Oracle Cloud Guard

Cloud Security Posture Management for Oracle Cloud Infrastructure

September 2020, Version 1.0

Purpose statement

This document provides an overview of features and enhancements included in Oracle Cloud Infrastructure. It is intended solely to help you plan your I.T. projects.

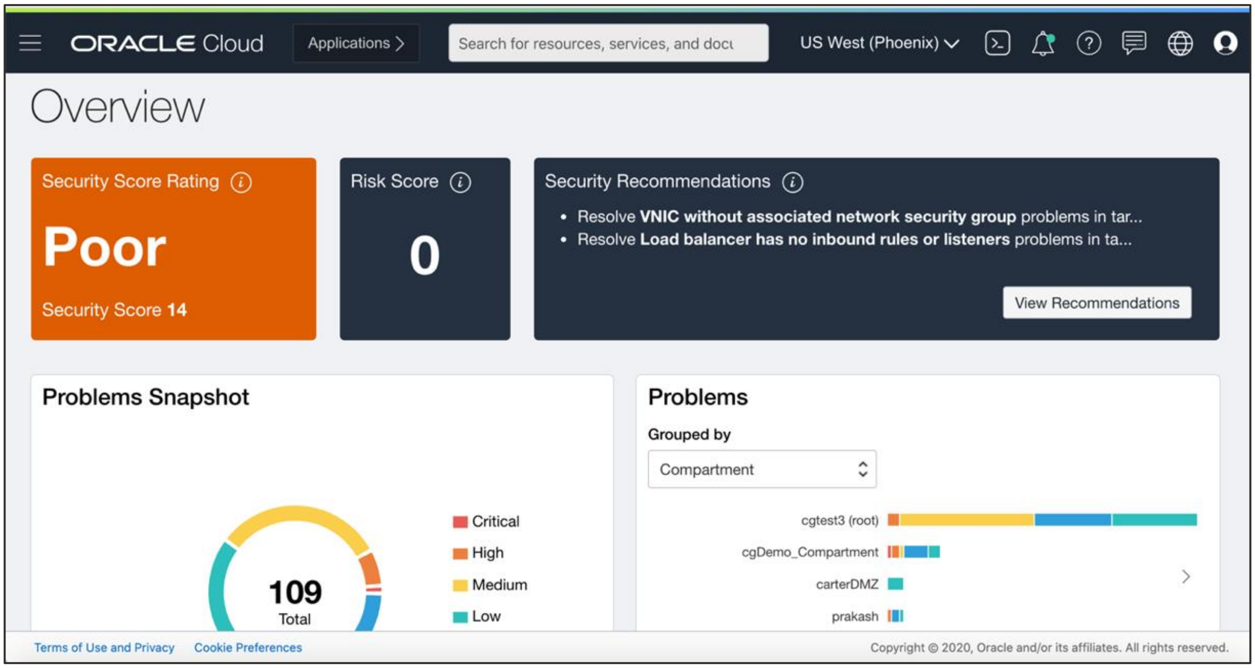
Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

Misconfigured resources and insecure activity in the cloud represent one of the most difficult problems for security professionals. Misconfigured cloud tenancies around cloud resources can present themselves in many different ways; from publicly accessible object storage buckets, unencrypted data storage, sensitive ports open to the internet. The behavior of users and administrators within the cloud are also a concern. Insecure activity in a cloud infrastructure offering is difficult to detect as it oftentimes spans beyond simple detection rules and can be generated from authenticated users. Insecure activity can oftentimes be attributed to different parts of the cyber kill chain such as: intrusion, reconnaissance, exploitation, privilege escalation, exfiltration, etc.

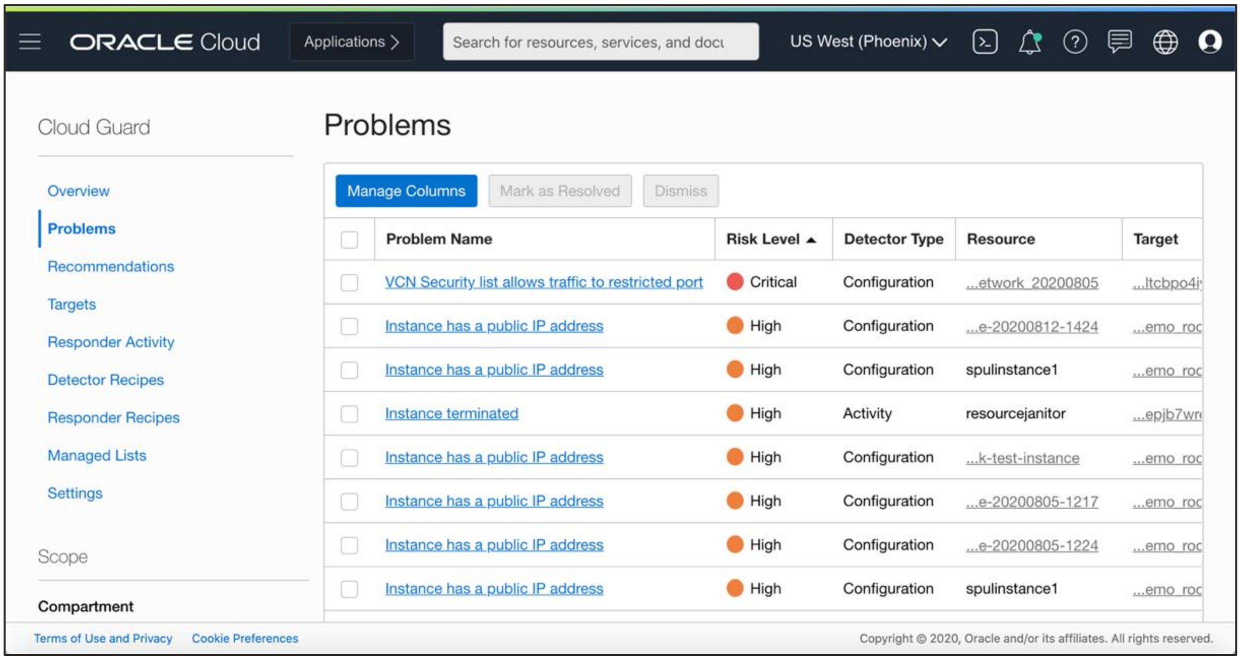
Oracle Cloud Infrastructure Cloud Guard is a cloud security service that detects misconfigured resources and insecure activities. Cloud Guard acts as a log and events aggregator that directly integrates with all major Oracle Cloud Infrastructure services (Compute, Networking, Storage, etc.) providing actionable results. Cloud Guard offers the flexibility to take action on security issues manually or automatically with conditional operators.



- Resolve **VNIC without associated network security group** problems in tar...
- Resolve **Load balancer has no inbound rules or listeners** problems in ta...

In the Cloud Guard Overview, administrators are provided a single view into their overall cloud security posture within their OCI tenancy. The dashboard incorporates a number of different analytics that help security personnel identify, triage, and prioritize different cloud security issues. Cloud Guard incorporates the use of a cloud security scorecard, so that administrators have a quantitative measure to manage risk over time. Furthermore, security issues which are referred to as problems in Cloud Guard are automatically assigned a severity and can be grouped by compartment, region, or resource type within the dashboard.

Issues that Cloud Guard identifies are called Problems. Cloud Guard presents problems in the Cloud Guard console the same way you would manage security issues in traditional security operations center workflows. Problems are listed in a queue and are categorized either as a resource misconfiguration or insecure activity. Security analysts can drill down into a problem and leverage the problem details such as the resource name, resource type, compartment, detection time, etc. to further investigate. Problems are uniquely identified with a resource identifier and can be remediated, marked as resolved, or dismissed. For compliance reporting use-cases, Cloud Guard maps problems related to misconfigured resources to Center for Internet Security (CIS) Benchmarks.

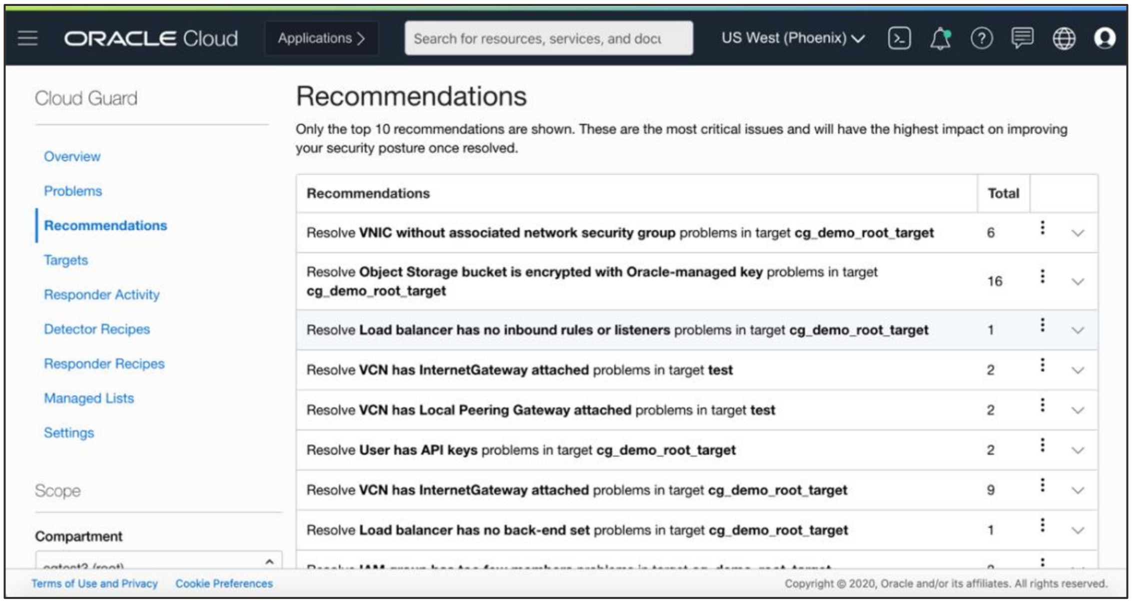


Problems

□	Problem Name	Risk Level ▲	Detector Type	Resource	Target
□	VCN Security list allows traffic to restricted port	● Critical	Configuration	...etwork_20200805	...ltcbpo4i
□	Instance has a public IP address	● High	Configuration	...e-20200812-1424	...emo_roc
□	Instance has a public IP address	● High	Configuration	spulinstance1	...emo_roc
□	Instance terminated	● High	Activity	resourcejanitor	...epjb7wr
□	Instance has a public IP address	● High	Configuration	...k-test-instance	...emo_roc
□	Instance has a public IP address	● High	Configuration	...e-20200805-1217	...emo_roc
□	Instance has a public IP address	● High	Configuration	...e-20200805-1224	...emo_roc
□	Instance has a public IP address	● High	Configuration	spulinstance1	...emo_roc

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

Cloud Guard embeds Oracle security expertise and provides end users out-of-the-box recipes that detect cloud common security issues (i.e., detector recipes) and can automate remediation processes (i.e., responder recipes). Cloud Guard detector recipes can be cloned and modified with the input settings appropriate for that resource. Cloned recipes can be enabled or disabled and can apply different severities to issues. Cloud Guard detector recipes have rule-based conditions based on time, system version, user, tag, IP address metadata, and resource identifier. As Oracle adds additional rules to its managed recipes, these new rules will also appear in the cloned recipes with the default configuration. This way, as Cloud Guard expands its coverage for more security issues, customers inherit that expansion. Responder recipes, which automate remediation, can provide close that gap in response time and incorporate security playbook themes such as: removing public access, disabling a user, stopping an instance, rotating an API key, and pushing event notifications to information security communications channels. In this way, Cloud Guard provides customers a cloud detect-and-respond framework that helps security organizations scale.



Recommendations

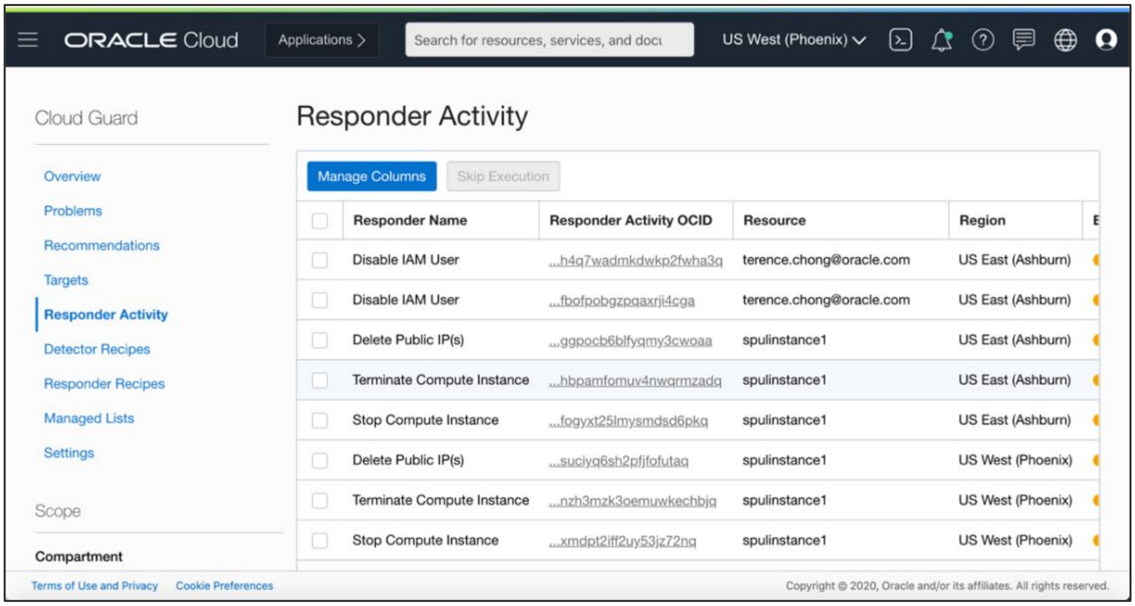
Only the top 10 recommendations are shown. These are the most critical issues and will have the highest impact on improving your security posture once resolved.

Recommendations	Total
Resolve **VNIC without associated network security group** problems in target **cg_demo_root_target**	6
Resolve **Object Storage bucket is encrypted with Oracle-managed key** problems in target **cg_demo_root_target**	16
Resolve **Load balancer has no inbound rules or listeners** problems in target **cg_demo_root_target**	1
Resolve **VCN has InternetGateway attached** problems in target **test**	2
Resolve **VCN has Local Peering Gateway attached** problems in target **test**	2
Resolve **User has API keys** problems in target **cg_demo_root_target**	2
Resolve **VCN has InternetGateway attached** problems in target **cg_demo_root_target**	9
Resolve **Load balancer has no back-end set** problems in target **cg_demo_root_target**	1

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

In addition to aggregating logs and events for managed cloud services in Oracle Cloud Infrastructure, Cloud Guard ingests metadata and threat intelligence data across Oracle Cloud Infrastructure that help correlate a specific cloud security attack type. For instance, a threat actor that has compromised an account within a cloud tenancy will sometimes use an IP address associated with command-and-control server or a Tor proxy to hide their location. Since Cloud Guard ingests network-based threat intelligence data, it can detect and correlate insecure activity from suspicious IP addresses.

Responders give security operations personnel the ability to remediate problems in Cloud Guard as specified by a corresponding security playbook. If a specific type of problem is detected, you can enact a responder to lower the mean time to respond. At its core, a responder is a serverless compute function that automatically triggers based on the event criteria (i.e. the type of problem). Cloud Guard gives administrators the option to remediate problems manually or automatically so analysts can focus their attention on more advanced cloud security issues.



Responder Activity

☐	Responder Name	Responder Activity OCID	Resource	Region
☐	Disable IAM User	...h4q7wadmkdwkp2fwha3q	terence.chong@oracle.com	US East (Ashburn)
☐	Disable IAM User	...fbofpobgzpqaxrji4cga	terence.chong@oracle.com	US East (Ashburn)
☐	Delete Public IP(s)	...ggpocb6blfyqmy3cwoaa	spulinstance1	US East (Ashburn)
☐	Terminate Compute Instance	...hbpamfomuv4nwqrmzadq	spulinstance1	US East (Ashburn)
☐	Stop Compute Instance	...fogyxt25lmysmdsd6pkq	spulinstance1	US East (Ashburn)
☐	Delete Public IP(s)	...suciyq6sh2pfjfofutaq	spulinstance1	US West (Phoenix)
☐	Terminate Compute Instance	...nzh3mzk3oemuwkechbjq	spulinstance1	US West (Phoenix)
☐	Stop Compute Instance	...xmdpt2iff2uy53jz72nq	spulinstance1	US West (Phoenix)

Copyright © 2020, Oracle and/or its affiliates. All rights reserved.

In summary, Cloud Guard provides security administrators the cloud detect-and-response framework needed to lower the mean time to respond and scale out security operations centers. Cloud Guard can be deployed in your OCI tenancy quickly and provides embedded security expertise out-of-the-box. Try Cloud Guard today in Oracle Cloud Infrastructure commercial regions.

Learn more about Oracle Cloud Guard and try Oracle Cloud for free today.

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Disclaimer: This document is for informational purposes. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document may change and remains at the sole discretion of Oracle Corporation.