ORACLE 11g DATABASE

SECURITY SOLUTIONS FOR ORACLE EXADATA DATABASE MACHINE

KEY FEATURES AND BENEFITS

- Encrypt sensitive application data with no application changes. Benefit from cryptographic acceleration with Intel® AES-NI and Oracle SPARC T-series
- 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
- 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

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.

Security Considerations for Oracle Exadata Database Machine

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 access attempts at the operating system level, on backup media or in database exports. No triggers, views or other costly changes to applications are required. TDE leverages performance and storage optimizations of the Oracle Exadata Database Machine, including Smart Scans and Hybrid Columnar Compression (EHCC). Compression interoperates seamlessly with TDE because it takes place before the data is encrypted, and it reduces encryption performance overhead because there is less total data to encrypt. Oracle Linux or Oracle Solaris running on the Compute Nodes automatically leverage hardware cryptographic acceleration available in Oracle SPARC and Intel® XEON® CPUs. This additional performance boost provides up to ten times faster encryption and decryption, a key benefit 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 making 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 and 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 operations even by those who may

otherwise have the necessary privileges through default roles.

Oracle Exadata Database Machine with Oracle Audit Vault and Database Firewall

As organizations consolidate on Exadata, it is critical that they audit database activity using the database's native auditing capabilities. Oracle Database native auditing effectively requires less than 5% overhead in most cases. Additionally, Oracle's 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. The firewall's highly accurate grammar analysis engine can evaluate in-bound SQL and compare it with a white list of approved application SQL statements. Unrecognized statements such as those containing a SQL injection would immediately trigger a policy exception. The firewall can then alert on, substitute a new SQL or block any unapproved SQL from reaching the Oracle Exadata Database Machine. Audit records from the firewall can be combined with native database audit records gathered directly from the Oracle Exadata Database Machine and consolidated in a secure, common repository that seamlessly scales up over time. Built-in compliance reports and real-time alerting capabilities provide auditors and internal security personnel an efficient means of reviewing activity both inside and outside of the Oracle Exadata Database Machine.

Application Certification

Oracle Advanced Security, Oracle Database Vault, and Oracle Audit Vault and 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 these applications, and existing application data can be encrypted using Oracle Advanced Security TDE.

Contact Us

For more information about database security for the Oracle Exadata Database Machine, visit oracle.com/database/security or call +1.800.ORACLE1 to speak with an Oracle representative.

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

Hardware and Software, Engineered to Work Together

ORACLE