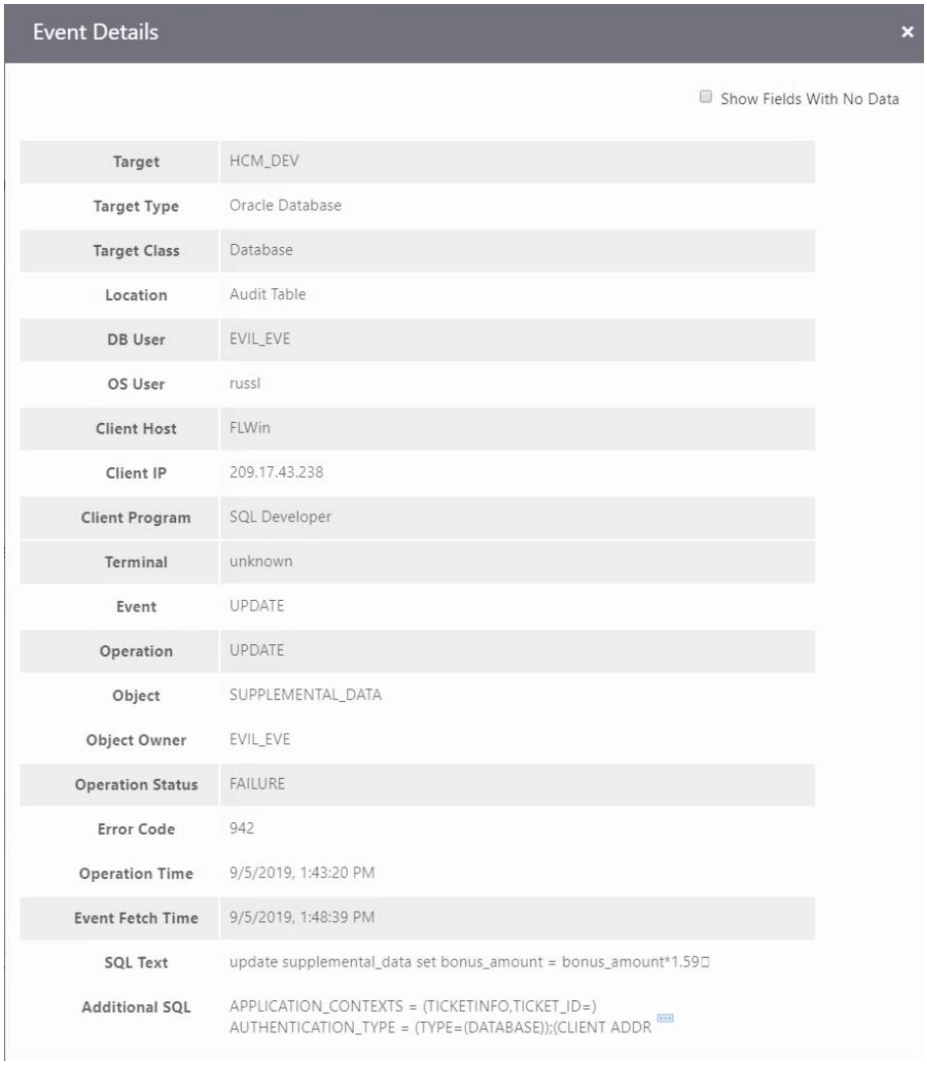
The Data Safe dashboard (shown on page 5) lets you quickly spot trends in activity, including alerts. From the dashboard, you can also check on the status of the audit trails (audit trails tell Data Safe where in the database to look for audit data) and see the overall auditing activity.



Admin Activity Reports

Setting up Activity Auditing in Data Safe is a simple 3-step process: 1) Select the targets you want to audit 2) Provision audit policies specifying what audit information will be collected 3) Create audit trails that tell Data Safe from where to collect audit information.

Many organizations don't really know how secure their databases are, how much sensitive data they have, or where their sensitive data is located.



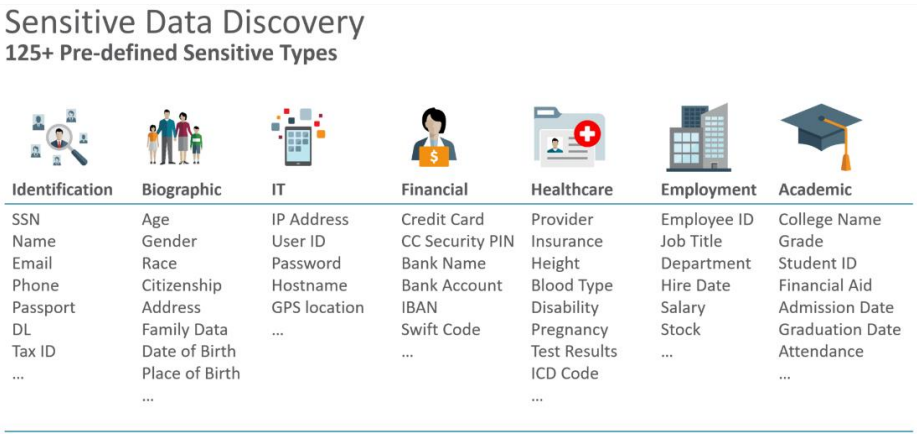
Audit record event details

Once this is done, Data Safe automatically retrieves audit data and stores it in the secure Data Safe repository (separate from the database being monitored so it can't be deleted or altered). You can set up alerts on key events based on the predefined set of alerts available in Data Safe Activity Auditing. Interactive reports allow you to look at audit data, filter it as needed, and create scheduled reports to meet your security and compliance needs.

Step 4: Data Discovery

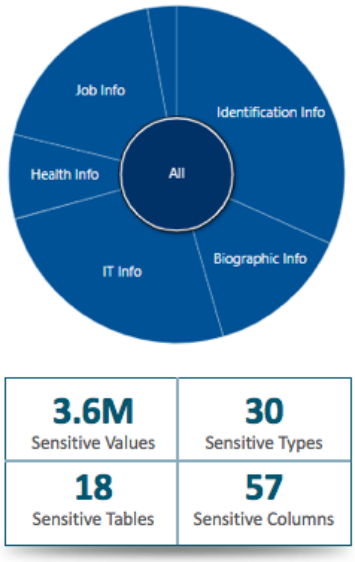
With multiple development teams and data distributed over multiple databases, it's not always easy to know where your sensitive data is. In order to protect your data, you need to understand what kind of sensitive data you have, how much of it you have, and where it resides. Sensitive Data Discovery helps you decide what to protect. It identifies and classifies 125+ sensitive types of data, such as personally identifiable information, IT data, financial data, employment data, and health data.

Data Masking maintains relational integrity with data transformations including shuffle masking, conditional masking, compound masking, SQL expression masking, user-defined masking, and other masking formats.



Data discovery: pre-defined sensitive data types

You can select the sensitive data categories that you want to discover, such as personally identifiable information or healthcare information. You can also easily define custom categories of new sensitive data types that match your organization's requirements.

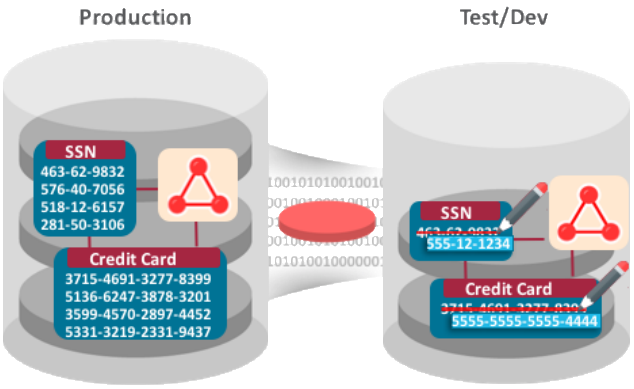


Data discovery reports on sensitive data

Step 5: Data Masking

Being able to share production data with test and development teams helps you to improve the quality of your applications through real-world data. But copies of production systems carry all the sensitive data (and the risk associated with that data) into environments which are not as well protected as your production environments. Besides, the sensitive data such as credit card numbers are not really needed. This is where Data Masking comes in. Data Masking replaces sensitive data in an application database with fictitious but realistic values. You can then share those data sets with application developers, application testers, and partners. This gives them a realistic data set for testing and developing applications — without exposing sensitive data. As Data Masking is integrated

with Data Discovery, a compatible masking format is automatically suggested for any discovered sensitive data. Data Safe lets you discover and mask sensitive data with just a few clicks.



Data masking reduces risk by obfuscating sensitive data.

The Data Masking feature of Oracle Data Safe uses the information discovered during the sensitive Data Discovery process to create data masking policies to protect, for example, social security numbers, credit card numbers, financial data, salary information, and personal health information. Data masking replaces real data with disguised, yet realistic, data within development, testing, and partner databases, and includes more than 50 predefined masking formats.

A Hypothetical Scenario Involving Sensitive Patient Data

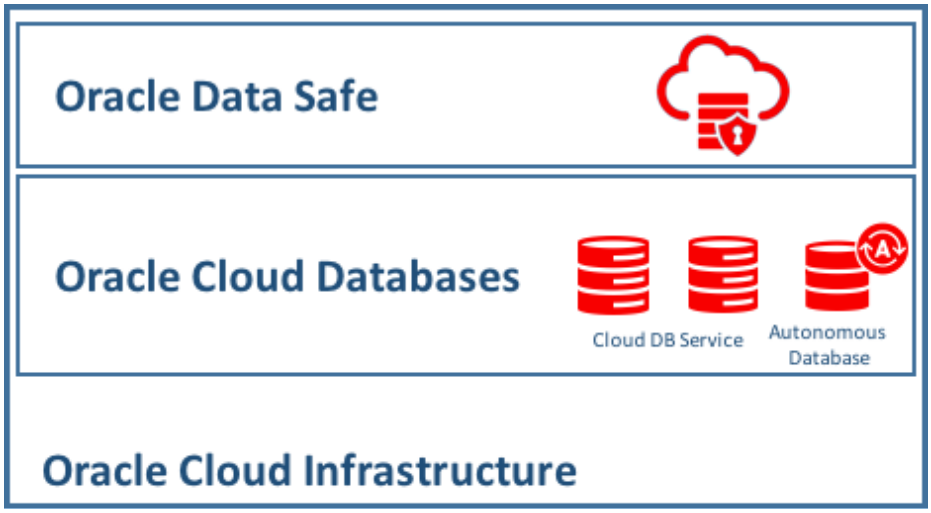
Consider a database used by a healthcare organization to store the results of diagnostic test results. With Oracle Data Safe, the security team can assess the database configuration (including password policies, parameter settings, and patch levels) to ensure the database is configured according to best practices. They can then quickly assess database users to identify which users have privileges that make them most at risk for inappropriate access to data and configure audit policies to monitor their database activity. They can use sensitive Data Discovery to scan the database to identify which schemas, tables and columns contain sensitive patient data. When copies of the database are made for test and development or partners, they can now automatically replace the sensitive data with realistic looking data. And they can do all of this from a single console in just a few minutes.

Bringing it All Together

Data Safe runs on Oracle Cloud Infrastructure and is a key part of an over-arching security strategy that runs from the infrastructure itself to our latest self-securing Oracle Autonomous Database. In the following sections, we'll explore this relationship in more detail.

Oracle Autonomous Database handles a number of crucial security concerns for its cloud customers automatically, including:

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



The relationship of Oracle Data Safe to Autonomous Database and Oracle Cloud Infrastructure

Oracle Autonomous Database includes AI and machine learning technology to protect your database management systems from both external attacks and malicious internal users. For example, the database can apply security patches automatically, without downtime.

Better Database Security with Oracle Autonomous Database

Oracle Data Safe extends the self-securing capabilities of the Oracle Autonomous Database to protect data while it's in use and to continuously monitor the users who access that data. We have a multi-pronged strategy to protect your data and free DBAs to focus on high-value tasks such as understanding their data and instituting proper protections and controls.

Oracle Autonomous Database is a revolutionary cloud service that simplifies database administration and tuning tasks, including automatically maintaining security configurations. For example, by automatically applying patches in a rolling fashion across the nodes of a cluster, Oracle Autonomous Database secures itself without application downtime. Security patches are applied every quarter or as needed to the firmware, operating system, clusterware, and database — with no downtime.

Patching is just part of the picture. The database also protects itself with always-on encryption. Encryption protects your data in situations where a breach allows a hacker to access the data blocks directly. This practice ensures that even if database files with sensitive data are copied, they are useless to cybercriminals. Oracle Autonomous Database encrypts customer data while it is in motion, at rest, and in backups.

By liberating database administrators from the daily repetitive management chores such as database tuning, patching, and backups, Oracle Autonomous Database allows DBAs to focus on high-value tasks such as application management and keeping sensitive data secure.

Security at Multiple Layers with Oracle Cloud Infrastructure

Oracle secures today's complex database environments with an intelligent, cloud-based platform that prevents, detects, and rapidly responds to security threats.

For example, Oracle Cloud Infrastructure is based on seven core pillars to ensure customers have the isolation, data protection, control, and visibility required for a robust cloud infrastructure. Oracle's machine learning algorithms add intelligence to security operations center (SOC) activities and a cloud access security broker (CASB) automatically detects threats to cloud applications. At the edge, Oracle security services include distributed denial of service (DDoS) Protection and a web application firewall to defend against internet-based threats. Finally, Oracle assumes the responsibility of protecting your infrastructure with a highly trained, 24/7 network operations center (NOC) staff. Oracle's security technology, process, and operations reduce the risk, cost, and complexity of moving to the cloud. With multiple layers of defense, Oracle combats cyber threats with core-to-edge cloud services that secure your data and thwart cyber threats.

Extending Security to On-premises Databases

The benefits delivered by Oracle Data Safe can also be applied to Oracle Databases running on-premises or in compute instances on Oracle Cloud Infrastructure. This capability enables users to leverage the same security features they are using to keep their cloud databases secure for their on-premises databases, without the need to deploy on-premises products or solutions. Reports and audit data for all databases are stored securely in the cloud, and the Data Safe dashboard provides a single, unified view of database security across all databases, regardless of where they are deployed.

Conclusion

As databases move to the cloud, enterprises need to proactively monitor how their data is managed and accessed, and by whom it is used. While cloud providers secure your infrastructure and the platform services, it's up to you to secure your applications, users, and data. The Oracle Data Safe cloud service integrates all your security needs including assessing your configuration and users, auditing user activity for compliance, and identifying sensitive data for masking — all through a single dashboard that allows you to quickly and easily secure your data assets in databases running in the cloud or on-premises.

To learn more about Oracle Data Safe, visit:
http://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 facebook.com/oracle twitter.com/oracle