KuppingerCole Report

EXECUTIVE VIEW

By Alexei Balaganski

March 16, 2021

Oracle Data Safe

Oracle Data Safe is a cloud-based service that improves the security of Oracle databases on-premises and in the cloud by identifying risky configuration, users, and sensitive data, which allows customers to closely monitor user activities and ensure data protection and compliance.

By **Alexei Balaganski**
ab@kuppingercole.com

Content

1 Introduction

As recent market trends indicate, companies are increasingly adopting cloud-first strategies for their business developments. Scalability, flexibility, and predictable costs are the primary factors for the growing adoption of cloud services. Achieving better agility and innovation, lowering the time to market for their digital services, eliminating the costs of maintaining their own infrastructures – these are just some of the drivers that motivate businesses to migrate their applications, workloads, and, of course, data to public clouds. This trend has been ongoing for over a decade, but the global pandemic that forced most employees to work from home for months has boosted cloud adoption even further.

Unfortunately, changes to system deployment patterns, workforce realignment, and the adoption of new technologies complicate the security landscape. The number and sophistication of massive data breaches and cyberattacks that even the largest and best-prepared enterprises are facing nowadays continue to grow. Harsh compliance fines imposed by regulatory frameworks (PCI DSS, CPRA, or GDPR to name just the most notorious ones) further raise the losses. Unsurprisingly, protecting sensitive corporate data is becoming the highest priority for all organizations, even those that lack the necessary manpower and expertise to enforce it.

This continuous struggle of business drivers against security and compliance challenges has led to the current situation where hybrid IT infrastructures are the new norm, with organizations forced to maintain separate, often incompatible infrastructures on-premises and in a cloud (or in multiple clouds). The complexity brought by hybrid and multi-cloud IT infrastructures has massively increased the efforts needed to keep track of all sensitive information managed by an organization, to say nothing about classifying the data according to its sensitivity and then selecting and enforcing appropriate data protection and governance capabilities.

Many companies would love to outsource parts of these efforts to a qualified third party, just like they already do with less sensitive workloads. Indeed, the trend of consuming security tools delivered from the cloud is gaining popularity in recent years, and the ongoing pandemic has been a major boost for it as well. A “security cloud” that can replace a whole stack of traditional single-purpose security appliances but without the onerous task of separately deploying, operating, and integrating stand-alone tools. A unified security control center benefits distributed enterprises as well as small businesses working mostly from home.

A unified management console that replaces numerous disconnected security tools helps address an even more crucial problem: the general lack of full visibility across environments that makes the daily job of a security expert painfully complicated. Centralized management, analytics, and reporting can also greatly simplify the enforcement of regulatory policies and early detection of the changes that eventually may lead to compliance violations.

While cloud-based solutions for securing endpoints (Endpoint Detection and Response / EDR) and network access (Secure Access Service Edge / SASE) have proven to be quite popular with businesses, especially during the pandemic lockdown months, most companies still seem to be quite wary about cloud-delivered data protection services. The primary reason for this is, of course, the general reluctance of customers to expose their highly sensitive on-prem data to a service hosted and managed by a third party: this has massive compliance and security implications when data sovereignty is compromised or if the service itself has security problems. Under regulations like GDPR, such a data breach will be extremely costly.

An additional concern is the security solution's complexity both in deployment and usage. This is especially noticeable when all a vendor offers is a suite of security tools for on-prem and cloud deployment. Some of those tools might not be well-integrated and may even come from recent acquisitions. After all, when opting for cloud-based security solutions, customers expect the convenience of a SaaS service but at the same level of assurance as traditional enterprise on-premises products.

This is exactly where Oracle offers a value proposition that very few competitors can match. On the one hand, the company is a veteran database vendor with decades of experience in database security and data protection. On the other, as a relative latecomer to the cloud market, the company had a chance to learn from the requirements of their enterprise customers and implement many data security and compliance controls directly in Oracle cloud services.

Last but by no means least, Oracle's database portfolio is designed around a single multi-model database management platform with full feature parity on-premises and in the cloud, thus dramatically reducing the architectural complexity for hybrid deployments compared to any other cloud service provider.

With the next-generation, secure-by-design cloud infrastructure and the Autonomous Database with multiple data protection capabilities built-in, Oracle is ready to remove the majority of the compliance and security burden from their customers.

A critical pillar in this secure-by-design cloud architecture is Oracle Data Safe, the unified control center for Oracle databases for automating data governance and risk management activities.
We reviewed Data Safe when it was first released back in 2019, but Oracle has substantially expanded the service's coverage and market positioning since which warrants an updated review.

2 Product Description

Oracle Data Safe is a cloud-based service for data protection, governance, and compliance for Oracle databases. It helps analyze the sensitivity of their data and evaluate the associated risks, mask sensitive information, implement and monitor security controls, assess user risks and analyze their activity, and address data security compliance requirements. Data Safe serves as a unified control center that allows customers to monitor and manage existing security capabilities of the Oracle Database, as well as correlate automatically-collected activity data with business risk context to help mitigate them sooner.

The Oracle Data Safe service is architected to be extensible, with additional security functions to be added in the future, yet tightly integrated to support consistent experience, unified alerting and reporting, and a single audit trail. It is globally available in every region of the Oracle Cloud, so customers concerned with data sovereignty can ensure that the information the service is collecting never leaves a certain geographic region.

The initial release of Data Safe focused on supporting Oracle Databases (both autonomous and unmanaged) in Oracle's cloud. In October 2020, a major update was introduced. Now Data Safe can connect to any Oracle database, including on-premises instances, instances managed by the Oracle Cloud@Customer private cloud stack, any type of database on the Oracle Cloud or indeed in other clouds like Amazon AWS and Microsoft Azure. This change has led to a major rethinking of the place of Data Safe within Oracle's security portfolio: the service is no longer positioned as just an add-on for the Autonomous Database services but is now a standalone top-tier cloud service that supports monitoring Oracle databases regardless of their location.

Data Safe is available at no additional cost to paid subscribers of DBaaS services in the Oracle Cloud. In fact, the company has made a considerable effort to make the service as easy to enable for every newly provisioned database instance as possible. Perhaps the next logical step would be to turn it on for all cloud databases automatically, following the company's "always-on security" claim, but at the moment, Oracle DBaaS customers can activate Data Safe with just a single mouse click.

To enroll an external database instance hosted on-premises or in any other public cloud, a secure connection between it and Data Safe must be established first. Existing capabilities for connecting corporate networks to Oracle Cloud, such as VPN Connect or FastConnect, can be utilized for this. An easier and more convenient alternative is using an Oracle Data Safe On-Premises Connector, a software agent installed on the customer's network. It establishes an encrypted outgoing connection to Data Safe that can serve multiple databases on the same on-premises network. Of course, a direct connection to a database instance with a public IP is also possible. It's worth noting that enrolling external database instances into Data Safe comes at a cost, but 30-day free trial access to the service is available.

After registering database targets in Data Safe, customers can start working from the main dashboard that

shows a graphical summary of all assessments performed by the service. The dashboard shows the charts with statistics for database security assessments, user assessments, data discovery, user and administrative database activities, open alerts, and service usage statistics. The overview can be filtered by target databases.

From this page, all functional areas of Data Safe can be accessed directly. A selection of security and compliance reports is also available through this UI.

So, let's have a look at the functional areas that are currently available in Oracle Data Safe:

Database Security Assessment

While Oracle databases are usually provisioned with a sensible set of secure-by-default parameters, their configuration can drift from the baseline, exposing the database to various attacks whether from insiders or outsiders. The service analyzes current database configuration, user accounts, and security controls, and then reports the findings with recommendations on how to reduce identified risks. A recently added feature allows saving any historical state of a database as a separate baseline profile and then comparing the most recent assessment to it, detecting potentially dangerous changes, and reverting them if necessary.

The service's findings are delivered as actionable reports, with individual recommendations ranked by risk and relevance for specific compliance frameworks like GDPR, US DISA STIG, or CIS. Of course, in the case of an Autonomous Database instance, most of these adjustments are handled transparently, but even in this case, some decisions can only be made by customers. For unmanaged or on-premises databases, this assessment supersedes and greatly expands the traditional DBSAT command-line tool.

User Risk Assessment

Another crucial area of data security and governance is identifying potential risks of privileged users having too broad access rights to sensitive data. The principle of least privilege is a common approach towards data protection, but only customers themselves can make an informed decision whether a particular privilege is needed for a legitimate business purpose.

Data Safe evaluates all database users and identifies potential abuse of privileges, taking both static (user type, role, password policy, etc.) and dynamic (history of past activities, last login) factors into account. The results of the assessment, including the list of the riskiest users along with all their available privileges, are presented to the customer. The initial release does not provide any automated mitigations against these users, focusing more on reporting capabilities and highlighting those database accounts that would pose the greatest risk if compromised.

Data Discovery and Classification

Data Safe scans for various types of sensitive information, ranging from personally identifiable information (PII) to finance, health, employment, or even IT-related data – over 140 types in total. Additionally, users can define their own custom types using regular expressions. Templates that contain preconfigured sets of sensitive types for various geographies and industries are provided out of the box – again, users can create their own to avoid cluttering their scans with irrelevant detections.

Data Safe also creates reports identifying the location of sensitive data within the database schema, and how many such values are present in the database, helping customers come up with an appropriate risk mitigation strategy. Although the classification engine is driven by regular expressions and lacks the sophistication of specialized AI/ML-based solutions, the results are comprehensive and the performance impact on the database is minimal. If there are any changes to the schema due to patches, upgrades, or customization, support for incremental discovery avoids the need to run the discovery process all over again. Still, we hope to see more concise, executive-focused discovery reports with clear KPIs in the upcoming releases.

Sensitive Data Masking

If sensitive data is discovered in a database, it can be desensitized with various data masking transformations according to policies defined by customers. Data Safe provides out-of-the-box support for over 50 predefined masking formats for various data types: national identifiers, credit card numbers, Social Security Numbers, dates, numbers, or strings. Data Safe's data masking is a mature and comprehensive technology that supports complex masking transformations for various scenarios: from development and testing to business analytics or industry-specific regulations.

Data Safe provides an easy interface for defining and applying masking policies to various sensitive data types across multiple columns, tables, or databases. In addition, the reporting service provides visibility into how much data has been desensitized.

User Activity Auditing

Finally, Data Safe provides an interface for managing the audit, compliance, and alert policies for each registered database instance. Although the audit data is generated in the database, the service offers convenient means for enabling various types of activity auditing, applying pre-defined audit and alert policies, and collecting the audit data in its centralized repository.

Extensive reporting capabilities allow users to access the collected audit data for all database targets interactively or through customizable reports in various formats, for security specialists or compliance auditors. These reports can be very useful for forensic analysis of activities across all databases, leading to a better understanding of who did what and when.

3 Strengths and Challenges

Oracle Data Safe represents a critical building block in the overall data protection, governance, and compliance architecture that the company has designed by combining its core database technology with the next-generation cloud infrastructure. When we reviewed the service nearly two years ago, we couldn't but praise its straightforward and easy-to-use approach to data risk assessments but were somewhat disappointed that it was only available for cloud-hosted database instances.

In 2020, Oracle addressed this limitation, and Data Safe has achieved feature parity across all types of Oracle databases regardless of their deployment location. Now, Data Safe can be recommended as an essential security service to every Oracle DBA without further reservations. Thanks to additional improvements in the service's deployment and a selection of different secure connectivity options, customers can now leverage Data Safe for all their Oracle database deployments whether on-premises or on any cloud. Arguably, Oracle Data Safe's only limitation is that it only supports Oracle Databases, which probably won't change soon.

However, Data Safe further demonstrates Oracle's sharp focus on providing database security across its whole portfolio. As a result, for the third year in a row, Oracle was recognized as the overall leader in the latest edition of KuppingerCole's Leadership Compass on Database and Big Data Security.

Strengths

- Centralized management, analytics, and guidance for data protection and governance technologies for databases
- Support for all types of Oracle databases on-prem and in the cloud with full feature parity
- Easy but secure deployment (single click for cloud instances)
- Comprehensive auditing, reporting, and alerting functions
- Improved actionable mitigation recommendations
- No extra cost for any paying Oracle cloud database customers

Challenges

- Only supports Oracle databases due to reliance on existing core DB technologies
- Data classification capabilities lack AI/ML sophistication
- Lacks executive-oriented business KPI statistics

4 Related Research

Leadership Compass: Database and Big Data Security – 80294
Market Compass: Cloud-delivered Security – 80208
Executive View: Oracle Data Safe – 80076
Executive View: Oracle Autonomous Database – 70964
Executive View: Oracle Database Security Assessment – 70965

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.