APPSIAN

DATA SHEET

Application Security Platform for PeopleSoft

Appsian's Application Security Platform offers PeopleSoft users a contextual, granular-level approach to securing their PeopleSoft environments

Key Use Cases

Integrate SAML-based Identity Providers with PeopleSoft

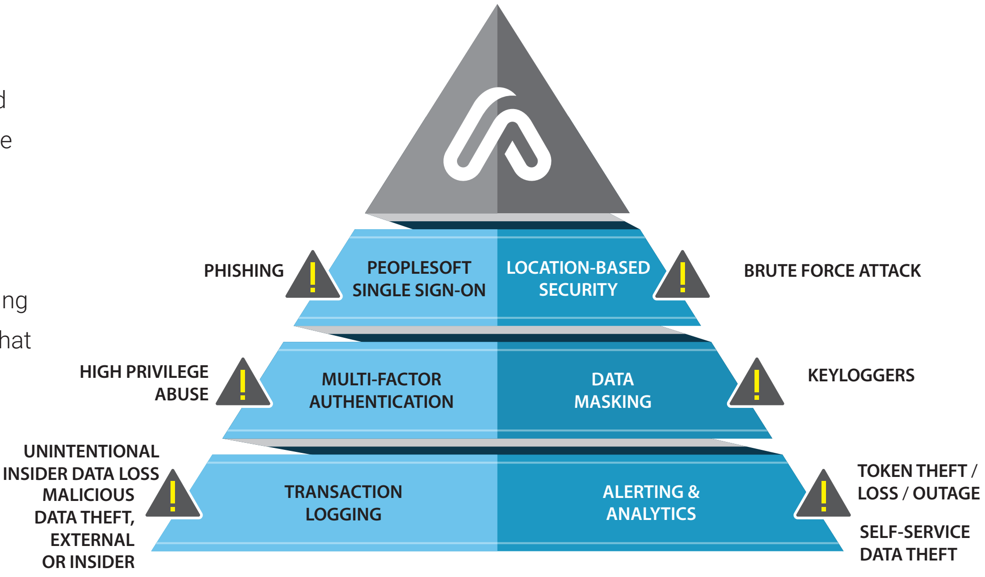
Centralize user provisioning, password policies, and implement Single Sign-On for PeopleSoft to improve security and convenience

Deploy dynamic context-based access controls

Improve security across PeopleSoft without impeding productivity by enforcing context-specific policies that balance security priorities with usability demands

Gain direct visibility into PeopleSoft activity

Enhance PeopleSoft logging capabilities to capture all user activity at the field, page, and component levels.



Perform forensic investigations with full context

Capture a complete audit trail of all user activity enriched with user attributes and tagged with PeopleSoft artifacts

Expedite detection and response with visualized analytics

Equip your security operations center with real-time visualized dashboards fed with enriched logs to quickly spot suspicious activity and drill down to root out issues.

Access Management

Validate user identity with authentication measures such as SSO and MFA to improve intrusion prevention capabilities.

Appsian's PeopleSoft Single Sign-On

Simplify the user login process while achieving greater user engagement and enhanced security compliance. Appsian's PeopleSoft Single Sign-On integrates natively within PeopleSoft to enable SAML assertion without additional hardware or customizations.

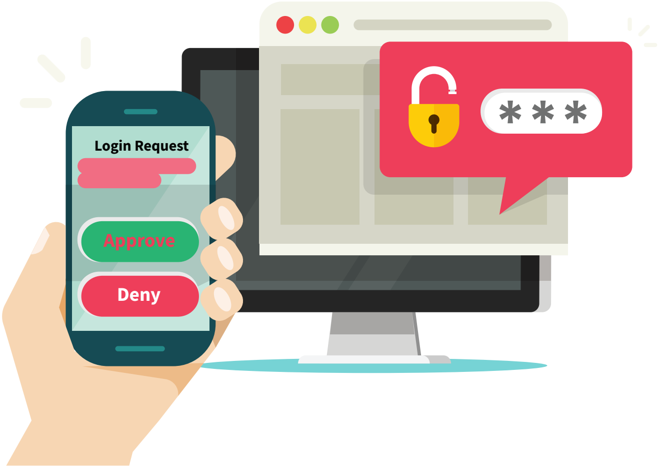
- Registers ADFS, Shibboleth, or other SAML-based Identity Providers
- Facilitates the Authentication process to:
  - Eliminate login action if a user is already authenticated with SAML
  - Advance login action if a user is not already authenticated
  - Allows manual logins
- Works with PeopleSoft's account provisioning
- Rules to map token to PeopleSoft ID
- Control access based on:
  - Authentication Location trust
  - Federated Identity Provider trust
- Generate logs based on:
  - Identity provider trust
  - Failed logins

Two-Factor Authentication

- Apply 2FA at application login, and inside PeopleSoft at the page or field levels.
- Integrates PeopleSoft with all 3rd party token providers such as OKTA, DUO, SecureAuth and more.
- Token delivery via SMS, email, phone, or mobile app.
- Prevents 2FA outage token loss theft
- Effective provisioning of 2FA tokens
- Drive high privilege user adoption of 2FA

PS_TOKEN Security

- Protects PeopleSoft against the (PS_TOKEN) TokenChpoken attack



Access Control

Protect sensitive data within PeopleSoft from unauthorized access by enforcing granular, context-aware access policies such as limiting PeopleSoft users to self-service only when outside your corporate network.

Control access to PeopleSoft based on:

- Device type
- Activity type
- User attributes
- IP address

Enforce granular access policies such as:

Allow/block access to PeopleSoft fields, pages, and components
Allow/block specific user actions (i.e. running queries)
Force multifactor authentication at login and inside PeopleSoft

Privileged Access Management

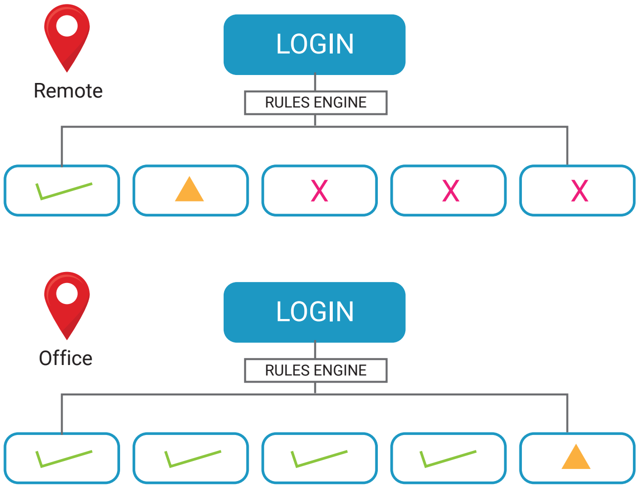
Improve control and visibility of your highest risk user accounts.

- Controlled access for shared batch or admin accounts
- Addresses known security risks and compliance issues at PeopleSoft customers by removing shared account access

> "Given the definite gaps in the ERP application, I don't know how we could live without the capabilities of the Application Security Platform; I don't know how you would protect your data. It is just not optional in today's environment."
>
> *– Matthew Scott, IT Manager, Penn State University*

Delegate Access

- Allows Campus Solution Solutions customers to grant granular access to students to view grades, financial aid, schedules and more
- Controlled access for students' parents/guardians/delegates



Data Loss Prevention

Prevent unauthorized exposure of sensitive information and combat insider data leakage with dynamic, context-aware DLP policies for PeopleSoft. Block the download of data, for example, from outside a corporate network.

Dynamic 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
- Deploys field-level DLP controls with no code changes needed to PeopleSoft records
- Filters out sensitive data at the presentation layer, resulting in no additional maintenance requirements for PeopleSoft updates

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 sensitive data 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, or require a MFA challenge before data is revealed
- Log all click-to-view actions to have a structured record of sensitive data access

Query Masking

Query Manager has the capability to run reports and quickly exfiltrate extensive data records. Add additional layers of security to PeopleSoft Query Manager to block functionality by role or location, or require a MFA challenge for reauthentication.

Improve GDPR Compliance

Reduce exposure of PII with dynamic 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-production environments to control access for development or testing teams. Further secure remote resources with location-based access controls.

Activity Logging

Default PeopleSoft logging capabilities are insufficient to meet today's modern security requirements – Appsian's Application Security Platform digs deeper. Transaction-level activity logging captures granular, real-time information on who a user is, what they're trying to access, and where they're coming from.

Capture granular log data such as:

- User ID
- IP Address
- Search Key
- Browser
- Date & Time
- PeopleSoft Page, Field, and Component
- Login Page, Portal Content, iScript

Creation of Targeted Logs

- Failed login activity
- Activity for specific content (i.e. PII)
- For specific roles (i.e. administrators, 3rd parties, etc.)
- Click-to-view activity of masked sensitive data

Flexible and configurable logging

Regulatory Compliance

Direct visibility necessary for compliance

View and record all activity inside PeopleSoft to align to compliance requirements such as GDPR, CCPA., and more.

Improve auditing capabilities

Eliminate much of the complexity that comes with database audits and provide streamlined methods for administrators to run reports and perform audits

Visibility / Insight
Compliance (GDPR)

Real-Time Analytics

Accelerate threat detection, reporting and response with pre-configured dashboards. Real-time data trends are aggregated, enriched, and visualized with PeopleSoft Security Analytics

Log Enrichment Process

Appsian uses an in-depth understanding of PeopleSoft to correlate log activity with common actions that organizations should be aware of – eliminating the time-consuming need to translate unstructured logs into actionable information.

Intrusion Prevention

- Authentication attempt trends
- Geographical locations of access
- Brute Force attack detection

Data Loss Prevention

- Trending data by sensitivity
- Trending privileged user access
- Security changes tracking

Incident Response

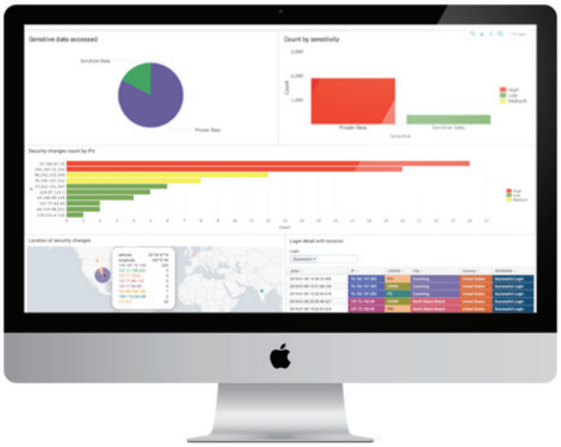
- Forensics at User ID and IP levels
- Detecting breaches / attacks

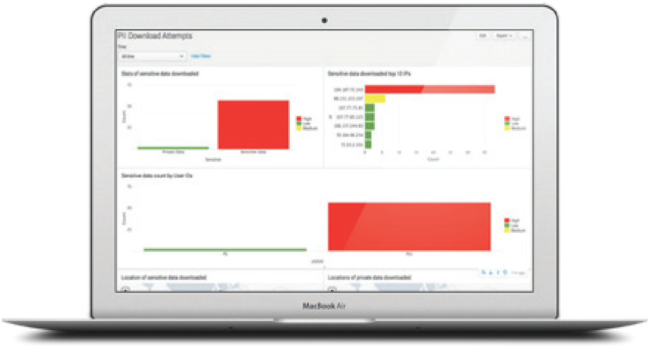
Critical Insights for Data Privacy Compliance

- View real-time access trends of sensitive data such as personally identifiable information (PII) and protected health information (PHI)
- Drill down to see all access of specific records

Improve Post-Breach Forensics

- Execute a rapid response to possible security threats
- Eliminate much of the manual work required for performing audits
- Remain compliant with new data privacy regulations (ex. GDPR)


Sensitive data accessed
Count by sensitivity
Security changes count by IPs
Location of security changes
Login detail with location



Unified Rules Engine

Appsian's Application Security Platform leverages a centralized rules engine to apply contextual policies throughout PeopleSoft. Residing natively inside the PeopleSoft architecture, the rules engine can combine PeopleSoft artifacts with contextual access data to enforce granular security policies.

Policy Templates

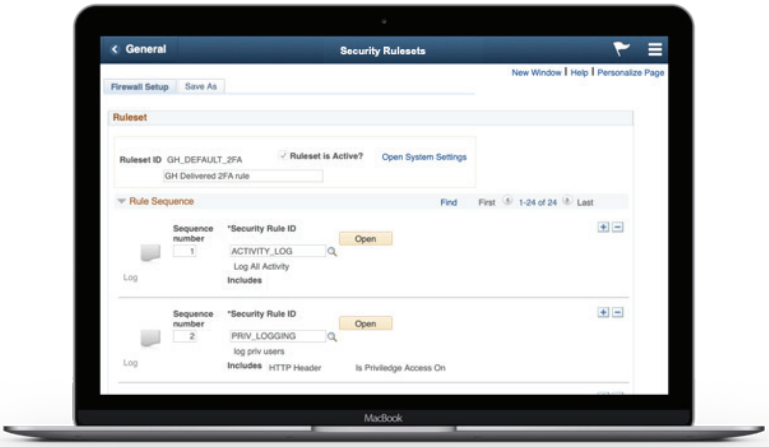
Utilize pre-built templates for common roles, use cases, or compliance requirements to expedite implementation

Versatile Configuration

Create custom policies with contextual logic to conform to any corporate or regulatory requirement

Native to Your PeopleSoft Environment

Incorporate artifacts within PeopleSoft to build policies specific to your organization's PeopleSoft environment (i.e. customizations)



Ruleset

Ruleset ID GH_DEFAULT_2FA ✓ Ruleset is Active? Open System Settings

GH Delivered 2FA rule

Rule Sequence

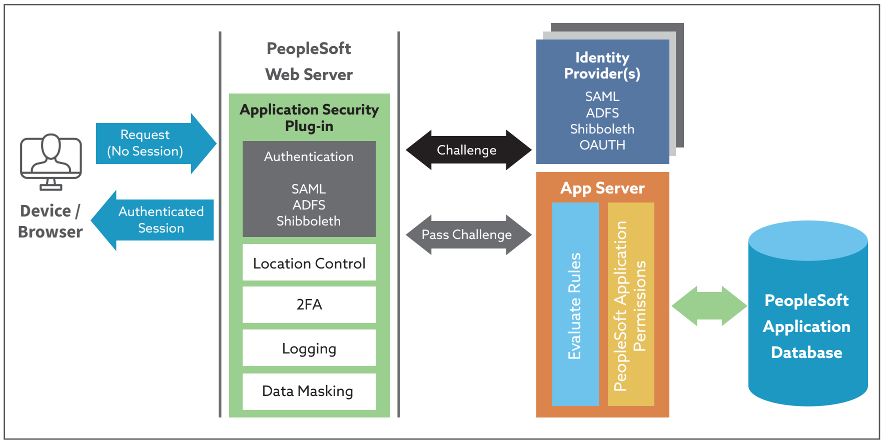
Log | Sequence number 1 | *Security Rule ID ACTIVITY_LOG | Log All Activity | Includes

Log | Sequence number 2 | *Security Rule ID PRIV_LOGGING | log priv users | Includes HTTP Header | Is Priviledge Access On

- Combine DLP and access control rules to enforce granular policies
- Configure rules tied to PeopleSoft fields, pages, and components
- Dynamic policy framework leverages triggers and response actions
- Build policies using Boolean logic, nested rules, and rule groups
- Selectively target or exclude specific users and define exception rules

Architecture

As a native PeopleSoft solution, Appsian's Application Security (ASP) platform resides inside the PeopleSoft Web Server and requires no additional hardware.



Implementation

ASP's package is installed on the web server along with a package in the application database. Implementation typically takes less than 4 weeks to go live.

Performance

Residing natively within the PeopleSoft Web Server, ASP is inline and avoids network hops that delay performance. Load tests return results within the margin of error of normal PeopleSoft installs.

Maintenance and Updates

Full support team available 24/7 to assist with any challenges. Updated software packages are made available to customers with each PeopleSoft update.

APPSIAN
Formerly GreyHeller

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

☎ (469) 906 - 2100

✉ info@appsian.com