ORACLE

Oracle Database Security Central: Unified visibility, policy control, and investigation across the database estate

Unify user risk, sensitive data, configuration posture, and policy governance in one control plane.

August, 2026, Version [1.0]

Modern database estates span on-premises, cloud, and multi-cloud environments, yet security teams still rely on siloed tools to manage risks with users, sensitive data, configurations, and data governance policies. As a result, they are often forced to assess risk, review security posture, and apply security controls one database at a time, making it difficult to detect risk exposure across the fleet, enforce policy consistently, and operate at scale.

Oracle Database Security Central (Security Central) provides centralized visibility to risk and controls across the database estate, aligns security policies across the fleet, and converts findings into prioritized actions. It specifically delivers a 360-degree view of users, data, configuration, and security posture, combined with unified policy management and a more resilient deployment model.

For customers, this can help surface higher-risk conditions where privileged access, sensitive data, configuration weaknesses, and suspicious activity overlap. The resulting context can support faster investigations, more informed remediation decisions, reduced database security exposure, and ongoing preparation for regulatory and internal control reviews.

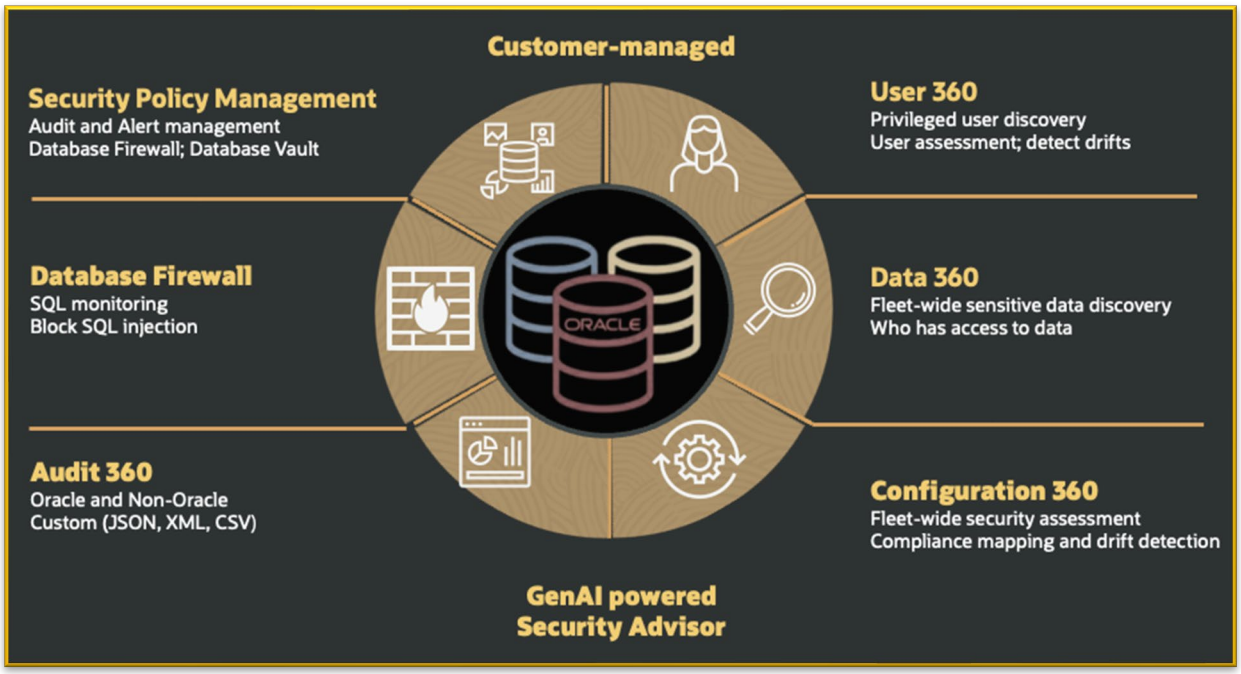

Figure 1. Oracle Database Security Central

Key Features and Benefits

Broader visibility

User360, a core capability within **Oracle Database Security Central**, helps teams understand user risk across the fleet. It identifies privileged and high-risk users, maps direct and indirect access paths, surfaces stale and dormant accounts, and tracks entitlement drift over time so reviews can focus on the users that create the most exposure.

Data360, a core capability within **Oracle Database Security Central**, extends to fleet-wide sensitive-data visibility. It discovers sensitive data across the estate and applies repeatable classification methods to more than 181 sensitive data types, helping teams identify and protect the same data consistently across environments.

Configuration360, a core capability within **Oracle Database Security Central**, adds continuous security posture visibility across the fleet. Teams can define baseline settings, detect drift, map findings to frameworks such as CIS, DISA STIG, or GDPR, and prioritize the issues that increase exposure.

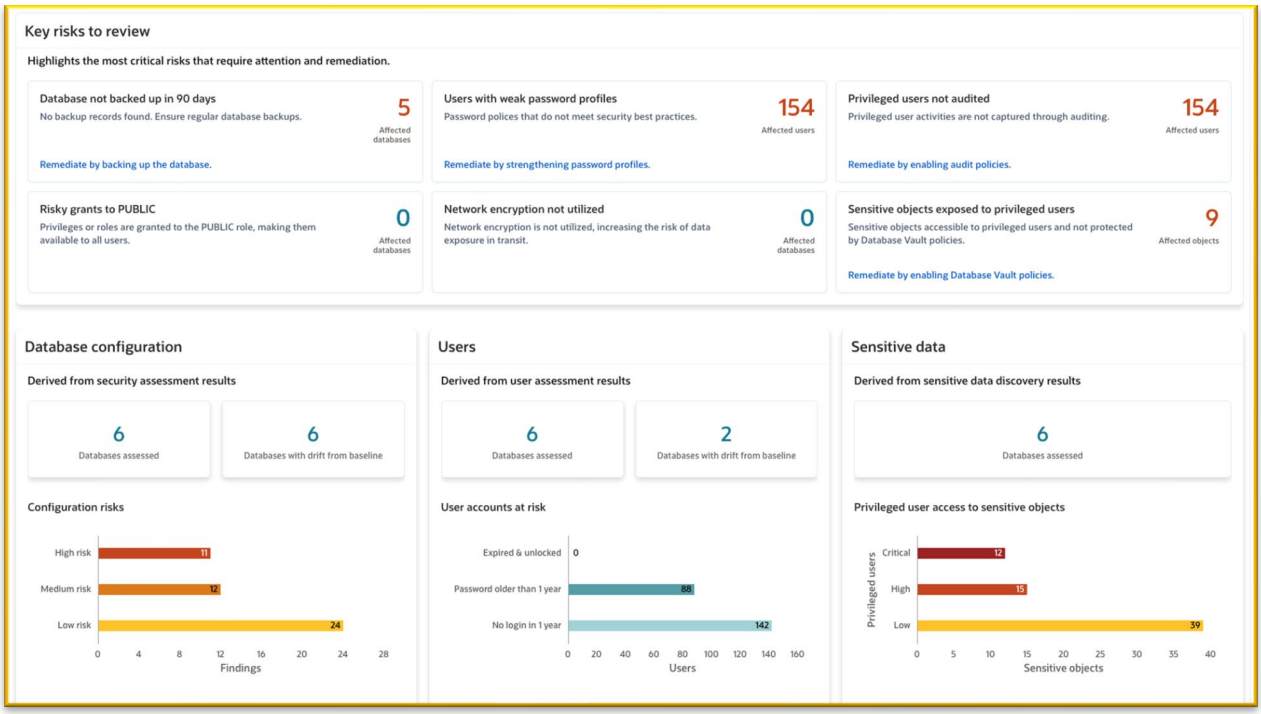

Figure 2. Broader Visibility

Stronger control and prevention

With full visibility and drift tracking for users, data, and configurations, you can apply consistent controls to monitor, detect, and prevent policy violations across the database fleet. Security Central combines periodic risk assessment with continuous monitoring, giving teams both a point-in-time view of risk and real-time visibility into database activity.

Unified Policy Management gives you one place to create, standardize, and enforce these policies across the estate. That helps reduce inconsistency, simplify policy administration, and apply the same control intent more consistently across many databases. With the unified policy console, you can create, deploy, and retire audit, alert, Database Vault, Database Firewall, and SQL Firewall policies across the Oracle fleet. Create, deploy, and retire alert and Database Firewall policies across the Oracle and non-Oracle database fleet.

Security Control Center brings together user activity, user entitlements, data discovery results, and posture findings, correlating these signals to quantify fleet-wide risk and guide more effective remediation. Instead of reviewing each finding in isolation, teams can identify the combinations that matter most, for example, a high-risk user with access to sensitive data on a system that has drifted from baseline.

Database Firewall inspects SQL with a patented grammar-based engine and uses source, program, and DB/OS user context to enforce trusted paths, alert on suspicious access, and block unauthorized SQL, including SQL injection attacks, before it reaches the database. Database Firewall delivers near-zero overhead in blocking mode, less than 100 microseconds per SQL statement, even at high throughput.

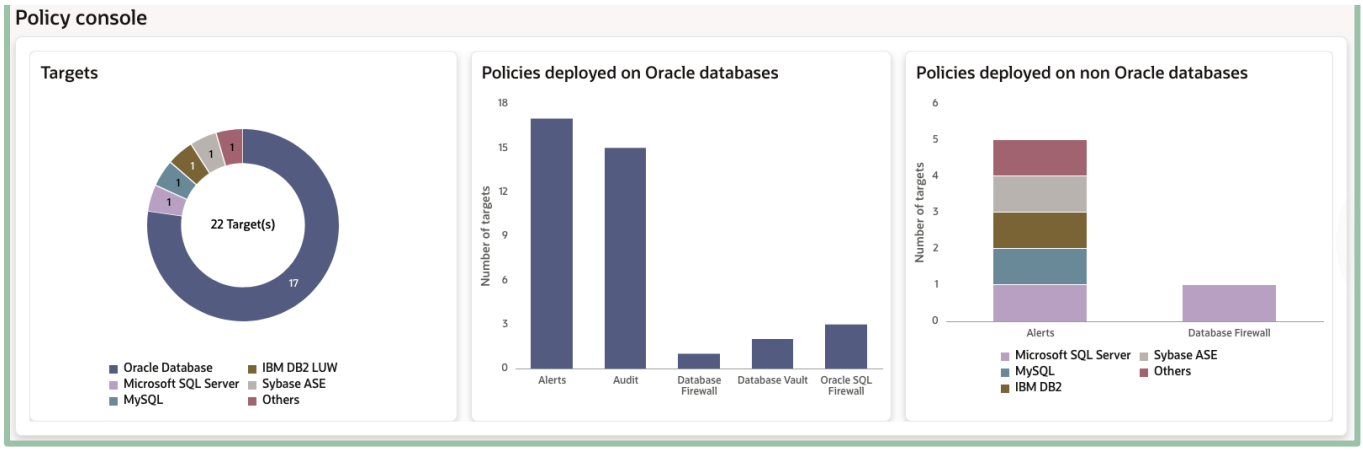

Figure 3. Unified Policy Console

Centralized evidence for investigation and compliance

Through self-service **compliance dashboards** and mapped assessments, the team can sustain audit readiness continuously instead of assembling evidence only at audit time by providing pre-defined reports for GDPR, PCI, GLBA, HIPAA, IRS 1075, SOX, and UK DPA, and by mapping security assessment findings to standards like DISA STIG and CIS with CVE visibility to prioritize remediation, helping organizations manage ongoing audits efficiently.

For investigations and day-to-day oversight, Security Central also offers out-of-the-box activity reports with interactive filtering and Audit Insights, scheduling, PDF/XLS export, and self-audit reporting.

AI Advisor and Assistant

AI Advisor in Oracle Database Security Central enables natural language queries across user activity, risk, and compliance posture, while also providing step-by-step guidance for security configuration and management tasks. Policy-based alerts help teams identify suspicious activity with more precise, lower-noise detection. AI Assistant allows administrators to define alert conditions in natural language and automatically translates intent into structured policy logic that can be applied directly, helping reduce false positives, simplify policy creation, and minimize manual errors.

Existing Oracle Audit Vault and Database Firewall (AVDF) customers

Security Central builds on Oracle Audit Vault and Database Firewall (AVDF), preserving secure audit collection across Oracle and non-Oracle databases, operating systems, directories, and custom audit sources in XML, JSON, and CSV; patented grammar-based Database Firewall for SQL-aware prevention; and reporting, alerting, and compliance dashboards. It helps teams move from isolated findings to prioritized action by correlating risk across the fleet. For existing AVDF customers, Security Central extends the platform into a broader security command center model.

Deploy and operate securely across hybrid estates

Oracle Database Security Central is delivered as a preconfigured software appliance for consistent deployment and governance across hybrid estates

Deployment options: x86-64 infrastructure (on-premises), OCI Marketplace images, Virtual Image, AWS, and Azure cloud (image-based).

High availability and resilience: Oracle Real Application Cluster enabled architecture for high availability, adds automatic failover and load balancing.

Operations and automation: CLI automation**,** automated retention and archival via lifecycle policies

Ecosystem integrations: Open schema integration with pull method, syslog integration for SOC/SIEM integrations. SSO support from the IdPs.

Deployment model: Agent, Agentless, Remote Agent, Proxy, Out-of-Band

Supported target types: Oracle Databases, Microsoft SQL Server, MySQL, PostgreSQL, IBM Db2, and MongoDB. It can also collect audit data from operating systems, directories, and custom audit sources like XML, JSON, and CSV formats.

Getting started

- Explore the Security Central product page here
- Read the launch blog
- Read the detailed blog
- Try with Security Central LiveLabs

ORACLE

Connect with us

Call +**1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com facebook.com/oracle twitter.com/oracle