KuppingerCole Report

EXECUTIVE VIEW

By Mike Small

March 30, 2021

Oracle Cloud Guard

Poorly managed security controls within a cloud services tenant's resources are increasingly the cause of security incidents and compliance failures. CSPM (Cloud Security Posture Management) tools provide functionality to address this challenge. This report provides a review of Oracle Cloud Guard which strongly matches KuppingerCole's recommended functionality for CSPM within the Oracle Cloud Infrastructure

By **Mike Small**

sm@kuppingercole.com

Content

1 Introduction

Most organizations now depend upon cloud services to deliver business-critical applications and this has increased in response to the coronavirus pandemic. This hybrid IT delivery environment gives rise to many challenges in the areas of management, security, and compliance. These challenges arise because cloud services are not well integrated into the normal IT security processes and technologies used by organizations. CSPM (Cloud Security Posture Management) solutions provide a way to identify and control some of these risks.

As organizations go through digital transformation, they are adopting DevOps using IaaS / PaaS cloud services to create new applications and to modernize their existing ones. This avoids the need for capital expenditure as well as the lengthy procurement delays involved when new hardware is needed. In addition, some organizations are now using cloud services to back up their business-critical data. This increases the need to ensure that DevOps use of cloud services takes care of security and compliance.

While the major cloud service providers go to great lengths to secure the infrastructure of their environments, it is up to the tenant to secure their use of these services. This is often outside the skills of DevOps teams or is overlooked, and this can lead to the existence of critical vulnerabilities which can be exploited by cyber-adversaries. These vulnerabilities often include poorly secured accounts used by the tenant to administer the cloud service and that provides cyber adversaries with uncontrolled access to the cloud-based assets. Often, the normal governance controls do not cover these cloud accounts leading to excessive privileges and dormant credentials. The access controls on cloud-based assets are often improperly configured allowing public access to business resources and data. Sensitive or controlled data may be copied and even shared with third parties for testing purposes.

The tenant may not fully exploit the tools provided by the cloud service. The tenant may not actively manage and secure the complete inventory of cloud resources and assets being used. The tenant's in-cloud technical stack including network, OS, Middleware, and applications may be vulnerable through poor configuration and lack of up-to-date patches.

CSPM solutions provide the capabilities needed to address these challenges in a consistent way. They help to identify the in-cloud elements being used within IaaS / PaaS and their potential vulnerabilities. CSPM assists in protecting these in-cloud components by enforcing security policies and implementing best practice controls. They identify deviations from policies providing alerts and automatically remediate issues.

This report covers Oracle Cloud Guard which is an OCI (Oracle Cloud Infrastructure) service that helps tenants to monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud.

2 Product Description

Oracle Cloud Guard is an OCI service that helps tenants to monitor, identify, achieve, and maintain a strong security posture on Oracle Cloud. The tenant can use the service to examine their OCI resources for security weakness related to configuration, and their administrators for risky activities. When Cloud Guard detects weaknesses, it can identify corrective actions and assist in or automate implementing these.

Cloud Guard detects security problems within a customer tenancy by ingesting activity and configuration data about resources in each region, processing it based on detector rules, and correlating the problems at the reporting region. Identified problems will be used to produce dashboards and metrics and may also trigger one or more provided responders to help resolve the problem.

Oracle Cloud Guard works together with Oracle Security Zones to provide an always-on security posture. With Security Zones and Cloud Guard the tenant can define policy compliance requirements for groups of resources. Security Zones and Cloud Guard can then enforce these policies to automatically correct and log any violations.

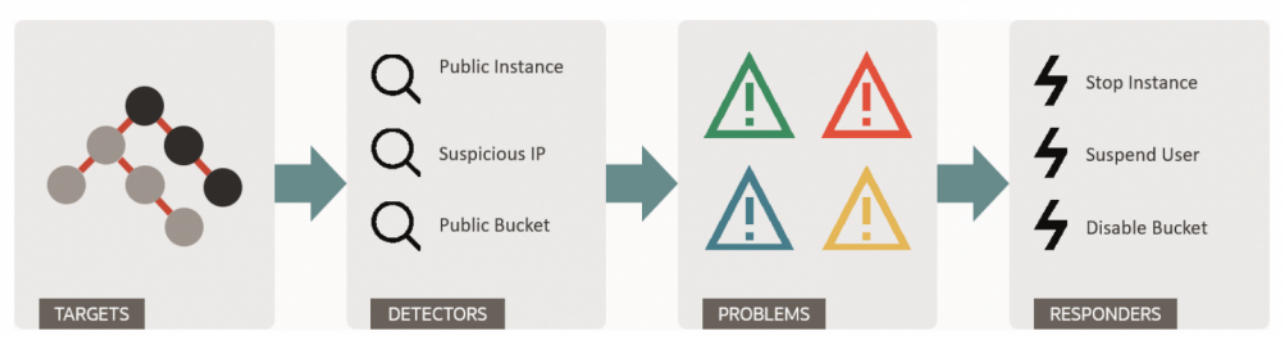

Figure 1: Cloud Guard Flow (graphic reproduced with permission from Oracle)

Targets define the scope of what Cloud Guard is to check. For Oracle Cloud, customers can define multiple targets in multiple regions, and Cloud Guard aggregates all of that for a holistic view. Detectors perform checks and identify potential security issues based on their type and configuration. Oracle Cloud Guard includes Oracle defined checks and the tenant can create their own or modify the ones provided. If any check is triggered the detector reports a problem. Responders define the actions that Cloud Guard can take when a detector has identified a problem. The available actions depend upon the type of resource and similar to the detectors Oracle provides responses which can be used or modified by the tenant.

As well as mitigating problems, Cloud Guard provides two key metrics on the overall security posture the

Risk Score and the Security score. Security Score provides an overall assessment of the strength of security posture. Risk Score complements the Security Score by providing an assessment of the total risk exposure of the tenant. These help to assess what could be "small but insecure" and "large but overall secure" environments correctly.

2.1 Key Capabilities

At KuppingerCole, we look for the certain key capabilities in CSPM solutions. The solution should support a zero-trust governance-based approach to cloud access security. The following paragraphs describe how Oracle Cloud Infrastructure and Cloud Guard provides these capabilities. Key capabilities include:

Strong Authentication -- the cloud services are configured by the tenant through the tenant's administrative accounts. Illegitimate access to these accounts poses a significant risk and so it is essential the access to these is controlled. The use of multifactor authentication for all users with OCI console access is a recommended CIS control.

OCI IAM supports two-factor authentication using a password and a device that can generate a time-based one-time password. Cloud Guard can be enabled to detect accounts with console access for which this is not enabled and create a Problem to alert or remediate. In addition, it can be enabled to ensure that the OCI IAM enforces policies for password strength.

Administrator Privileges -- in a large organization there will likely be many administrators of the OCI tenancy with responsibilities delegated to allow them to manage groups of assets. These delegated administrators should only have the access rights necessary to perform their task. This limits the scope of mistakes or malicious acts.

OCI IAM can implement the principle of least-privilege security principle to create service-level administrator groups and assign specific users to the appropriate groups. This limits the scope of each administrator and minimizes the number of users with whole tenancy administrative control. Cloud Guard can be enabled to detect accounts with excessive privileges and create a Problem to alert or remediate.

Object Storage Security -- one of the benefits of cloud object storage is that data that needs to be widely available can be easily accessed over the internet. However, many of the tenant's assets held in object storage will contain confidential data that need to be secured against unauthorized access. Creating storage buckets with public access is a common security concern and failing to encrypt confidential data held in the service can lead to a breach of regulatory obligations if that data is leaked.

OCI Object Storage provides capabilities to limit access to individual buckets and Oracle Object Storage buckets support encryption with a Customer Managed Key. By default, Object Storage buckets are encrypted with an Oracle managed key. This provides an additional level of security on the tenant's data. Cloud Guard can be enabled with detectors that verify that Object Storage buckets are encrypted with the Oracle-managed key Detector Rule and will generate Problems if Object Storage Buckets are configured

without a customer managed key.

Virtual Network Configuration -- The very nature of a cloud service means that it is accessed over an external network and is exposed to the internet. Organizations normally implement strict controls within their network, but the in-cloud virtual network may not be included in their processes. There are many potential risks from this that depend upon the nature of the applications being hosted in the cloud service. The major common risk is unauthorized root / administrator access to the servers using SSH or Windows Remote Desktop Access. There should be strict controls to prevent unauthorized external administration and in-cloud lateral movement by cyber adversaries. Unused ports should be closed and only the types of IP traffic relevant to the hosted applications permitted

Within OCI VCN (Virtual Cloud Network), security groups provide stateful filtering of network traffic to and from OCI resources. Oracle recommends restricted access to port 22 and 3389. Cloud Guard can be configured to create alerts (Problems) if a policy violation is detected. It can also generate Problems if other tenant specified ports are configured to be open.

Virtual Servers Configurations -- unpatched or poorly configured in-cloud virtual servers can pose a risk since they may contain vulnerabilities that could be exploited by cyber adversaries. The organizational policies for server configuration and patching should also be applied to the in-cloud virtual servers.

Currently Cloud Guard provides the capabilities to scan the IaaS network configuration to ensure that rule as set up to control ingress and unauthorized lateral movement.

Compliance Policies -- organization may have to comply with the obligations imposed by a wide variety of regulations and laws. While the controls implemented may map to multiple obligations, it is often hard to work out this cross-compliance mapping. It is helpful to have out-of-the-box policies and reports showing how the tenant's cloud security posture complies with standards such as ISO/IEC 27001, NIST, PCI-DSS, GDPR, CCPA etc.

Currently Cloud Guard Cloud Guard aligns with the CIS Foundations benchmark standard for OCI. Additional compliance features are expected post-GA.

Security Posture Management - The solution should provide the capability to identify and remediate vulnerabilities in the configuration of cloud services. One primary focus of CSPM has previously been on SaaS clouds however, the use and management of IaaS is now becoming more important. Areas that should be covered include administrator privileges, excessive access rights to assets and other risky service configurations.

Oracle Cloud Guard helps secure the customer's use of Oracle\'s infrastructure platform today. Cloud Guard is expanding to address additional SaaS services while growing the depth and breadth of IaaS protection. It can automate protection and policy enforcement for cloud resources in near real time.

Cloud Guard also monitors and alerts on detected suspicious behaviour and remediates misconfigurations to help maintain compliance status.

3 Strengths and Challenges

Cloud Security Posture Management is an important tool for organizations to ensure that they use cloud-delivered services in a secure and compliant manner. It is often the case that the tools and capabilities from the cloud service provider for their tenant to secure the use of the service are not fully exploited. OCI provides very comprehensive capabilities for the tenant to secure their use of the services. Oracle Cloud Guard is a solution that is backed by the expertise and experience of Oracle's technical teams.

This is an excellent first version that complements Oracle Security Zones and integrates with other OCI capabilities to provide an assessment the security posture of a tenant's usage of OCI. This first version covers some important areas out of the box. However, it is still lacking in the coverage of many areas provided by freestanding CSPM solutions. These include out-of-the-box coverage of access governance elements such as excessive privileges and orphan account detection. While it covers rudimentary VCN configuration to limit administrator access it does not cover zero trust. It aligns with the CIS foundation standards for OCI but does not provide out of the box reports for how well the tenant complies with this. There is no mention of out of the box policies or reports for major compliance frameworks and standards such as ISO/IEC 27001, NIST, PCI-DSS, GDPR, CCPA etc.

Strengths

- A solution with the backing of Oracle technical expertise.
- Aligns with the CIS foundation standards for OCI.
- Native integration OCI capabilities.
- Enhances the posture management enforcement of compartment resources. provided by OCI Secure Zones.
- Alerts on OCI Object Storage buckets with public access permissions.
- Monitors cloud network configuration.
- Integrates with other OCI services such as IAM.
- Currently offered without extra charge.

Challenges

- Does not provide out-of-the-box policies for common standards or frameworks other than CIS.
- Does not cover access governance such as excessive privileges and orphan accounts out-of-the box.
- Does not cover container workload security posture out-of-the box.
- Does not provide compliance status reports for common regulations out-of-the-box.

4 Related Research

Market Compass: Cloud Access Security Brokers - 80079

Architecture Blueprint: Identity and Access Management - 72550

Architecture Blueprint: Hybrid Cloud Security - 72552

Advisory Note: Maturity Level Matrix for Cyber Security - 72555

Advisory Note: Security Organization Governance and the Cloud - 72564

Advisory Note: Cloud Services and Security - 72561

Advisory Note: How to Assure Cloud Services - 72563

Architecture Blueprint: Access Governance and Privilege Management - 79045

Architecture Blueprint: Identity and Access Management - 72550

Leadership Compass: Identity as a Service (IDaaS) IGA -- 80051

Leadership Compass: Identity Governance & Administration -- 80063

Content of Figures

Copyright

KuppingerCole Analysts support IT professionals with outstanding expertise in defining IT strategies and in relevant decision-making processes. As a leading analyst ompany, KuppingerCole provides first-hand vendor-neutral information. Our services allow you to feel comfortable and secure in taking decisions essential to your business.

KuppingerCole, founded in 2004, is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as for all technologies fostering Digital Transformation. We support companies, corporate users, integrators and software manufacturers in meeting both tactical and strategic challenges and make better decisions for the success of their business. Maintaining a balance between immediate implementation and long-term viability is at the heart of our philosophy.

For further information, please contact clients@kuppingercole.com.