Solution Brief

Assess. Design. Build. Manage.

Oracle Database Security Services

BUSINESS CHALLENGES

Public announcements of major IT security breaches have become an almost daily occurrence. The causes of publicized breaches are diverse and include individual hackers conducting nuisance attacks, criminal elements aggressively searching for valuable personal information for identity theft, and even state-sponsored wholesale theft of intellectual property. And even if a security breach is not the result of malicious action, many governing bodies have mandated reporting any accidental or innocent viewing of restricted data, often with costly consequences and loss of customer goodwill.

Most IT organizations have implemented strong policies to deny unauthorized access at the firewall level as well as thorough vetting of internal personnel and IT resources. However, this ignores the unfortunate reality that *as much as 80% of all security breaches occur within an organization's firewall.* Often these internal breaches occur because sufficient security hasn't been implemented within these firewalled boundaries, especially the database itself. Some of the demands of providing this intense level of security include, but are not limited to:

- An organization's sensitive data *must* be secured from unauthorized access at all times, including its initial capture through customer-facing applications, its transfer via public IP networks to the organization's IT systems, and its storage anywhere within that system.
- Anyone who accesses a system must be restricted to act only upon information relevant to that individual's security clearance. Additionally, once an individual's access has expired, those credentials must be revoked, and revocation evidence must be captured to prove regulatory compliance.
- Once an actor is permitted to access a system, access to sensitive data – especially the personal, medical, financial, or other privileged customer information - must be *audited* to prevent and track potential malicious use of that data.
- Application users that need access to *portions* of sensitive data for verification purposes – for example, the last four digits of a customer's credit card number – must be blocked from viewing those data in their entirety.
- Sensitive data should be encrypted so that it cannot be accessed even if application security is breached via exploits such as SQL injection. Encryption also prevents DBAs from accidentally accessing sensitive data stored within a database's physical structures.
- Even though their roles may demand access to representative production data, DBAs, QA managers, and application developers must be prohibited from viewing sensitive data during data loading, application development, and system testing.
- Finally, the guardians of any IT system must be guarded as well. When a trusted actor legitimately modifies security privileges within a system, those actions must be tracked and analyzed to detect and prevent possible collusion or malicious intent.

SOLUTION DESCRIPTION

Fortunately, Oracle Database technology provides multiple solutions to answer these security challenges. OnX provides proven solutions that leverage the broad range of Oracle Security and Advanced Security features:

- *Complete Security Review.* OnX will evaluate your organization's current security environment, following your transaction stream from customer facing applications through your IT systems' firewall and internal network, application servers, and eventually arriving at the Oracle database(s) that capture those transactions.
- *Database Security.* We will evaluate whether the appropriate recommended best practices are being leveraged throughout your Oracle database environment and assess the risks of any shortfalls due to either procedural or technology lapses, including:
    - Managing user identities for both application users as well as IT staff

- *Encrypting* network traffic as well as the sensitive data stored within an Oracle database and corresponding its backup and recovery components (e.g. RMAN backups, DataPump export dump files)
- *Implementing database security policies* to deny or compartmentalize access to / actions upon sensitive data within database objects
- *Auditing* for suspicious activity, regardless of source – either *outside* the firewall or *internal* to your IT organization
- *Masking / subsetting* of production data while cloning it for required testing and development

> Optionally, an IT organization's security can be evaluated through a *vulnerability assessment test* (VAT) provided through an independent team that purposefully attempts to breach security at several levels. Ideally, this evaluation should be conducted twice – both *before* and *after* improved security elements are implemented.

SOFTWARE ENVIRONMENT EXPERTISE

> Applications – Oracle E-Business Suite, PeopleSoft, Data Warehouse, Custom In-House, etc.

> Databases – Oracle 8i, 9i, 10g, 11g, 12c

> High Availability, Disaster Recovery, and Replication – Real Application Clusters (RAC), Automatic Storage Management (ASM), Oracle (Active) Data Guard, Oracle GoldenGate

KEY ORACLE SECURITY FEATURES

> *End-To-End Security.* Oracle provides the ability to secure a data element's lifespan within an IT system via SQL*Net-network encryption, Database Firewall, and various advanced security access methods, including token-based security.

> *Identity Management.* Oracle provides excellent methods to control access to IT systems through LDAP-compliant solutions such as Oracle Internet Directory (OID) and Microsoft Active Directory. Oracle also provides Oracle Identity Management services that control actors' access to systems while providing the necessary regulatory reporting for security governance..

> *Encryption.* The Oracle Database leverages state-of-the-art data encryption technology that complies with recognized industry and government standards. Data can be encrypted at any level within the database, even down to individual columns within a table; database backup files and exported data can also be encrypted. Oracle offers several methods to generate retain encryption keys, including *Oracle Key Vault*.

> *Auditing.* Oracle automatically audits a highly-privileged actor's activities. S*tandard* auditing tracks use of specific privileges and actions against specific database objects, and *fine-grained auditing* (FGA) tracks actions against specific rows and columns within database tables. It's even possible to detect excessively-generous system and object privileges that haven't yet been used.

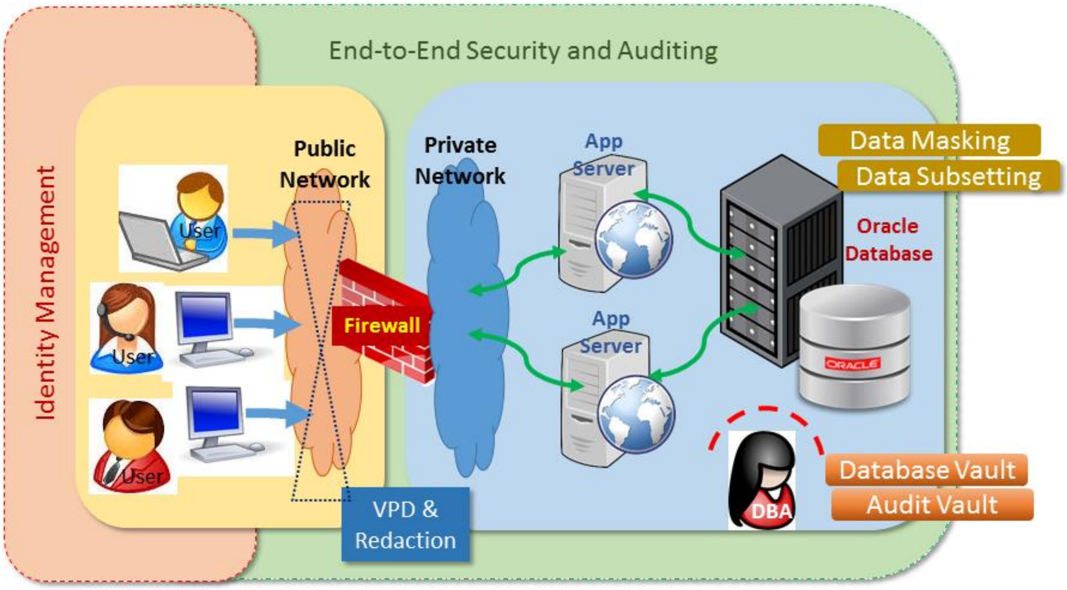
> *Virtual Private Database* (VPD) implements customizable security policies to deny access to sensitive data within database tables, and *Oracle Label Security* provides row-level data security.

> *Data Redaction* offers several methods to edit-mask, hide, or jumble production data at the point of application retrieval, thus limiting full access to only white-listed users.

> *Data Masking and Subsetting.* Oracle *Data Masking* enables creation of obfuscated copies of production data so it can be used for testing and evaluation, while *Data Subsetting* offers the ability to capture smaller portions of production data for more focused testing purposes – all without ever exposing sensitive data to application developers, QA testers, or DBAs.

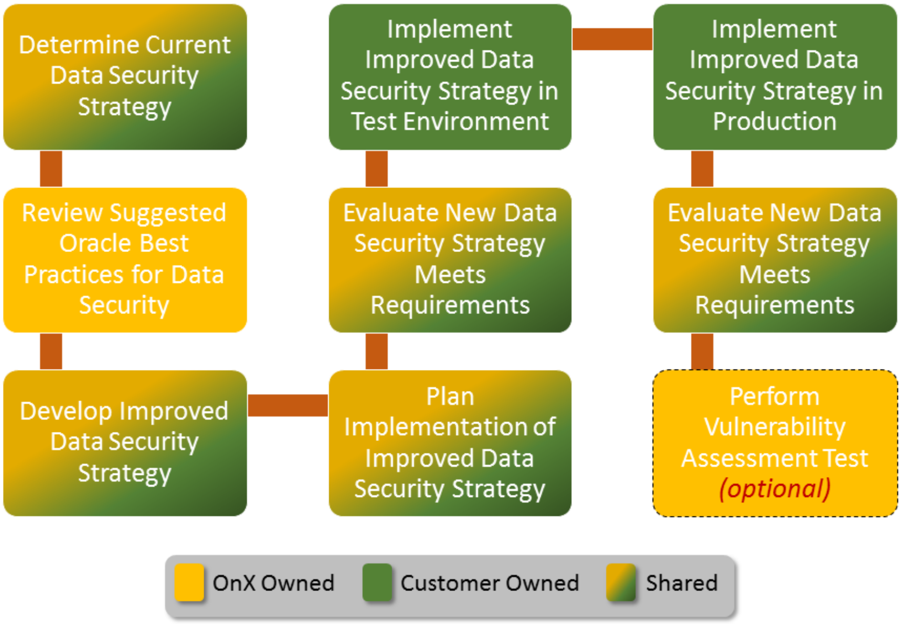
> To "guard the guards," Oracle's *Audit Vault* prevents privileged users from tampering with audit logs in an attempt to hide suspicious behavior, and *Database Vault* prevents DBAs from viewing the very data that they are handling.

The illustration below shows how these Oracle Security features interact within a typical IT system:



DATABASE SECURITY: EVALUATION AND IMPLEMENTATION APPROACH

The OnX team provides a broad range of Oracle solution service offerings for evaluating and implementing an appropriate yet robust security solution for our customers. These proven solutions combine industry standards, Oracle recommended best practices, and on-staff expertise to provide an optimal solution for your organization's required level of security. They consist of well-designed, tested, and documented reference architectures, configurations, and implementation services for varied Oracle environments. As a part of every deployment, the OnX team works with its clients and their stakeholders to develop, test, and implement an optimal security environment to meet your needs. A typical security evaluation and implementation scenario will include many or all of the activities shown below:


Determine Current Data Security Strategy
Review Suggested Oracle Best Practices for Data Security
Develop Improved Data Security Strategy
Plan Implementation of Improved Data Security Strategy
Evaluate New Data Security Strategy Meets Requirements
Implement Improved Data Security Strategy in Test Environment
Implement Improved Data Security Strategy in Production
Evaluate New Data Security Strategy Meets Requirements
Perform Vulnerability Assessment Test (optional)
OnX Owned
Customer Owned
Shared

SOLUTION VALUE

Once an appropriate data security plan has been implemented, it should be transparent to an organization's application user community. However, it's not unusual for the entire organization to realize collateral benefits as well. OnX's proven data security solutions consist of jointly designed, tested, and documented reference architectures, configurations, and implementation services for Oracle application and database environments. The benefits obtained include, but are not limited to:

- **Minimized risk** of data theft, both from outside the firewall by malicious actors as well as within the firewall by comprised employees and subcontractors
- **Improved detection and reporting** of external threats as well as potentially suspicious behavior, including documented evidence of actual maleficent behavior should criminal action be warranted against internal resources
- **Improved regulatory compliance and reporting** for government and industry security mandates (e.g. Sarbanes-Oxley, California S.B. 1386, UK Data Protection Act) should such reporting be necessary
- **Improved ROI** by leveraging the full functionality of licensed Oracle data security features and technologies
- **Increased productivity** by transferring knowledge OnX's Oracle data security expertise to your IT staff

RELATED SERVICES

OnX can assist you in any and every phase of project lifecycle. Whether you need help to design, provision, integrate, upgrade, or optimize your infrastructure, we have the right resources with just the skills and expertise you need. OnX offers a complete portfolio of related services, including assessments, planning and design, implementation, and troubleshooting and support services:

- Database Health Check
- Oracle Cloud Services
- Oracle Database Migration or Upgrade Planning Workshop
- Oracle Database Performance Tuning Services
- Oracle Database Upgrade Services
- Oracle GoldenGate Services
- Oracle Backup and Recovery Solution Services
- Oracle Database Disaster Recovery Services
- Oracle ZFS Services
- Oracle Engineered Systems Services
  - Exadata Configuration Services
  - Exadata Migration Services
  - Exadata Optimization Services
- Application Services
  - Application Testing and Optimization Services
  - Application Lifecycle Management Testing-as-a-Service
  - Enterprise Service Management Assessment

PROJECT MANAGEMENT

OnX includes project management as part of all projects to manage the overall project team, create and maintain the project plan, communicate status on a recurring basis and facilitate escalations as needed. This helps to minimize risks and ensure timely and successful service delivery. Additionally, OnX maintains a knowledgebase of "lessons learned" comprised of feedback from all service deliveries to help prevent unforeseen delays and other impact on the project.

WHY ONX?

> We have proven our success by delivering over 1,100 projects annually.

> Our experience designing and integrating enterprise data center solutions gives our clients access to skills and expertise beyond their in-house IT teams and traditional resellers.

> OnX’s industry certifications across a broad selection of best-in-class IT manufacturers and technologies gives us access to information, tools, techniques, and enablement beyond those available to in-house IT teams.

> OnX utilizes its acknowledged industry, OEM, and IT best practices to capture lessons learned during each engagement to reduce client risk.

> OnX applies its professional methodology and project management experience to each and every project.