

SOLUTION BRIEF

Exposing PeopleSoft Self-Service Applications to the Internet

Best Practices for Maintaining Security

Abstract

User engagement relies greatly on the ease of accessing information, the flexibility in fulfilling transactions, and the time taken in the process. To continue delivering efficiency for the modern workforce, Oracle has introduced the Fluid UI – a strategic step towards upgrading the PeopleSoft user experience by making transactions mobile-friendly. The Fluid page rollout is focused on enabling transactions that make the most sense for PeopleSoft customers/users. Self-service modules like benefits enrollment, time entry, approvals, student self-service, etc. have been prioritized so that users can fulfill tasks on their own time 1) without depending on access to a desktop computer or 2) having to divert time and focus from their primary responsibilities.

Despite the benefits of mobilizing and opening applications for remote access, security ramifications are a major concern of most PeopleSoft customers. Rightfully so, since PeopleSoft applications house your organization's most sensitive data including PII of students, employees, vendors and even job applicants. Expansion of access to sensitive data beyond a secure network perimeter also increases the risk of threats and more successful breaches. The proliferation of user-centric threats adds to the risk, as hackers increasingly target individual users and devices - leveraging the human-error factor to their advantage.

So how do organizations maintain strict data security policies when access to PeopleSoft is available outside a secure corporate network? In this solution brief, we will discuss how organizations can achieve a secure remote access environment for PeopleSoft - using contextual access controls and fine-grained data security features.



The Evolution Of The Threat Landscape

As enterprise applications are exposed to the public internet, organizations are experiencing a shift in their threat landscape. More and more successful enterprise data breaches are originating from the application level (accessed with valid credentials), completely circumventing the secure corporate networks that organizations rely on to keep sensitive data safe.

- Recently there's been a huge influx of phishing attacks. Despite training and awareness programs, employees continue to fall for phishing attacks. According to the 2019 *State of the Phish* report, 83% of global security respondents experienced phishing attacks in 2018, up from 76% in 2017.
- In last two years the average number of incidents involving malicious insiders increased by 53% and 2019 is predicted to be the costliest year to date when it comes to malicious insider threats.
- Black Hat's *Hacker Survey Report* found that 73% of hackers say that traditional perimeter security firewalls and antivirus software are irrelevant or obsolete, and 85% of hackers named humans as most responsible for security breaches.

It is evident that the focus of cybercrime has shifted from the network to end-users. Therefore, expanding access only increases the attack surface for cybercriminals and malicious insiders to exploit.

Best Practices And Recommendations

As threats evolve organizations must improve their security posture. In addition to refining policies and procedures, new age security solutions such as contextual access control and fine-grained data security can significantly reduce the probability of user-centric breaches. By enforcing additional authentication measures, improving access controls, and gaining visibility into user actions, organizations can confidently roll out self-service functionality knowing that their PeopleSoft applications are secure.

Evaluate required security upgrades

Expanding access for PeopleSoft self-service applications can have a great impact on workforce productivity, talent retention, and user satisfaction. As a result, organizations might be encouraged to fast-track an ESS rollout project. However, it is essential to evaluate the security concerns associated with remote access beforehand. An analysis of threat vectors, business needs, regulations, and the sensitivity level of your data assets is a vital step to achieving a secure PeopleSoft environment. To truly benefit from mobile and remote access capabilities, it is important that organizations evaluate the risks and strike a balance between convenience and data security.

Strengthen identity management

With the rise in credential compromise caused by social engineering attacks and poor password management, PeopleSoft's primary security model of Username & Password authentication is no longer an effective method on its own. It is important that organizations prioritize the use of an additional layer of identity authentication to validate access, especially from outside a secure corporate network. Organizations can implement multi-factor authentication (MFA) challenges to reduce successful access attempts in case valid user-credentials are compromised. In fact, according to the Black Hat hacker survey report, MFA has been considered as the top most 'tough to beat' feature by hackers.

Enhance ERP access controls

Deploying PeopleSoft self-service often includes expanding access to the public internet. By allowing access outside a secure corporate network, organizations expose themselves to new risks posed by cybercriminals and insiders alike. Equipping PeopleSoft with contextual access controls allow organizations to better align to the principal of least privilege, in turn, eliminating unnecessary privileges and drastically reducing user-centric risk. To reduce your remote attack surface, it is essential that organizations set restrictions and only allow bare minimum access for specific low-risk transactions.

Mask sensitive data fields

Data masking is a best practice for protecting sensitive data fields such as social security numbers, direct deposit information, patient ids and more from unnecessary exposure. By hiding records partially or fully, organizations can significantly reduce the risk of data theft. In the interest of added security, organizations must implement dynamic data masking governed by contextual information, so that even valid users are unable to access sensitive data remotely on personal devices.



Build deep visibility into user activity

In the context of self-service, organizations are opening themselves up to an entirely new scope of access. Rather than all activity coming from a single, trusted corporate network and uniform set of corporate devices, users are now accessing your sensitive PeopleSoft applications from thousands of unfamiliar end-points. This venture into the unknown requires deep visibility into user activity to be able to detect suspicious access. Additionally, building the capability to monitor, track and record user-actions on a granular level, along with the context of activity, organizations can facilitate logs for audits and regulatory reporting and allow security teams to discover, investigate, and respond to suspicious transactions promptly.

Challenges

Poor password practices negatively impact productivity and security efforts

Out-of-the-box, PeopleSoft's native authentication is username and password based and does not enforce strong password policies. With multiple enterprise applications to access, employees tend to set up easy to remember passwords that are also easy to crack. To avoid the use of weak passwords, IT teams enforce mandates around setting up strong passwords which are difficult to remember, which leads to recurring password reset requests. Frequent password reset requests can result in users delaying or abandoning administrative transactions - defeating the purpose of making self-service mobile and available remotely.

- No native SAML support

Organizations can rectify this by establishing a centralized authentication system or a Single Sign-on (SSO). However, PeopleSoft applications lack native SAML support - the widely accepted identity federation standard. As a result, PeopleSoft applications cannot connect with SAML supporting ID providers and are likely to be alienated from other enterprise applications. Most off-the-shelf SSO providers are unaware of this limitation and suggest custom development when faced with the roadblock during implementation/testing. A custom development is costly and time-consuming as it requires specialized knowledge, extensive development, and often the purchase of additional hardware.

Limitations of front door MFA

Most off-the-shelf MFA solutions are limited to login level only. While front-door MFA challenges can be effective in keeping malicious hackers out of PeopleSoft applications, they pose several constraints, i.e. lack of security against insider threats, and decreased employee productivity.

- Login level MFA is ineffective for insider threats

While a login level MFA can protect your applications against external bad-actors, a malicious insider with the ability to successfully pass these challenges can still access, download, distribute, and potentially misuse PII for personal gains. Therefore, to fully leverage the benefits of MFA it is essential to extend the functionality to field, page and component levels.

- MFA fatigue impacts user engagement

The added disruption of recurring MFA challenges at login can avert users and impact engagement rates. Frequent MFA challenges can force users to avoid self-service transactions resulting in low engagement with critical HR/ administrative initiatives - eventually defeating the purpose of opening self-service for remote access. Since most self-service transactions are low-risk, organizations must focus on protecting high-risk transactions and sensitive fields.

- Rigid rulesets

To enforce MFA challenges for high-risk transactions, organizations need to tie authentication policies with contextual information. However, traditional MFA solutions cannot integrate with PeopleSoft's underlying rules. As a result, organizations are left with rigid rulesets and limited ability to configure MFA policies that meet their employees' and business' unique needs.



Static access control

PeopleSoft allows organizations to implement access controls based on static rules. User-roles or permission lists govern these restrictions, thereby allowing users to access all the sensitive information or nothing at all. With increased access from outside a secure network, organizations need more flexibility to control what users can access based on contextual information such as the location of access, user-privilege and more. For example - high-risk transactions such as financials, payroll, etc. must be blocked for external access despite the privilege level of a user.

Limitations of native data masking

PeopleSoft's existing data masking functionality is limited to Bank Account Number, Date of Birth and National ID. The native masking also depends on static, role-based rules; therefore, users who have the privilege to view sensitive data can view it all, no matter where they are accessing the application from. As a result, sensitive data fields are vulnerable to exposure if privilege user credentials are stolen or when privileged users download data on personal/home computers using queries. To ensure that data masking is effective for remote access, masking rules need to be contextually aware of where access is coming from and dynamically applied (inside or outside a secure corporate network).

Logging capabilities are not user-centric

Out-of-the-box, PeopleSoft offers high-level logging designed primarily for debugging and troubleshooting. These logs do not provide information on what data was accessed or any details on the context of access such as who obtained it, when, or from where. However, with the rise in user-centric threats, contextual information tied to user activity logging becomes instrumental in monitoring, reporting, and incident response – especially when the scope of access is expanded beyond a secure network firewall.

Solution

Appscan's Application Security Platform (ASP) addresses end-to-end PeopleSoft security requirements that come with the expansion of access. Uniquely designed for PeopleSoft, ASP provides security features that are contextually aware and deploys defenses based on user privilege, business requirements, and the sensitive nature of the data/transactions. ASP plugs into your PeopleSoft web server and enhances the security of your applications, without impacting user experience or requiring additional customization efforts and hardware.

Dynamic Access Controls

ASP allows customers to establish dynamic access controls based on contextual attributes such as the location of access, IP address, user privilege and nature of a transaction. Customers can set restrictions for specific modules or transactions, or prompt users with MFA-gated checkpoints when an access attempt is made from outside a secure corporate network. Organizations can also entirely block high-risk transactions from remote locations while still allowing access to low-risk transactions such as benefits enrollment, time-entry, expenses, approvals and more.

Contextual MFA with field-level data protection

Appsian's MFA solution allows organizations to enforce identity challenges at the field, page, and component levels in PeopleSoft. It is the only solution of its kind that enables IT teams to create contextual rules based on PeopleSoft artifacts and user attributes such as user id, location, IP address, privileges, data sensitivity and more. With ASP's contextual MFA in place, users can be challenged to reconfirm their identity (using a voice call, OTP, or push notifications) when attempting to view sensitive records or perform high-risk transactions.

By using the context of access to enforce MFA challenges, ASP matches the level of risk to the appropriate level of security. This approach maintains robust security while avoiding arbitrary security measures that plague user productivity and engagement. For example, enforcing more robust MFA policies when a user is requesting access from a coffee shop versus at the office.



Dynamic Data Masking

ASP allows organizations to enforce dynamic data masking policies to mask or redact any field in PeopleSoft. Using the context of access and data attributes, organizations can implement full-field, partial-field, and click-to-view masking to ensure that only authorized users who need to see data can see it, and only when they should.

Coupled with ASP's field-level MFA, data masking can also be utilized to provide conditional access to allow users to view specific data fields by performing an identity authentication challenge. Additionally, using a click-to-view functionality, organizations can efficiently track access to sensitive data records and trace back on user activity in case of a suspicious transaction.

Single Sign-On

Apsian's PeopleSoft SSO Connector is the only solution that sits natively within the web server and allows PeopleSoft to support SAML technology; thus, enabling organizations to use SAML-based identity providers for authentication with PeopleSoft applications. By removing the hassle of managing multiple passwords, PeopleSoft SSO reduces the burden on IT teams and makes password management easier. It also empowers users to transition between all enterprise applications, including PeopleSoft, with one strong set of credentials - improving usability and boosting employee engagement.

Logging and Analytics

Apsian's Application Security Platform (ASP) enables granular logging and user activity monitoring for PeopleSoft. ASP allows customers to capture user activity data paired with contextual user information such as device, location, IP address, etc. The transaction level data is recorded in a structured format that can efficiently highlight malicious events, provide actionable data for incident response, and offers ready-to-use audit and compliance reports. With a click-to-view feature, all activity involving sensitive data can then be tagged with the corresponding user role, IP, location, and time of access. Additionally, with ASP's Real-Time Analytics, these detailed logs can be further visualized on Splunk leveraged dashboards to highlight trends and patterns in user activity and data usage for enhanced data discovery and exploration.

Conclusion


Mobile self-service transactions offer an abundance of convenience and flexibility for both users and administrators. Leveraging remote and flexible working that frees users from fixed office and desk environments, organizations can significantly boost productivity, reduce turnaround time, and save associated costs. To manage the increased access surface and the corresponding risk to data assets, organizations must build a proactive security strategy.

Application security efforts can be maximized by implementing multiple layers of contextual controls aimed at enhancing visibility, strengthening user authentication and improving governance. While adding fine-grained security features such as data masking, least privilege, MFA, etc. can allow organizations to avoid certain risk vectors upfront, visibility into user activity can allow faster incident response for malicious events and their aftereffects.



8111 Lyndon B Johnson Fwy. Dallas, TX 75251

© AppSian 2019

 (469) 906-2100

 info@appsian.com