

ORACLE EXADATA DATABASE MACHINE

SECURITY OVERVIEW

KEY FEATURES AND BENEFITS

- Encrypt sensitive application data with no application changes
- Prevent access to application data through privileged user credentials
- Enforce data access through the application tier
- Prevent unauthorized application changes
- Monitor inbound traffic for SQL injection threats
- Cryptographic acceleration with Intel® AES-NI integration
- Consolidate, report and monitor database audit records
- Centralized management through Oracle Enterprise Manager
- Pre-configured templates for many applications including Oracle E-Business Suite, Oracle Peoplesoft, Oracle Siebel, SAP and more
- Industry standard encryption algorithms (AES, 3DES)

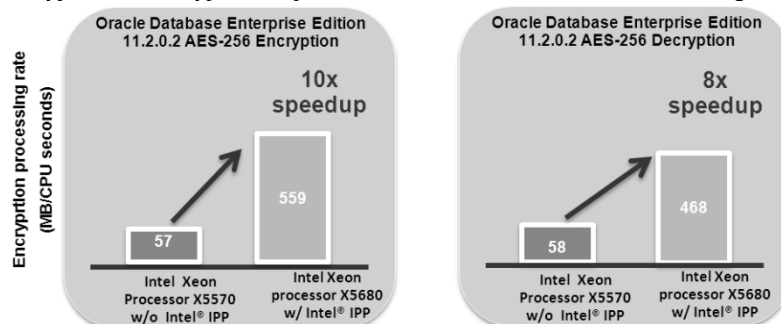
The Oracle Exadata Database Machine delivers extreme performance and superior data security. As organizations consolidate their data, more and more sensitive information ranging from email addresses to credit card numbers now resides in a single database, giving organizations the ability to secure and monitor that data more efficiently than ever before. Oracle Exadata Database Machine customers can protect data at both the database and storage tiers without giving up performance.

Oracle Exadata Database Machine Security

Data breaches continue to make headlines as hackers and criminal organizations launch sophisticated attacks on large data repositories seeking credit card numbers, email addresses and other sensitive information. While distributed databases provided security through physical separation, they are costly to operate and often impede businesses agility. Data consolidation provides increased business efficiencies, cost savings and ultimately stronger security as fewer databases need to be secured and monitored. The Oracle Exadata Database Machine can utilize Oracle's industry leading database security solutions to block threats and detect unauthorized activity. Misuse of privileged user credentials, insider threats, and SQL injection are just a few of the threats that can be detected and prevented.

Oracle Exadata Database Machine with Oracle Advanced Security

Oracle Advanced Security transparent data encryption (TDE) protects sensitive data such as credit card numbers and email addresses from attempts to access at the operating system level, on backup media or in database exports. No triggers, views or other costly changes to the application are required. TDE leverages performance and storage optimizations of the Oracle Exadata Database Machine, including the Smart Flash Cache and Hybrid Columnar Compression (EHCC). Compression interoperates seamlessly with TDE because it takes place before the data is encrypted. Oracle Enterprise Linux running on the Compute Nodes automatically leverages the hardware cryptographic acceleration available in its Intel® XEON® 5600 CPUs. This additional performance boost provides up to 10 times faster encryption and decryption, important for data consolidation and warehousing.



Oracle Exadata Database Machine with Oracle Database Vault

Oracle Database Vault protects against misuse of stolen login credentials, application bypass, and unauthorized changes to applications, including attempts to make copies of application tables. Oracle Database Vault realms form a protective boundary around existing applications, blocking administrative accounts from having ad-hoc access to application data or make unauthorized application changes. Oracle Database Vault command rules enable policy based controls to be deployed inside the Oracle database, limiting who, when, where and how the database and application data is accessed, creating a trusted path to the application data. Command rules can enforce policies on commands such as *create*, *drop*, *connect* and *truncate*, preventing unauthorized database, even by those who may otherwise have the necessary privileges through default roles.

Oracle Exadata Database Machine with Oracle Audit Vault

As organizations consolidate on Exadata, it is critical that they audit database activity using Oracle Database 11g native auditing capabilities. Oracle database native auditing effectively requires less than 5% overhead in most cases. Audit data from the Oracle Exadata Database Machine can be automatically consolidated and secured by Oracle Audit Vault. The built-in compliance related reports and real-time alerting capabilities provide auditors and internal security personnel an efficient means of reviewing of activity inside the Oracle Exadata Database Machine.

Oracle Exadata Database Machine with Oracle Database Firewall

Oracle Database Firewall can be deployed in front of the Oracle Exadata Database Machine and configured to monitor in-bound SQL traffic over Oracle SQL*Net and the TCP/IP protocol. Oracle Database Firewall's highly accurate grammar analysis engine can efficiently evaluate in-bound SQL and compare the SQL with a white list of approved application SQL statements. Unrecognized statements such as those containing a SQL injection would immediately trigger a policy exception. Oracle Database Firewall can then alert on, substitute a new SQL or block any unapproved SQL from reaching the Oracle Exadata Database Machine.

Application Certification

Oracle Advanced Security, Oracle Audit Vault, Oracle Database Vault, and Oracle Database Firewall can be used with applications including Oracle E-Business Suite, Oracle PeopleSoft, Oracle Siebel, Oracle JD Edwards EnterpriseOne, Oracle Financial Services (iFlex), and SAP. Pre-defined and extensible Oracle Database Vault policies are available for all of the previously listed applications and existing application data can be encrypted using Oracle Advanced Security TDE.



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

Copyright © 05/ 2011, 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
0109