

VNA-SB-038 | Zero-Trust Identity (Entra/Okta VPD) & SLED Cooperative Procurement | Zero-Trust SSO & Row-Level Security (VPD / RAS) | Redwood Sandstone

Microsoft Entra ID & Okta SSO Federation + Row-Level Security (VPD / RAS) for Oracle & APEX

Transition from Database-Account Logins, Shared Passwords & Unfiltered Table Access in Legacy Oracle Apps to Entra ID / Okta OIDC/SAML Federation + Oracle Real Application Security (RAS) / VPD + Audit with automated binary/AST metadata profiling, deterministic cost-control levers, auto-generated BRD and test documentation, and a fixed-fee 4-phase delivery roadmap.

Search Queries & Scope Covered: oracle apex microsoft entra id sso | okta saml oidc oracle apex authentication | oracle virtual private database vpd apex | oracle real application security ras multi tenant

SOURCE LEGACY STACK (STACK X)		MODERNIZED TARGET ARCHITECTURE (STACK Y)	
Database-Account Logins, Shared Passwords & Unfiltered Table Access in Legacy Oracle Apps		Entra ID / Okta OIDC/SAML Federation + Oracle Real Application Security (RAS) / VPD + Audit	
SSO/MFA CUTOVER	ROW-LEVEL ISOLATION	SHARED DB PASSWORDS	AUDIT TRAIL
2 Weeks	100% DB-Enforced	Eliminated	End-to-End

1. Problem Space & Architectural Bottlenecks

- Critical business operations remain trapped in Database-Account Logins, Shared Passwords & Unfiltered Table Access in Legacy Oracle Apps, creating audit risk, manual reconciliation overhead, and rising support costs.
- Duplicate queries, cloned reports, and undocumented triggers make impact analysis slow and expensive across secured database tables & multi-tenant views.
- Lack of automated binary-to-database metadata mapping causes traditional consulting shops to pad estimates with 40% manual discovery buffers.
- Leadership needs a predictable, fixed-fee phased timeline with verifiable test specifications and zero-downtime cutover guarantees.

2. Technical Solution & Reference Architecture

- 2.1 Automated Phase 0 AST & binary scan mapping Database-Account Logins, Shared Passwords & Unfiltered Table Access in Legacy Oracle Apps artifacts directly to live Oracle dictionary metadata and profiling production data.
- 2.2 Target architecture built on Entra ID / Okta OIDC/SAML Federation + Oracle Real Application Security (RAS) / VPD + Audit, consolidating cloned queries into governed core SQL views with runtime Smart Filters.
- 2.3 Automated generation of full Business Requirements Documents (BRD), Technical Approach Docs, Testing Specifications, and Verified Test Results.
- 2.4 Zero-trust SSO/MFA (Entra ID / Okta) paired with database-enforced row-level security (VPD / RAS) and SQLcl Liquibase CI/CD pipelines.

3. Artifact-by-Artifact Conversion & Modernization Matrix

Legacy Artifact / Baseline Workload	Modernized Oracle / Cloud Target	Engineering Method & Outcome
Source Tier: Database-Account Logins, Shared Passwords & Unfiltered Table Access in Legacy Oracle Apps	Entra ID / Okta OIDC/SAML Federation + Oracle Real Application Security (RAS) / VPD + Audit	Automated AST & Metadata Uplift (85%-95%)
Primary Footprint: Active Internal & External Application Users	Oracle APEX 24.2 Redwood UI + PL/SQL APIs	Binary-to-DB Metadata Mapping + Pilot Sprint
Workload & Queries: Secured Database Tables & Multi-Tenant Views	Canonical Core SQL Views + Runtime Smart Filters	Query Fan-Out Clustering (75%-90% Reduction)
Undocumented Legacy Business Rules & QA	Auto-Generated BRD, Approach Doc, Test Specs & Results	100% Automated Documentation & utPLSQL / Playwright

4. Oracle APEX & Ancillary Engineering Toolchain

- Oracle APEX 24.2 & Universal Theme (Redwood Light Flavors)
- Oracle Database 23ai / Autonomous Database (ATP / ADW)
- Viscosity Automated Binary (.fmb/.rdf) & AST Metadata Profiler
- Auto-Doc Engine (BRD, Approach Doc, Test Specs & Test Results)
- Oracle REST Data Services (ORDS) & APEX Office Print (AOP)
- SQLcl Liquibase CI/CD, utPLSQL & Playwright Regression Suites

Anonymized Production Proof: Implemented Microsoft Entra ID (Azure AD) single sign-on, role-based access control, and database-enforced row-level security for an international life-sciences laboratory platform on Oracle APEX.

5. Principal Architect Q&A

Q: What are the primary levers that control the cost of Entra ID / Okta SSO + Oracle VPD & RAS?

A: Cost is controlled by five levers: (1) collapsing cloned query fan-out across secured database tables & multi-tenant views into canonical core SQL views, (2) percentage of business logic already in database packages vs. UI triggers, (3) production data quality profiled during Phase 0, (4) external integration/SSO count, and (5) cutover downtime requirements.

Q: How does your tool convert binaries (.fmb, .rdf, etc.), map database metadata, and generate documentation?

A: Our automated analyzer parses legacy binaries and source files, extracts every trigger, query, and UI control, cross-references them against live database dictionary metadata (ALL_TAB_COLUMNS, ALL_DEPENDENCIES), profiles actual column data distributions, and automatically generates the Business Requirements Document (BRD), Technical Approach Doc, Test Specifications, and Verified Test Results.

Q: What does a typical project timeline look like from kickoff to production cutover?

A: Projects follow four gated phases: Phase 0 (Weeks 1-2: Binary AST Scan, Data Profiling & Auto-Generated BRD), Phase 1 (Weeks 3-6: Core Schema Uplift & Working Pilot), Phase 2 (Weeks 7-12: Automated Conversion Sprints & Test Spec Execution), and Phase 3 (Weeks 13-16: Parallel Run, Zero-Downtime Cutover & 30-Day Hypercare).