**Publication date:**
January 2022
**Author:**
Rik Turner
Roy Illsley

# Built-in versus bolt-on: Where to get your security for the cloud

OMDIA

Brought to you by Informa Tech

Omdia commissioned research, sponsored by Oracle

# Contents

# Omdia view

## Summary

Cloud adoption proceeds apace in enterprise IT. The software as a service (SaaS) delivery mode for cloud computing mushroomed into a giant market segment fully a decade ago, and now, as businesses become more comfortable with cloud generally, the infrastructure and platform as a service (IaaS and PaaS) modes are growing even more rapidly.

According to Omdia's ICT Enterprise Insights survey (see the **Further reading** section below), public cloud use (measured as the percentage of an organization's workloads running in some form of public cloud—IaaS, PaaS, or SaaS) has increased from 25% in 2019 to 46% in 2021. Cleary, SaaS leads the charge and remains the largest part of the market, because its SaaS adoption requires the least work by the organization turning to the cloud for its application requirements. By contrast, both IaaS and PaaS entail deeper levels of commitment, with developers getting involved to create, and IT operations to maintain, app estates.

This evolution of enterprise application infrastructures raises the question of how best to secure an organization's code and data once it resides in the cloud. IaaS and PaaS providers, hereafter referred to as the cloud service providers (CSPs), sell compute and storage, plus core functions such as databases. They also bundle into their services, often at no extra charge, a considerable amount of security functionality such as identity and access management (IAM), encryption, and key management.

However, in addition to those "built-in" security capabilities, third-party, dedicated cybersecurity vendors offer their own technologies for deployment in those same clouds, often by participating in the marketplaces operated by the CSPs. They offer functionality that is not available from the CSPs themselves, such as next-generation firewalls (NGFWs), intrusion detection/prevention systems (IDPS), privileged access management (PAM), and cloud permissions management (CPM). That said, they also offer some areas of cybersecurity capability that overlaps with what the CSPs themselves bundle into their services, raising the obvious question in the customer's mind: do I use what my CSP offers me, or should I go to a dedicated third-party security vendor?

How should an enterprise customer gauge the value of the "bolt-on" security technologies vis-à-vis the built-in ones? Obviously, the latter are free to use, but beyond this narrow financial dimension, are there also operational advantages to leveraging the built-in compared to the bolt-on options? Are there even scenarios in which the built-in capabilities of cloud services are as good, or even better, than those that are bolted on, from a pure security perspective? In other words, can your cloud assets ever be secured better by the capabilities built into the service by the CSP than by third-party security products?

This white paper aims to address that question, looking at the pros and cons for both the “built-in” and the “bolted-on”, specifically in the context of Oracle’s cloud service offering, a.k.a. Oracle Cloud Infrastructure (OCI), considering the security technologies it includes as default in the service and what dedicated security vendors that are in its marketplace have to offer.

# Key messages

- The ability to demonstrate a clear roadmap by the cloud provider for its built-in security capability evolution is critical.
- Fragmented and/or isolated security solutions present both a risk and an opportunity.
- Obtaining a holistic view of the entire environment from bare metal to SaaS is needed to reduce the operational burden and increase the security of the cloud.

## Emerging cloud technologies present new security threats

### How does the CSP address new cloud technology paradigms?

A key consideration is how the built-in security capabilities cover the rapidly changing cloud-native technologies such as containers, serverless, and infrastructure as code (IaC), and the new security challenges they represent.

Containers present different security risks from virtual machines, and serverless environments introduce still further opportunities for security exploits. IaC brings a new level of convenience for developers, but if done wrongly, it can also expand an organization's attack surface.

A further complication for security consideration is the emergence of the edge—moving the compute to where the data is generated, both for real-time analysis and reporting. This is particularly significant as much of the edge will be based on cloud-native technologies. The CSPs have recognized the importance of the edge and introduced specific offerings such as Oracle Dedicated Region Cloud@Customer and Exadata Cloud@Customer that customers can deploy to provide an edge cloud for these distributed workloads.

### Dedicated start-ups represent a risk in their own right

There are, of course, products from third-party security providers that aim to address these new technologies. However, the vendors in question tend to be small start-ups, thereby increasing the number of security products and solution providers, which in itself constitutes a security risk. It not only means more supplier relationships for an organization to manage, but also, when those suppliers are smaller and younger companies, the risk that they may fail, go out of business, or be acquired by another vendor that an organization does not want to do business with.

Thus, a major question is how the cloud provider's built-in security evolves. Does the cloud provider have a future roadmap that demonstrates continued innovation, or is it a reactive approach providing solutions for only mature technologies?

# Understanding Oracle's built-in security technologies

Oracle launched Oracle Cloud Infrastructure (OCI), which underpins both its IaaS and PaaS offerings, in October 2016, and since then, it has been building out both its geographical reach and technical capabilities. In terms of security for its cloud services, the company has built in a range of products, including:

- **Identity and access management**—Oracle's SaaS-delivered identity service, OCI IAM, allows enterprises to manage and automate the end-to-end lifecycle of user identities, providing users with secure, fine-grained access to enterprise resources and assets.

- **OCI Certificates**—Oracle can issue its own digital certificates via the OCI Certificates service. This enables people, computers, and organizations to exchange information securely over the internet using public key cryptography. Certificates can also be used to validate access rights to cloud workloads. The facility also prevents the need for customers to go to a third-party certification authority.

- **OCI Bastion**—an ephemeral access service, providing restricted and time-limited secure access to resources that don't have public endpoints and require strict resource access controls, such as compute instances, bare metal and virtual machines, MySQL, ATP, Oracle Container Engine for Kubernetes (OKE), and any other resource that allows Secure Shell (SSH) protocol access.

- **Oracle Data Safe**—a service that helps customers identify configuration risk, establishing a security baseline and monitoring the database for drift away from that baseline. It scans the database to locate and classify sensitive data, statically masks sensitive data in test and development systems, assesses user security, and monitors user activity. Data Safe is a single console to manage the day-to-day security and compliance requirements of Oracle databases and is included with OCI database services (including Oracle Cloud@Customer) and is available for Oracle databases running on-premises or in third-party clouds.

- **Oracle Cloud Guard**—a service that helps customers monitor, identify, achieve, and strengthen their security posture on OCI and can, therefore, be categorized as a cloud security posture management (CSPM) service. Customers use it to examine their OCI resources for security weakness related to configuration, as well as their operators and users for risky activities. Upon detection of a problem, Cloud Guard can suggest, assist, or take corrective actions, based on your configuration. It also raises alerts from other OCI security services like Vulnerability Scanning, Data Safe, and Certificates.

- **Oracle Security Zones**—a service enabling customers to set up and enforce security policies for cloud compartments in OCI, with a policy library and embedded best practices to enable security controls related to CPSM. As such, it supplements Oracle Cloud Guard and OCI IAM with additional enforcement controls that can be applied to resources in compartments.

- **OCI Vulnerability Scanning Service** (VSS)—helps customers eliminate risk from unpatched vulnerabilities and open ports by assessing and monitoring their OCI instances. It integrates with Oracle Cloud Guard, enabling customers to identify vulnerabilities and common misconfigurations, thus improving the security postures of their OCI instances.

**Table 1: Oracle's built-in cloud security services**

| Product name | Category |
|---|---|
| OCI IAM | Identity and access management |
| OCI Certificates | Digital certificates |
| OCI Bastion | Ephemeral access |
| Oracle Data Safe | Unified database cloud security platform |
| Oracle Cloud Guard | Cloud security posture management |
| Oracle Security Zones | Security posture enforcement |
| OCI Vulnerability Scanning Service (VSS) | OCI instance vulnerability management |

Source: Omdia

# Security should be designed into any cloud and provided as part of the service

The rationale for Oracle's development of security technology to support its OCI cloud services is to make security easy to use, prescriptive, and integrated. The company argues that security should be foundational and built-in, enabling customers to avoid having to make trade-offs between security and cost. Security services are integrated into OCI itself and, indeed, are some of the same tools Oracle uses to protect its 60-plus different SaaS and PaaS services, all of which are delivered from the OCI IaaS platform.

As cloud use is forecast to continue to grow, any cloud architecture must have designed-in security that provides customers with the confidence to use the cloud services. Omdia considers that "built-in" versus "bolt-on" is a question of making the cloud inherently secure to use (built-in) while also increasing its applicability to specific use case scenarios (bolt-on). In other words, these two offerings should be seen as complementary not competitive, and where overlap exists, customers should consider the simple questions of what they would expect a CSP to provide, and what a specialist security capability is.

# Comparing the operational strengths and weaknesses of third-party security offerings

## Heterogeneity

One major advantage of security products from third-party vendors compared to those of the CSPs themselves is their heterogeneity. Clearly, a dedicated security vendor has a vested interest in being

able to work on all the main cloud platforms, including OCI, and must therefore support their different technological approaches to delivering cloud computing.

By contrast, CSPs need only concern themselves with delivering security for their cloud infrastructure, and indeed, some may even see it as advantageous to do so, since customers on their platform will be able to use security technology that is not necessarily available on their competitors'.

This issue is worth bearing in mind if you have already embarked upon, or are seriously considering, a multicloud strategy in which different types of workloads and computing requirements are distributed across several CSPs. If, on the other hand, you have opted to go all-in on a single provider such as Oracle, the third-party vendors' heterogeneity offers no advantage.

### Management overhead/complexity

On the flipside, of course, is the additional complexity of deploying and managing third-party security tools on top of your cloud estate. These tools may require their own dedicated management console, managing them separately from the cloud workloads themselves, thereby potentially reproducing the dreaded "swivel chair" management issue of multiple consoles that is still so common in on-premises environments. And of course, the more third-party platforms you use, the greater the potential for swivel chair headaches. Furthermore, third-party security tools may also require additional resources to run inside the CSP or may expose API access keys to connect remotely to the CSP.

### Tighter integration with the underlying cloud platform

Another potential advantage of security tools and products from the CSP is their tighter integration with the underlying platform itself. You should expect, even demand, that a CSP's own security tools have the highest-level access to any data on performance and configuration and can leverage all the CSP's extensive analytical tools to detect misconfigurations and/or anomalous behavior. It should also be able to recommend security fixes or even execute them automatically if you so desire.

Third-party security tools, by contrast, may struggle to obtain the same degree of granularity from each of the CSPs they work on, not least because the way they need to extract such data to derive insights from it may differ from one CSP to another.

What follows are a few examples of customers benefiting from OCI's built-in security capabilities to protect their cloud assets.

## Obtaining a holistic picture of an organization's security position is critical from a risk management perspective

### Darling Ingredients

One example of a company that is using Cloud Guard is Darling Ingredients, a processor of biowaste that recycles it into new bioproducts. The OCI customer turned to Cloud Guard to monitor its

progress as its production instance was deployed into a tighter security zone within the Oracle cloud. Darling likes the graphical user interface and graph ability of the service, enabling both its cyber and SecOps teams to log in at the end of each deployment stage. Darling emphasizes that, as a built-in capability, there is no integration effort on the part of its team before they can start using it.

### Healthcare provider

A large healthcare provider recently benefited from Oracle Data Safe's focus on data security when they refreshed their staging database but neglected to remove or disable access to the environment for production users. Data Safe identified that the test system had been updated with dozens of accounts privileged to view sensitive data. Within minutes of discovery, this customer was able to address the risk by disabling the inappropriate accounts and then use Data Safe's activity auditing to validate that none of those accounts had been used to view protected healthcare information (PHI).

### Soho Media

Soho Media, a design studio working in the fields of strategy, brand identity, visual communication, advertising, and web design, uses Data Safe to secure its databases, monitoring and assessing user activity within the database. The company says it has found Data Safe easy to implement and use, yet still robust enough to satisfy its enterprise requirement to protect personal data and comply with regulations like EU GDPR.

## Demonstrating the security benefits of an integrated, holistic approach

### Accenture

Another example is professional services giant Accenture, which again uses Cloud Guard to assess its security posture on an ongoing basis, enabling it to adjust its response actions as required. It highlights the ease of use of the service and the fact that, as a built-in feature, it comes at no extra cost. And as a services company, Accenture is also highlighting these aspects of Cloud Guard to its customers, arguing that it underscores how Oracle built OCI with security front and center of its design principles.

### ALEF

A Cloud Guard customer that is now adding the OCI Certificates service to the range of Oracle services it is using is Italy's Advanced Laboratory Economics and Finance (ALEF), which describes itself as "a laboratory for financial economics." ALEF develops technology to address public and private firms', banks', and insurance companies' complex financial problems, such as its software modules for Monte Carlo simulations. An OCI customer, ALEF employs Cloud Guard for the maintenance of its security posture, praising the service's ease of use, and is now expanding into the use of OCI Certificates for the many automations it develops. The certificate's creation and expiry are determined by rules it sets up in the OCI console, making it easier to comply with rules created by regulators and auditors.

### Avatack

A customer using OCI IAM is Avatack, one of the world's leading adhesive tape manufacturers. To improve processes and security, Avatack selected OCI and Oracle's cloud identity service along with Oracle Content Management, Oracle Analytics Cloud, and Oracle Autonomous Data Warehouse. OCI IAM automates single sign-on processes for an improved user experience and provides the team with supervisory reporting. The enterprise-class security offered by OCI also enabled Avatack to receive top ranking in a required security audit and assessment report.

# Conclusion

Security products/services delivered by a cloud service provider (the “built-in”) and those provided by third-party security vendors (the “bolted-on”) both have their place, and indeed can often be complementary. However, when an enterprise seeks to address the security requirements of a specific, single cloud environment rather than a multicloud one, there are both operational and financial advantages.

The built-in technology benefits from its deeper integration with the cloud provider’s infrastructure. There are advantages in terms of simplicity, in that the integration comes as default, which means the enterprise customer can effectively turn on the security function “at the flick of a switch”, as it were, without the need for extensive configuration work from their security team.

Beyond that, the deeper integration, made possible by using security technology from the cloud provider themselves, enables the customer to get more comprehensive telemetry on which to base decisions about what remedial action to take.

And finally, there is the financial dimension. In the case of OCI, the vendor’s decision not to make security a profit center in its own right means it is either free or, at most, charged for at cost. In contrast, bolt-on security vendors obviously must derive profit from any product they supply to the cloud customer.

# Appendix

## Further reading

*2021 ICT Enterprise Insights in Cloud Computing* (November 2020)

## Author

**Rik Turner**
Principal Analyst, Cybersecurity
customersuccess@omdia.com

**Roy Illsley**
Chief Analyst, IT Ecosystem and Operations
customersuccess@omdia.com

## Get in touch

www.omdia.com
askananalyst@omdia.com

## Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

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 your company identify future trends and opportunities.

## 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.