

Database Security products

Oracle Database Vault (certified)

<http://www.oracle.com/us/products/database/database-vault-066514.html>

Oracle Database Vault helps organizations address regulatory mandates and increase the security of existing applications. Regulations such as Sarbanes-Oxley, Payment Card Industry (PCI) Data Security Standard (DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and similar global directives call for separation-of-duties and other preventive controls to ensure data integrity and data privacy.

- Safeguard application data stored in the Oracle database
- Implement separation-of-duty and other real-time preventive controls
- Prevent application-bypass with multi-factor policies

Oracle Audit Vault (certified)

<http://www.oracle.com/us/products/database/audit-vault-066522.html>

Oracle Audit Vault provides a secure and highly scalable audit warehouse, enabling simplified reporting, analysis, and threat detection on audit data. Organizations can enforce privacy policies, guard against insider threats, and address regulatory requirements such as Sarbanes-Oxley and PCI.

- Transparently collect and consolidate audit data
- Detect threats quickly
- Simplify compliance reporting

Oracle Advanced Security – TDE and Network Traffic Encryption (certified)

<http://www.oracle.com/us/products/database/advanced-security-066516.html>

With Oracle Advanced Security, customers can transparently encrypt all application data or specific sensitive columns, such as credit cards, social security numbers, or personally identifiable information (PII) by encrypting data at rest in the database as well as whenever it leaves the database over the network or via backups.

- Transparent encryption for Oracle database traffic, disk backups, and exports.
- Encrypt the entire tablespace or specific sensitive columns

Oracle Database Firewall (interoperable)

<http://www.oracle.com/us/products/database/database-firewall-160528.html>

Oracle Database Firewall monitors database activity on the network to help prevent unauthorized access, SQL injections, privilege or role escalation, and other external and internal attacks - all in real time.

- Block, substitute, alert and pass, or log unauthorized SQL
- Monitor for unauthorized use of local console, keyboard or remote session
- Heterogeneous database activity consolidated into a centralized database for reporting

Oracle Label Security

<http://www.oracle.com/us/products/database/label-security-066519.html>

Oracle Label Security manages access to data on a "need to know" basis in order to protect data privacy and achieve regulatory compliance.

- classify every row in a table, ensuring restricted access to sensitive data
- Provides a policy-based administration model to establish custom data classification

Oracle SecureFiles (certified)

<http://www.oracle.com/technetwork/database/features/secure-files/index.html>

SecureFiles is specifically engineered to deliver high performance for file data comparable to that of traditional file systems while retaining the advantages of the Oracle database. SecureFiles offers the “best-of-both-worlds” architecture from both the database and filesystem worlds for storing unstructured data.

- Compression
- Encryption
- Advanced Logging

Oracle Fine Grained Auditing (certified)

<http://www.oracle.com/technetwork/database/focus-areas/security/index-083815.html>

Fine Grained Auditing (FGA), introduced with Oracle9i, can be understood as 'policy-based auditing'. As opposed to the standard auditing functionality, FGA lets you specify the conditions necessary for an audit record to be generated. Audit trail records created by Fine Grained Auditing can be captured and analyzed in **Oracle Audit Vault**, automatically alerting the security team about possible malicious activity.

Oracle Enterprise Manager

Oracle Data Masking (interoperable)

<http://www.oracle.com/us/products/database/data-masking-161222.html>

With Oracle Data Masking, sensitive information such as credit card or social security numbers can be replaced with realistic values, allowing production data to be safely used for development, testing, or sharing with out-source or off-shore partners for other non-production purposes.

- De-identifying sensitive data is critical technology in data privacy protection
- Use production data freely in non-production environments
- Masking rules defined once, then applied for every non-production refresh

Real User Experience Insight (interoperable)

<http://www.oracle.com/technetwork/oem/uxinsight/realuserexperienceinsight-085193.html>

Oracle Real User Experience Insight helps identify lost revenue from frustrated users, reduce support costs by lowering call center volumes, accelerate problem resolution of poorly performing applications, and help businesses adapt to changing needs by providing insight into business trends and user preferences. It integrates performance analysis and usage analysis into a single offering, enabling business and IT stakeholders to develop a shared understanding into their application users' experience.

ORACLE IDENTITY MANAGEMENT SOLUTIONS

Oracle Access Manager (certified)

<http://www.oracle.com/us/products/middleware/identity-management/oracle-access-manager/index.html>

Oracle Access Manager provides an identity management and access control system that is shared by all your applications. The result is a centralized and automated single sign-on (SSO) solution for managing who has access to what information across your entire IT infrastructure.

- Identity administration combined with access control
- Apply access security with scalability and high availability
- Strong authentication for secure access control

Oracle Adaptive Access Manager (interoperable)

<http://www.oracle.com/us/products/middleware/identity-management/oracle-ada-access-mgr/index.html>

Oracle Adaptive Access Manager 11g provides superior protection for businesses and their customers through strong yet easy-to-deploy multi-factor authentication and proactive, real-time fraud prevention.

- Easy-to-deploy multifactor authentication
- Install, manage, and create security snapshots and delegate administration to reduce costs and simplify fraud prevention
- Risk analysis can trigger real-time alerts and follow-up actions

Oracle Directory Services

Oracle Internet Directory (certified)

<http://www.oracle.com/technetwork/middleware/id-mgmt/overview/index-082035.html>

Oracle Internet Directory is a LDAP v3 compliant directory with meta-directory capabilities. It is built on the industry leading Oracle database and is fully integrated into Oracle Fusion Middleware and Oracle Applications. Thus, it is ideally suited for Oracle environments or enterprises with Oracle database expertise.

NOTE: all links are public oracle.com links.

Oracle Virtual Directory (interoperable)

<http://www.oracle.com/technetwork/middleware/id-mgmt/index-093158.html>

Oracle Virtual Directory provides Internet and industry-standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations. This accelerates the deployment of applications and reduces costs by eliminating the need to constantly adapt those applications to a changing identity landscape as user populations are added, changed, or removed.

Oracle Identity Federation (interoperable)

<http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-federation/index.html>

(This applies to discussions about SAML for user identity, especially cloud integration)

Oracle Identity Federation 11g provides a flexible multi-protocol federation server that can be deployed with your existing identity and access management systems. With its support for leading standards-based protocols, it ensures the interoperability to securely share identities across vendors, customers, and business partners without the increased costs of managing, maintaining, and administering additional identities and credentials.

- Create trusted relationships between partners and agencies
- Simplify the integration process between business domains with open architecture
- Accelerates federation by enabling identity providers and service providers to connect seamlessly

Oracle Identity Manager (certified)

<http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-manager/index.html>

Oracle Identity Manager 11g is the role and user administration solution that automates the process of adding, updating, and deleting both user accounts and attribute-level entitlements across enterprise resources.

- Multiple connectors for the administered resources
- Comprehensive auditing and reporting features
- Sophisticated workflow for approvals (multiple and automatic) and lifecycle

Oracle Information Rights Management (interoperable)

<http://www.oracle.com/us/products/middleware/content-management/information-rights-mgmt/index.html>

Oracle Information Rights Management 11g secures and tracks sensitive digital information everywhere it is stored and used. Oracle Information Rights Management uses encryption to extend the management of information beyond the repository.

- Control, audit, and revoke access to information and track usage
- Destroy remote content based on business rules
- Expire out-of-date content and redirect users to updated content

Oracle Web Services Manager (interoperable)

<http://www.oracle.com/us/products/middleware/identity-management/oracle-web-services-mgr/index.html>

Oracle Web Services Manager is a J2EE application designed to define and implement Web services security in heterogeneous environments, provide tools to manage Web services based on service-level agreements, and allow the user to monitor runtime activity in graphical charts.

- Define and enforce access control policies for Web services
- Implement security with minimal disruption to existing applications
- Protect any Web service regardless of the platform

Oracle Web Cache (interoperable)

<http://www.oracle.com/technetwork/middleware/ias/index-089317.html>

Oracle Web Cache is a content-aware server accelerator, or reverse proxy, for the web tier that improves the performance, scalability, and availability of Web sites.

NOTE: Request Filtering - Oracle Web Cache provides request filtering. With request filtering, Oracle Web Cache can detect and reject unwanted or malformed requests or can validate legal requests without ever reaching the application.

Oracle Web Cache 11g Overview (see page #8)

<http://www.oracle.com/technetwork/middleware/ias/webcache11goverview-128137.pdf>

Oracle Sun iPlanet Web Proxy Server (interoperable)

<http://download.oracle.com/docs/cd/E19392-01/816-6143-10/filters.htm>

The proxy server provides the capability to use a URL filter file to determine which URLs the server supports. For example, instead of manually typing in wildcard patterns of URLs to support, you can create one text file that contains URLs you want to restrict. This feature lets you create one file of URLs that you can use on many different proxy servers.

- Use a file of URLs to configure what content the proxy server retrieves
- Filter URLs based on their MIME type
- Use regular expressions in each of the three sections: protocol, host:port, and path/filename
- Block file uploads and other requests
- Remove outgoing headers from the request

ORACLE GOVERNANCE, RISK and COMPLIANCE

Application Access Controls Governor (certified)

<http://www.oracle.com/us/solutions/corporate-governance/access-controls/index.html>

Oracle Application Access Controls Governor provides real-time monitoring and proactive enforcement of crucial access policies, such as those that support segregation of duties (SOD). The system anticipates potential SOD conflicts before they arise, and even prevents any assignment of roles or responsibilities within an application that would compromise proper segregation of duties. Application Access Controls Governor also extends key access controls to "super-users" and temporary or contract workers.

- Real-time monitoring and enforcement of SOD controls
- Simplify SOD maintenance through automated simulation and remediation
- Comprehensive library of best practice SOD controls

Enterprise Transaction Controls Governor (certified)

<http://www.oracle.com/us/solutions/corporate-governance/transaction-controls/index.html>

Oracle Enterprise Transaction Controls Governor continuously monitors transactions against policies to detect suspicious transactions or redundant business practices that get in the way of performance. By spotting anomalies in everyday transactions, the system prevents cash leakage. Escalation of risk, fraud, and costly remediation are avoided.

- Increase visibility into the actual operations of the controls environment
- Mitigate exposure to error, misuse, and fraud from out-of-policy business transactions
- Create policies and analyze controls using an intelligent and interactive interface

NOTE: all links are public oracle.com links.