ORACLE DATA SHEET

Oracle Managed Security Vulnerability Assessment Service for Oracle Cloud (IaaS/PaaS)

ORACLE
Advanced Customer Services

Oracle Managed Security Vulnerability Assessment Service for Oracle Cloud provides Oracle Cloud customers with periodic security reviews of their IaaS/PaaS environments detailed reports of identified security vulnerabilities, and information on how to mitigate potential security risks. Customers gain the insight they need to keep their most sensitive data protected.

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
- Removes need to hire in-house or third party expertise
- Continuous reporting shows ongoing progress with vulnerability management goals

KEY BUSINESS BENEFITS

- Scalable solution offering comprehensive security coverage
- Fully managed service–vulnerability assessment as a service
- Flexibility to select monthly or quarterly scanning
- Available for Windows and Linux environments

Vulnerability Assessment Services for Oracle Cloud (IaaS/PaaS)

Oracle Vulnerability Assessment Service is a Managed Security Services offering that includes external scans from the internet, internal scans, analysis of results, and reports containing details of findings and remediation recommendations. The service uses industry leading vulnerability assessment tooling from Qualys to give the highest levels of vulnerability compliance when combined with Managed Security Services vulnerability assessment expertise.

The QualysGuard scanners operate from within the Oracle Cloud Infrastructure. External scans validate that private hosts/services are not exposed to the internet, while internal scans are aimed at providing vulnerability information related to the hosts or services running on those hosts. No customer information is stored in the QualysGuard public cloud, including vulnerability details or the Oracle Cloud services.

QualysGuard scan reports are parsed through a custom Managed Security Services analytics engine to remove false positives and add details about compensating controls where available. This analytics engine produces a "Technical Report", which provides the customer with vulnerability details grouped according to service and product category.

In addition to QualysGuard scan reports and the "Technical Report", customers also receive an Executive Summary report. The Executive Summary gives a high-level overview of scan execution findings and remediation recommendations. 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.

This service is managed by an Oracle Managed Security Services Manager assigned to the account. The Security Service Manager is a single point of contact who works closely with the customer's security team.

RELATED SERVICES

- Managed Security Services
- Managed Identity Services
- Managed Compliance Services
- Managed Database Cloud Service
- Managed Applications Unlimited for Oracle Technology Cloud
- Managed Cloud Help Desk for Applications Unlimited
- Advanced Monitoring and Resolution
- Solution Support Center

Executive Summary

The Executive Summary provides a consolidated and concise report of key findings with recommendations customized to the environment (OS version) and installed software, including third party products where appropriate. The report provides the customer's security management team with a complete view of new, existing, and fixed vulnerabilities.

The report is made up of three 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 displayed 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.

Recommendations

Oracle is uniquely qualified to provide recommendations on Oracle owned applications based on knowledge shared within Oracle.

Finding #	Title	Sev.	Category	Recommendation	Downtime Required	Environments Impacted	New
1	Windows Updates	3-5	Operating System – Windows	Windows Patches are applied quarterly as part of Oracle Managed Cloud Services Standard Windows Patching Process	Yes	HYPERION Prod NonProd	Yes*
2	.NET Framework 4.5	5	Operating System – Windows	Microsoft ended support for .NET 4 - 4.5 on January 12, 2016. Log an RFC to the applications team to verify if Microsoft .NET is required for the operation of the application and to determine the recommended upgrade path based on application support matrix. If it is not required it must be removed.	Yes	HYPERION NonProd	No
3	.NET Framework	3-5	Operating System – Windows	Log an RFC to the applications team to verify if Microsoft .NET can be upgraded and will not affect the operation of the application. If upgrade is possible it needs to be upgraded to the latest supported version.	Yes	HYPERION Prod NonProd	No
4	Linux	3-5	Operating System – Unix	Raise an RFC to run the provisioning tool 'od-provision' to apply the latest available Patch Set Update for Oracle Enterprise Linux.	Yes	EBSO Prod NonProd	Yes*
5	Oracle WebLogic Server	5	Webserver	Apply the latest PSU for WebLogic Server	Yes	IDM Prod NonProd	Yes*

Remediation

The executive report compares vulnerability assessment results over a period of time, giving security trend information in a 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.

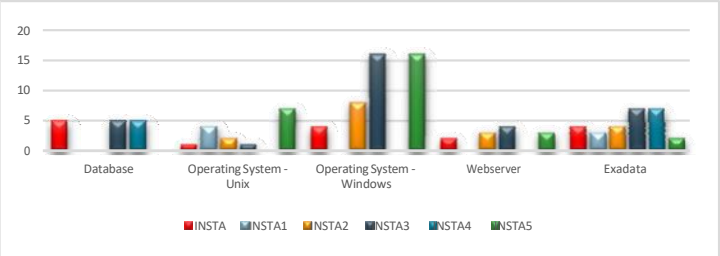
Technical Report

A Technical Report is generated using the analytics engine and custom scripts to remove false positives and/or add information about compensating controls where available. The Technical Report represents the scanned data in various formats such as:

- 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 with Oracle Advanced Customer Services

Oracle Advanced Customer Services has many years of experience in implementing Oracle security products and services, and securely managing security for customer environments in Oracle Cloud or on premises.

The broad portfolio of Managed Security Services can help customers minimize security risks, and meet compliance requirements. With these services, customers can be confident that their Oracle security solution is expertly configured and managed, and that hidden vulnerabilities to their Oracle environment are detected and addressed proactively before they can become a threat. Oracle Managed Security Services can set the stage to use cloud services safely or to integrate with external service providers minimizing risk exposure.

ORACLE

CONTACT US

For more information about Oracle Managed Security Services Vulnerability Assessment Service for Oracle Cloud (IaaS/PaaS), visit oracle.com/mcs, email us at acs_ww@oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services