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.
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.