

# Oracle Managed Security Services for Oracle Cloud and On-Premises

**ORACLE**  
Customer Success  
Services

Oracle Managed Security Services help customers protect their data in Oracle Cloud or on-premises and meet their internal security and regulatory requirements in an efficient and cost-effective manner. End-to-end security services packages include ongoing management, monitoring, and reporting service for customers who are leveraging Oracle security products and services.

## Security throughout the lifecycle

Data security, integrity, privacy, and compliance with regulatory requirements are a top priority for most companies—no matter if they run their databases and applications in their own data centers or on cloud. Oracle is addressing those needs with a broad range of offerings. To ensure the highest level of protection and to mitigate risk introduced with change, it is essential to expertly maintain and manage those Oracle security products and services in the environments where applications and databases are deployed throughout their lifecycle.

Oracle Managed Security Services has many years of experience in implementing Oracle security products and services and in managing security for customer environments in Oracle Cloud or on-premises. Customers can be confident that hidden vulnerabilities to their Oracle environment are detected and addressed proactively before they can become a threat. Oracle Managed Security Services provide

- **Lifecycle management:** Ongoing monitoring, configuration and change management, problem management, proactive advisory to relieve customer teams from day-to-day administration tasks
- **Seamless service delivery management:** Coordination by a Security Delivery Manager through periodic status reviews, comprehensive reporting, and proactive guidance
- **Predictable cost:** Clearly defined services scope at a fixed monthly fee enabling transparent cost and delivery planning

## Key features

- Complete lifecycle management including monitoring, configuration and change management, problem management, and reporting
- Proactive detection and prevention of vulnerabilities through assessments and targeted tests
- Seamless service delivery management throughout the engagement
- Predictable cost and transparent delivery planning

## Key business benefits

- Data security, integrity, and privacy in Oracle Cloud and on-premises
- Keeping sensitive data protected continuously
- Risk prevention
- Compliance with internal and external security regulations
- Full functionality of Oracle security software for high protection
- Predictable cost and timeframe of service delivery

## Vulnerability and threat prevention services

SERVICE	SERVICE SUMMARY
<b>Operational Readiness for Oracle Cloud Guard</b>	<p>Help accelerate adoption and improve configuration of Oracle Cloud Guard based on your specific requirements.</p> <p>Service features include</p> <ul style="list-style-type: none"> <li>• Guidance on Oracle Cloud Guard setup and OCI tenancy security recommended practices to reduce the noise for security operations teams</li> <li>• Expert advice to help enable custom recipes and responder setup for specific customer workloads</li> </ul>
<b>Vulnerability Assessment Service</b>	<p>Infrastructure scans of hosts/virtual machine(s) (VM) to help detect vulnerabilities within your Oracle environments.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>• Implementation of quarterly internal and external vulnerability scans of the hosts/virtual machines for the target environment</li> <li>• Detailed scan report and analysis reports including applicability, risks, and trends for remediation of vulnerabilities</li> </ul>
<b>Web Application Vulnerability Assessment</b>	<p>Scans an internet-facing web application to help detect security vulnerabilities introduced by change management events.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>• Implementation of quarterly scans to identify cross-site scripting, SQL injection, cookie tampering, malicious file execution, and other web-based vulnerabilities or misconfigurations</li> <li>• Scan and analysis report providing details on applicability, risks, and trends for remediation of vulnerabilities</li> </ul>
<b>Web Application Firewall Service</b>	<p>Help protect internet-facing applications sites against malicious attacks.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>• Integration of Web Application Firewall (WAF) for your internet-facing applications</li> <li>• Enablement of IP Intelligence filtering policies in the WAF for client connections to protected sites</li> <li>• Configuration of WAF policies in a monitoring and blocking mode</li> <li>• Periodic activity reports</li> </ul>
<b>Penetration Testing Service</b>	<p>Simulated attack on an internet-facing web application environment to help identify and demonstrate vulnerabilities</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>• Experienced Oracle ethical hackers simulate actions of a competent and motivated hacker from the public internet.</li> <li>• Comprehensive scan and analysis report providing information about security risks found, severity ratings, and remediation recommendations</li> </ul>
<b>File Integrity Monitoring Service</b>	<p>Monitoring and alerts of unauthorized changes to system and application files to help detect potential vulnerabilities of your Oracle environment</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>• Management of file integrity monitoring (FIM) policies on defined target nodes</li> <li>• Integration of target nodes with Oracle's Security Operations Center enabling continuous incident monitoring and response services</li> </ul>



### Related services

- Security Account Manager
- Managed Identity and Access Management
- Managed Compliance Services
- Advanced Management for Hybrid Cloud
- Managed Application Cloud Services
- Managed PaaS Service
- Oracle Cloud Priority Support

## Database Security Services

SERVICE	SERVICE SUMMARY
<b>Database Security Risk Assessment</b>	<p>In-depth security assessment of the Oracle Database and workloads, including a risk-based report of findings and remediation recommendations.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>Comprehensive database risk assessment with 120+ database checks and application environment context</li> <li>Executive and technical scan reports with risk assessment and remediation guidance</li> </ul>
<b>Advanced Data Security Service</b>	<p>Ongoing security compliance monitoring and audit management for target Oracle Databases registered in Oracle Data Safe</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>Provisioning and management of audit, compliance, and alert policies and reporting on alerts, auditing, and trends across databases</li> <li>Security recommendations and advisory on remediation of issues</li> </ul>
<b>Database Encryption Service</b>	<p>Encryption of sensitive data in the Oracle Database to help secure it against system or operating system level attacks and unauthorized access.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>Ongoing management, monitoring, and reporting</li> <li>Transparent Database Encryption (TDE) to encrypt data stored in the file system layer of the database</li> </ul> <p>Required Oracle Database Security technology: Oracle Advanced Security Option–Transparent Database Encryption*</p>
<b>Database Vault Service</b>	<p>Apply fine-grained access controls and restrict unauthorized users from accessing your data.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>Setup, design, and configuration of Oracle Database Vault realms and policies</li> <li>Implementation, testing, monitoring, and reporting</li> </ul> <p>Required Oracle Database Security technology: Oracle Database Vault</p>
<b>Database Audit Service</b>	<p>Detection and alert of suspicious unauthorized database activities that compromise the security of your database.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>Configuration of Oracle Audit Vault and client-side agents for Oracle Database</li> <li>Configure Oracle's recommended auditing policies</li> <li>Configure standard Oracle Audit Vault Reports to enable automatic report distribution</li> <li>Operational monitoring of Audit Vault and Audit Vault agents</li> </ul> <p>Required Oracle Database Security technology: Oracle Audit Vault</p>
<b>Data Masking Service</b>	<p>Help reduce security risks by masking production data in a non-production Oracle database while preserving its integrity.</p> <p>Service features include:</p> <ul style="list-style-type: none"> <li>Definition of mask formats for the data elements</li> <li>Development and testing of Oracle Enterprise Manager data masking scripts</li> <li>Deployment, testing, and execution of data masking scripts</li> </ul>

Required Oracle Database Security technology: Oracle Data Masking and Subsetting Pack\*

\*PaaS Database Cloud Service or Exadata Cloud Service subscriptions may include this option.

Take advantage of Oracle Managed Security Services to protect your most sensitive data against vulnerabilities in Oracle Cloud or on-premises.

---

## Connect with us

Call +1.800.ORACLE1 or visit [oracle.com/acs](https://oracle.com/acs)  
Outside North America, find your local office at [oracle.com/contact](https://oracle.com/contact)

 [blogs.oracle.com/advanced-customer-services](https://blogs.oracle.com/advanced-customer-services)

---

Copyright © 2023, 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.

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.

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. 0523

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail [REVREC\\_US@oracle.com](mailto:REVREC_US@oracle.com).