

Oracle Database Breach Support

ORACLE[®] Advanced Customer Services

Oracle Database Breach Support is a post-data intrusion service that analyzes a customer's security configuration and practices making recommendations on an actionable plan for improved security health.

KEY FEATURES

- Tailored package of services leveraging Oracle Database recommended security practices to identify and address security vulnerability
- Local and remote delivery options using innovative Oracle Advanced Support Cloud
- Up to five (5) days of onsite assistance from an Oracle Advanced Support Engineer
- Oracle Technical Account Manager

KEY BENEFITS

- Reduces security risks due to database configuration issues
- Tightens database security practices and standards
- Identifies and fixes critical security patches and upgrades that place systems at risk
- Discovers undocumented security gaps

TECHNICAL ACCOUNT MANAGER:

Throughout the entire engagement, the Oracle Technical Account Manager is your Oracle single point of contact as they manage all activities.

Reduce the Risk of Additional Data Loss by Securing Your Information from the “Inside Out” with Oracle Database Breach Support

Oracle Advanced Customer Services provides post database breach support in a flexible, cost-effective framework that can be customized and tailored to your unique database security need. The offering is designed to analyze your environment post database breach to ensure further exposure to data loss is minimized or eliminated.

The package has multiple components, beginning with an **Oracle Security Review and Recommendation**, focused on both your database and the underlying operating systems. All phases of the security review are overseen by an Oracle Advanced Customer Services **Technical Account Manager** to ensure seamless movement from kick off to completion. Also included are up to five (5) days of onsite support from an Oracle **Advanced Support Engineer**, experienced in database and operating system security.

The package is inclusive of a “planning and design” phase to ensure the security review recommendations are built into an executable deployment plan that quickly secures any additional exposure.

In-Depth Database Defense for Maximum Security

Oracle Security Review and Recommendation is an assessment designed to help customers understand their current level of Oracle Database security against Oracle recommended practices. Oracle Advanced Customer Services engineers collect database security related information via questionnaires, scripts, and database configuration snapshots of the environment. The information is then analyzed and reports built based on Oracle's recommended practices to achieve a more secure operational environment. The security review is focused at the database and operating system level, and can be expanded to include any pre-existing Oracle Database security products, including:

- Advanced Security
- Audit Vault and Database Firewall
- Database Vault
- Data Masking
- Label Security

KEY BENEFITS

- Single point of contact
- Helps ensure project success by coordinating meetings, organizing documentation, tracking communication, and establishing timelines

ADDED VALUE

- Develop a roadmap for database security optimization

Typical activities of the Oracle Security Review and Recommendations include publishing a “Report of Findings” covering review of:

- Database Security Patches
- Oracle Authentication and Password Security
- Oracle Accounts Management
- Oracle Net Services and Secure Communication
- Data Dictionary Protection
- Privilege Abuse and Privilege Escalations
- Oracle Directories and Oracle Files Protection
- Access Control
- Database Activity Monitoring for:
 - Oracle Database Audit
 - Oracle Fine-Grained Audit
 - Oracle Fine-Grained Access Control or Row Level Security

Fix the Downstream Challenges Caused by Poor Deployment Planning with Oracle Supportability Planning and Design Service

A key component of the Oracle Database Breach Support offering is the **Oracle Supportability Planning and Design** service. Including this planning and design offering in the package allows Oracle to take the next step and use the **Oracle Security Review and Recommendations** “Report of Findings” to build a detailed deployment plan specific to your database security configuration and business requirements. The deployment plan is built with future supportability and maintenance in mind, and lays out the installation steps and procedures required for successful implementation.

Typical activities include:

- Creation of detailed design documents focused on ongoing supportability
- Deployment planning consisting of key milestones
- Customer Checkpoint Review to validate analysis findings
- Verification checklist to ensure configurations works as designed post install

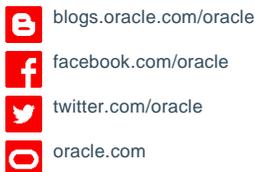
Benefits:

- Clearly map how to harden your Oracle Database
- Identify procedural or process changes to reduce risk
- Provide roadmap for needed database security updates and additional security product installation

Oracle Database Breach Support is your best offense for preventing additional data encroachment, securing your IT Investment from the “inside out”.



CONNECT WITH US



CONTACT US

For more information about Oracle Database Breach Support, visit oracle.com/acs, email us at acs_ww@oracle.com or call +1.800.oracle1 to speak to an oracle representative.

Integrated Cloud Applications & Platform Services

Copyright © 2018, 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. 0318