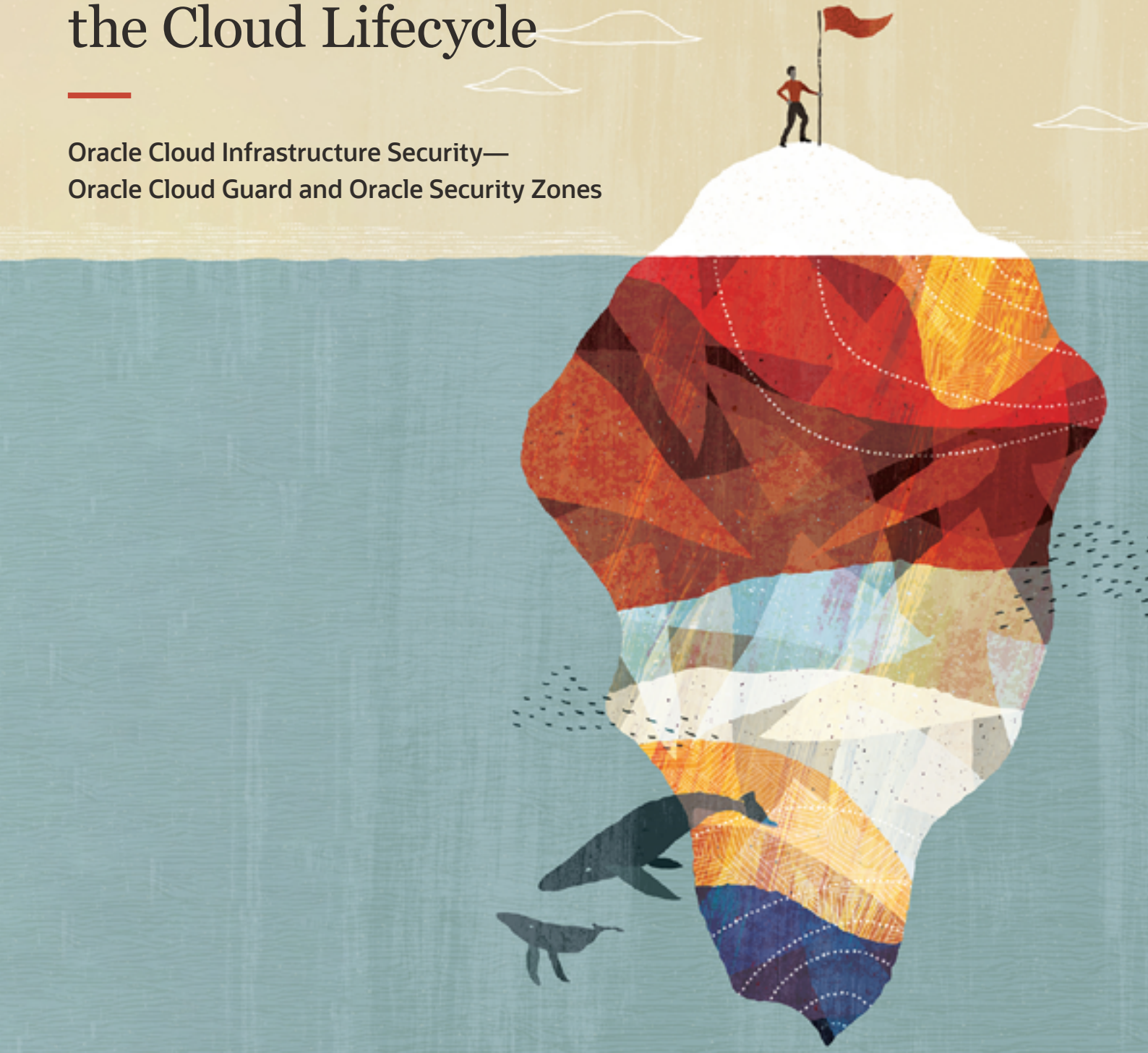
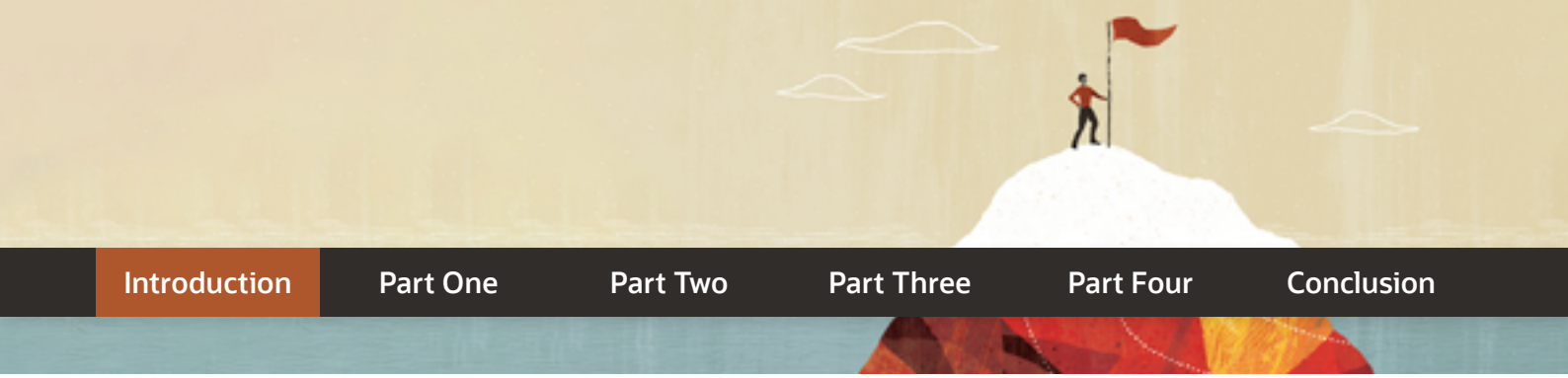
ORACLE

Keep Your Data Secure Throughout the Cloud Lifecycle

Oracle Cloud Infrastructure Security—
Oracle Cloud Guard and Oracle Security Zones





Introduction

The benefits of the cloud have grown too strong for businesses to ignore—it offers lower infrastructure spending costs, greater business agility, and flexible scalability. That's why more companies are migrating their business-critical enterprise workloads to the cloud than ever before.

In fact, according to the Oracle and KPMG Cloud Threat Report, today, nearly 90 percent of companies are using software as a service (SaaS) and 76 percent are using infrastructure as a service (IaaS)—and 50 percent expect to move all their data to the cloud in the next two years.[1]

But unfortunately, despite the benefits it gives companies, increased cloud adoption still has its costs. Many companies have developed new security blind spots as their IT teams and cloud service providers work to secure their data. And it's causing areas of concern—Gartner forecasts that by 2025, 99 percent of cloud security failures will be the customer's fault.[2]

*Gartner forecasts that by 2025, **99 percent** of cloud security failures will be the customer's fault.*

Enterprise cloud security and privacy administrators have a lot of responsibility already. They're expected to be knowledgeable about cloud security services, know how to deploy them without sacrificing business continuity, and correctly manage secure resource configurations in a rapidly changing environment. When you consider that most public-cloud tenants mix on-premises, cloud, and multicloud deployments at scale, overcoming this challenge can be difficult—even with a well-staffed team of cloud security experts.

A new approach to security posture management

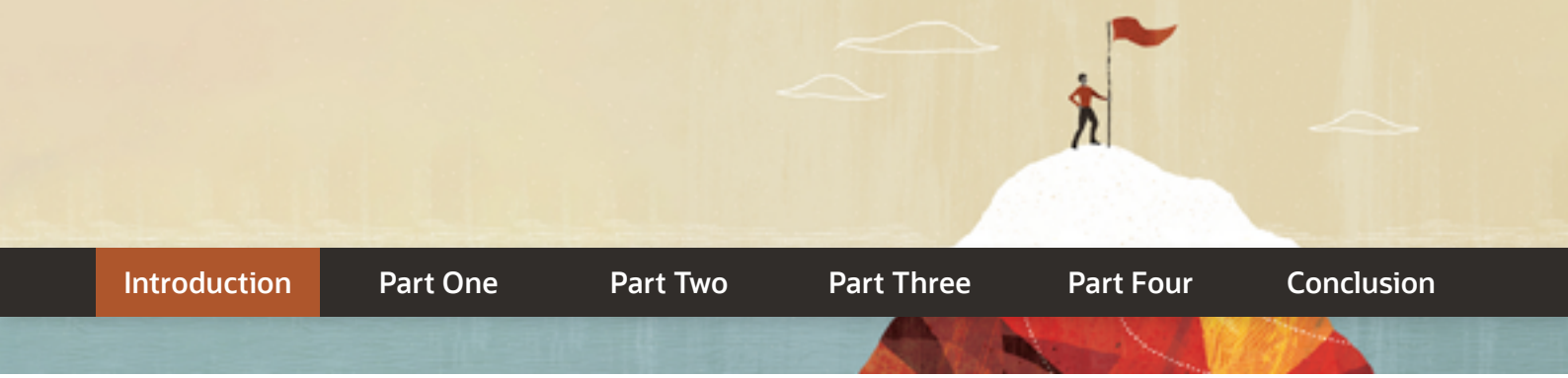
Oracle wants cloud security and privacy administrators to feel confident when securing cloud infrastructure workloads. To achieve this, security must be easy to deploy and maintain. It also needs to be automated and sophisticated enough to protect the most critical workloads and data—all while allowing security professionals to more easily apply their expertise to meet security objectives.

That's why Oracle Cloud Infrastructure is introducing new security cloud services for cloud security posture management (CSPM) and cloud security orchestration and automation and remediation (SOAR) of Oracle Cloud Infrastructure tenancies.

Cloud security posture management removes the barriers typically encountered when securing cloud services. It's made possible by embedding security expertise, centralizing configuration management and monitoring, and automating remediation workflows.

[1] "New Study: IT Pros Are More Worried About Corporate Security Than Home Security," press release, May 14, 2020, on Oracle website, oracle.com/corporate/pressrelease/cloud-threat-report-2020-051420.html.

[2] Kasey Panetta, "Is the Cloud Secure?" Gartner article, October 10, 2019, gartner.com/smarterwithgartner/is-the-cloud-secure/



A two-pronged security strategy for security posture management

Cloud security posture management of Oracle Cloud Infrastructure tenancies consists of two cloud security services:

- Oracle Security Zones: Special compartments designed to enforce implicit and explicit security policies.
- Oracle Cloud Guard: A scalable data processing security service that acts as the command center for Oracle cloud security posture management. Oracle Cloud Guard gives a comprehensive picture of the security and risk posture of a customer's tenants in Oracle Cloud Infrastructure.

Oracle Security Zones and Oracle Cloud Guard mark a new approach to cloud security, giving customers the ability to avoid insecurely configured cloud services at different stages of the resource configuration lifecycle.

Oracle Security Zones focuses on a preventative strategy that can inhibit the creation of resources that violate security requirements, while Oracle Cloud Guard offers a detect-and-respond framework that allows for additional context before remediation is enforced.

Oracle Security Zones and Oracle Cloud Guard are cloud security services that support the entire Oracle Cloud Infrastructure ecosystem supporting the traditional console user interface as well as programmatic interfaces (such as Oracle Cloud Infrastructure API, CLI, SDK, and so on).

This two-pronged approach helps Oracle Cloud users deploy securely from day one, and provides the means to continuously monitor security and risk across the entire Oracle Cloud Infrastructure ecosystem.

Oracle Cloud Infrastructure security designed for all users and data

Oracle Security Zones and Oracle Cloud Guard add security automation and embedded expertise to Oracle Cloud—making it easy for any cloud user to operate securely.

Oracle Cloud Infrastructure is an infrastructure-as-a-service (IaaS) offering, architected on security-first design principles.

These principles include isolated network virtualization for superior customer isolation compared to earlier public-cloud designs, and hardware root-of-trust technology to reduce risks from compromised firmware. Oracle Cloud Infrastructure benefits from tiered defenses and highly secure operations that range from the physical hardware in our data centers to the web layer.

Many of these protections also work with third-party clouds and on-premises solutions to help secure modern enterprise workloads and data wherever they reside.

Much like the security-first Oracle public-cloud design, Oracle Security Zones and Oracle Cloud Guard continue to emphasize security themes such as resource configuration and activity monitoring, secure compartment design, and security automation. These new security services are part of the core design concepts for Oracle Cloud Infrastructure, including:

- High customer isolation
- Protection from firmware-based attacks
- Ubiquitous data encryption
- Automatic patches to the operating system
- Sophisticated data protection

Oracle's focus on automation and ease of use aims to set a new bar for security, giving every cloud user—not just those tasked explicitly with security—the power to operate, develop, and scale securely in the public cloud.

Part One

Automating security in a cloud compartment with Oracle Security Zones

Oracle Security Zones act as special Oracle Cloud Infrastructure compartments that enforce implicit and explicit security policies.

Oracle Cloud Infrastructure also offers a Maximum Security Zone, which enforces a superset of prescriptive and compulsory policies. These policies can help prevent data exfiltration and enforce a continuous maximum security posture.

Policies that are enforced in Oracle Maximum Security Zones are:

- No public internet in or out
- All data encrypted with customer-managed HSM keys
- Only bastion access to hosts
- No databases without backups
- No instances without hardened images

Due to the nature of the policies, resources inside an Oracle Maximum Security Zone cannot be moved out unless to another Oracle Maximum Security Zone. Additionally, to prevent configuration drift, the security configurations of an Oracle Maximum Security Zone cannot be disabled.

Part Two

A holistic picture of security and risk posture management with Oracle Cloud Guard

Oracle Cloud Guard is a unified security solution that provides a global and centralized approach to customer asset protection, and acts as the command center for Oracle cloud security posture management.

Oracle Cloud Guard acts as an aggregator that collects a wide range of data—including log, event, and threat intelligence data—from different sources, both native and nonnative, across Oracle Cloud Infrastructure. The source data is polled frequently and fed into a detection and correlation engine for additional insights, such as details about a specific user or network address.

If Oracle Cloud Guard detects any misconfigured resources or insecure activity drifts with a detector, it generates what are called security problems to be flagged for response. Detector recipes can be configured with additional conditional logic, and they're designed to be deployed out of the box, or customized to meet individual detection scenarios. Security problems are put into a queue that can be filtered by risk level, compartment, problem type, and more.

Administrators can refer to recommendations to remediate specific problem types, and they can automate remediation using the responder's recipes. With this capability, Oracle Cloud Guard provides a high-level overview of your security posture in Oracle Cloud Infrastructure. It offers the toolkit needed to automate the remediation of trivial security problems, but the granularity to dig deeper into more complex issues helping you scale your security operations team.

Oracle Cloud Guard base concepts

Detectors

A detector is a Cloud Guard component that identifies problems based on configuration or activity.

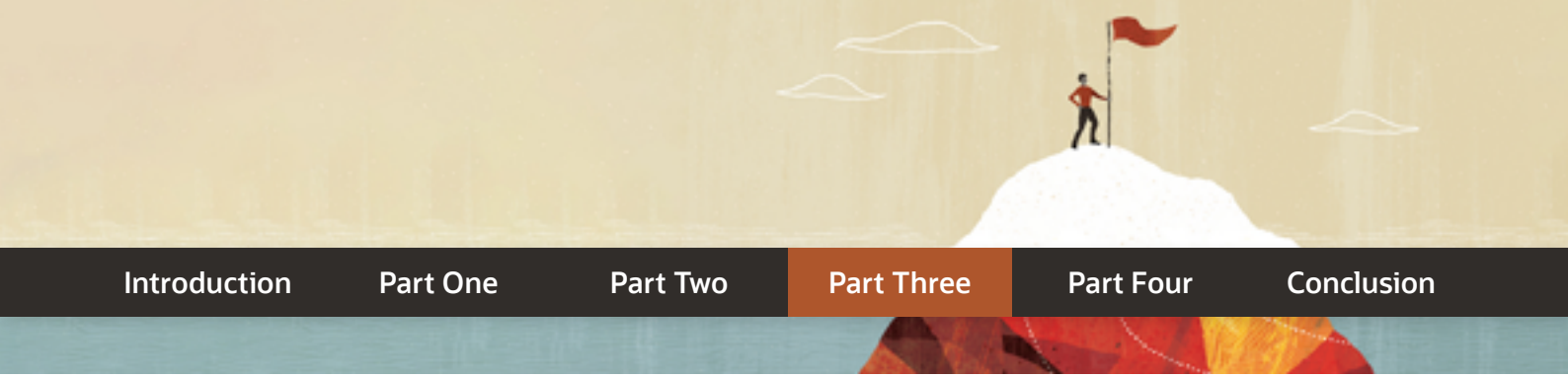
Correlation engine

Problems

A problem is any action or setting on a resource that could potentially cause a security problem.

Responders

A responder takes an automated action to resolve a security problem.



Part Three

Shifting the cloud security shared responsibility model with Oracle Security Zones

According to the 2020 Oracle and KPMG Cloud Threat Report, 96 percent of IT professionals are familiar with what's called the cloud security shared responsibility model.

But while most are familiar, few are experts. In the same report, it was revealed that only 8 percent fully understand the shared responsibility model for all types of cloud services.[3]

*Only **8 percent** of IT professionals fully understand the cloud security shared responsibility model for all types of cloud services*

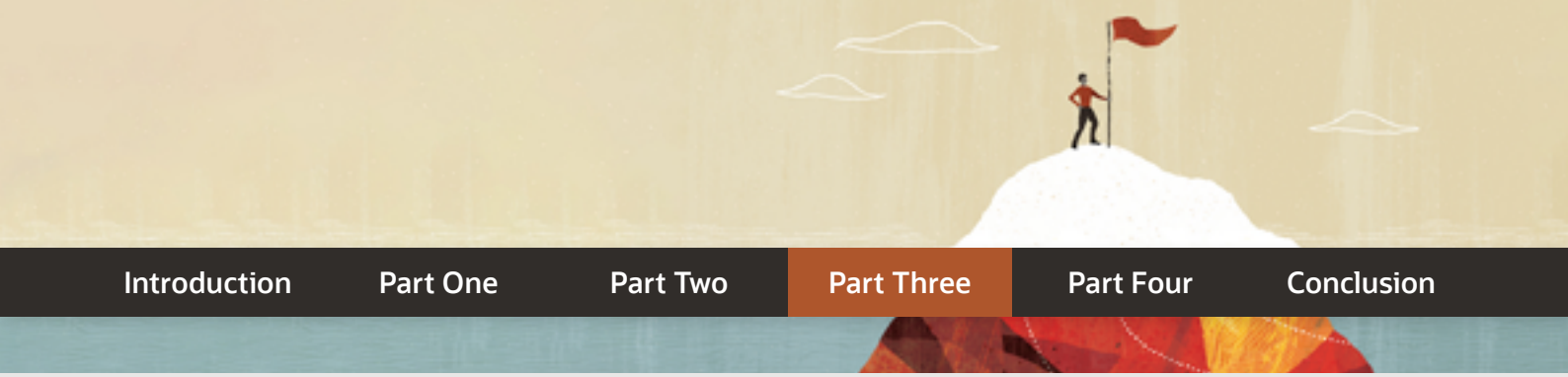
Oracle Security Zones is helping to change this. With the introduction of Oracle Security Zones, Oracle is shifting the cloud security shared responsibility model so that the cloud service provider can provide additional assistance to the customer. Layers of the shared responsibility model that IaaS customers were traditionally responsible for are being partially covered by Oracle Security Zones. And with Oracle Security Zones, configuration management, monitoring, and enforcement are improved.

In addition, there is additional protection provided by various enforcement points including the control plane, the data plane, and Oracle Cloud Guard for reactive enforcement. This will enable customers to focus more on the security strategy for the rest of their data and applications.

Oracle Security Zones can assist with the cloud security shared responsibility model in multiple ways, including:

- Denying public access to Oracle Cloud Infrastructure resources, such as databases and object storage buckets
- Enforcing the policy that detached storage resources must reside in the same secure compartment as the compute instance
- Encrypting resources with storage functions—such as block volumes, object storage buckets, and databases—with a customer-managed key

[3] "Oracle and KPMG Cloud Threat Report 2020," Oracle, oracle.com/cloud/cloud-threat-report/.



Security consumer responsibility

Service provider assistance

Without Oracle Security Zones

The cloud security shared responsibility model looks similar to the following example:

On-premises	Iaas Infrastructure as a service	Paas Platform as a service	Saas Software as a service
User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

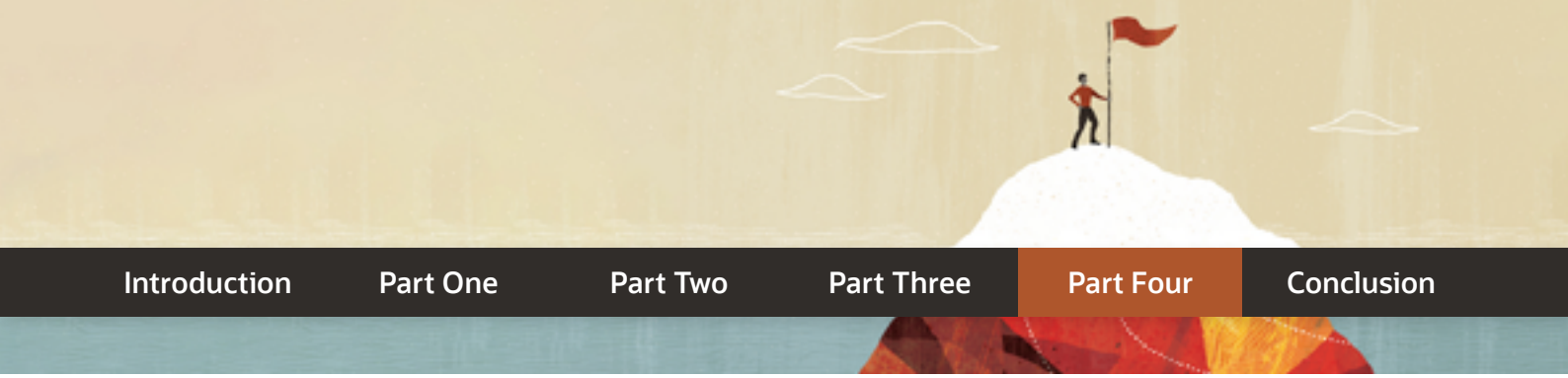
With Oracle Security Zones

Oracle will assist customers with the data, application, and guest OS layers.

On-premises	Iaas Infrastructure as a service	Paas Platform as a service	Saas Software as a service
User Access/Identity	User Access/Identity	User Access/Identity	User Access/Identity
Data	Data	Data	Data
Application	Application	Application	Application
Guest OS	Guest OS	Guest OS	Guest OS
Virtualization	Virtualization	Virtualization	Virtualization
Network	Network	Network	Network
Infrastructure	Infrastructure	Infrastructure	Infrastructure
Physical	Physical	Physical	Physical

Examples of control-plane enforcement policies in Oracle Security Zones include:

- **At the data layer:** Without customer-managed keys for encryption (such as keys in Oracle Cloud Infrastructure Vault), the creation of block volumes and object storage buckets is prevented.
- **At the application layer:** The creation of an internet gateway in VCN for public access is prevented.
- **At the guest OS layer:** The creation of a compute instance without a sanctioned image is prevented.



Part Four

Stepping up security in Oracle Cloud Infrastructure

Oracle Security Zones and Oracle Cloud Guard are built into Oracle Cloud Infrastructure and are available to all cloud customers. Oracle's approach means you can gain full visibility of your global security posture and identify any areas of risk.

With Oracle's approach to cloud security posture management, you can reduce the barriers to deploying and maintaining security in the public cloud. This includes:

- **Embedded security best practices:** Oracle Security Zones provides implicit and explicit policies that help prevent the introduction of unauthorized cloud settings that put critical data at risk.
- **Centralized configuration management and monitoring:** Oracle Cloud Guard maintains oversight of your entire Oracle Cloud Infrastructure ecosystem. At its core, Oracle Cloud Guard is a highly scalable and modular data-processing cloud security service that takes in signals from Oracle and third-party sensors, detects areas of risk, and shuts them down before they can be exploited. Cloud security administrators don't have to stitch together multiple tools to achieve the desired workflow of risk identification, validation, notification, and remediation.
- **Automated remediation:** Oracle Cloud Guard's built-in responders can generate alerts, launch multipath workstreams, or eliminate the threats that represent risk.
- **Security for all Oracle Cloud users:** Oracle Security Zones and Oracle Cloud Guard are available to customer tenancies on Oracle Cloud Infrastructure, delivered as infrastructure native services without the need for additional purchases.

Conclusion

Take your first step towards a new security posture:

Find out more about Oracle Security Zones and Oracle Cloud Guard today.

And read our new guide to explore what the security architecture of Oracle Cloud Infrastructure has to offer.

Learn more about the latest threats in the Oracle and KPMG Cloud Threat Report.