



SOLUTION BRIEF

PeopleSoft Multi-Factor Authentication

Expand MFA to Secure Sensitive Data at the Field, Page, and Component Level

Abstract

According to IBM's insider threat report¹, 60% of security breach incidents are caused by users with insider access. While security teams are primarily focused on protecting your infrastructure from malicious outsiders, insider threats continue to cause a significant number of data breaches. To safeguard sensitive data from both internal and external threats, embedded security solutions such as Multi-factor authentication (MFA) are being mandated and adopted widely.

Conventional MFA solutions are predominantly implemented to prevent malicious outsider access, as they're intended to reconfirm the identity of a valid user. However, once a valid credential successfully passes an MFA challenge at login, the data inside the application remains vulnerable to insider threats via privilege misuse, unintentional data leakage, data exfiltration and more. Due to the high volume of sensitive data contained in PeopleSoft (PII on hundreds of pages), the scope of a possible data leakage incident can be significant.

Adding further complexity, MFA sits at an intersection between security and possible annoyance, as MFA challenges can interfere with users attempting to accomplish tasks in PeopleSoft. When a user's experience is disrupted by an MFA challenge, users can push back – forcing security professionals to compromise on the frequency of challenges. If MFA rulesets are limited to a 'one-size-fits-all' / 'all-or-nothing' configuration, the quality of the overall user experience and value of the security both suffer.

To minimize threats by outsiders and malicious insiders, organizations must bring MFA capabilities inside their PeopleSoft applications. Because breach trends have indicated that valid credentials are typically leveraged to breach sensitive data, forcing challenges at the field, page, and component level becomes necessary. In addition, with the added levels of challenge, the issue becomes – how can you implement stricter security measures without sacrificing user experience?



Challenges

Limitations of MFA at the login-page

Multi-factor authentication was originally intended to keep external threats out by protecting an application's perimeter. It does this by adding a second form of verification at login to ensure a user is who they say they are. And it still does this well.

The challenge now is that insider threats, such as privilege abuse and data leakage, are on the rise. According to a 2018 survey by Cybersecurity Insiders², 53% of organizations confirmed facing insider attacks in the past year, and 27% reported that insider attacks have become more frequent.

PeopleSoft's primary security model of Username & Password authentication is limited to an application's login – a limitation that still exists with 3rd party MFA add-ons. After a user passes login, you have no way of protecting the data across your PeopleSoft applications.

This gap in security control means that a malicious insider with access to high privileged credentials could simply pass login and then have access to your PeopleSoft systems to download, distribute, and potentially misuse Personally Identifiable Information (PII).

MFA 'Disruption' Causes Fatigue

By design, MFA inherently adds an extra step to a user's workflow when logging into an application. Including this disruption at every login instance can quickly result in frustrated users, especially when paired with an SSO solution originally intended to provide seamless access.

Forcing all users to pass frequent MFA challenges, regardless of what they are trying to do or where they're coming from, can often make the whole process seem arbitrary to users. This can ultimately lead to users succumbing to 'MFA fatigue'.

MFA fatigue can lead to:

- Application avoidance for low-risk transactions, as users are likely to put off or abandon them altogether
- Desensitizing MFA challenges, posing a security risk of involuntary conditioned responses to authorized/illegitimate challenges. (ex. unconsciously passing a mobile 2FA challenge out of habit)
- Risky MFA practices to remedy fatigue, such as allowing users to stay logged in for an extended amount of time after a successful MFA challenge – making applications vulnerable to active breach attempts

Limited Rulesets Force Compromise

The balancing act between Security and UX can at times seem like a zero-sum game. Improving security with MFA comes at the expense of disrupting user experience. The tradeoff is well-known; most MFA solutions have basic features built-in to reduce MFA challenge frequency, such as storing trusted devices or networks.

While these features are on the right path, the stakes are higher when MFA is implemented for a large user-base with varied use-cases and usage rates, as it is with PeopleSoft. A 'one-size-fits-all' solution doesn't work here.

Most off-the-shelf MFA solutions lack the ability to integrate with PeopleSoft's underlying rules and policies. As a result, organizations are left with rigid rulesets having little ability to configure their MFA policies to meet the unique needs of various employees.

Under these constraints, organizations must take a 'greatest-good' blanketed approach in configuring MFA rulesets – leaving outliers to suffer – or exclude outliers such as admins altogether. Either path forces compromise and limits the full potential of Security and UX efforts.

Solution

Appian's MFA for PeopleSoft allows organizations to expand MFA functionality to the field, page, and component levels. Our MFA solution plugs directly into the PeopleSoft Web Server without any additional infrastructure or customizations, allowing customers to build MFA rules using existing PeopleSoft attributes such as who the users are, what data they are trying to access, their location of access and more.

Unlike traditional off-the-shelf MFA solutions, Appian's MFA can leverage all existing PeopleSoft artifacts. This opens up new possibilities for sophisticated MFA use cases, adding flexibility where it's needed most in order to strike a balance between security priorities and usability demands.



Utilizing contextual rules, customers can better control the occurrence of MFA challenges, thereby reducing MFA fatigue and improving user experience while maintaining thorough security. For example, enforcing more robust MFA policies when a user is accessing an application from a coffee shop versus at the office, or, forcing an MFA challenge mid-session only if a network change occurs but limit occurrence if a network has been authenticated already.

Combined with Appian's Application Security Platform (ASP), organizations can record MFA activity in detailed access logs for an extra safeguard. Recording access at the MFA challenge and beyond allows organizations to keep a log dedicated to sensitive data access – filtering out the noise of less critical activity.

To maintain the integrity of sensitive information, it is essential that MFA challenges are tied to user behavior, privilege, and the organization's governance policies so that data remains secure while the MFA challenge itself is as relevant as possible considering the context of access.

Our solution plugs directly into the PeopleSoft Webserver to:



Enforce robust, contextual access policies based on a rules engine within PeopleSoft



Authorize devices, IP addresses, and locations to allow secure remote access



Keep sensitive information protected from bad internal actors



Allow users to authenticate sessions using a voice call, OTP or push notifications



Govern the occurrence of MFA challenges for ease of use without compromising security or user experience


¹<https://www.ibm.com/security/campaign/guardium-insider-threats>

²<https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf>



8111 Lyndon B Johnson Fwy. Dallas, TX 75251

© AppSIAN 2019

 (469) 906-2100

 info@appsian.com