KuppingerCole Report

EXECUTIVE VIEW

By Mike Small

May 10, 2022

Oracle Security Zones

Poorly managed security controls within a cloud services tenant's resources are increasingly the cause of security incidents and compliance failures. Today's dynamic infrastructure and development methodologies need a dynamic approach to cyber security. This report reviews Oracle Security Zones that enforce resource-based security policy on Oracle Cloud Infrastructure.

By **Mike Small**

sm@kuppingercole.com

Content

1 Introduction

The on-demand availability of cloud services has provided a way to develop and deliver new applications and services that are more flexible, more responsive to changing demand, and more cost effective than traditional approaches. This is made possible by the just-in-time nature of virtual cloud infrastructure combined with the 'shift left' DevOps trend, and increasingly based on containers and micro services. However, this trend towards dynamic virtual infrastructure creates security challenges. The legacy approach to IT security assumes a comparatively static environment and this is not optimal for the needs of today's dynamic infrastructure and development methodologies. Dynamic just-in-time infrastructure and development requires a dynamic just-in-time approach to IT security.

When IT services were delivered directly from owned physical equipment, the procurement costs, processes, and delays meant that change was slow, and innovation was hard. IT security tools and approaches evolved to manage the security risks associated with this static environment. Controls could be applied after equipment was installed, and the IT estate could be accurately catalogued in a Configuration Management Database (CMDB). Because change was highly managed, risks were relatively static, and manual or partially automated security management processes were enough. For example, weekly scanning could find and fix any newly discovered vulnerabilities and identities, and manual processes were adequate to manage access permissions.

This is no longer the case when using cloud services where infrastructure is virtual, and resources are created and destroyed dynamically as they are needed. The inventory of these virtual resources is not fixed but is constantly changing as demand fluctuates and applications are deployed. In this dynamic environment all the well-known risks, such as unpatched vulnerabilities, still exist but, in addition, there are new risks. These new risks may arise from the new kinds of services that the cloud offers, such as serverless computing, or result from the misconfiguration of cloud services by users that haven't fully mastered the components or platform that they are using.

One area of concern is around DevOps and rapid deployment. The traditional approach to the deployment of IT service elements involved prior risk assessment and the implementation of appropriate security controls. However, the flexibility provided by DevOps and the elastic nature of cloud services makes it easy to rapidly deploy new service elements without strictly enforced checks. In the race to deploy functionality, it is often the case that security takes second place.

This can lead to the cloud service elements being misconfigured in ways that can then be exploited by cyber adversaries. Furthermore, in this dynamic environment the virtual infrastructure components have privileges and, where these are excessive, there are additional vulnerabilities that can be exploited. It is important that cloud environments provide cyber security capabilities to ensure that security and compliance policies are enforced dynamically during application development and deployment, without slowing DevOps down.

Dynamic just-in-time IT needs dynamic just-in-time security controls. These controls must be policy based and implemented automatically as IT service elements are created, modified, moved, and deleted. This is best implemented by the cloud service itself since this has intimate knowledge of the customers' resources as well as the control plane to enforce controls.

This report describes how these objectives are achieved by Oracle Cloud Security Zones which are a set of security capabilities provided by the OCI (Oracle Cloud Infrastructure).

2 Product Description

Oracle Security Zones provide policy-based capabilities to protect the customer's resources within the Oracle Cloud Infrastructure. This helps customers to manage their cloud security posture and ensure that their use of the service meets their compliance obligations. Security Zones complement Oracle Cloud Guard which provides visibility into the customer's security posture by assigning security policies that will be enforced on the customer's OCI infrastructure resources.

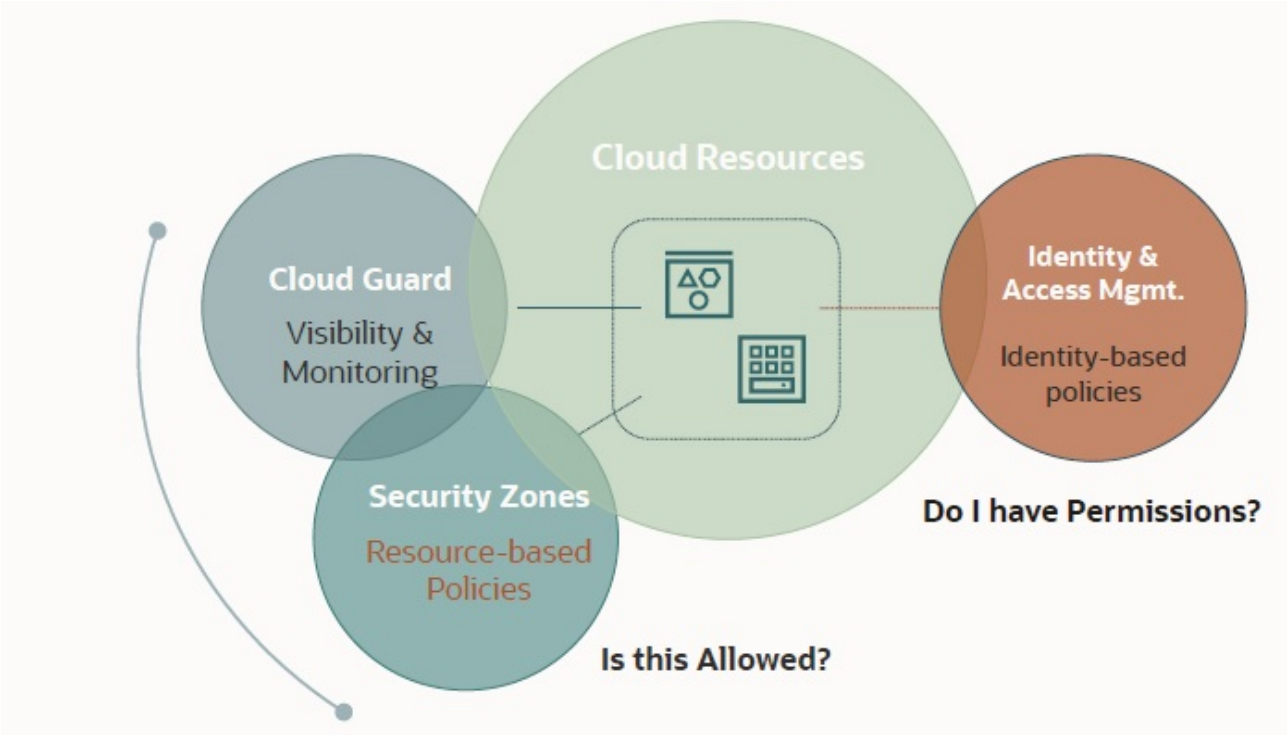

Figure 1: Oracle Security Zones in context (image reproduced with the permission of Oracle)

Oracle Security Zones enforce resource-based security policy on cloud infrastructure and help customers to implement effective cloud security practices by enforcing security posture from the start. Customers can create Security Zones, which overlay one or more infrastructure compartments with a customer-defined set of security policies. The resources created inside a security zone are subject to all applicable security zone policies that have been applied.

Security Zones complement identity and access management (IAM). Security Zone policies are associated with OCI resources, and these are enforced at the infrastructure control plane. Hence, the Security Zone

polices cannot be directly overridden by privileged account operations.

OCI released Security Zones in Sept 2020, as Maximum-Security Zones, which enforced strict security policies and made these policies immutable. In May 2022, Oracle introduced a new version of Security Zones, which enables customers to define their own Security Zone policy sets and change security policy whenever needed.

- Customers can select and apply the security policies that support their desired security posture to OCI resources within their Compartments. Resources currently included in Security Zones are Networking, Compute, Storage, Database, Encryption, Backups, and Require sanctioned images. Security Zones policies enable the customer to restrict resource movement, restrict resource association, deny public access, require encryption, and ensure data durability. Security Zones provides the enforcement element of cloud security posture management and pairs with Oracle Cloud Guard for infrastructure monitoring.

2.1 Implementing Dynamic Security with Security Zones

OCI enables organizations to respond rapidly and flexibly to new and changing business needs. However, in this dynamic IT environment there is a risk that security controls will be missed or misconfigured. For example, when business application components are moved from development and test to production the controls and configuration typically need to be changed. When a standard compute resource is used for different purposes the security controls may need to be adapted. When sensitive or regulated data is being processed it is essential that data be protected. The following use cases illustrate how Oracle Security Zones helps to protect this dynamic IT environment.

Guardrails — Customers can use Security Zones to enforce prescriptive guardrails to protect their resources against mistakes as well as malicious actors. For example, they can prevent resources from being moved to locations where they would breach compliance obligations. They can prevent resources from being exposed to the internet and enforce data protection by ensuring that data is encrypted. They can also ensure security hygiene such as ensuring that data is backed up automatically or enforce the use of customer-managed encryption keys.

Application Protection — Security Zones can help provide appropriate levels of protection for the OCI resources involved in the delivery of customer applications. Business applications rely on several technology layers each of which needs appropriate security policies. API / Web servers and load balancers that are exposed to the Internet face a greater risk of external attack. Security Zones can ensure that the appropriate restrictions are enforced on OCI resources in places where internet access is required. Application servers do not need access to the internet but are open to other forms of attack. Security Zones can provide protection for the OCI resources used, and the data they process. Databases that support

business applications may hold sensitive or regulated data with enhanced risks, should a breach occur. Oracle Security Zones policies help protect the OCI resources that these databases use and help ensure the security and durability of the data.

High Security — Government agencies and critical infrastructure industries are subject to stringent regulations. Satisfying the security needs of these users requires a comprehensive range of security controls. The Maximum Security Zone recipe provides a strong security policy set reflecting OCI best practices and Oracle's knowledge of compliance obligations across a wide range of government and industry sectors. High security customers often bring unique requirements and the desire for customized infrastructure to meet exacting needs. The Maximum Security Zones policy set provides a starting point, which is easily modified to reflect a customer's specific requirements.

Resource Protection Policies

When the customer creates or updates resources in a Security Zone, OCI validates the operations against the policies set for the Security Zone. If any policy is violated, that operation is denied. The May 2022 Security Zones release allows customers to define their own Security Zones by selecting which policies to enforce from a predefined list.

These predefined security policies for OCI resources address the following:

- Restrict Resource Movement — Prevent resources from being moved from a Security Zone to a compartment outside the Zone (with lower levels of protection or no protection).
- Restrict Resource Association — Ensure that resources within a Security Zone do not depend on resources outside that Security Zone.
- Deny Public Access — Prevent resources in a Security Zone from being accessible from the public internet.
- Require Encryption — Ensure that all resources in a Security Zone are encrypted using customer-managed keys. OCI Vault provides the capabilities to manage the master encryption keys that protect data and the secret credentials used to securely access resources.
- Ensure Data Durability — Require that databases in the Security Zone are configured to perform automatic backups, and ensure that backups remain within the zone.
- Ensure Data Security — Prevent data from being copied outside of that Security Zone.
- Use Only Configurations Approved by Oracle — Require resources in the Security Zone to have the Oracle-approved security features enabled and configured.

Administration

Oracle Security Zones provides protection for critical OCI resources, yet this protection is only likely to be used if it is easy to administer. Customers can administer Security Zones using the web-based Console,

REST APIs, the Command Line Interface (CLI), or SDK. Terraform is also supported for automation. OCI provides services integrated IAM for authentication and authorization, which covers all the above interfaces. By default, only users with explicit Administrative permissions can access Security Zones.

Tenants have the flexibility to apply, create, and change custom policy sets. In addition, a tenant can delegate administrative access to developers as well as security administrators. All Security Zone policy changes are independently monitored by Oracle Cloud Guard, which automatically reflects active Security Zone policies with Cloud Guard monitoring targets.

3 Strengths and Challenges

Oracle Security Zones provides dynamic policy-based capabilities for tenants to secure cloud resources within OCI compartments. By providing true policy enforcement capabilities, Oracle's Cloud Security Posture Management solution extends beyond the visibility and monitoring commonly seen in competitive offerings. Security Zone policies are applied dynamically to resources in one or more compartments where resources can be created, changed, used, or removed; as long as the action doesn't conflict with applied security policy.

This enhancement to Security Zones provides flexibility for tenants to choose the level of protection that they need based on their requirements. A Maximum Security Zone recipe is available as a starting point, which customers can now edit to be more reflective of their needs. In general, Security Zone policies are based on Oracle best practices and tend to reflect the needs of governments and other highly regulated industries.

Expanding on the aspect of flexibility, a Security Zone can now be applied to existing workloads. The security posture of existing compartments can be improved simply by applying Security Zone policy. Cloud Guard will detect existing misconfigurations so customers can fix problems found initially, and Security Zone policy enforcement will prevent future violations from occurring.

Security Zone policies are enforced at a control plane level to provide robust protection against compromise. However, weakness in tenant administrative practices and entitlement management could still be exploited to maliciously change Security Zone policies and weaken security posture.

Many OCI resource types are currently addressed by Security Zone policies, and Oracle says that more are planned. It would also be helpful if Oracle provided mappings of Security Zone policies to common frameworks and standards to make it easier for tenants to select the policies they need.

Strengths

- Provides policy-based protection for OCI resources.
- Policies are based on Oracle best practices.
- Maximum Security capabilities for customers that require that.
- Tenant can customize policy sets.
- Can be used as guardrails to prevent mistakes leading to reduced security posture.
- Supports customised protection for different elements in the application stack.
- Protection enforced dynamically as resources are created.
- Wide range of OCI resources are protected.
- Protection enforced at the OCI control plane.
- Integration with Oracle Cloud Guard.

Challenges

- Need more predefined administrative roles that govern who can create/modify/delete a Security Zone to improve appeal for high security use cases.
- Security Zones policies do not yet address network traffic policy beyond gateways.
- Security Zone policies do not yet offer managed immutability.
- Does not provide out-of-the-box mapping of policies to common industry standards and frameworks.

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.