Data Protection for Oracle Cloud Data Warehousing

Software Solution Discovers, Audits, Masks and Secures Data in OCI and On Premise

BENEFITS

Prevents data breaches and compliance violations

Automation improves protection, cost-efficiency and productivity

Complements and extends Oracle database security

Deploys quickly and easily offering fast time-to-protection

Supports OCI, hybrid and on-premises data warehouses

FEATURES

Automatically discovers sensitive data

Automatically creates data masking and access policies

Enforces sensitive data masking and data access policies in real-time

Audits user, application, query and data usage

Integrates with SIEM and other security systems

Alerts staff in real-time to threatening or suspicious behavior

For more information visit http://www.teleran.com

Data Warehouse and Analytics Protection Challenges

Data warehouse usage patterns are unpredictable and complex. They are accessed by powerful analytical applications that enable users to circumvent native database security controls through inferencing, brute force, and other techniques.

Discover, Audit, Mask and Protect Sensitive Data

Teleran's data protection software is specifically designed to address the unique vulnerabilities of data warehouses. It delivers three critical capabilities: 1) Discovering sensitive data such as personal identifiable information (PII). 2) Providing auditing of sensitive data access. 3) Delivering dynamic data masking and granular access controls that prevent unauthorized or suspicious transactions from any ad-hoc access tool or application. Teleran's solution addresses data privacy regulations like PCI, HIPAA, CCPA, GDPR and others.

Data Protection for Oracle Cloud Data Warehouses

- **Automated PII Discovery** identifies sensitive data in databases related to leading data privacy regulations
- **Automatically Creates Sensitive Data Masking and Access Control Policies** integrated with Discovery process
- **Closes Native Database Gaps** by preventing inferencing or brute force attacks that database masking functions do not address
- **Continuous Auditing** tracks PII access by user, query, and application
- **Patented Real-time Policy Action Engine** dynamically masks sensitive data or prevents inappropriate and non-compliant data access
- **Automated Alerting** communicates real-time warnings to security staff
- **Network Agent** installs quickly and requires no performance degrading "in-the-database" agents or monitors