NEXTLABS® | Deloitte.

Prevent Data Loss Across the ERP Landscape

Contents

Prevent Data Loss Across the ERP Landscape 03

What Type of Data is Found in ERP System? 04

Understanding Data Loss in ERP Systems 05

Approach for Preventing Data Loss in ERP 07

Prevent Data Loss with NextLabs Zero Trust Data Security Suite for ERP 08

Case Study 11

Prevent Data Loss Across the ERP Landscape

Shaping the digital backbone of an enterprise, Enterprise Resource Planning (ERP) systems are instrumental in unifying core business processes, a feature that deepens the risk of data loss and underscores the importance of preserving data accuracy and compliance. Embodying highly sensitive information, data in ERP systems mandate stringent access control measures to prevent unauthorized data extraction.

Furthermore, when data flows from ERP systems into downstream systems such as data warehouses and analytics platforms, it calls for a secure end-to-end data pipeline. Enterprises need to ensure there is no data loss in both ERP and downstream systems, each possessing its own distinct access controls and permissions.

In this white paper, we will dive into the methods used to prevent data loss within ERP systems. We tackle challenges such as safeguarding essential business data for big data analytics, managing the complexities of evolving systems, handling extensive data volumes, and ensuring data integrity. Relevant to key ERP systems such as SAP ERP, SAP/S4HANA, Microsoft Dynamics 365, and Oracle, this paper offers strategic insights for organizations seeking to enhance their data security measures in the dynamic ERP environment.

What Type of Data is Found in ERP System?

As central hubs for diverse business functions, ERP systems are instrumental in enabling intelligent decision-making. At the heart of these systems lies a wealth of data types, which includes:

- **Transaction Data**: Captures every business transaction and serves as a record for auditing and tracking business activities.
- **Financial Data**: Provides a comprehensive view of the organization's financial health, essential for strategic planning, regulatory compliance, and fiscal management.
- **Human Resources Data**: Encompasses employee information, pivotal for workforce planning, performance management, and ensuring compliance with labor laws.
- **Customer Data**: Records customer interactions, preferences, and history, manages customer relationships, targeted marketing efforts, and sales strategies.
- **Supply Chain Management Data**: Tracks the flow of goods and services, from procurement to distribution, helps optimize supply chain efficiency and responsiveness.
- **Product and Logistics Data**: Involves details of product management and distribution, key for inventory control, product development, and efficient logistics operations.
- **Compliance and Risk Management Data**: Aids in identifying, assessing, and mitigating operational risks, key to maintaining legal and regulatory compliance.
- **Business Analytics Data**: Derived from various sources, this data is instrumental in strategic decision-making.

The diverse spectrum of valuable data highlights how ERP systems are vulnerable not only to cyberattacks but also to internal risks like fraud and conflicts of interest. These vulnerabilities, along with the need for strong Segregation of Duties (SoD), underscore the importance of compliance in ERP systems. Protecting against data loss in ERP systems is crucial for maintaining business continuity and safeguarding trade secrets, positioning it as a strategic imperative for any forward-thinking enterprise.

Understanding Data Loss in ERP Systems

Linked to multiple applications and networks, the interconnected nature of ERP systems creates multiple potential points of entry for attackers. The risk is compounded in remote work and mobile device usage, where personal and professional data coexist on the same device and increase the chances of accidental data breaches.

The vast number of users and services accessing ERP systems also complicates access control requirements, which can pose a roadblock in efficient collaboration among workforces. Safeguarding against data loss requires a delicate balance between accessibility and security, so that employees can perform their tasks effectively without compromising data integrity and confidentiality.

In addressing the data loss challenges associated with ERP systems, it is crucial to establish comprehensive security requirements that safeguard data at every level. These requirements form the backbone of a robust ERP data security strategy:

- **Secure Data at All Access Points:** The first line of defense in protecting data in an ERP system is to secure data at the source, at rest, in use, and on the move. Encrypting data at rest and in transit prevents unauthorized access and ensures that even if data is intercepted, it remains unreadable. Additionally, securing data at its source involves implementing strict controls over data entry points to prevent malicious injections or unauthorized access.

- **Secure the Application Itself:** This involves regularly updating and patching the software to address vulnerabilities, using strong authentication methods to control access, and conducting regular security audits and assessments to identify and mitigate potential risks.

- **Implement Strong Security Measures for Data Sharing:** When sharing data, whether internally or with external partners, prevent unauthorized extraction with encrypted channels for data transmission, strict access controls and authentication processes for data retrieval, and data loss prevention tools to monitor and control data transfer.

- **Encrypt Data during Transmission and ETL:** When aggregating data from multiples sources into a data lake or enterprise data warehouse, particularly during ETL (Extract, Transform, Load) processes, special attention must be paid to data encryption to prevent unauthorized exposure. Implementing logical data segregation, which involves classifying and controlling access to data based on sensitivity, user roles, or functional requirements, is key to enhancing security and privacy within these processes.

By meeting these requirements, organizations can significantly enhance the security of their ERP systems, reducing the risk of data breaches, and ensuring operational continuity.

Approach for Preventing Data Loss in ERP

The next step would be to translate security requirements into practical, effective strategies that cater to unique operational needs. The below approach does not dictate a linear progression; organizations can start from any point, ensuring alignment with best practices in data security:

- **Data Classification:** Know your data within the ERP and apply appropriate labels based on sensitivity levels and apply corresponding security measures.
- **Data Segregation:** Automatically segregate data based on roles or functions, thereby enforcing separation of duties.
- **Redaction and Obfuscation:** Implement dynamic data masking and redaction techniques to hide or anonymize sensitive information.
- **Need-to-know Access Control:** Implement attribute-based access control (ABAC) to ensure that users have only the necessary permissions to perform their specific task.
- **Secure Data at Rest:** Protect data against misuse of credentials by privileged users/super admins with techniques such as encryption.
- **Secure Data in Use:** Control access and usage of unstructured data within the ERP system with industry standard DRM tools.
- **Data Lifecycle Management:** Establish policies for the entire data lifecycle, including creation, storage, transmission, retention and destruction.
- **Prevent Data Leakage:** Implement DRM solutions and data extraction policies to prevent unauthorized access and breaches of ERP data.
- **Real-time Monitoring and Prevention:** Utilize tools for continuous monitoring of data activities and respond to anomalies in real time.

Prevent Data Loss with NextLabs Zero Trust Data Security Suite for ERP

NextLabs’ Zero Trust Data Security Suite effectively implements the aforementioned strategies, integrating functionalities of data access security, externalized authorization management, data loss prevention, and enterprise digital rights management into one comprehensive suite. The software suite applies policy-based enforcement to prevent data breaches and safeguard data in real time, with its dynamic authorization and attribute-based access control technology.

Features of the Suite include:

Zero Trust Policy Platform with Real-Time Enforcement

CloudAz continuously verifies every access request to ERP systems, regardless of origin. It makes authorization decisions based on user behavior and context, ensuring secure access.

Strengthened Governance

CloudAz manages data effectively throughout its lifecycle, encompassing features such as policy auditing, access control, and data classification. It implements policies and standards governing data collection, storage, sharing, and usage within an organization. This approach not only prevents security violations but also fortifies data governance. By employing policy-driven security controls, CloudAz automates zero trust data protection and compliance measures.

Data-Centric Security

Implementing policy-based access controls is key to ensuring that data is secured at all stages, whether in use, in transit, or at rest. NextLabs offers a suite of policy enforcers (Application Enforcer, SkyDRM, and Data Access Enforcer) to proactively prevent unauthorized access of data across applications, file repositories and databases, even in compromised systems.

Preventing Wrongful Extraction

Application Enforcer automates the enforcement of data extraction policies to mitigate data leakage at the point of access.

Encryption for Data Protection

SkyDRM employs Digital Rights Management which controls access and usage of encrypted files, thereby enabling secure collaboration without the risk of data loss. Data Access Enforcer (DAE) uses Format-Preserving Encryption to encrypt data in use, preventing unauthorized direct access of sensitive data and complying with relevant regulations.

Segregation and Masking

DAE protects data at rest through techniques such as dynamic data segregation, redaction, and obfuscation, to mask sensitive information in ERP systems.

Automation and Prevention

CloudAz's Dynamic Authorization policy engine operates by analyzing real-time attributes to make authorization decisions, which are promptly implemented by policy enforcers, thereby streamlining the automation of security measures. This ensures that access rights are granted based on up-to-the-minute information.

Monitoring, Tracking, and Auditing

A key goal is to ensure visibility across all data flows. CloudAz facilitates continuous monitoring and tracking of data movements and user activities within ERP systems, which is essential for an effective strategy to prevent data loss.

Case Study

In the following case study, we delve into the practical implementation of strategies for preventing data loss, focusing on how they effectively address the data security challenges of globalized corporations. The study will focus on issues related to sensitive information management in SAP systems and ensuring robust export compliance and intellectual property protection.

Case Study

Part 1: Automating Need-to-Know Access in SAP for a Multinational Oil & Gas Company

Challenge: A leading oil and gas corporation needs to protect sensitive information related to vendors and partners, mask Personally Identifiable Information (PII) and financial data, to comply with data privacy regulations.

Solution

Ensure data privacy with dynamic data masking

Using zero trust policies to dynamically mask data with modified content.

Enhance SAP security through automated role provisioning

Integrating automated role provisioning within the SAP system ensures that access rights are granted in alignment with current roles, establishing 'need-to-know' access.

Efficient compliance management

Automated systems can be configured to comply with industry-specific regulations, ensuring the company is compliant without constant manual monitoring.

Part 2: Strengthening Export Compliance and IP Protection

Challenge: The chemicals division of this multinational oil and gas firm needs to manage export compliance and safeguard intellectual property (IP) in dealings with external suppliers and potential joint venture partners. Their existing Role-Based Access Control (RBAC) system is struggling to keep pace with the demands of the extended enterprise.

Solution

Fine-grained access control

Use ABAC to evaluate policies and attributes in real-time for export compliance and IP protection.

Digital rights management to protect data shared externally

Persistent control of access and usage of digital information stored in file regardless of where it exist. Access rights are updated in real time as employees transition between departments, projects, or locations.

Simplify policy management

Simple and quick implementation of policy changes, which are automatically enforced across the global enterprise, keeping pace with evolving business needs.

Summary

This white paper has comprehensively addressed the pressing need for robust data loss prevention strategies within ERP systems, which are integral to the operational efficiency and strategic decision-making of modern enterprises. We have explored various aspects of data security, from the types of data stored in ERP systems to the specific challenges and methods employed to prevent data loss.

Key takeaways include the importance of securing data at all access points, updating and patching ERP software, implementing strong security measures for data sharing, and ensuring data segregation and privacy during ETL processes. Additionally, it highlighted the significance of data classification, need-to-know access control, secure data handling, lifecycle management, and real-time monitoring. These strategies are crucial for protecting a wide range of data types, including transactional, financial, HR, customer, supply chain, compliance, and business analytics data, against the complexities of evolving systems and extensive data volumes.

Looking ahead, the landscape of data security is set to evolve dramatically. We foresee an era where sophisticated cyber threats become more prevalent, necessitating advanced security measures. The rise of emerging technologies like AI and blockchain is anticipated to redefine data security practices, offering both new opportunities and challenges. Furthermore, the global landscape of data protection regulations is continuously evolving, requiring businesses to stay agile and informed. Organizations must prepare to adapt to these changes proactively, ensuring compliance while safeguarding their data assets.

NEXTLABS®

Follow Us

https://www.nextlabs.com/contact-us

NextLabs®, Inc. provides data-centric security software to protect business critical data and applications. Our patented dynamic authorization technology and industry leading attribute-based policy platform helps enterprises identify and protect sensitive data, monitor and control access to the data, and prevent regulatory violations – whether in the cloud or on premises. The software automates enforcement of security controls and compliance policies to enable secure information sharing across the extended enterprise. NextLabs has some of the largest global enterprises as customers and has strategic relationships with industry leaders such as SAP, Siemens, Microsoft, and IBM. For more information on NextLabs, please visit http://www.nextlabs.com.