ABSTRACT

As your organization tackles its digital transformation journey, cloud-based ERP is often seen as a solution to many of these problems. However, modernizing legacy ERP systems like SAP ECC, Oracle PeopleSoft, and Oracle EBS creates a quandary: How do you maximize the access and availability of your ERP without sacrificing the security and integrity of your business-critical data during a digital transformation?

WHITEPAPER

Implementing enterprise resource planning (ERP) systems has always been both mission-critical and notoriously difficult. They must align with business processes, but the organization distributes those processes across multiple departments. Legacy ERP systems, often considered a large one-time investment, lack the flexibility necessary to scale with your business.

As your organization tackles its digital transformation journey, cloud-based ERP is often seen as a solution to many of these problems. However, modernizing legacy ERP systems like SAP ECC, Oracle PeopleSoft, and Oracle EBS creates a quandary: How do you maximize the access and availability of your ERP without sacrificing the security and integrity of your business-critical data during a digital transformation?

Why is Modernizing ERP a Mission-Critical Business Goal?

Legacy ERP systems were originally designed to provide workers easy access to data and business processes when they were located securely inside the literal four walls of the office and protected by network perimeter controls and firewalls. Whether you wanted to modernize your ERP or not, you likely found yourself rapidly adopting to remote access requirements in 2020. In response to COVID-driven stay-at-home orders, companies needed to accelerate their digital transformation strategies. This move included ERP systems.

As you look toward a post-pandemic business model as part of your digital transformation, you might be considering maintaining a hybrid workforce—giving employees more flexibility to work from different locations, including the office or entirely from home. Thus, modernizing your ERP is a mission-critical business goal for several reasons, including:

- Securing access beyond the firewall (and on any device)
- Gaining greater visibility and control over ERP data access
- Managing business process risks and reducing financial risk
- Maximizing your ERP investment

However, these systems were not designed to meet the dynamic access requirements of a remote workforce, leading to large security and compliance gaps that put companies at risk of experiencing devastating data breaches and millions lost to business policy violations.

ERP Data Security and Privacy Controls are Notoriously Difficult to Implement

When undergoing digital transformation, organizations often struggle trying to secure their ERP systems and maintain the integrity of business-critical data. Most companies need to take a hybrid approach that connects their legacy on-premises deployment to their new SaaS applications.

Organizations struggle trying to prioritize and mitigate risks for several reasons. However, three fundamental challenges exist:

- Data storage arrangements: Inability to control infrastructure increases data leakage and corporate espionage risks.
- Authentication: Continued brute force attacks and credential theft increase data security and privacy risks.
- Access controls: Complex identity and access relationships reduce the ability to control who accesses resources.

Traditional on-premises ERP deployments used role-based access controls (RBAC) with static permissions lists. However, the inherently static nature means that these alone fail to
protect data, particularly in remote or hybrid work environments and may not effectively scale with business growth or your digital transformation.

For example, legacy ERP security models assign roles to user profiles. The user profile defines the data that the person can use. The permissions list is the set of pages the user can access and actions the user can take.

These static controls protect data across on-premises deployments where the applications and users sit inside the organization’s network. Since remote access to on-premises ERP is dynamic, these legacy controls increase security and privacy risks when implemented for modernized ERP projects.

5 Strategies for Setting Data-Centric Security and Privacy Controls for a Hybrid ERP Deployment

Companies adopt digital transformation to leverage speed and agility, enabling them to scale operations. At the same time, they still need to maintain their on-premises systems. To protect information, organizations need data-centric and scalable access controls that align with their systems and business goals.

1. Identify Assets and Assess Risk
For effective access controls, the first step is to identify all data that you store, process, and transmit. Second, you need to assess the data’s criticality and risk level. Finally, you need to identify users who access information and assess the risk they post to the organization.

As part of this, you should consider:
- Standard users
- Privileged users
- Users’ payment processing authority level
- Financial information
- Personally identifiable information
- Sensitive corporate information

Once you assess user and data risk, you can create a plan that helps you migrate the information securely. When setting controls, you should limit access according to the principle of least privilege and create fine-grained access privileges.

2. Normalize Data Access Across Integrated Applications
With SaaS applications, organizations no longer need to commit to a single platform. They can pick and choose the applications that best meet their needs, which can mean integrating multiple vendors.

As you build out your application stack, you need to maintain appropriate access controls. This can be difficult when vendors define access rights differently. Many organizations worry that normalizing access data requires an expensive, labor-intensive overhaul of their Identity and Access Management programs.

However, if you focus on visibility instead of connectivity, you can leverage automated tools that help you see into user access. Tracking user access in a single location, despite disparate access definitions, enables you to protect data security and privacy even across different application vendors like SAP and PeopleSoft.

3. Leverage Contextual Attributes
A primary benefit of hybrid on-premise and cloud ERP systems is the ability for people to work wherever they want. However, that same flexibility drives many of the security and privacy risks companies face. Adding context to your access permissions is another way to secure data. After setting your role-based controls, you should consider adding context such as time of day, geographic location, and IP address. With these attribute-based access controls (ABAC), you can more granularly define how users interact with data, making it easier to detect anomalies.

4. Enable Step-Up Multi-Factor Authentication
ABAC also enables you to use step-up multi-factor authentication (MFA). Step-up authentication is a process where users need to re-authenticate into an ERP application when they attempt a privileged function or transaction. ABAC enables you to trigger step-up MFA when your system detects an abnormal attribute, often one associated with credential theft.
For example, one of your users always logs in from California, USA. If the user tries to access the ERP’s payment module from Ontario, Canada, the system will notice that this is an outlier, an abnormal attribute for this user. The system can require re-authentication, additional proof that the person is who they say they are. If this is a cybercriminal leveraging stolen credentials, then the step-up authentication acts as an additional security and privacy control, preventing unauthorized access.

5. Continuously Monitor User Behavior Around Data Access and Usage

Modernizing your ERP security and privacy controls also includes continuously monitoring for anomalous and suspicious activity. Gaining a granular view into data access and use is a way to proactively mitigate risks that can arise in a remote workforce accessing ERP solutions. Continuously monitoring access can help you gain insight into employee productivity, cybersecurity risks, and insider fraud. Tracking when and how employees use data gives you a way to set baselines for “normal” activity—any deviations from this warrant further investigation.

For example, a user consistently accesses your ERP between 8 am and 5 pm from a location in the United States. If the user suddenly accesses the system at 2 am, the anomalous activity could indicate fraud. Even if you’re using step-up MFA to prevent that activity, you still need to investigate the event. While it may be someone with insomnia, it can also be an employee trying to steal information or money.

Digital Transformation and ERP Modernization are Two Sides of the Same Coin

The term digital transformation can mean different things to different organizations. To some, it’s a clever way to say, “moving the cloud.” To others, it’s about rethinking old operating models. And in the case of this white paper, it’s also about updating and modernizing legacy ERP technology.

Organizations with legacy ERP systems must determine the right mix between digital transformation and modernization so they’re not “sacrificing” data security, privacy, or compliance policies. Taking a proactive, data-centric approach to ERP security and data privacy during your company’s digital transformation can mitigate risks before they turn into realities.

About The Appsian Security Platform

The Appsian Security Platform (ASP) combines sophisticated controls to secure user authentication, dynamically control user access to data / pages / transactions, limit data exposure, and provide granular user behavior visibility. Legacy ERP customers can create a data-centric strategy to detect, prevent, and respond to risk while proving regulatory compliance.

Appsian provides the fastest path to strengthening ERP data security & compliance for some of the largest organizations in the world using SAP, Oracle E-Business Suite, and Oracle PeopleSoft. Using a software platform designed for intrusion prevention, data loss prevention, threat detection & response, Appsian helps legacy ERP customers attain the deepest levels of control and visibility. Appsian is an Oracle and SAP technology partner and has 275+ customers worldwide.

To learn more, visit www.appsian.com