Oracle Managed Security Services for Oracle Public Cloud – Vulnerability Assessment Services for Oracle Cloud (IaaS/PaaS)

**Key Business Benefits**
- Scalable solution offering comprehensive security coverage
- Fully Managed Service – single point of contact, working closely with the customer
- Flexibility to select Monthly or Quarterly scanning
- Available for Windows & Linux environments

**Key Features**
- Enhanced visibility of vulnerabilities, which assists in managing the organization’s security risk posture
- Support compliance with regulations such as HIPAA and PCI
- Fully Managed Service – single point of contact, working closely with the customer
- Removing need to hire in-house or 3rd party expertise
- Continuous reporting shows ongoing progress with your vulnerability management goals

**Vulnerability Assessment Services for Oracle Cloud (IaaS/PaaS)**

Oracle Vulnerability Assessment Service is a Managed Security Service (MSS) offering provided by Oracle MSS organization, utilizing QualysGuard scanning service. The service includes external (from the Internet) and internal (scanners are whitelisted with the ACLs on the hosts) scans. The QualysGuard scanners operate from within the Oracle Cloud Infrastructure. External scans are aimed to validate that private hosts/services are not exposed to the Internet, while internal scans are aimed at providing vulnerability information that may be present on the hosts or services running on those hosts. No Customer’s information, including vulnerability details or their Oracle Cloud Services, is stored in the public QualysGuard cloud.

QualysGuard scan reports are parsed through a custom MSS analytics engine to remove false positives and add details about compensating controls, where available. The MSS analytics engine produces a ‘Technical Report’, which provides Customer with vulnerability details grouped according to service and category.

In addition to QualysGuard scan reports and the Technical Report, Customers are also provided with an Executive Summary Report. The Executive Summary is a high level overview of the scans. The report includes trend analysis to help customers see the effects of remediation work performed since the previous scan, and changes in the security posture for their Oracle Cloud Services.

The service is managed by an Oracle MSS Security Service Manager who is assigned to the account. The Security Service Manager is a single point of contact, working closely with Customer’s own security team.
Report can be created to ensure compliance with a variety of different types of regulatory compliance, security policy compliance, or compliance with a data privacy policy.

**Data Privacy** – Reports contain findings for malicious software, patches, peer-to-peer software detection, and passwords related vulnerabilities. This information provides the basis for a data privacy policy and anti-malware strategy.

**PCI** – The PCI Data Security Standard details security requirements for members, merchants, and service providers that store, process or transmit cardholder data. To demonstrate compliance with the PCI Data Security Standard, merchants and service providers may be required to conduct network security scans on a quarterly basis.

**Sarbanes-Oxley** – In general, all reported findings relating to file permissions, level of system access, audit logs, and passwords are good candidates for creating a scan template for SOX compliance.

### Executive Summary

The Executive Summary provides a consolidated and concise report of the key findings, with recommendations custom to the environment (OS version) and installed software base (including 3PP where appropriate). The report provides the customer security management team with a complete view of new, existing, and fixed vulnerabilities.

The report is made up of 3 key elements:

- **Findings**
  
  Using internal processes and custom tools, the Executive Summary gives Customers a true representation of vulnerabilities within the scanned assets. The findings are shown in a series of bar graphs showing vulnerabilities by severity, operating systems detected, and services detected, as well as the number of vulnerabilities over time. This report includes no detailed vulnerability information.

- **Recommendations**
  
  Oracle is uniquely qualified to provide recommendations on Oracle owned applications, based on knowledge shared within Oracle.

- **Remediation**
  
  The executive report compares vulnerability assessment results over a period of time, giving security trend information in summary format. The reports also include a chart showing vulnerabilities that open by the date they were first reported. This allows the customer to target their remediation by severity and age.
Technical Report

A Technical report is generated using the MSS analytics engine and custom scripts to remove false positives and add information about compensating controls, where available. The Technical Report represents the scanned data in various formats that include:

- Grouped according to service and category
- Grouped according to instance
- Custom charts to highlight trends

The Technical Report is delivered as an excel spreadsheet, which allows customers to use the data within the report to create business specific reports or KPI's.

Excerpt from the Technical Report.

Security Practice at Oracle Managed Cloud Services

Oracle Managed Cloud Services (OMCS) is a key pillar of Oracle’s Cloud strategy. Managed Security Services form part of the wider OMCS portfolio of cloud service offerings including: Oracle application management Services on IaaS or PaaS, PaaS Lifecycle Management Services, and Functional Helpdesk Services for Oracle Applications or SaaS customers.

CONTACT US

For more information about Oracle Managed Security Services, visit omcscloudmarketplace_ww@oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Integrated Cloud Applications & Platform Services

Copyright © 2017, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0717

Oracle is committed to developing products and services that help protect the environment.