Security Toolset

ennVee

Data Masking & Auditing on Oracle E-Business Suite

Securing Legacy & Cloud ERP Systems Data

Having a proper data masking practice can make or break an organization's longevity. While internal employees are typically required to sign data security agreements, it can be tasking to mark all "sensitive" data, and also to pinpoint the culprit in the event of a data breach.

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). Though many companies already mask certain data like credit card numbers, SSN, etc., there are volumes of data that companies do not consider to be sensitive. As more and 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 E-Business Suite data from being compromised by internal and external threats.

E-Business Suite Data Masking

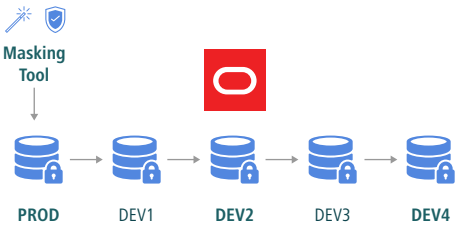
Our toolset is simple to build and use, and mindful of the sensitivity of your Oracle E-Business Suite systems data. Many industry-leading manufacturing, automotive, financial services, logistics and transportation customers have utilized ennVee's data masking capabilities and tool set to supercharge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

Highlights

- We have identified all tables and we have logic to mask the data.
  Every company can decide on masking logic, and data representation, if required.
- Simple setup, can be scheduled as concurrent programs on development after clone
- Our logic ensures that data is always masked and on-schedule
- Works on Oracle EBS 11.5.10, R12.1.x, R12.2.x
- Non-intrusive: runs in the background, meaning you will never have to worry about instance availability during data masking. While access to sensitive data is restricted to direct access, the instance is always available for usage.
- Additional areas of coverage: Payment Card Industry Data Security Standard (PCI-DSS 2.0), State Privacy Regulations (employees, customers, vendors, etc.), and HIPAA Privacy Standard/Rule

How it works

A table list is initially generated covering all data and use cases.



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

E-Business Suite Auditing

Highlights

- Track access to tables (rather than mask)
- Application-specific data: we know who is allowed access and allow them to track their activity. This does not affect performance and we have a report of everything. Users will receive an alert when a violation occurs.
- Builds a data access process
- 1 hour to implement, and 1 SOX individual to determine what can and cannot be done

ennVee
Worldwide Headquarters, 900 E. Diehl Road Suite 209, Naperville, IL 60563, USA
phone: 888.848.6059 email: sales@ennvee.com ennvee.com
linkedin.com/company/ennvee-technogroup-inc- facebook.com/ennveetechnogroup

Gold Microsoft Partner

ORACLE Gold Partner

ennVee is a professional services firm that provides systems integration, enterprise application management services, and industry-specific IT solutions. Since 2003, our team has grown to over 200 technology experts delivering results across industry verticals including Hi-Tech Manufacturing, Logistics and Transportation, Construction and Engineering, Retail, Public Sector, and Financial Services. We help our clients address complex business requirements by translating technology into solutions that impact, scale, and align both business and IT.