

Is “Why Not Both?” Oracle’s New Product Strategy?

I firmly believe that one of the key success factors of a product strategy in any industry is to be able to offer customers just the right amount of choice. Looking back at the history of such companies as Ford, Kodak, IKEA, or Apple, we can see that their success was to a large extent in their ability to sell not just a product, but an entire lifestyle, a single, convenient solution for all their customers’ problems, whether real or just invented by marketing departments. Of course, this approach does not work every time, as the eventual fate of Kodak indicates. Customer requirements, just like technology, fashion and other societal factors, change all the time, and the product ecosystems have to adapt or risk extinction...

In a sense, Oracle is undergoing a similar transformation now, as the company is reinventing itself as a major player in the cloud service provider market. This has naturally required major changes in Oracle’s strategy, transitioning from the old “hermetic” way towards open, mutually beneficial partnerships with other vendors and even direct competitors like Microsoft Azure. The most obvious sign of this change, as we have mentioned many times before, is the idea that instead of catching up with competitors on their established playing fields (for example, trying to offer cheaper infrastructure than AWS), Oracle should focus on its unique services that no other competitor can offer, like the Autonomous Database, and promote efficient and convenient multi-cloud architectures through 3rd party integrations.

Essentially, whenever a customer is facing a supposed dichotomy, having to choose between a solution from Oracle or from a competitor, the company’s answer now boils down to a well-known meme: why not both? Practical examples of this strategy can be seen in supporting direct interconnects between Oracle and Azure cloud datacenters in many regions or even in making MySQL HeatWave a first-class open source alternative to Oracle’s own database even for enterprise use cases.

Basically, we can see a major transformation in the market of cloud services, both for data management and in general. Before, customers had to make fundamental choices before starting a new project, such as selecting the underlying database layer: should they opt for the universal approach with Oracle Database or choose the broad range of specialized engines from AWS. This choice has effectively robbed them from most of the future flexibility, should something go wrong and the initial selection prove to be suboptimal.

Nowadays, customers are free to use Oracle's database services but, say, connect them to applications running on Microsoft Azure and AI services from GCP. And, of course, these services are expected to be truly and independently elastic to accommodate for unexpected changes in demand and to minimize operational costs for customers. This is what I call the right freedom of choice that underlines the real modern "multi-cloud native" approach.

However, Oracle does not stop there and in a sense, adopts the same strategy even within its own product ecosystem. The latest example of this I can see in the recent announcement of Multi-VM Autonomous Database on Exadata Cloud@Customer, Oracle's private cloud platform. Even if it sounds too technical at first sight, it is really all about giving customers real choice of running both the Exadata Database Service and Autonomous Database Service simultaneously on the same hardware deployed in their data centers and managed by Oracle Cloud Infrastructure (OCI).

Previously, customers of Oracle's managed private cloud platform were able to choose whether they wanted to run the traditional, enterprise-proven databases on a particular Exadata Cloud@Customer system for their business-critical applications or instead opt for the fully managed, self-tuning Autonomous Database instances, favored by modern developers on a separate Exadata Cloud@Customer system. They had to make a choice once and then stick to it for the whole lifecycle of the platform.

Now they can have both. Thanks to the improvements in the underlying management platform, customers can create multiple clusters of virtual machines on the same Exadata Cloud@Customer infrastructure and then configure each cluster for the type of database service that they need independently. This is implemented as a set of self-service workflows that can be delegated to different roles, such as developers, application DBAs and DB fleet managers.

From a security and governance perspective, the role of fleet managers is particularly interesting and has a follow-on positive impact on developers. The fleet manager defines the runtime environment isolation and SLAs at the cluster level, according to corporate governance best practices, and then gives each developer or operational team visibility into a subset of environments along with access controls and quotas that limit the resources they consume.

Exadata Cloud@Customer's built-in security helps secure the actual databases, but it's up to the fleet administrator to ensure that corporate governance is defined for each environment – functional governance like defining backup retention policies, failover capabilities, update scheduling, and where data is stored throughout its lifecycle in order to meet data residency requirements. Operational governance like separation of dev-test from production, secure isolation between application teams, and mission-critical workload separation are also managed by them.

As a result, individual developers and application DBAs no longer have to think about security and governance requirements, and they can just take the operating environments given to them and do whatever they need within their assigned quotas, increasing their personal productivity.

However, for organizations as a whole, the governance and compliance benefits of this approach are also obvious. Instead of having to manage multiple disconnected development, test, and staging environments separately from production instances, now companies using Exadata Cloud@Customer

can benefit from applying the same policies across all their data and at the same time significantly reducing the administrative effort and data friction between organizational units. Another win for “Why not both” indeed!

© 2022 KuppingerCole Analysts AG. All rights reserved. Reproduction and distribution of this publication in any form are 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 disclaims 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 does 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