

DATA SHEET

Data Masking & Auditing on Oracle E-Business Suite

Security & Compliance Tool Set

OVERVIEW

Securing Legacy & Cloud ERP Systems' Data

The way in which data is used for development work poses a new threat to the many companies using ERP software like Oracle E-Business Suite (EBS). As more modules are utilized (AR, AP, GL, SCM, MSC, CSI, XLA, CSC, etc.), the challenging of controlling what is sensitive and who is accessing it becomes more pervasive.

ennVee's security toolset safeguards your sensitive Oracle EBS data from being compromised by internal and external threats.

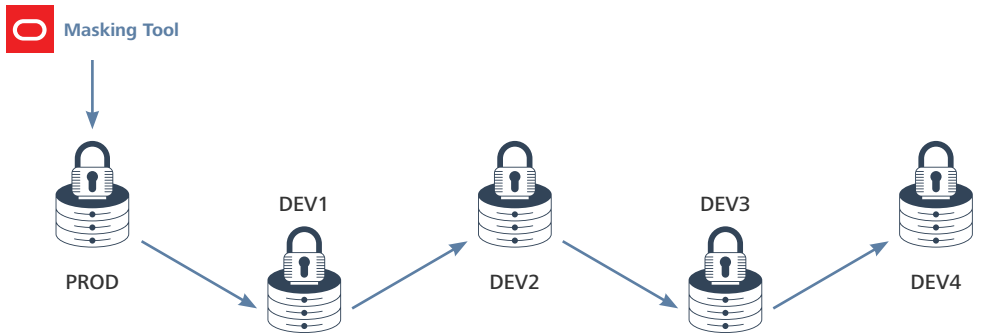
Data Masking on Oracle EBS

Our toolset is simple to build and use, and mindful of the sensitivity of your Oracle E-Business Suite systems data. Many industry-leading manufacturing, automotive, financial services, logistics and transportation customers have utilized ennVee's data masking capabilities and tool set to supercharge their data security practices.

Key Features

We have identified all tables and have logic to mask the data. Each company can determine the masking logic and data representation (if required.)

How It Works



A table list is generated and provides coverage for all data and use cases:

1. Installed on Prod
2. Will not execute on PROD (even if run by accident)
3. No additional changes required when new modules are implemented
4. Zero management overhead

- Easy setup: can be scheduled as concurrent programs on development after clone
- Logic ensures that data is always masked and on-schedule
- Less intrusive: runs in the background and the instance is always available during masking
- Supports Oracle EBS 11.5.10, R12.1.x, R12.2.x.

Coverage Areas

- Payment Card Industry Data Security Standard (PCI-DSS 2.0)
- State Privacy Regulations (employees, customers, vendors, etc.)
- HIPAA Privacy Standard/Rule

Auditing on Oracle EBS

Key Features

- Track access to tables, rather than mask
- Application-specific data ensures that we know who is allowed access and can allow them to track their activity
- No negative impact on performance and we have a report of everything
- Users are alerted when a violation occurs
- Builds a data access process
- One-hour implementation
- Requires one SOX individual to determine what can and cannot be done