APPSIAN™

DATA SHEET

Dynamic Data Masking for PeopleSoft

Combine Contextual DLP Policies with Dynamic Data Masking for Fine-Grained Control Over Sensitive Data Exposure

Appsian Security Platform's dynamic data masking capabilities provide fine-grained control over which sensitive data fields can be masked for any specified user, in the context of any situation.

- Apply full, partial, and click-to-view masking or complete redaction to any data field in PeopleSoft
- Control unnecessary exposure of sensitive data for improved security and compliance
- Deploy flexible functionality that protects data without hindering usability

Contextual DLP Policies

- Configurable rules engine enforces policies to control access/exposure to any field, page, or component within PeopleSoft based on user and data attributes
- Field-level DLP controls require no code changes to PeopleSoft records
- Filters out sensitive data at the presentation layer, resulting in no additional maintenance requirements for PeopleSoft updates

Dynamic Data Masking and Redaction

- Deploy role-based and attribute-based policies for dynamic data masking
- Mask/Redact any field within in PeopleSoft based on the context of access
- Implement masking policies in prod. and non-prod. environments

Click-to-View Field Masking

- Protect against unnecessary exposure of sensitive data while still allowing users to view data with expressed intent
- Use click-to-view to unmask data, with optional MFA challenge for data reveal
- Log all click-to-view actions to have a structured record of sensitive data access

Query and Search Masking

- Apply the same field-level masking policies to query and search results
- Block query functionality by role or location, or gate access with a MFA challenge

Increase Security
Apply a level of security that matches the level of risk with contextual data masking policies.

Improve GDPR Compliance
Reduce exposure of PII with data masking across PeopleSoft. Click-to-view functionality protects against unnecessary exposure while logging intentional access of sensitive information.

Protect Non-Production Environments
Implement masking functionality across non-prod environments to control access for development or testing teams.