Ovum
TMT intelligence | informa

Oracle bakes security into its DNA

Publication Date: 16 Nov 2018 | Product code: INT003-000287

Maxine Holt

Ovum view

Summary

At the inaugural Oracle Security Summit held at the company's stunning Santa Clara campus in September 2018, analysts heard how the myriad security products and services offered by the software and services monolith are further being enmeshed in the overall cloud portfolio and refocused on promoting business outcomes. This is welcome news for enterprises, service providers, and partners, all of which are looking to consolidate their security products and settle on fewer platforms to run these products.

Without doubt, Oracle's focus on the cloud is benefiting customers that want to reduce reliance on their own data centers. Interestingly, the vast majority of Oracle cloud customers are new to the company, with many of the organizations currently using its traditional on-premises software yet to begin or complete their journey to the cloud, a huge potential market for Oracle's cloud platform. This is backed up by Ovum's ICT Enterprise Insights for 2018–19, which found that the adoption of cloud services is a priority for fewer than 10% of surveyed organizations.

Oracle's messaging has been adjusted to recognize that nearly every organization has a heterogenous IT environment, combining on-premises, multicloud, public cloud, private cloud, and hybrid cloud: the real world. As explained by Eric Olden (senior vice president and GM security and identity, IDM Enterprise), this messaging is backed up by a layered approach to security: the "Trust Fabric" and complemented by a strong focus on security as part of Oracle's DNA.

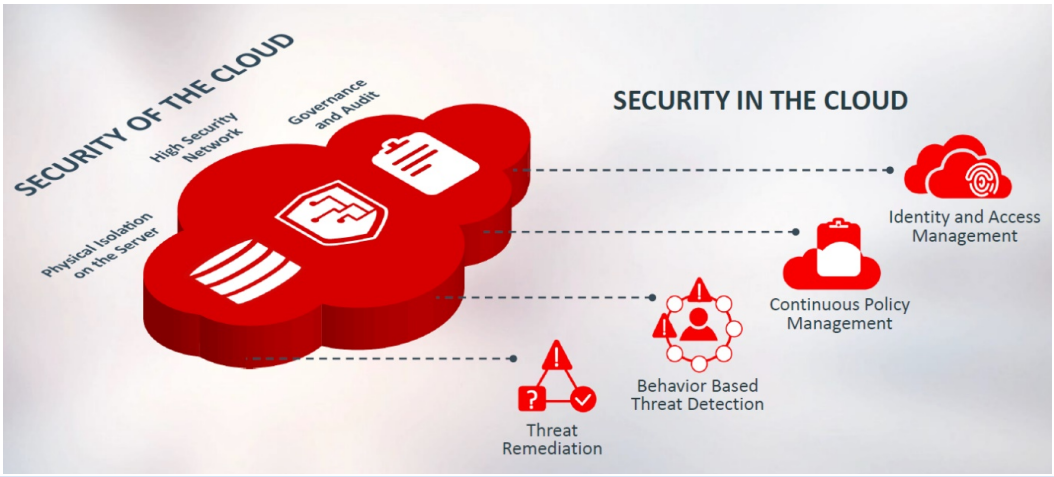
Security in and of the cloud

Increasing automation is evident across the enterprise and service provider IT landscape, where it is used to improve services and augment roles performed by humans. Oracle is no stranger to automation across its cloud platform and services, and this is working its way into security.

Oracle has recognized not only the importance of security (a basic requirement) but also that security can be used as a competitive differentiator when ingrained into products, services, and culture. Security can be offered *as* products and services, and can also be baked *into* existing products and services.

Placing bets on increasing volumes of customers (new and existing) availing themselves of its cloud platform, Oracle picks up on two angles of security: security OF and IN the cloud (see Figure 1).

Figure 1: Oracle Security OF and IN the cloud



Source: Oracle

Security of the cloud (baking security into its products and services) incorporates physical isolation on the server, a high-security network, and governance and audit. Security *in* the cloud (security-focused products and services) incorporates identity and access management (IAM), continuous policy management, behavior-based threat detection, and threat remediation.

People, process, and technology are central to the autonomous services built on Oracle's cloud platform. Taking inputs from data, applications, users, devices, and systems, these autonomous services aim to reduce the mean time to detection and resolution for security incidents and breaches. Investments have been made into security analytics, identity management, database security, infrastructure security (incorporating the acquired internet performance management capabilities from Dyn), and cloud security, providing visibility and control over multicloud environments including software-as-a-service (SaaS), platform-as-a-service (PaaS), and infrastructure-as-a-service (IaaS). The intention is for Oracle customers to benefit through reduced operational costs alongside improved productivity and better risk mitigation.

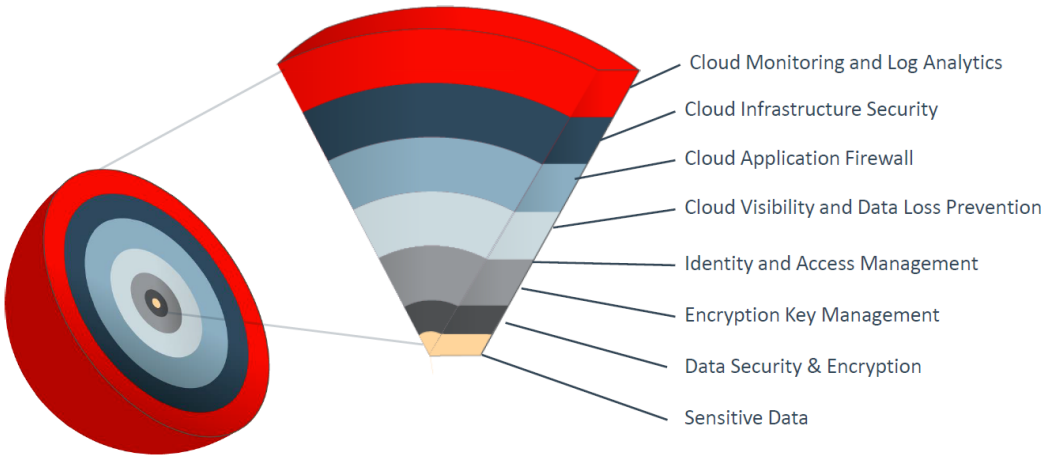
Trust is an essential component of cloud platforms

The cyberthreat landscape is evolving and morphing at an incredibly fast rate. Couple this with the enterprise digital transformation journey that inevitably exposes new threat vectors, and enterprises are faced with risks that are complex to assess and threats that are difficult to prevent, detect, and respond to. Enterprises are increasingly recognizing that the security of cloud platforms is generally superior to what can be delivered in-house, but the additional attack vectors are increasing the identified risks and these risks must be mitigated in line with the organization's risk posture.

Although the journey to the cloud, and especially multiclouds, is still in the early stages for many organizations, more is expected of the cloud today than ever before. Security must be built in from the outset, rather than bolted on as an added extra.

To address this, Oracle has developed its "Trust Fabric" as part of security in and of the cloud. According to Olden, the Trust Fabric aims to create secure, trusted, agile, and compliant enterprise computing built for the cloud, and incorporates a layered security model (see Figure 2).

Figure 2: Oracle Trust Fabric layered security model



Source: Oracle

A layered approach to security is widely recognized as the only way for organizations to achieve a reasonably comprehensive security posture. The level of "comprehensiveness" will depend on the number and quality of layers of security. In the Oracle Trust Fabric, these layers are designed to help organizations understand the comprehensive approach as well as support compliance expectations.

The Trust Fabric is managed via a virtual security operations center (SOC) focused on autonomous detection of security threats and response to security incidents and breaches. Furthermore, the Trust Fabric is designed to deliver unified security across an enterprise's entire cloud journey. This requires integration to create a fully integrated security portfolio incorporating security across Oracle apps and services.

Security is part of the DNA

In one of the sessions, analysts heard from two individuals with various responsibilities for security at Oracle, including Oracle's own security for the cloud platform. This is where we saw evidence of security being baked into the DNA of the organization, with a security-positive culture at the core. Yes, Oracle products are used extensively, but the technology is supplemented by strong processes and a swathe of people who are well-versed in security best practice. Security governance drives the overall ethos, and risk and compliance come into play extensively.

This security DNA is certainly reflected in the overall messaging from Oracle, particularly across its cloud portfolio. Helping enterprises on their cloud journey, and recognizing that a heterogeneous environment (multicloud and on-premises) is the norm, has positioned Oracle well in pursuing business outcomes with its customers.

Going forward, Oracle can develop its business-outcomes discussions with customers to include total cost of ownership (TCO). It can tap into the significant market of existing on-premises customers yet to begin or develop their journey to the cloud, highlighting the cost benefits of taking (for example) cloud security services. Although this has the potential increase Oracle's revenues from an individual customer, it can also reduce the overall TCO for the customer, a conversation that most organizations will welcome, at least once they've decided to start their journey to the cloud.

Appendix

Further reading

“Autonomous becomes Oracle watchword in cloud” ENS002-000028 (May 2018)

“Oracle’s autonomous cloud portfolio drives greater developer productivity and operational efficiency” INT003-000091 (March 2018)

"Oracle’s PaaS delivery of blockchain is a smart move" INT003-000060 (February 2018)

“Oracle’s approach to the cloud is clearly differentiated” INT003-000037 (January 2018)

Author

Maxine Holt, Research Director

maxine.holt@ovum.com

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

Ovum
TMT intelligence | informa

CONTACT US

ovum.informa.com
askananalyst@ovum.com

INTERNATIONAL OFFICES

Beijing
Dubai
Hong Kong
Hyderabad
Johannesburg
London
Melbourne
New York
San Francisco
Sao Paulo
Tokyo