Ovum

Oracle Data Safe consolidates database security

Publication Date: 17 Sep 2019 | Product code: INT002-000256

Tony Baer

Ovum view

Summary

It is hardly news that security is among the chief concerns for senior IT management, and as enterprises look to the cloud for moving their mission-critical systems, the question of whether data can be secured in the public cloud has grown more important than ever. *Managed* cloud database service providers have made significant headway in automating the security of their services from external attacks, and in an era when cyberthreats are rapidly mutating, there is a solid case to be made that some cloud service providers are better equipped to repel incoming cyberthreats compared to your typical enterprise IT organization. But even if enterprises embrace these emerging managed services, they are still on the hook for developing and enforcing policies regarding access to and privacy protection of the data itself. Until now, that process has required a variety of standalone tools and has been challenging to track. Oracle's new Data Safe service, part of the Oracle Public Cloud, is the first service to unify the data security tasks that are the responsibility of the customer, and, like Oracle Autonomous Database service offerings, it takes a giant step in fulfilling the promise of IT simplification.

Database security in the cloud is a shared responsibility

We have gone on record as saying that *managed* database services, offering prescriptive approaches to packaging database cloud services, provide the biggest bang for the buck when it comes to delivering on the cloud's promise of IT simplification. When it comes to security, *managed* database-as-a-service (DBaaS) services typically handle network security and monitoring, operating system and virtual machine (VM) security and patching, and database security patches and upgrades.

For enterprises seeking to migrate their databases to the cloud, Ovum believes that DBaaS services will become the default option. Oracle in turn has taken DBaaS to the next level by introducing the Oracle Autonomous Database. While managed DBaaS services automate housekeeping steps such as updating and patching, autonomous takes it a step further by applying machine learning to optimize how the database runs. It does not eliminate the database administrator (DBA), but it does eliminate much of the non-value-added legwork that they traditionally perform. On the horizon, the Oracle Autonomous Database will eventually take that yet another step further by expanding the use of machine learning to performance tuning and security.

But even with automation, and with Oracle Public Cloud's latest autonomous database services, security remains a shared responsibility between Oracle and the customer. For starters, the cloud service provider should not inspect the customer's data, modify customer-controlled configuration settings, or second-guess permission grants for end users; those are the customer's responsibility. Protecting data, including identifying which data is sensitive, identifying what data to mask, and conducting risk assessments regarding different classes of users accessing specific categories of data, is also the customer's burden.

Until now, the tasks of conducting security assessments, identifying and masking sensitive data, and auditing data access have typically involved multiple standalone tools.

Oracle Data Safe unifies customer data security tasks on a single pane of glass

Oracle is introducing Data Safe, a new free cloud-based service. It brings configuration assessment, user assessment, sensitive data discovery, data protection with masking, and auditing of data access onto a single pane of glass. Underneath the hood, it implements these functions as microservices. The service is agentless, and only requires network connectivity.

Among its features are the following:

- Database security assessment shows which security controls are in use, the security-relevant parameters, and a summary of user data privileges. Its assessments identify gaps against best practices and provide reports with recommendations.
- Sensitive data discovery detects over 125 specific data types, which in turn can be extended by the administrator with additional custom data types. It can be run on demand.
- Sensitive data masking masks the sensitive data identified earlier through over 50 predefined masking formats (the customer can also implement their own custom masking transformations), and provides reports of the number of values masked.
- User risk assessment pinpoints high-risk users suspected of having excess privileges, and provides audits of data access and password policies. For instance, it can pinpoint inactive users or those who have not changed their passwords recently.
- User activity auditing can be configured on the fly to collect audit data automatically, generating reports that can be customized.

Oracle Data Safe will initially be made available only to Oracle DBaaS cloud customers. But as a cloud-based tool, it could be made more widely available. While we have been talking about cloud, Oracle Data Safe could also be used to scan and inspect on-premises databases.

The next step in cloud simplification

Oracle's introduction of Data Safe is timely, given the obvious fact that security is top of mind for most CIOs – and even more so as they consider moving their data to cloud services. A survey commissioned by Oracle, presented in its *Security in the Age of AI* report, revealed that security is by far the top concern – it was the top priority cited by a sample of nearly 800 C-suite executives, public policymakers, and technology industry professionals.

We also view it as timely given the growing adoption of cloud DBaaS services. Ovum has long believed that *managed* services provide the biggest bang for the buck when it comes to simplifying – and securing – IT operations. And, as we forecast in our *2019 Trends to Watch: Big Data* report, productivity will be the headline for analytics, data management, and artificial intelligence (AI) this year. We believe that in the long run, cloud providers running managed services will be in a better position to keep current with external cyberthreats.

Oracle Autonomous Database goes a long way toward simplifying life for the DBA. But to bring the promise of IT simplification full circle, there needs to be a way to consolidate all those configurations, audits, and reports that IT operations and DBAs must undertake to secure the data in their databases. To date, most cloud service providers have not concentrated these tasks in a single place or tool. Oracle Data Safe takes a big step in making them visible and enforceable from a single pane of glass.

Appendix

Further reading

"Oracle extends Autonomous Database to transaction processing," INT002-000155 (August 2018)

"Oracle bakes security into its DNA," INT003-000287 (November 2018)

"Oracle's second-generation cloud is designed to be enterprise grade," INT003-000329 (February2019)

2019 Trends to Watch: Big Data, INT002-000201 (December 2018)

Author

Tony Baer, Principal, dbInsight

tony@dbinsght.io

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at consulting@ovum.com.

Copyright notice and disclaimer

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Boston
Chicago
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
Paris
San Francisco
Sao Paulo
Shanghai
Singapore
Sydney
Tokyo