



Market Insight Report Reprint

Oracle positions database, identity and built-in features for cloud security

March 31 2021

Fernando Montenegro, Scott Crawford

Cloud security is routinely listed as a key concern in any cloud transformation, but the issue is even more pronounced for larger enterprises, which need a robust security posture from their cloud suppliers. Oracle Cloud is looking to meet this demand anchored on its experience with databases and identity, coupled with built-in security features.

451 Research

S&P Global

Market Intelligence

This report, licensed to Oracle, developed and as provided by 451 Research, LLC, was published as part of our syndicated Market Insight subscription service. It shall be owned in its entirety by 451 Research, LLC. This report is solely intended for use by the recipient and may not be reproduced or re-posted, in whole or in part, by the recipient without express permission from 451 Research.

Introduction

With the strategic importance of digital transformation and the increased adoption of cloud-based infrastructure, enterprise security teams are being asked to do a lot – enable innovation at scale, but do so in a secure manner, avoiding insecure practices that may have downstream effects on regulatory efforts or other undesired security outcomes. This need is well understood by cloud suppliers, which have poured significant resources into security architecture and offerings. As Oracle Cloud pursues a broader share of the market, the company is positioning its experience with databases and identity as key, plus the security features it built into its offering.

THE 451 TAKE

Oracle is looking to capitalize on two key assets: First and foremost, how to leverage its enterprise strength in databases and business applications into a seamless on-ramp for enterprises moving to cloud; and second, how to do so while applying lessons learned from current industry practices for securing cloud resources. This is an observation on the vendor's cloud business in general but it is clearly visible within its approach to cloud security – its current offerings target what it sees as common pains felt by typical enterprise customers, which may favor more centralized control in various aspects. Security teams looking at how to deploy secure Oracle Cloud environments are likely to find that many of the common controls and features take on a more integrated and centralized approach.

There are also two key aspects to keep in mind: First, compared with other cloud providers, there's understandably a smaller pool of external expertise to draw from; second, some of the services often more associated with security operations such as vulnerability scanning, threat intelligence integration and others are not yet available from Oracle, meaning that for now, customers need to bring in their existing capabilities.

Details

During a recent company update, Oracle emphasized that having security features 'built-in' its overall offering is a key component of its strategy for positioning Oracle Cloud against competing offers, knowing that customers are likely to be receptive to the message of optimizing security objectives for Oracle Cloud with less effort. The vendor indicated that it is anchoring its security capabilities across the pillars of its autonomous database, the 'gen2' Oracle Cloud Infrastructure, and its offerings in terms of identity management.

The company is looking to leverage two key capabilities for offering secure databases in the cloud. First, it is highlighting the role of automation and platform homogeneity in reducing the likelihood of security incidents. Second, it is using its previous capabilities with securing traditional, on-premises databases. This includes providing features such as Transparent Data Encryption, Oracle Data Safe and Database Vault. Oracle Data Safe performs data security tasks such as reporting configuration analysis, discovering and masking sensitive data, and providing activity reporting, while Database Vault is built to provide stronger segregation of duty controls.

Oracle's position is that the relative recency of its cloud architecture – the current version was launched in late 2016 – allowed it to incorporate more security considerations and learnings into its design. This includes having a tenant and compartment design philosophy that is aimed at matching requirements from enterprise security and compliance teams with a preference for supporting default secure configurations. The underlying infrastructure is similar to other suppliers, with Oracle offering features such as network isolation and hardware-based security for use by secure boot processes or bootstrapping workload identities. Like other providers, Oracle also highlights compliance with numerous regulatory mandates, public standards and frameworks.

The two key security services Oracle Cloud currently offers for infrastructure are Cloud Guard and Maximum Security Zones. Cloud Guard is aimed at providing reporting and control over cloud security posture configurations. Maximum Security Zones is an additional feature that enables preemptive control over sensitive cloud configuration options for compartments/zones marked as sensitive.

Oracle is also counting on leveraging its expertise and market penetration in identity and access management (IAM) as a key pillar for cloud security. The vendor argues that the centralized approach it takes to authentication and authorization across the Oracle Cloud Infrastructure services, coupled with streamlined support for multi-factor authentication and integrated auditing, will be appealing to those looking to map common enterprise patterns for IAM into a cloud supplier. The company also plans to extend this IAM model to cover its SaaS applications.

The existing adoption of Oracle's identity portfolio reflects its longstanding role in enterprise application platforms, and highlights one way in which the vendor's key pillars in security may help differentiate its cloud offerings. We expect Oracle to continue to highlight not only these aspects of Oracle Cloud for these business purposes, but also its investments in security overall.

CONTACTS

The Americas

+1 877 863 1306

market.intelligence@spglobal.com

Europe, Middle East & Africa

+44 20 7176 1234

market.intelligence@spglobal.com

Asia-Pacific

+852 2533 3565

market.intelligence@spglobal.com

www.spglobal.com/marketintelligence

Copyright © 2021 by S&P Global Market Intelligence, a division of S&P Global Inc. All rights reserved.

These materials have been prepared solely for information purposes based upon information generally available to the public and from sources believed to be reliable. No content (including index data, ratings, credit-related analyses and data, research, model, software or other application or output therefrom) or any part thereof (Content) may be modified, reverse engineered, reproduced or distributed in any form by any means, or stored in a database or retrieval system, without the prior written permission of S&P Global Market Intelligence or its affiliates (collectively, S&P Global). The Content shall not be used for any unlawful or unauthorized purposes. S&P Global and any third-party providers, (collectively S&P Global Parties) do not guarantee the accuracy, completeness, timeliness or availability of the Content. S&P Global Parties are not responsible for any errors or omissions, regardless of the cause, for the results obtained from the use of the Content. THE CONTENT IS PROVIDED ON "AS IS" BASIS. S&P GLOBAL PARTIES DISCLAIM ANY AND ALL EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, FREEDOM FROM BUGS, SOFTWARE ERRORS OR DEFECTS, THAT THE CONTENT'S FUNCTIONING WILL BE UNINTERRUPTED OR THAT THE CONTENT WILL OPERATE WITH ANY SOFTWARE OR HARDWARE CONFIGURATION. In no event shall S&P Global Parties be liable to any party for any direct, indirect, incidental, exemplary, compensatory, punitive, special or consequential damages, costs, expenses, legal fees, or losses (including, without limitation, lost income or lost profits and opportunity costs or losses caused by negligence) in connection with any use of the Content even if advised of the possibility of such damages.

S&P Global Market Intelligence's opinions, quotes and credit-related and other analyses are statements of opinion as of the date they are expressed and not statements of fact or recommendations to purchase, hold, or sell any securities or to make any investment decisions, and do not address the suitability of any security. S&P Global Market Intelligence may provide index data. Direct investment in an index is not possible. Exposure to an asset class represented by an index is available through investable instruments based on that index. S&P Global Market Intelligence assumes no obligation to update the Content following publication in any form or format. The Content should not be relied on and is not a substitute for the skill, judgment and experience of the user, its management, employees, advisors and/or clients when making investment and other business decisions. S&P Global Market Intelligence does not endorse companies, technologies, products, services, or solutions.

S&P Global keeps certain activities of its divisions separate from each other in order to preserve the independence and objectivity of their respective activities. As a result, certain divisions of S&P Global may have information that is not available to other S&P Global divisions. S&P Global has established policies and procedures to maintain the confidentiality of certain non-public information received in connection with each analytical process.

S&P Global may receive compensation for its ratings and certain analyses, normally from issuers or underwriters of securities or from obligors. S&P Global reserves the right to disseminate its opinions and analyses. S&P Global's public ratings and analyses are made available on its Web sites, www.standardandpoors.com (free of charge) and www.ratingsdirect.com (subscription), and may be distributed through other means, including via S&P Global publications and third-party redistributors. Additional information about our ratings fees is available at www.standardandpoors.com/usratingsfees.