Brought to you by Informa Tech

OMDIA

Publication date:
19 Nov 2021
Author:
Omdia Analyst,
Rik Turner, Principal Analyst, Emerging Technologies

Oracle extends web application firewall to internal apps

Omdia view

Summary

Oracle is expanding its web application firewall (WAF) capabilities, adding WAF features to its load balancer so as to protect so-called internal or private apps—i.e., those to which only an enterprise's own employees, and possibly also business partners, have access because they are not internet-facing. Thus, Oracle's WAF can now be used to protect apps within the Oracle Cloud Infrastructure (OCI) in third-party clouds and residing on a customer's premises. Omdia considers this a significant move in that it may force other cloud service providers to consider how good their cloud-based WAF offerings are at supporting hybrid and multicloud environments.

Differences between cloud and on-premises security

Cloud security is an evolving art in which new branches are emerging, each with its concomitant acronym: along with cloud security posture management (CSPM) and cloud workload protection platforms (CWPPs) there is now a need to add cloud permissions management (CPM), infrastructure-as-code (IaC) security, API security, and specific security platforms for the newer workload formats such as containers and serverless. There is even a new catch-all term: cloud-native application protection platform (CNAPP) to encompass them all.

Beyond those capabilities, however, there is also the question of who is best placed to deliver them, which is something that has never really been an issue in the on-premises world. In this scenario, one group of vendors provided the infrastructure (servers, storage, and networking gear) while another supplied the technology needed to secure it (firewalls, identity management systems, encryption platforms, etc.).

There were, of course, exceptions, with storage vendors enabling full-disk encryption and database vendors enabling individual fields, rows, or columns to be encrypted to protect the data. Nonetheless, the providers of IT infrastructure and those that supplied the security platforms that protected it enjoyed a largely peaceful and symbiotic coexistence and one that was mutually beneficial.

CSPs offer security but often only for their own platform

In cloud computing, on the other hand, the companies providing the services whether in infrastructure-, platform-, or software-as-a-service (IaaS, PaaS, or SaaS) delivery modes often feel a desire, if not a need, to provide the security around it. Cloud service providers of all stripes provide identity management, as well as encryption and key management.

The leading players in IaaS and PaaS also have a WAF service and offer protection from distributed denial-of-service (DDoS) attacks, particularly if they also have a content delivery network (CDN) as part of their cloud offering. What has tended to differentiate their offerings from those of third-party and dedicated security vendors offering products that work on their cloud platforms, often via their marketplaces/app stores, has been the latter's heterogeneity.

In other words, while a CSP has every interest in providing security that works well on its platform, it has often been considered nonsensical if not counterproductive for it to enable security on its competitors' clouds. AWS, for instance, makes no secret of the fact that it develops security for assets (workloads and data stores) on AWS, referring customers that want multicloud security to the third-party security specialists whose wares are available on its marketplace.

Oracle goes "cloud-inclusive"

Oracle got its WAF technology in early 2018 when it acquired dedicated next-generation application security vendor ZenEdge. The latter was obviously heterogeneous in its offering as any dedicated security vendor must be, supporting all and any of the leading cloud platforms. The question, therefore, was whether the buyer would double down on that heterogeneity or instead make the ZenEdge platform increasingly OCI-specific.

Furthermore, there was a precedent, namely the cloud access security broker (CASB) technology Oracle had acquired two years earlier, in 2016, when it bought specialist startup Palerra. That platform, which had worked across any SaaS application, was refocused to work specifically on OCI-based apps.

Now, however, Oracle's latest move with its WAF represents a break from the conventional CSP security model, offering protection for application infrastructure and workloads no matter where they reside: in OCI, on a customer's premises, in multicloud, and anywhere in between. And indeed, with the extension of its WAF capabilities to its load balancers, it is even supporting internal, i.e. non-Web applications, a development that is particularly important for enterprise customers in segments such as financial services.

The vendor calls its strategy a "cloud-inclusive" one, which is clearly recognition of the fact that many Oracle customers are still on a journey to the cloud, and indeed that some of their workloads may never move off their premises. It also demonstrates an awareness of enterprises' growing interest in deploying into a multicloud environment rather than putting all their eggs into one cloud-based basket, so to speak.

Appendix

Further reading

Omdia Universe: Selecting a Cloud Service Provider, 2021–22 (October 2021)

Oracle launches significant upgrade in customer experience (October 2021)

Oracle puts MySQL on autopilot with new AI/ML-fueled capabilities for both transactional and analytical workloads (August 2020)

SWOT Assessment: Oracle Cloud Infrastructure (May 2020)

Author

Rik Turner, Principal Analyst, Cybersecurity

askananalyst@omdia.com

Citation policy

Request external citation and usage of Omdia research and data via citations@omdia.com.

Omdia consulting

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

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.

CONTACT US

omdia.com

askananalyst@omdia.com