Maintaining Security Measures of Oracle Netsuite

Very often, companies tend to complain that their Netsuite application security settings not compliant as per requirements. There is a constant struggle in maintaining application security and sustaining them throughout. In reality, there are several factors that companies must take care of in order to maintain security in the right way. Some to mention are:

·	Understanding processes

·	Mapping processes to job functions

·	Connecting job functions to roles and permissions

·	Reviewing the **Segregation of Duties** Conflicts

If all these functions are taken care of, then the security setup can be maintained in the best possible way. Then the only thing left would be to monitor the above factors consistently. No matter what the situation is, we will define the steps that the company can follow to obtain the right security conditions and to maintain it well.

Today, the best scenario is a cloud-based enterprise solutions ready to use, with the need for bigger infrastructure for hardware, security, backups, or any type of disaster recovery.

However, this is a major concern - the security of the cloud-based enterprise solutions. If the company has all of its data, systems, and applications under control, then there are minimal chances of any compromise to their security.

For a leading cloud-based enterprise solution provider like Netsuite, it is important to have world-class security in order to gain customer trust and win the market competition. Sentri for Netsuite is one such solution that will be compromised on data security and compliance. Sentri for Netsuite provides robust AI-driven **SoD monitoring** with out of box. Sentri not only detects the conflict, but also uses proprietary data mining technology, to find the way in which the Segregation of Duty Conflicts.

Sentri for Netsuite works on an intelligent next-generation technology that helps the user to implement, upgrade, or re-implement the security policies irrespective of the environment. Sentri for Netsuite focuses on three main objectives - your workflows, administrative access, and finally the end-user security. It mitigates all security risks, it is being provisioned, ensuring that the security of data, systems, and applications is compromised.

Sentri for Netsuite offers various functionalities that benefit its users and offers holistic data security in all means.

1.	Segregations of Monitor Duties - Monitors, Identifies, and Prevents possible SOD violations across Netsuite environment.

2.	Access Provisioning and De-provisioning.

3.	Self-Service Access - Saves effort in manual approvals, and maintains access controls on cloud and on-premise

4.	Access Certification - Automate risk-based certification or quarterly certification.

A business is always vulnerable to internal threats. However, with a strong security backup like a Netsuite, they can provide a secure environment for their data, systems, and applications.

For more information about our products and solutions **www.sentriapp.com**

About the Author

About Sentri

Sentri is a one-stop solution to your **Identity Access Governance** (IAG), Integrated Risk Management (IRM) and Governance Risk Compliance (GRC) requirements. Our Intelligent Enterprise Identity Platforms are built to provide holistic data protection against data breaches, identity thefts, and financial frauds. We realize the value of a robust IT landscape, which acts as a strong spine for any business. To the business of the business, we offer path-breaking customizable access solutions that empowerment management, securing apps and data infrastructure for cloud and on-premise platforms.