

# Oracle Database Security Assessment

This report provides an executive summary of Oracle’s Database Security capabilities based on recently published KuppingerCole research. It covers both the company’s traditional database security solutions and the innovative Autonomous Database cloud platform.



by **Alexei Balaganski**  
[ab@kuppingercole.com](mailto:ab@kuppingercole.com)  
April 2018

## Content

|   |          |
|---|----------|
| <b>1 Summary.....</b>                           | <b>2</b> |
| <b>2 Oracle Database Security Suite .....</b>   | <b>4</b> |
| <b>3 Oracle Autonomous Database Cloud .....</b> | <b>5</b> |
| <b>4 Copyright .....</b>                        | <b>6</b> |

## Related Research

Leadership Compass: Database Security – 70970<sup>1</sup>

Executive View: Oracle Autonomous Database – 70964<sup>2</sup>

---

<sup>1</sup> <https://www.kuppingercole.com/report/lc70970>

<sup>2</sup> <https://www.kuppingercole.com/report/ev70964>

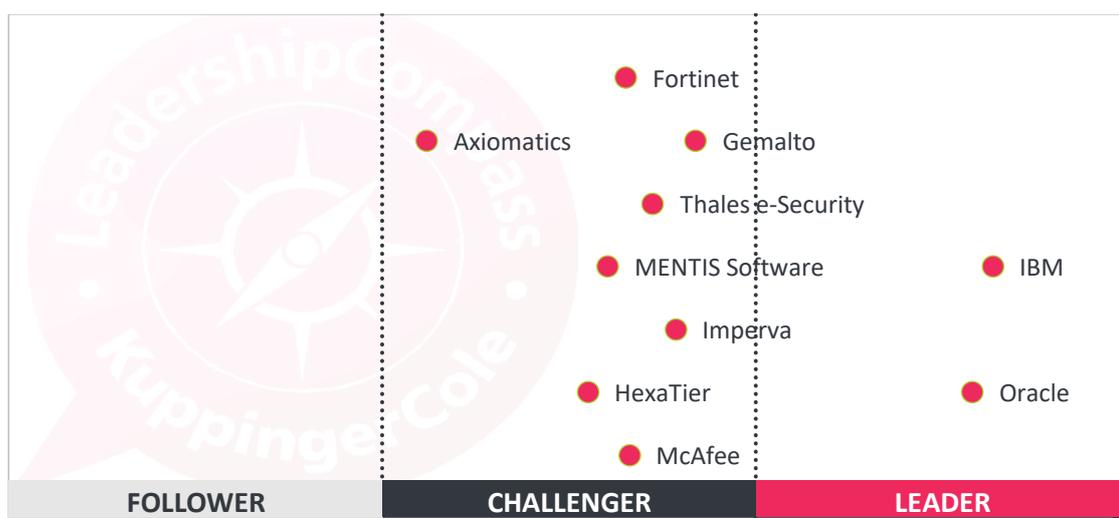
## 1 Summary

Databases are still the most widespread technology for storing and managing business-critical digital information. Growing amounts of the most valuable and sensitive corporate data must be protected against compromises of their integrity and confidentiality without affecting their availability for business processes. The number of security risks databases are open to is substantial, covering the information itself stored and processed in databases, underlying computing and network infrastructures, as well as applications accessing the data.

Databases have long been a prime target for cybercriminals of all sorts: from nation-state actors to business competitors or even malicious insiders. And as compliance regulations, such as the European Union’s GDPR, are getting stricter, a successful data breach can destroy both CIOs and the companies they work for. Unfortunately, recent breach statistics indicate that the number of attacks on critical verticals like healthcare, financial or government organizations continues to grow, with millions of records stolen daily.

Over 90% of breaches involved highly regulated personal and financial data, and less than 5% of breach victims reported that their current data protection measures were instrumental in preventing the breach. Attack scale is getting larger as well: the Equifax breach alone has affected half of the US population. Without a doubt, security has become the most important database capability, more than performance, manageability, availability, or anything else. Database security is becoming the new cybersecurity frontier.

In March 2017, KuppingerCole published the Leadership Compass on Database Security – a multivendor report covering multiple functional areas of database security. Although our analysis covered a mixture of both large veteran vendors and smaller, but innovative players, the results clearly indicate that only the largest companies that offer a wide range of products addressing different database security risks can be identified as leaders – see below.



Overall Leaders in the Database Security segment [Note: There is only a horizontal axis; vendors to the right are positioned better]

KuppingerCole has recognized Oracle among the distant overall leaders in database security, thanks to the combination of the company's global market presence, broad range of database security products and services in all eight functional areas covered in the analysis, as well as its impressive financial strength.

Perhaps the only reason that has prevented Oracle from claiming the overall leader title in our last year's report was its somewhat less than stellar score in the Innovation Leadership rating – at the time, we have recognized other vendor's contributions higher. Since then, however, the company has more than made up for this shortcoming by announcing the Oracle Autonomous Database – a truly disruptive innovation comparable to the recent developments in other fields of information technology like machine learning or serverless computing.

Oracle Autonomous Data Warehouse Cloud (ADWC) was released in March 2018, and KuppingerCole reviewed the solution soon afterwards, concluding that Oracle Autonomous Database is the world's first fully automated cloud database platform powered by machine learning. By eliminating human factor from database management, ADWC provides unprecedented security, reliability and performance for enterprise data management in the cloud.

The key findings of the report are summarized below:

- Human error is a major factor in security breaches. By introducing intelligent automation for all aspects of database management, Oracle ADWC not only reduces labor and costs for customers, but completely eliminates the human factor as a threat vector.
- Since ADWC completely eliminates administrative user controls, this dramatically increases its resiliency against malicious insiders, advanced hacking attacks as well as misconfigurations and other honest mistakes.
- Initial provisioning is the only step requiring human interaction: after defining the intended workload type, geographic location and resource policies, everything else is configured automatically according to the best practices in availability, security and performance.
- Since data encryption, access control and auditing are always enabled by default, sensitive data remains secure and compliant throughout its full lifecycle.
- Autonomous database instances support regular patching and upgrades with no downtime, as well as automated backup and disaster recovery functions. For demanding customers, a mission-critical SLA is offered with an impressive 99.995% availability level without any exceptions.
- Thanks to flexibility of the Oracle Exadata database machines running in the Oracle Cloud, ADWC instances support automated performance optimization and elastic resource usage, which ultimately leads to substantial cost reduction compared to traditional database servers.

On the whole, with the Autonomous Data Warehouse Cloud, Oracle has created a unique offering for the most demanding database customers that combines enterprise-grade performance and scalability with the highest level of security and compliance for sensitive corporate data by eliminating human factor and replacing it with industry best practices powered by the company's decade-long expertise and machine learning.

## 2 Oracle Database Security Suite

### Strengths

- Comprehensive product portfolio for all areas of database security
- Deep integration with other Oracle's Data Provisioning, Testing and Cloud technologies
- Multiple compliance management and reporting tools and services
- Hybrid Cloud Management for seamless operations across different environments

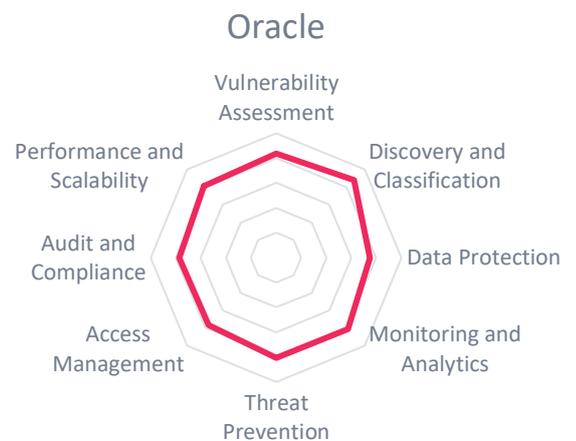
### Challenges

- A number of products are available only for Oracle Databases

The breadth of Oracle's database security portfolio is impressive: with a number of protective and detective products and a number of managed services covering all aspects of database assessment, protection, monitoring and compliance, Oracle Database Security can address the most complex customer requirements, both on premises and in the cloud.

It's worth noting that some of these products are specifically designed for Oracle Databases, which makes Oracle's data protection solutions less suitable for companies using other types of databases. Other products, such as auditing, monitoring and test data management solutions, support multiple database types.

|                         |                 |
|-------------------------|-----------------|
| <b>Security</b>         | strong positive |
| <b>Functionality</b>    | strong positive |
| <b>Integration</b>      | strong positive |
| <b>Interoperability</b> | strong positive |
| <b>Usability</b>        | strong positive |



Key components of the Database Security suite are:

- Oracle Key Vault for centralized management of encryption keys
- Oracle Audit Vault and Database Firewall for controlling SQL Injection, detecting anomalies, and supporting forensic analysis
- Oracle Database Vault for enforcing trusted path access to data and controlling privileged users
- Oracle Advanced Security for encryption and redaction of sensitive data
- Oracle Data Masking and Subsetting for targeted archiving and static masking of sensitive data for nonproduction purposes
- Oracle Label Security to enable multi-tenant usage of data tables at the data row level
- Oracle Database Security Assessment Tool for configuration analysis and sensitive data discovery

### 3 Oracle Autonomous Database Cloud

The concept of Autonomous Database is without doubt a disruptive innovation comparable to the recent developments in other fields of information technology like machine learning or serverless computing. By combining its decade-long experience in developing enterprise database solutions, the latest AI-powered innovations in the Oracle Database 18c and the scalability and performance of the dedicated Exadata hardware platform, Oracle has created a unique offering for the most demanding enterprise database customers, which finally shifts the competitive struggle from the playing field of other cloud service providers into the territory where Oracle, as a leading database company, has traditionally been a dominant player. Even as the first member of the new service family, the Oracle Autonomous Data Warehouse Cloud already demonstrates impressive scalability, performance and security benefits (not to mention cost optimization).

Of course, Autonomous Database may not be the optimal solution for every data management project in the cloud. To use the popular analogy that compares a wide range of managed database solutions currently available on the market with diverse types of vehicles, one could say that for many customers, a compact car or even a bicycle are still perfectly fine. But if your project calls for a jumbo jet instead, you will find one, and a pilotless electric-powered one to boot, in the Oracle Cloud.

| Strengths  | Challenges   |
|--|--|
| <ul style="list-style-type: none"> <li>● Fully automated cloud database platform combining enterprise-grade dedicated hardware with the latest Oracle Database release</li> <li>● Automated provisioning according to the best practices in availability, security and performance</li> <li>● Completely eliminates administrative user access, increasing resiliency against human errors, malicious insiders and hackers</li> <li>● Automated patching, backup and disaster recovery with no downtime; impressive 99.995% availability SLA</li> <li>● Automated performance optimization, independent resource scaling lead to substantial cost reduction</li> </ul> | <ul style="list-style-type: none"> <li>● Available in the Oracle Cloud only, further enforcing vendor lock-in</li> <li>● The first product from the series doesn't yet contain all promised features, limited to certain workload types</li> </ul> |

## 4 Copyright

© 2018 Kuppinger Cole Ltd. All rights reserved. Reproduction and distribution of this publication in any form is forbidden unless prior written permission. All conclusions, recommendations and predictions in this document represent KuppingerCole's initial view. Through gathering more information and performing deep analysis, positions presented in this document will be subject to refinements or even major changes. KuppingerCole disclaim all warranties as to the completeness, accuracy and/or adequacy of this information. Even if KuppingerCole research documents may discuss legal issues related to information security and technology, KuppingerCole do not provide any legal services or advice and its publications shall not be used as such. KuppingerCole shall have no liability for errors or inadequacies in the information contained in this document. Any opinion expressed may be subject to change without notice. All product and company names are trademarks™ or registered® trademarks of their respective holders. Use of them does not imply any affiliation with or endorsement by them.

## The Future of Information Security – Today

**KuppingerCole** supports IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst company, 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 Analyst Company headquartered in Europe focusing on Information Security and Identity and Access Management (IAM). KuppingerCole stands for expertise, thought leadership, outstanding practical relevance, and a vendor-neutral view on the information security market segments, covering all relevant aspects like: Identity and Access Management (IAM), Governance & Auditing Tools, Cloud and Virtualization Security, Information Protection, Mobile as well as Software Security, System and Network Security, Security Monitoring, Analytics & Reporting, Governance, and Organization & Policies.

For further information, please contact [clients@kuppingercole.com](mailto:clients@kuppingercole.com)