pathlock

Achieve a Zero Risk PeopleSoft Environment

Systematically Eliminate Risk with a Convergence of IAM, IGA, and GRC

www.pathlock.com

Table of Contents

Introduction 3

The Challenge of Managing PeopleSoft Identity and Access 4

Understanding Zero Risk: Zero Risk vs. Zero Trust - What's the Difference 5

Converging IAM, IGA, and GRC to Eliminate Risk 6

6 Critical Capabilities to Implement Zero Risk 8

What to Look for in a Zero Risk Solution for PeopleSoft 10

Eliminate Risk in PeopleSoft with Pathlock 11

Introduction

In today's increasingly digitized business environment, ubiquitous access to mission-critical applications, transactions, and data is a requirement. Whether access is taking place behind or entirely outside the firewall - evolving cybersecurity threats, compliance regulations, and complexities around managing identity are putting increasing pressure on your PeopleSoft Administration team.

Organizations must manage the daunting task of safeguarding access to their PeopleSoft application and data from internal and remote users, which can include third-party service providers combined with a constant flow of requests from users for changes to existing levels of access. On top of that challenge, they must manage potential security breaches from hackers attempting to gain unauthorized access to systems and data.

Additionally, they must maintain effective Separation of Duties (SoD) controls for various regulatory compliance mandates such as Sarbanes-Oxley, the Gramm-Leach-Bliley Act, etc. This creates an atmosphere of constant battling to maintain effective security controls to mitigate the organization's risk exposure.

This eBook will enable you to address these challenges by taking a comprehensive and proactive approach to managing identities, access, governance, and risk across your PeopleSoft applications.

The Challenge of Managing PeopleSoft Identity and Access

PeopleSoft applications process and store vast amounts of customer, employee, and financial data that are constantly accessed by an increasing number of users from various locations, devices, and network connections.

These dynamic access requirements make detecting PeopleSoft security threats a significant challenge. Unfortunately, PeopleSoft has static security controls and manual reporting, creating blind spots that result in security and compliance gaps.

Additionally, PeopleSoft systems' lack of native SAML support makes it challenging to integrate an enterprise Single Sign-On (SSO) and Multi-Factor Authentication (MFA) with PeopleSoft. This lack of integration plays a critical role in why many PeopleSoft systems operate independently of enterprise IAM strategies, requiring users to have separate passwords and IT teams to manage separate identity databases. Both lead to increased liabilities, cumbersome password resets, and multiple databases to provision as users onboard and offboard.

The Joiner-Mover-Leaver Process Also Introduces Risk

According to **Verizon's 2022 Data Breach Investigations Report**, 82% of all breaches involved the human element. Whether that's phishing or using stolen credentials, hackers are finding ways to capitalize on human error. With employees constantly coming and going in the Joiner-Mover-Leaver landscape, it's difficult to stay on top of all those accounts and keep them secure, opening the floodgates to malicious actors.

⚠ **Joiner Risk:** With any new hire, you want to ensure they have easy access to company platforms during the onboarding process. But without proper training on data policies and a lack of general best practices – misuse of company data is widely common for new employees

⚠ **Mover Risk:** When a user's role is changed, adding new access that requires approval from someone unfamiliar with the user and revoking access associated with the user's old role can cause a backlog of manual requests and approvals. This process can be challenging to track and fulfill.

In the absence of mature processes and centralized identity security tooling, companies typically resort to two scenarios to resolve this issue. They either grant the user access to everything and fix potential security issues later or give the user similar rights as another user. In the rush to get the employee up and running in their new role, security is all but forgotten because fixing it later rarely happens.

Leaver Risk: When an employee leaves the company, IT may think it has an easy solution: "I'll just disable the user's main account. Then we're good!" But that's not necessarily the case, especially if your business and devices aren't under centralized IT control. Former users could still obtain sensitive information if your company doesn't take steps to revoke their access from every angle.

Considering all the risks mentioned above, a successful risk mitigation strategy requires a cross-functional approach that takes into account users, their identities, the entitlements they possess, the applications they access, and the context of access.

Understanding Zero Risk

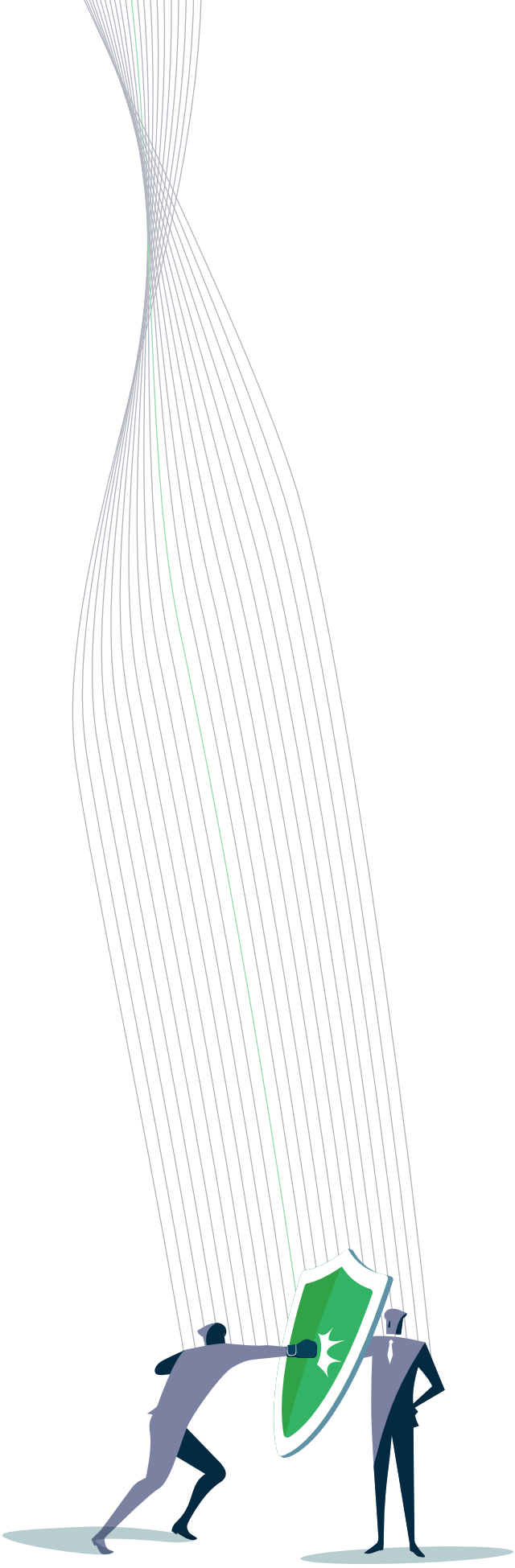
Whether it's PeopleSoft or any other enterprise application, managing and mitigating risk is critical to achieving stronger security and stricter compliance.

A Zero Risk methodology is a proactive approach to security that establishes a multi-layered foundation for secure application access. This approach allows organizations to confidently embrace new technologies and adapt to evolving threats while safeguarding sensitive data and enabling business growth in a dynamic digital landscape.

By using solutions that enable granular control and continuous visibility over data and transaction usage, organizations that employ a Zero Risk strategy will have a more scalable journey toward aligning with evolving security best practices and frameworks like NIST and COSO.

Zero Risk vs. Zero Trust - What's the Difference?

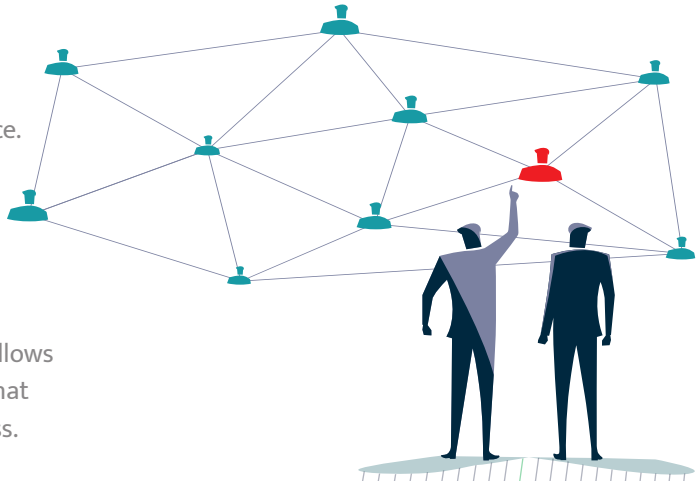
There has been a lot of talk about Zero Trust, which sounds similar to Zero Risk but is quite different. The challenge with Zero Trust is that it takes a significant amount of time, effort, and money to implement. Despite being around for several years, very few organizations have



been able to define a clear Zero Trust strategy and roadmap that prioritizes investments based on risk assessments. Furthermore, it requires buy-in from employees because it changes the way they work, which can cause friction and unauthorized workarounds.

On the other hand, Zero Risk is a cross-functional approach that involves IT Operations, Cybersecurity, Audit, Risk, and Compliance. The idea behind Zero Risk is to use a unified platform that removes control and visibility silos while aligning multiple functions towards a single, shared goal: eliminating external and internally driven risks across the business.

This is why Pathlock recommends a Zero Risk approach, which allows organizations to implement processes, controls, and solutions that address risks at multiple levels and not just at the point of access.



Converging IAM, IGA, and GRC to Eliminate Risk

Identity and Access Management (IAM) is a crucial policy framework that governs how users access PeopleSoft. It follows a specific methodology and timeline to ensure that users obtain the necessary access while adhering to security policies.

IAM plays an essential role in managing and protecting digital identities. It defines roles and access privileges for individual PeopleSoft users, ensuring that users can only access the system under specific circumstances, but also helps administrators oversee users and their actions.

IAM goes beyond managing identity, including password management, security, governance, reporting, auditing, and more. All these components play critical roles in safeguarding sensitive information and systems.

Identity governance and administration (IGA), an advancement of IAM, fuses identity and access policies with solutions that automate access reviews and user provisioning.

IGA solutions offer a range of features that enable the ingestion of Human Capital Management (HCM) data from applications like PeopleSoft (as the source of truth) to ensure that user information is accurate and up-to-date. These features also allow for automated provisioning of basic access rights based on department or position, as well as technical rule provisioning for more complex access rights.

In addition, automated access provisioning and deprovisioning streamline the onboarding and offboarding process, while automated certifications enable periodic review and validation of user access rights.

GRC: Where IGA Meets Access Controls

Managing and controlling identity and access is crucial in today's digital environment. While IAM and IGA play a vital role, there's still a need for an additional component to navigate the complexity of user access. This is where the combination of IGA and access controls comes into play, often called application GRC (Governance, Risk, and Compliance).

This integration amplifies automated provisioning by concurrently monitoring and managing the risk associated with the access granted by managers and IT teams. In terms of an organization's IAM maturity model, this incorporation (IGA and Access Control) represents a significant leap forward.

GRC solutions offer useful reports on high-level access activities. They help organizations identify who has too many permissions or is using sensitive permissions more than necessary. This is possible with the help of two tools: Emergency Access Management and Sensitive Access Risk Reporting.

The goal is to limit users' access to only the necessary permissions to perform their daily tasks. Nonetheless, if a user temporarily needs higher access for a specific task or in an emergency, this can be managed through an emergency access management process.

With this process, the user's request for additional access is approved, monitored, and reviewed. This way, users can get the access they need for special situations on a regular basis without the risk of having too many permissions, keeping the system secure, and complying with the organization's policies.

Furthermore, GRC solutions can provide in-depth Separation of Duties (SoD) risk analysis, identifying potential conflicts that can arise from granting elevated access. By adding this additional layer of control, GRC solutions create a more secure and compliant environment, ensuring that elevated access is carefully managed and monitored.

6 Critical Capabilities to Implement Zero Risk in PeopleSoft

The convergence of IAM, IGA, and GRC can be achieved with the right mix of capabilities. The six capabilities/solutions mentioned below enables PeopleSoft customers to create a proactive risk management ecosystem that enhances security, provides granular access control, and enforces compliance.

1. Automation for Identity Lifecycle Management

Identity lifecycle management is the starting point. It involves creating, managing, and deactivating user identities within the system. Every user is assigned a unique digital identity that requires continuous management. As user roles evolve or as they exit the organization, their access privileges must be updated or revoked. This constant maintenance prevents unauthorized access and potential security breaches.

However, as users shift roles and offboard, having an automated solution that looks for these changes and reassesses potential access risk is a critical component of maintaining compliance in an ever-changing user landscape. Automated, compliant provisioning is a straightforward best practice – especially for organizations with a high volume of users.

2. Access Control

Access control is the tool that enforces governance. It restricts access to resources, granting it solely to authorized entities. It plays a crucial role in preserving data confidentiality and integrity by ensuring that only authorized individuals can access specific data or applications. Access control is a vital component for maintaining information security and compliance.

3. Seamless Authentication via Single Sign-On

Single Sign-On (SSO) provides seamless authentication for users to access multiple applications or resources with a single set of credentials. This simplifies the login process and enhances security by reducing the risk of password-related breaches. To integrate a SAML-based SSO like Azure, Okta, Ping Identity, and many more with PeopleSoft, a native SAML handler is required. It is highly discouraged to use custom development and proxy servers as a workaround for the lack of native SAML integration due to security reasons.

4. Integrated Multi-Factor Authentication (MFA)

MFA is another authentication method that adds multiple steps to the process. MFA typically requires at least two of the following: something the user knows (like a password), something the user has (like a security token), and something the user is (like a fingerprint). This layered approach strengthens security, making it more challenging for unauthorized users to gain access. Like SSO, a separate MFA integration handler is required for PeopleSoft – especially if the goal is to challenge users dynamically (vs. preset rules) based on the context of their access.

5. Adaptive, Step-Up MFA

Adaptive authentication adjusts the authentication process based on perceived risk. For instance, if a user attempts to log in from a new device or location, the system might ask for additional verification. This dynamic approach balances security and user convenience. An integration handler is also required for deeper MFA integration at the transaction or data layer. This integration would enable a step-up form of authentication that would align with the more traditional definition of Zero Trust or "Never Trust Identity by Default."

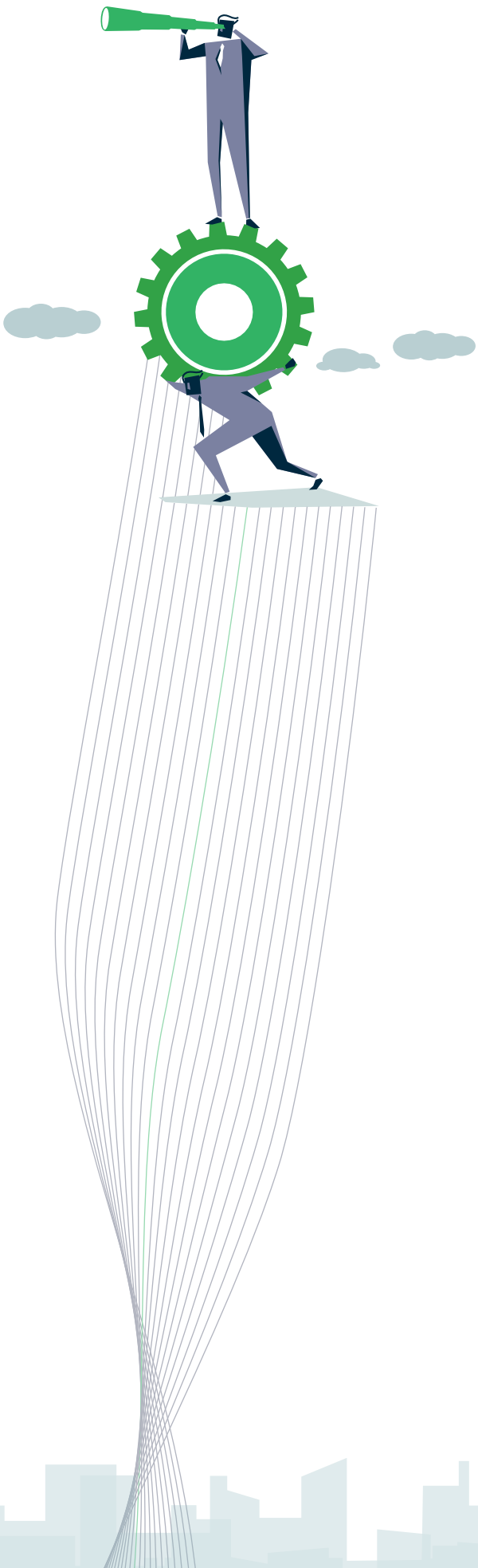
6. Identity Governance

Expanding access to applications like PeopleSoft means more devices, users, and varying contexts of user access. Implementing IGA improves visibility into identities and access privileges and helps security admins implement the necessary controls to prevent inappropriate or risky access.

In hybrid and remote access ecosystems, it's difficult to effectively manage user identities and access. This is especially relevant when access governance processes are executed manually, as users can be given excessive or unnecessary access to systems, applications or data. Thus increasing security risks and making the organization vulnerable to data breaches.

With IGA solutions, security personnel can track and control user access as part of application access governance efforts. They can secure users by ensuring that the right user accounts have the right access to the right systems while being able to detect and prevent inappropriate access. By implementing the right controls with IGA, enterprises can minimize risk and maintain regulatory compliance.

What to Look for in a Zero Risk Solution for PeopleSoft



While multiple vendors provide a range of IGA and GRC solutions, there are four key features that can have a significant impact on IGA and GRC initiatives.

1. Process Automation

Most identity management, governance, and compliance-related activities are repetitive in, and automation plays a key role in enforcing policies at the provisioning level. Managing account creation, approval workflows, and elevated levels of access, along with access certifications, puts an enormous burden on IT and functional teams. Automation translates into direct and indirect cost savings across IT, security, and compliance departments.

2. Cross-application Capabilities

Having the ability to provision users, recertify access, and manage SoD across applications with a centralized rules engine enables consistent compliance across the application landscape. Whether you are considering solutions just for PeopleSoft or beyond, having cross-application capability provides a scalable solution that reduces the burden on IT. Plus, it provides compliance and security teams with a full view of risk, which helps prioritize remediation and mitigation.

3. Continuous Monitoring of Sensitive Transactions

Instead of relying on periodic audits to detect compliance deviations after the fact, continuous monitoring of both controls and user activity within applications enables organizations to detect violations and suspicious activity as they happen. It also provides compliance managers with a clear view of key control activities. It ensures that they perform as intended while giving senior executives visibility into their organization's risk, security, and compliance status.

4. Leveraging Enterprise IAM Solutions like Okta, Azure, etc.

Customizations and additional hardware create risk, especially when authentication is involved. All IAM solutions like SSO and MFA should be natively integrated using a SAML integration handler specifically designed for PeopleSoft.

Eliminate Risk in PeopleSoft with Pathlock

Pathlock focuses on transforming access management and governance processes from manual to automated. Starting with support to natively integrate enterprise SSO and MFA solutions with PeopleSoft, Pathlock continuously monitors access, surfacing potential compliance conflicts and security threats. With Pathlock, you can streamline the detection and mitigation of access risks to avoid unauthorized access and potential data breaches.

Automated provisioning workflows enable the joiner, mover, leaver process to be compliant with governance policies and data regulations.

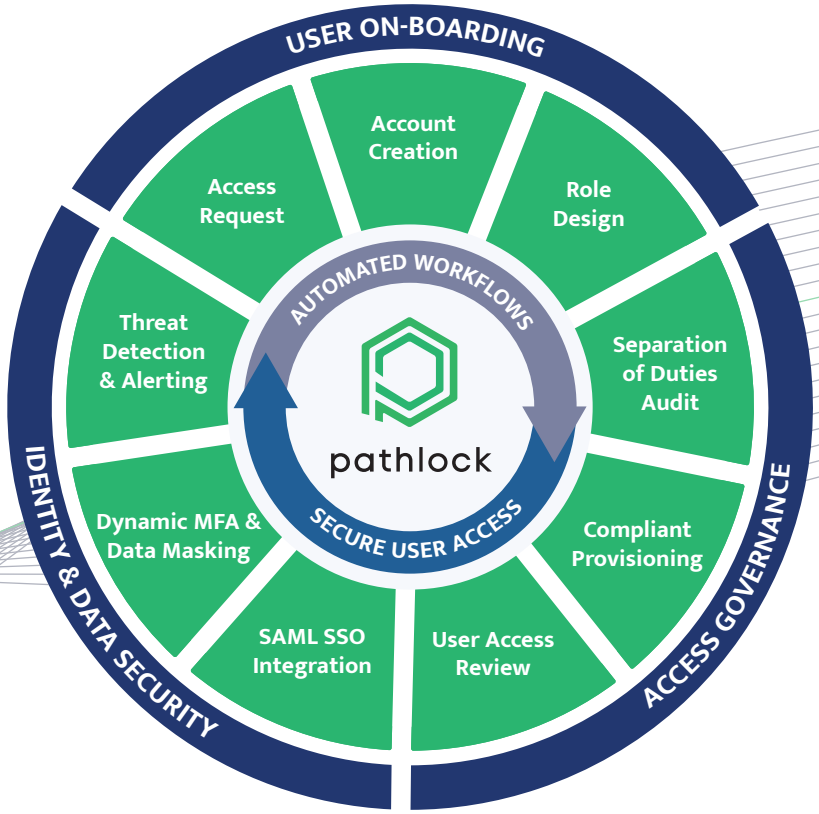
Dynamic, location-based access controls form the foundation of Pathlock's cybersecurity solutions. These controls ensure users have access only to necessary data and systems based on the context of access, enhancing security and mitigating the risk of unmanaged devices and unknown networks.

Pathlock offers extensive auditing and reporting capacities, enabling the monitoring of user activity and access rights. This information allows for informed decisions on strategy adjustments to best serve your organization.

Automation forms another key component of Pathlock's Zero Risk solutions. Automating procedures like user provisioning, password resets, and access reviews helps save time, reduce error chances, and improve overall organizational security.

Schedule a **personalized demo** today and learn how Pathlock can help you set your Zero Risk strategy in motion.

Reduce Time to Provision from Days to Minutes. Accelerate Time to Productivity. Strengthen Security and Compliance.



About Pathlock

Pathlock is the leading provider of security and compliance solutions for the PeopleSoft market. Solutions include Identity Governance automation: Provisioning, Separation of Duties, Privileged Access Management, and automated User Access Reviews. In addition, IAM integration for SSO (SAML), MFA, Data Masking, User Activity Analytics.

Pathlock helps hundreds of PeopleSoft customers all over the world keep their systems, users, and data secure and compliant.

For more information, visit **pathlock.com**