

# Veza for Oracle Applications

Modern Identity Security with Near Real-Time Access Control

Veza allows you to definitively answer the question of:

**Who** can take **what action** on **what resources**?

## Overview

Securing and managing access to Oracle applications is foundational for protecting sensitive data and ensuring compliance with regulatory standards. Organizations leveraging Oracle applications such as Oracle E-Business Suite (EBS), JD Edwards EnterpriseOne (JDE), Oracle Fusion Cloud ERP, and Oracle Databases often face challenges due to complex, siloed access control systems, overlapping **roles** and **responsibilities**, and the need to enforce least privilege across diverse environments. In addition, the constant need for continuous monitoring to prevent unauthorized access, privilege creep, and to maintain compliance with evolving regulations further complicates the process.

Veza offers a unified solution to achieve complete visibility, enforce least privilege, and streamline compliance across your Oracle environments.

## Challenges in Securing Access to Oracle Applications

Organizations face several challenges in managing access to their Oracle applications, including:



### Complex and siloed access control systems

Difficulty in understanding who has access to what, whether the access is appropriate, and ensuring that access controls are applied consistently across the environment.



### Unauthorized changes in user permissions

Organizations often lack the necessary tools to detect and respond to unauthorized changes or privilege escalation in real time.



### Over-permissioning and privilege abuse

Over-provisioned accounts and the inability to enforce least privilege lead to security risks and compliance gaps.



### Compliance management

Managing access in alignment with regulatory frameworks like SOX, PCI-DSS, GDPR, and internal policies can be a significant challenge.



## How Veza Solves These Challenges

Veza integrates directly with Oracle applications to provide deep visibility into **roles** and **responsibilities** associated with user access. With Veza's **Access Graph**, organizations can:

Automate access management

Enforce near real-time policy controls

Continuously monitor user activities to identify unauthorized access and reduce security risks

Veza provides the necessary tools to ensure organizations have complete control over who has access to Oracle applications and sensitive data.

## Key Benefits of Veza for Oracle Integrations



### Visibility & Control Over Access

Gain complete visibility into who has access to critical Oracle applications, including Oracle EBS, JDE, and Fusion Cloud ERP. Veza centralizes roles, responsibilities, entitlements, and access across Oracle environments.



### Enforcement of Least Privilege Access

Identify over-permissioned accounts and ensure users only have the access required for their roles. This reduces the risk of privilege abuse and ensures compliance with internal policies and external regulations.



### Continuous Monitoring & Alerts

Continuously track changes to user roles and responsibilities within Oracle applications. Receive real-time alerts for high-risk activities such as privilege escalation or unauthorized access, enabling swift responses.



### Streamlined Access Reviews & Compliance

Automate access certification and simplify the review process to ensure users have the appropriate access permissions. This aids in compliance with frameworks like SOX, GDPR, and other regulatory standards. Built-in reporting tracks changes over time for audit purposes.

## How Veza Enhances Access Control Across Oracle Applications

### Oracle E-Business Suite (EBS)

Managing **responsibilities** and roles in Oracle EBS can be complex due to its intricacy and the variety of permissions across different functions. With Veza, organizations can:

- Map **user responsibilities** and **roles** clearly within EBS
- Identify potential violations of separation of duties (SoD)
- Continuously monitor for privilege escalation and maintain compliance with internal and external audits

## JD Edwards EnterpriseOne (JDE)

JDE environments often have over-permissioned accounts, orphaned roles, and excessive permissions, increasing security risks. Veza helps by:

- Providing a comprehensive view of **user roles** and **responsibilities** across JDE
- Detecting orphaned accounts and reducing manual access reviews
- Enforcing least privilege by automating access management and audits, creating a more secure environment

## Oracle Fusion Cloud ERP

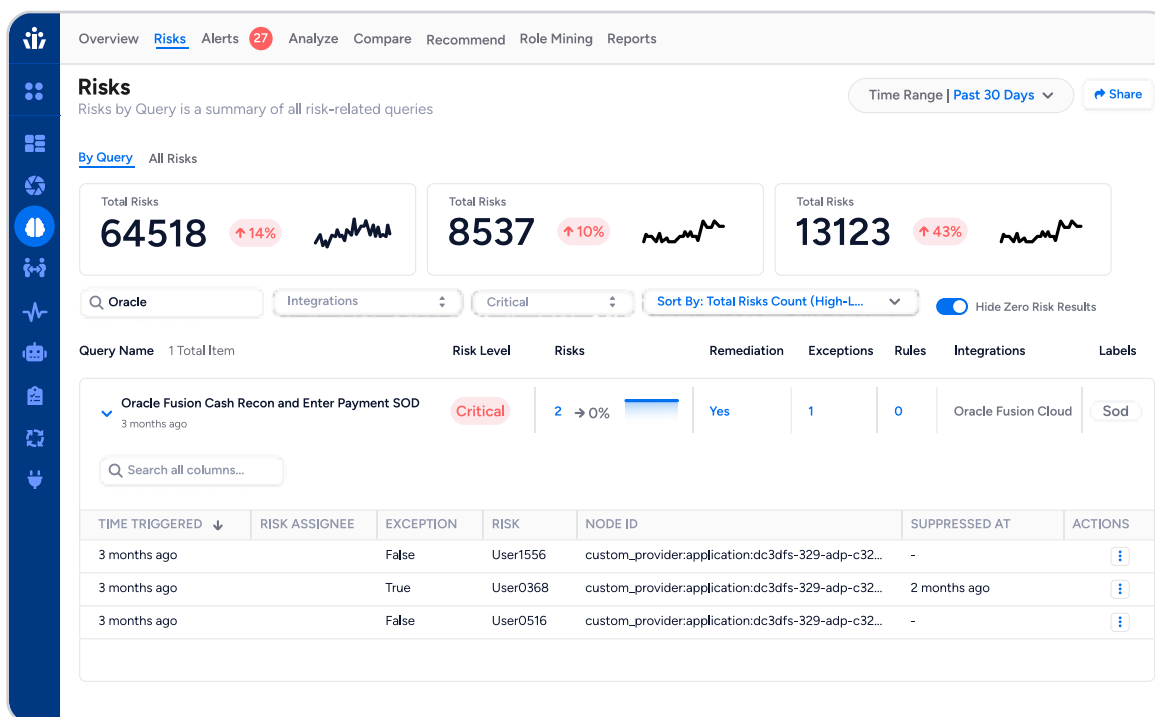
Transitioning to Oracle Fusion Cloud ERP requires strict access controls over sensitive data. Veza ensures:

- Near real-time monitoring of access to sensitive financial and customer data
- Identification and remediation of misconfigured **roles** and **responsibilities** leading to security gaps
- Policy-based access control to simplify governance and ensure compliance with GDPR, PCI-DSS, and other regulations

## Oracle Databases

For sensitive information stored in Oracle Databases, it's crucial to understand who has access, who can delete critical data, and how service accounts are configured. Veza helps by:

- Mapping **roles** and **responsibilities** related to sensitive data access
- Detecting inappropriate privilege assignments and unauthorized database access
- Ensuring compliance with internal access policies and external regulations



The screenshot displays the Veza Risks dashboard. At the top, there are tabs for Overview, Risks (selected), Alerts (27), Analyze, Compare, Recommend, Role Mining, and Reports. The Risks section shows a summary of risks by query, with three cards displaying total risks and percentage changes: 64518 (up 14%), 8537 (up 10%), and 13123 (up 43%). Below these cards are filters for Query (Oracle), Integrations, Critical, and Sort By (Total Risks Count (High-L...)). A toggle for 'Hide Zero Risk Results' is also present. The main table lists queries with columns for Query Name, Risk Level, Risks, Remediation, Exceptions, Rules, Integrations, and Labels. The first query is 'Oracle Fusion Cash Recon and Enter Payment SOD' with a Critical risk level and 2 risks. Below this, a table shows details for the query, including Time Triggered, Risk Assignee, Exception, Risk, Node ID, Suppressed At, and Actions.

TIME TRIGGERED	RISK ASSIGNEE	EXCEPTION	RISK	NODE ID	SUPPRESSED AT	ACTIONS
3 months ago		False	User1556	custom_provider:application:dc3dfs-329-adp-c32...	-	
3 months ago		True	User0368	custom_provider:application:dc3dfs-329-adp-c32...	2 months ago	
3 months ago		False	User0516	custom_provider:application:dc3dfs-329-adp-c32...	-	

# Seamless Integration with Veza's Platform

Veza integrates seamlessly with Oracle environments, whether on-premises or cloud-based.

## How It Works

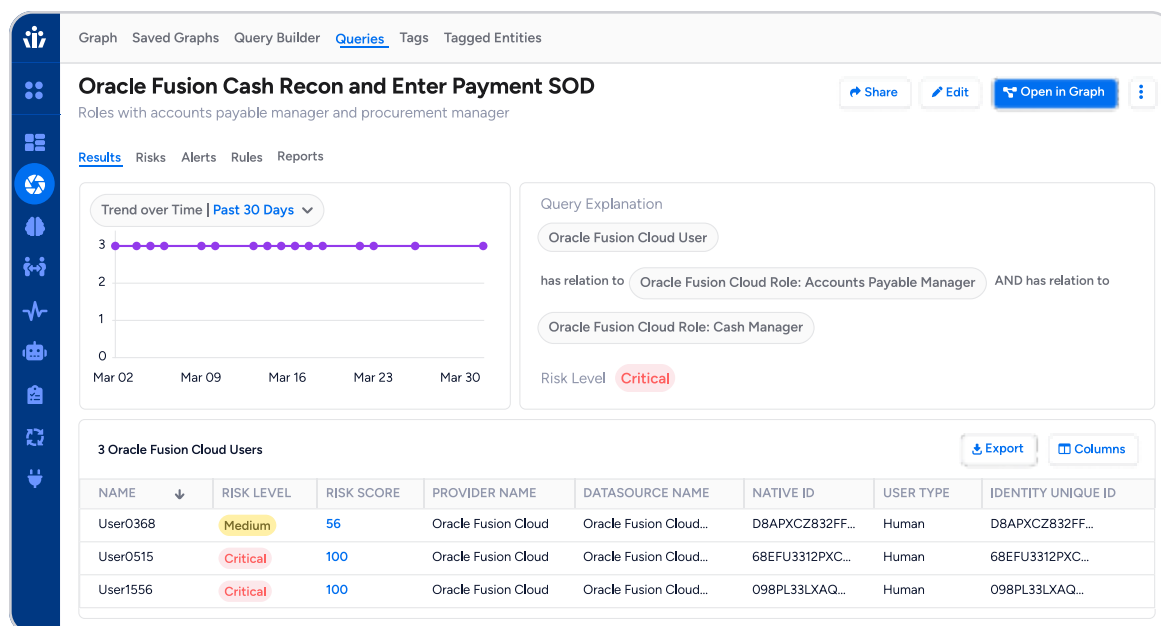
Transitioning to Oracle Fusion Cloud ERP requires strict access controls over sensitive data. Veza ensures:

- 1 Connect Veza to your Oracle applications via APIs or direct database connections.
- 2 Map roles and responsibilities within each Oracle application to gain full visibility into access permissions.
- 3 Implement access controls and policies via Veza's user-friendly interface to ensure users have the appropriate access level.
- 4 Monitor and report real-time on any changes to access or permissions, maintaining an audit-ready state.

## Next Steps: Explore Veza's Oracle Integrations

Ready to enhance your identity security posture with Veza's Oracle integrations? Whether securing Oracle EBS, JDE, Fusion Cloud ERP, or Oracle Databases, Veza provides the visibility and monitoring required to manage risk and compliance effectively.

To get started, reach out to our team to learn how Veza can integrate with your Oracle environment and help you implement best practices for identity security.



## Learn More About Veza

For more details, check out our platform page on [Veza Integrations](#).