APPSIAN

DATA SHEET

Best Practices for Securing PeopleSoft in a Mobile Environment

Enabling mobile access to PeopleSoft is a primary objective for many organizations. Naturally, there are security concerns when making transactions available on the internet.

Appsian has compiled a list of Best Practices as you approach your mobility project

Identity and Access Management Must Be Enhanced

- A username/password security model is not enough to effectively restrict unauthorized access. PeopleSoft passwords are inherently weak, easy to crack, and some users may have multiple passwords.

Align Authentication with an Identity Provider (IdP)

- This is typically accomplished with an enterprise Single Sign-On that is natively integrated with an IdP. For PeopleSoft, your IdP is the best authentication database because it is centrally provisioned and governed by your corporate password mandates.

Always Utilize Multi-Factor Authentication

- Multi-factor authentication is an effective method for verifying identity. While having this functionality at login should be a standard part of a security posture, it is recommended that an adaptive MFA be utilized.

- Adaptive MFA ensures that contextual attributes (ex. device, network, location) be the determining factor for deploying MFA challenges. This helps properly align levels of risk with access policies. Context of access varies in a mobile environment and your level of control should do the same.

Prevent the Unauthorized Exfiltration of Data

- Data leakage is the #1 cause of breaches. Data exfiltration becomes a greater risk when access is remote – mostly because devices are no longer regulated. Limiting the running of reports and queries when access is remote will help ensure data is not exfiltrated on an unauthorized device.
- Implementing masking on data fields will help limit the exposure of sensitive data.

Enhance Your Visibility into Data Access

- Simply put, if you are not logging access and usage data - then you're at risk. Having visibility into user behavior is critical in order to detect and remediate a security threat.
- Routine audits are critical for understanding what is happening inside your applications and if further steps need to be taken.

How Appsian Can Enable PeopleSoft for Mobile Access

Appsian delivers a sophisticated platform designed to give you complete control and visibility over your ERP data. We do this by:

Strengthening Your Ability to **Authenticate Users**

Strengthening Your Ability to **Manage Privileged Access**

Strengthening Your Ability to **Limit Data Exposure**

Strengthening Your Ability to **View User Activity**

Strengthening Your Ability to **Detect and Respond to Threats**

Appsian has enabled more than 250 PeopleSoft customers worldwide securely expand access to PeopleSoft. Let us show you how we can maximize your investment in PeopleSoft!

Visit www.appsian.com to Request Your Demonstration

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com