An Oracle White Paper
March 2011

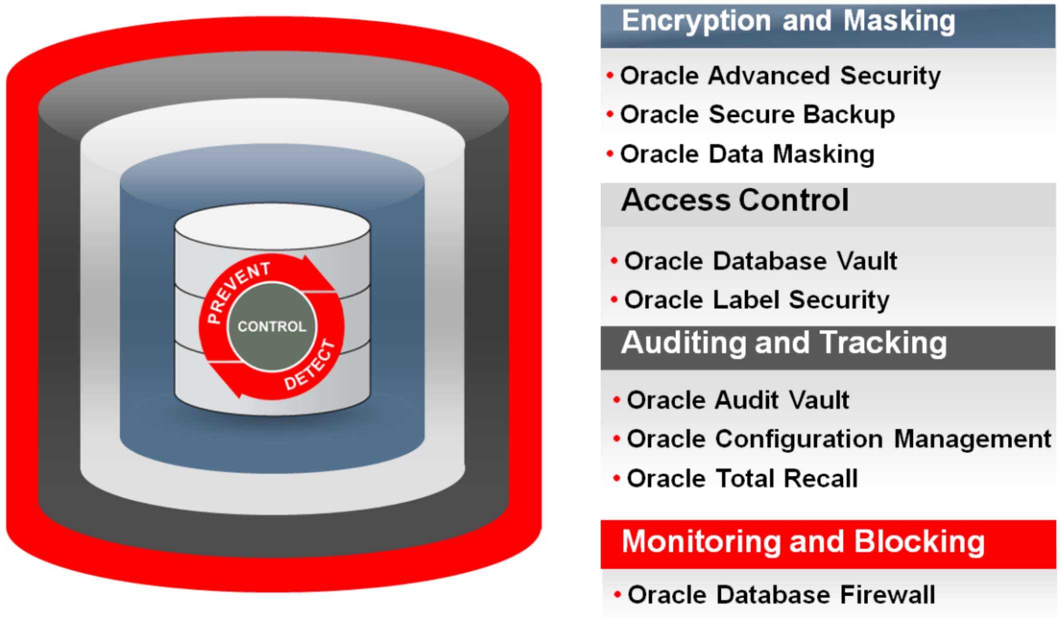
Cost Effective Security and Compliance with Oracle Database 11g Release 2

Introduction

Information ranging from trade secrets to financial and privacy data has become the target of sophisticated attacks. While most organizations have deployed perimeter firewall, intrusion detection, and anti-spam technologies, protecting data now requires a defense-in-depth, inside-out security strategy. By adopting this strategy organizations can better safeguard data, address regulations, and securely achieve business initiatives such as consolidation and cloud computing.

Oracle Database Security

Oracle's defense-in-depth security architecture can be divided into four areas spanning both protective and detective security controls. The four areas are encryption and masking, access control, auditing and tracking, monitoring and blocking.



Encryption and Masking

- Oracle Advanced Security
- Oracle Secure Backup
- Oracle Data Masking

Access Control

- Oracle Database Vault
- Oracle Label Security

Auditing and Tracking

- Oracle Audit Vault
- Oracle Configuration Management
- Oracle Total Recall

Monitoring and Blocking

- Oracle Database Firewall

Figure 1: Oracle Defense-in-Depth Security

Organizations can choose to deploy Oracle's defense-in-depth security controls in combination or individually. The approach and type of control used will depend on both internal and external factors such as sensitivity of data, regulatory and privacy requirements, deployment in the cloud, remote database administration, separation of duty, and physical platform access.

Encryption and masking are important for protecting data outside the access control perimeter of the database. This includes data residing on disk, data in test and development environments, data traveling over the network and data on backup. Operating system attacks leave open the possibility of unimpeded access to sensitive data via direct access to the files that comprise the database, bypassing the authentication and access controls enforced within the database. Usage of production data for testing and development purposes can unnecessarily expose sensitive data to individuals without a true need-to-know.

Strong access controls inside the database at the data layer enable organization to raise the bar on the security of existing applications as well as better secure data consolidated from multiple repositories. Limiting ad-hoc access to application data, even by those maintaining the database, not only helps address privacy and regulatory concerns, but can also block attacks on privileged user accounts.

While encryption and access control are key components to protecting data, even the best security systems are not complete without a monitoring system in place. Just as video cameras supplement audible alarms inside and outside businesses, monitoring what happens inside the database as well as what requests are inbound to the database are core to the principle of trust-but-verify as well as protecting against SQL injection attacks.

Encryption and Masking

Encryption For Data At Rest

Oracle provides robust encryption solutions to safeguard sensitive data against unauthorized access via the operating system or backup media. Oracle Advanced Security transparent data encryption (TDE) helps address privacy and regulatory requirements by encrypting personally identifiable information (PII) such as social security numbers and financial information such as credit card numbers. Oracle Advanced Security provides the ability to encrypt entire applications with TDE tablespace encryption as well as encrypting individual sensitive data elements with TDE column encryption. Oracle Advanced Security TDE enables organizations to deploy encryption across their Oracle databases quickly and cost effectively, preventing access to sensitive data through the operating system without any changes to existing applications and helping achieve compliance with a wide array of regulations.

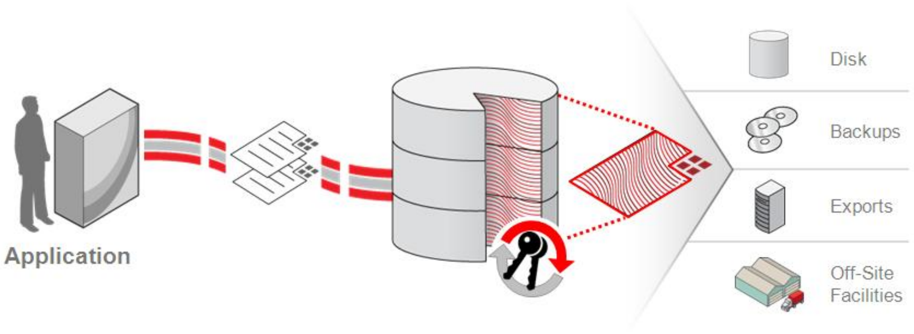


Figure 2: Oracle Advanced Security

Oracle Advanced Security TDE works by transparently encrypting data before writing it to disk and transparently decrypting when reading it off disk. The key difference between Oracle Advanced Security TDE and disk or volume based encryption solutions is that the data is only decrypted after a user has authenticated to the Oracle database and passed any associated authorization checks at the application or database level. Moreover, for strong authentication to the Oracle database, Oracle Advanced Security supports Kerberos, PKI and RADIUS.

With Oracle Advanced Security TDE, existing database backup routines continue to work, with the data remaining encrypted on the backup media. For encryption of entire database backups, Oracle Advanced Security TDE can be used in combination with Oracle RMAN.

Encryption key management is an important part of any data encryption solution. Oracle Advanced Security manages encryption key transparently using a two tier key architecture consisting of a single master encryption key and one or more data encryption keys. Out of the box Oracle Advanced Security stores the master encryption key in an encrypted PKCS#12 file known as the Oracle Wallet. Both the TDE master encryption key as well as the data encryption keys for TDE column encryption can be rotated as needed. Due to backup and recovery requirements, previously used master encryption keys are retained in the Oracle Wallet. Starting with Oracle Database 11g, the TDE master encryption key can be stored on a hardware security module (HSM). The HSM integration provides both centralized management of the master encryption keys and FIPS 140-2 level 2 or 3 certified encryption key storage. This is especially valuable when many databases are using Oracle Advanced Security. Oracle Advanced Security interoperates with HSM devices using the industry standard PKCS #11 interface.

Oracle Advanced Security TDE can be used across a wide variety of applications including Oracle E-Business Suite, Oracle Siebel, Oracle PeopleSoft, Oracle JD Edwards EnterpriseOne, Oracle Retail Applications (Retek), Oracle Financial Services (iFlex), Infosys Finacle, and SAP.

For high performance cryptographic processing, Oracle Database 11g Release 2 (11.2.0.2) with Oracle Advanced Security automatically utilizes the hardware cryptographic acceleration available in most of the Intel® XEON® 5600 CPUs by leveraging the Advanced Encryption Standard New Instruction (AES-NI). This additional performance boost is particularly valuable for data warehousing and other high-volume workloads.

Encryption For Data In Transit

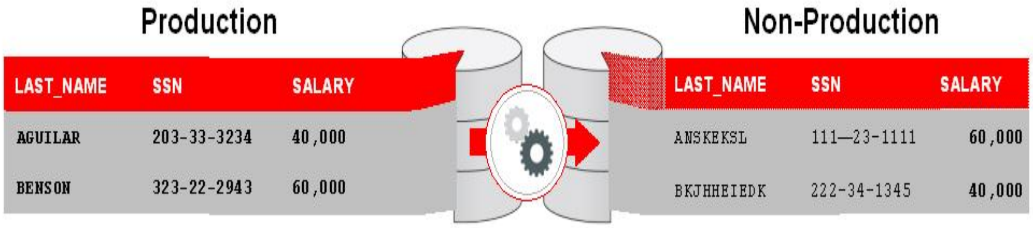
Oracle Advanced Security provides an easy-to-deploy solution for protecting all communication to and from the Oracle database, supporting both SSL/TLS based encryption as well as native network encryption for enterprises without a PKI infrastructure. For easy setup and deployment, the Oracle database can be configured to reject connections from clients that do not encrypt data on the wire, or optionally allow unencrypted connections. In addition, Oracle Advanced Security supports SSL/TLS hardware-based cryptographic acceleration.

Encryption For Data On Backup Tapes

Lost or stolen tapes can result in the loss of significant amounts of sensitive data. Oracle Secure Backup encrypts data written to tape and provides centralized tape backup management for the entire Oracle environment. It protects the Oracle database, and the associated UNIX, Linux, Windows and Network Attached Storage (NAS) file system data. Oracle Secure Backup integrates with Oracle database through Recovery Manager (RMAN) supporting versions Oracle Database 9i to Oracle Database 11g. With its optimized integration, it achieves faster backups than comparable media management utilities with less CPU utilization.

Data Masking For Non-Production

Oracle Data Masking also helps organizations comply with data privacy and protection mandates. With Oracle Data Masking, sensitive information such as credit card or social security numbers can be replaced with realistic but non-factual values, allowing production data to be safely used for development, testing, or sharing with out-source or off-shore partners for various non-production purposes. Oracle Data Masking uses a library of templates and format rules, consistently transforming data in order to maintain referential integrity for applications.



LAST_NAME	SSN	SALARY
AGUILAR	203-33-3234	40,000
BENSON	323-22-2943	60,000

LAST_NAME	SSN	SALARY
ANSKEKSL	111—23-1111	60,000
BKJHHEIEDK	222-34-1345	40,000

Figure 3: Oracle Data Masking

Access Control

The Oracle database provides a highly granular access control model, including support for roles and row level security. Oracle database technologies such as virtual private database have become widely popular for enforcing application security policies that traditionally would have been implemented using complex view based approaches. However, data breach investigations have shown that privileged user accounts and application bypass techniques have been leveraged to gain access to sensitive application data. In addition, privacy laws increasingly require restricted access to application data, even by those administering the database.

Privileged User Control

IT, database and application administrators fill highly trusted positions within the enterprise - maintaining operating systems, databases and applications. This includes not only applying patches to the database but also monitoring performance. Oracle Database Vault increases the security of the Oracle database by preventing unlimited, ad-hoc access to application data by administrative accounts while still allowing day to day administrative activity to proceed. Oracle Database Vault controls help block hackers from leveraging administrative accounts to gain access to sensitive application data. This is especially important as databases continue to increase in size and organizations look toward consolidation for increased efficiencies and cost savings.

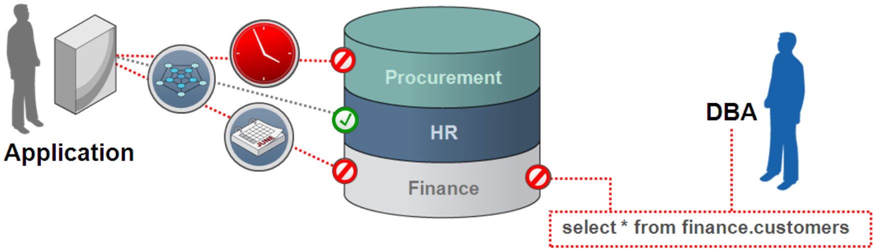


Figure 4: Oracle Database Vault

Oracle Database Vault can be used across a wide variety of applications including Oracle E-Business Suite, Oracle Siebel, Oracle PeopleSoft, Oracle JD Edwards EnterpriseOne, Oracle Retail Applications (Retek), Oracle Financial Services (iFlex), Infosys Finacle, and SAP.

Real Time Access Controls

In addition to strengthening access controls to application data through administrative accounts, Oracle Database Vault also enables operational controls within the Oracle database that can be used to prevent configuration drift, unauthorized application changes and ad-hoc access to the database and application data. Multiple factors such as IP address, time of day and authentication method can be used in a flexible and adaptable manner to enforce access control without making changes to the application. For example, access can be restricted to a specific middle tier, creating a "trusted-path" to the application data and preventing use of ad-hoc tools.

Security Administration

Oracle Database Vault creates a separate security dictionary within the Oracle database to store its policies. Management of the Oracle Database Vault policies can be delegated to a database security administrator who is separate from the Oracle database administrator. For smaller organizations, a single individual can have responsibility for both accounts using separate authentication credentials. In addition, Oracle Database Vault optionally enables a separate account management responsibility to be defined. This prevents existing privileged users from using their roles to create ad-hoc database accounts in the production environment that might compromise security of the database or application.

Data Classification

Oracle Label Security protects sensitive data by assigning a data label or data classification to each row in an application table. Oracle Label Security mediates access by comparing the data label against the label of the user requesting access. For transparency, the data label can be appended to the existing application table using a *hidden* column. Based on the policy of the organization, data labels can be defined to enforce a combination of hierarchical, compartmental and group access controls. High security organizations use Oracle Label Security to implement multi-level security (MLS) controls, enabling sensitive and highly sensitive data to be securely stored in the same application table, eliminating the need for multiple databases. Commercial organizations can use data labels to securely consolidate sensitive data, compartmentalize data for multi-tenancy, hosting, software-as-a-service and other security requirements.

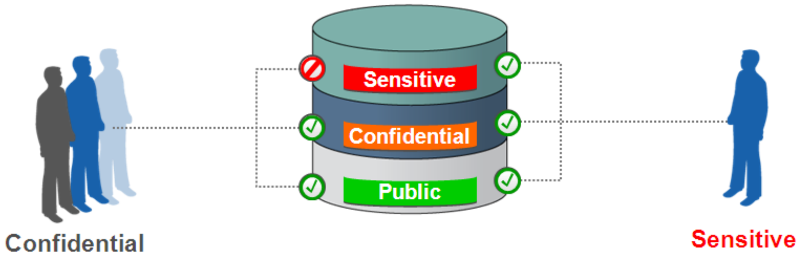


Figure 5: Oracle Label Security

Auditing and Tracking

While encryption, masking and access control technologies are key components to Oracle's defense-in-depth strategy, auditing events taking place inside the database as well as inbound SQL statements are critical to defending against sophisticated attacks such as insider threats and SQL injection attacks.

Auditing Database Activity

Examination of numerous data breaches has shown that auditing could have helped detect problems early, reducing the financial impact of data breaches. The Oracle database has the industry's most robust and fine grained auditing capabilities, enabling auditing to be turned on at the user, privilege and statement level. Fine grained auditing, introduced in Oracle9i, enables conditional auditing on specific application table columns. Oracle Audit Vault simplifies the review and maintenance of audit data by transparently collecting and consolidating the audit data generated by Oracle and non-Oracle databases, providing valuable insight into *who* did *what* to *which* data *when* – including privileged users who have direct access to the database.

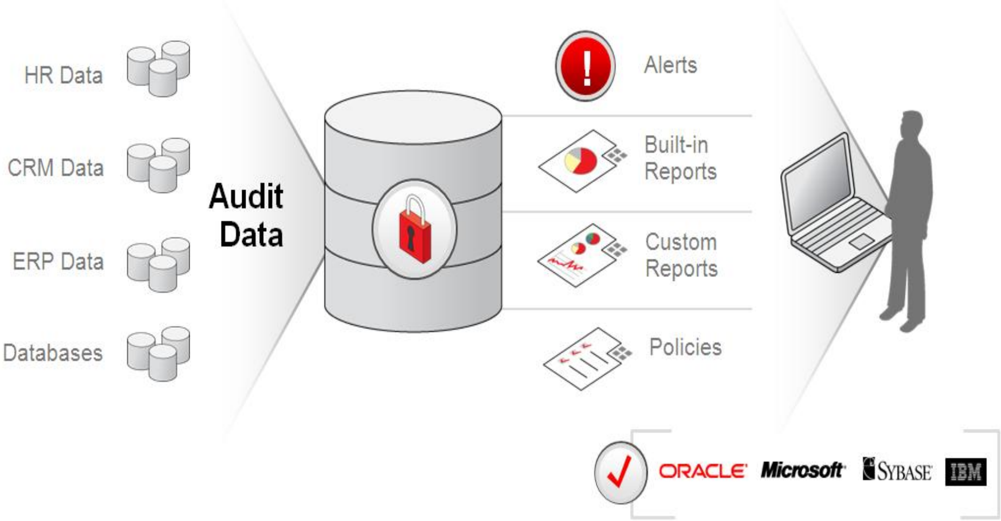


Figure 6: Oracle Audit Vault

With Oracle Audit Vault reports, alert notifications, and centralized audit policy management, the risks from internal threats and the cost of compliance are greatly reduced. Oracle Audit Vault leverages Oracle's industry leading database security and data warehousing technology for managing, analyzing, storing, and archiving large volumes of audit data.

Oracle Audit Vault provides standard audit assessment reports covering privileged users, account management, roles and privileges, object management and system management across the enterprise. Parameter driven reports can be defined that show, for example, user login activity across multiple systems and within specific time periods, such as weekends. Oracle Audit Vault provides an open audit warehouse schema that can be accessed from Oracle BI Publisher, or 3rd party reporting tools.

Oracle Audit Vault event alerts help mitigate risk and protect from insider threats by providing proactive notification of suspicious activity across the enterprise. Oracle Audit Vault continuously monitors the inbound audit data, evaluating audit data against alert conditions. Alerts can be associated with any auditable database event including system events such as changes to application tables, role grants, and privileged user creation on sensitive systems. Oracle Audit Vault collects database audit data from Oracle, Microsoft SQL Server, Sybase, and IBM DB2 LUW databases.

Configuration Management

Configuration management is a critical component in every enterprise's day-to-day IT operations. Oracle Configuration Management Pack forms the centerpiece of Oracle Enterprise Manager's ability to manage configurations and automate IT processes. A key component of this solution is Configuration Change Console, which reduces cost and mitigates risk by automatically detecting, validating and reporting on authorized and unauthorized configuration changes.

Compliance Assessments

Proactive assessment of key compliance areas such as security, configuration and storage help identify areas of vulnerabilities and areas where best practices are not being followed. Oracle Configuration Management Pack ships with over 200 built-in policy checks and the capability for administrator's to define their own custom policies.

Oracle Configuration Management Pack tracks violations of these policies in a similar manner as performance metrics. Notification rules can be applied and corrective actions can be assigned to violations. For example, if a well-known username/password is present in a database, or if an open port is detected in the Application Server, a corrective action could be defined to automatically disable the account and close that port.

Such proactive enforcement is supplemented with compliance reports. These reports denote the compliance score for targets. It is possible to view the compliance score over time, along with drilling down into the violations and impact for each target. Integration with problem ticketing solutions allow for policy violation information to be automatically sent to a ticketing system and incident tickets created without the need for manual intervention. The compliance dashboard enables administrators to have a quick view of how their systems comply with best security practices, and it allows them to drill down into the details. They can also see the historical trend and thus track progress towards compliance over time.

Data History and Retention

Regulatory and compliance regulations such as SOX, HIPAA and BASEL–II require retention of historical data. Additionally, businesses are increasingly realizing the immense value historical data can provide in terms of helping them understand market trends and customer behavior.

Organizations need an efficient mechanism to retain data for longer duration that does not involve application rewrites, 3rd party or handcrafted software solutions, or additional administrative overhead. Oracle Total Recall with Oracle Database 11g addresses these challenges by ensuring complete, secure retention and management of all your historic data. Oracle Total Recall, with the underlying technology, Flashback Data Archive, transparently tracks changes to database tables in a highly secure and efficient manner without requiring use of special interfaces or application changes.

Monitoring and Blocking

Data breach investigations have shown that SQL injection attacks have been one of the top hacking techniques used to steal sensitive data. Detecting and blocking SQL injection attacks requires a high performance SQL grammar analysis engine that can quickly determine whether an in-bound SQL statement is valid or should be blocked.

Database Firewall

Oracle Database Firewall is an active, real-time database firewall solution that provides white list, blacklist and exception list policies, intelligent and accurate alerts, and monitoring with very low management and administrative costs. Oracle Database Firewall is independent of the database configuration and operation. This independent boundary of protective shielding helps reduce the risk of data loss and helps organizations manage an ever changing landscape of regulations.

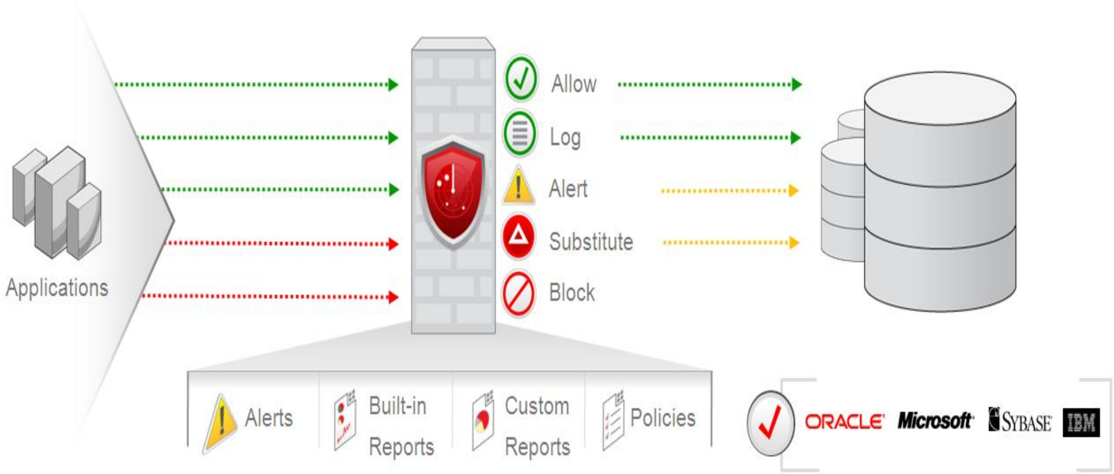


Figure 7: Oracle Database Firewall

Oracle Database Firewall examines the grammar of the SQL statements being sent to the database, analyzes their meaning, and determines the appropriate security policy to apply. Oracle Database Firewall can help recognize SQL injection attacks on applications and block them before they reach the database. This highly accurate approach provides a significantly higher degree of protection than first-generation database monitoring technologies that relied on recognizing the signature of known security threats. Oracle Database Firewall supports Oracle, Microsoft SQL Server, Sybase, and IBM DB2 LUW databases.

Application Certification

To help customers protect sensitive data and applications, Oracle has pre-certified Oracle database security solutions such as Oracle Database Vault and Oracle Advanced Security with numerous applications including Oracle E-Business Suite, Oracle Siebel, Oracle PeopleSoft, Oracle JD Edwards EnterpriseOne, Oracle Retail Applications (Retek), Oracle Financial Services (iFlex). Infosys Finacle and SAP have also completed certification with both Oracle Database Vault and Oracle Advanced Security. Oracle Database Vault and Oracle Advanced Security provide critical safeguards to protect data from ad-hoc access by privileged users both inside and outside the database. For monitoring, Oracle Audit Vault and Oracle Database Firewall can be deployed to monitor activity inside the database as well as inbound SQL traffic on the network. Please refer to application specific support notes for the most up-to-date certification information.

Oracle Exadata Database Machine

The Oracle Exadata Database Machine delivers extreme performance and scalability for all your database applications, including Online Transaction Processing, Data Warehousing , and consolidation of mixed workloads. Oracle's defense-in-depth, inside-out security strategy enables strong security for the Oracle Exadata Database Machine, helping prevent sophisticated attacks. Large data repositories are increasingly the target of attacks, making security especially important for the Oracle Exadata Database Machine.

Oracle Advanced Security and Oracle Database Vault provide critical safeguards for Oracle Exadata Database Machine deployments, encrypting data at rest and enforcing strong operational controls that prevent privileged accounts outside and inside the Oracle database from being leveraged to access sensitive data. Both Oracle Database Vault and Oracle Advanced Security can be deployed in the Oracle Exadata Database Machine the same way they are deployed on any other Oracle Database configuration (single instance, RAC, or Data Guard).

Oracle Advanced Security TDE automatically leverages hardware cryptographic acceleration capabilities provided by most of the new Intel® XEON® 5600 CPUs with AES-NI, making. Additionally, TDE tablespace encryption complements Exadata Hybrid Columnar Compression

(EHCC), allowing customers to achieve extreme performance, strong security and efficient storage.

Oracle Audit Vault and Oracle Database Firewall can be deployed individually or together with the Oracle Exadata Database Machine. Oracle Audit Vault consolidates and secures the audit records generated by the Oracle database. Oracle Database Firewall can be deployed in front of the Oracle Exadata Database Machine to monitor in-bound SQL for SQL injection threats.

Conclusion

Increasingly sophisticated threats combined with the push toward data consolidation and cloud computing are just a few of the reasons why Oracle's defense-in-depth approach to security is critical to safeguarding data. Data breach investigations have shown that security controls must be multi-layered to protect against threats that range from account misuse to SQL injection attacks. In addition, the ever changing regulatory landscape and renewed focus on privacy demonstrates the need for solutions to be transparent and cost effective to deploy. Oracle Advanced Security and Oracle Database Vault provide encryption and access controls to prevent account misuse from outside or inside the Oracle database. Oracle Audit Vault and Oracle Database Firewall provide detailed audit and monitoring capabilities, including the ability to monitor both Oracle and non-Oracle databases and prevent SQL injection attacks from reaching the database.

Cost Effective Security and Compliance with
Oracle Database 11g Release 2
March 2011

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

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