IDC

Lab Validation Executive Summary

ORACLE CLOUD INFRASTRUCTURE: Addressing Tenant Concerns with Deep Application Insights

RESEARCH BY:

Jay Bretzmann

Philip Bues

Executive Summary

Public cloud infrastructure providers face some unique security challenges as they virtually allocate cloud tenant resources across hundreds to thousands of clients. They're a big target worthy of extensive malware engineering designed to compromise the whole environment. Organizations were originally reluctant to migrate applications to the cloud because they didn't understand the capabilities in place to protect their data from attackers or even simple mistakes made by other tenants.

An industrywide shared infrastructure model was defined, delineating what providers and tenants must each responsibly secure. Providers have subsequently developed capabilities and tools to help prospective tenants lift, shift, monitor, and adjust application deployments often augmented by machine learning insights. Many adopters now believe public clouds are more secure than previous on-premises environments; tenants benefit from savings opportunities and the ready availability of integrated tools and professional security services and resources.

This second IDC Lab Validation effort further reviews the Oracle Cloud Infrastructure (OCI), highlighting security measures available to tenants, specifically threat management, cryptographic services, and risk management capabilities.

Continued next page...

Key Findings

- Oracle-curated targeted threat models help OCI tenants spot malicious behaviors the SIEM and UEBA tools often miss, leaving attackers to dwell for months.
- Machine learning model works on regionally stored data that is correlated with global insights while reviewing active techniques and attacks to create better risk scores.
- Rogue user detector rule includes password guessing, password spraying, elevated number of PARs, impossible travel, and privilege escalation sightings to discover malicious activity.
- OCI has access to some audit logging resources across a large base of tenancies it can review for evidence of attackers trying to breach client environments but does not read any private data.
- OCI Vault offers the flexibility to serve the wide-ranging needs of tenants. It accommodates both crypto neophytes and experts in regulated and unregulated industries.
- Shared, private, and external HSM options balance savings with security, while OCI software facilitates key reuse across data, certificates, secrets, and other use cases.
- The OCI WAF security research (CSIRT) team actively monitors and discovers new vulnerabilities and releases virtual patches for many exposures within 24–48 hours. Other third-party vulnerabilities feeds, antivirus solutions, and suspicious IP address lists are all available at no charge.

IDC Opinion

IDC can validate the security technology applied to critical new components of OCI: monitoring and threat prevention, protection against anomalies and malicious behaviors, easy-to-use cryptographic technologies, and integrations for multicloud vulnerability management with ecosystem partners.

The nature of threat feeds, attack behaviors, indicators of compromise, and integrated telemetry feeds is that the work is never done. More policies, rules, and recipes are always needed to stay current. For a cloud service provider, the key part to get right is the framework for collecting all the data and the dashboards and single-pane-of-glass views that help security teams quickly spot the sightings.

With this second Lab Validation project, IDC believes OCI has tackled some of the harder elements of its IaaS solution, surrounded them with APIs, and done it in a very easy-to-consume and affordable manner for its customers.

Download the Lab Validation Brief

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. As a premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets, IDC's Custom Solutions group helps clients plan, market, sell and succeed in the global marketplace. We create actionable market intelligence and influential content marketing programs that yield measurable results.