ORACLE DATA SHEET

Oracle Security Design and Hardening Support

ORACLE
Advanced Customer Services

Oracle Security Design and Hardening Support is a comprehensive database analysis and configuration offering, designed to address security vulnerability by applying Oracle recommended practices and implementing Oracle Database security product sets, processes, and procedures.

KEY FEATURES

- Tailored suite of services for planning and deployment of database security recommended practices and products customized to your industry and specific business needs
- Local and remote delivery options using the innovative Oracle Advanced Support Cloud
- Technical Account Manager: Throughout entire engagement, the Oracle Technical Account Manager is your single Oracle point of contact to manage all activities

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
- Helps ensure proper logging and auditing techniques are in place
- Single point of contact
- Technical Account Manager helps ensure processes are optimized, including communication, support, and change management for your environment

Reduce the Risk of Data Breach by Securing your Information from the "Inside-out" with Oracle Security Design and Hardening Support

Oracle Security Design and Hardening Support provides services in a flexible framework that can be customized and tailored to your unique database security needs.

The package has multiple components beginning with a security-specific **Plan and Design Phase** and ending with **Build and Deploy Phase** of the hardening database solution. The Oracle Advanced Customer Support Technical Account Manager oversees all phases of the offering to ensure seamless movement from kick-off to completion.

Plan and Design Phase: The Plan and Design phase focuses on building a supportable Database Security Deployment Plan specific to your configuration and business requirements. The deployment plan, built leveraging Oracle's recommended security practices, is designed to close off common vulnerabilities and identify database security products or procedures that need to be implemented.

Typical Activities Include:

- Process checks to ensure that default passwords, system IDs, and ports have been changed
- Identify unnecessary packages that may introduce security risk
- Recommend database security patches
- Identify unnecessary or vulnerable services to be disabled
- Ensure password enforcement and public privileges are scrutinized
- Examine and provide modification plans for security logging and auditing techniques
- Identify missing or needed Oracle Database security products (i.e.: Database Vault, Data Masking, Label Security, and Key Vault)
- Creation of a detailed Database Security Deployment Plan

ORACLE

OPTIONAL SERVICES

- Operating System Hardening
  - Time and materials engagement
- Installation of Oracle Database security products to enable:
  - Data encryption and redaction
  - Database firewalling and auditing
  - Data masking
  - Privileged user controls
  - Label based access control
  - Management of encryption keys and wallets

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

Build and Deploy Phase: This phase focuses on deployment of Oracle Database, Oracle Exadata, or Oracle SuperCluster hardening techniques in accordance with the Security Deployment Plan, and implementation of any optional Oracle Database security products. Oracle Advanced Support Engineers update database security configurations based on the customized deployment plan and build sheets, and apply any critical database security patches.

Typical Activities Include:

- Change default ports and listeners
- Remove unnecessary packages
- Install database security patches
- Disable useless or vulnerable services
- Enforce password security
- Update event audit settings
- Limit public privileges
- Operate System Hardening (optional via Time and Materials)
- Install Oracle Database Security Products (optional)
  - Advanced Security
  - Audit Vault and Database Firewall
  - Database Vault
  - Data Masking
  - Label Security
  - Key Vault

Benefits:

- Deploy proven database configurations that mitigate risk
- Decrease time to deploy with expert Oracle Advanced Customer Services installation
- Tighten database security practices and standards
- Identify and fix critical security patches and upgrades that place data at risk

In-Depth Database Defense for Maximum Security

Reducing risk at the database level with database hardening is key to securing your business critical data. Oracle Advanced Customer Services can strengthen these preventive measures by adding optional operating system hardening and/or database security product installation services into your Security Deployment Plan. Adding these optional services, and installing them to Oracle standards, will help ensure your investment, prevent data breaches, and satisfy the regulatory requirements.

ORACLE

CONTACT US

For more information about Oracle Security Design and Hardening Support, visit oracle.com/acs, 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