

Protecting Sensitive SAP Data with Dynamic Access Controls

Traditional SAP security authorization models are inefficient and risky. They burden security teams with redundant, manual role management and expose sensitive data to potential breaches and regulatory non-compliance. Without dynamic access controls, organizations struggle to adapt to evolving threats and regulatory demands, resulting in elevated risks and costly compliance violations.

Static Security in A Dynamic World

Traditional Role-Based Access Control (RBAC) models use static, role-based policies to govern user access to data fields. These coarse-grained policies fail to account for user and environmental attributes that could indicate contextual risk to sensitive SAP data. As a result, security teams are often bogged down by redundant and manual role redesigns, struggling to maintain an updated and secure access control system.

The limitations of RBAC models lead to several critical issues. Insecure data access increases the risk of data breaches and regulatory non-compliance. Organizations are left vulnerable to unauthorized access without considering contextual attributes, potentially exposing sensitive data. Notably, 74% of SAP breaches involve access to privileged accounts, further emphasizing an RBAC model's security flaws. This heightens the risk of data breaches and leads to costly compliance violations and a reactive approach to data governance.

The Need for a Dynamic Access Control with ABAC

Rather than manually reconfiguring role authorizations for every new user, evolving regulatory requirement, or shifting application landscape, envision a centrally managed policy engine that adapts in real-time to mitigate risks and ensure continuous data security. This dynamic approach allows for contextual identification of access control risks and automatic enforcement of preventative data security controls. By adopting an Attribute-Based Access Control (ABAC) model, security teams can proactively prevent cybersecurity threats, govern data access with greater granularity, and streamline regulatory compliance, thereby transforming the security posture of business-critical SAP systems.

Not only does the ABAC model avert regulatory compliance violations and fines, but it also eliminates the need for redundant role management and manual data discovery and classification efforts. By implementing ABAC, security teams can transition from reactive to proactive processes, centralize access control management, and streamline the categorization of unstructured data. This improvement in collaboration and visibility drives robust data security. Instead of constantly playing catchup as users and systems change, organizations can focus on strategic initiatives to safeguard valuable data more efficiently. These efficiency gains also lead to significant cost savings by improving internal budgeting and avoiding costly regulatory fines.

Dynamic Access Controls (DAC)

- Drive Security Efficiency
- Reduce Manual Effort
- Robust Risk Prevention
- Dynamic and Contextual Data Governance
- Automatically Log User Activity
- Standardize and Centralize Access Control Policies
- Streamline Data Privacy and Regulatory Compliance with Multiple Requirements
- Automate Classification of Unstructured Data

Streamlined Compliance and Governance

Adopting a Dynamic Access Control (DAC) approach doesn't just prevent risks to sensitive data and ensure regulatory compliance – it completely transforms the potential of your organization's data security and governance program. By standardizing access controls and applying preventative security controls based on dynamic policies, you streamline compliance efforts and reduce the burden of role management. Automated policy enforcement and comprehensive activity logging enable your organization to thrive amid the constantly evolving cybersecurity threat and regulatory compliance landscapes.

Enhanced Data Security with Dynamic Data Masking

The ABAC authorization model and Dynamic Data Masking capabilities are the cornerstone of the DAC product. The ABAC model serves as a centralized repository for all internal and external security and compliance policies relevant to your critical SAP applications. Creating and managing these policies is as simple as selecting options from a drop-down filter, allowing for easy updates as requirements change. Once defined, these policies require little to no overhead maintenance, effectively driving Dynamic Data Masking and other preventative data security controls. This approach not only anonymizes sensitive data but also ensures that access is granted based on contextual and dynamic criteria, significantly enhancing data security.

ABAC and Dynamic Data Masking

- Dynamically Obfuscate Sensitive Data Based on Risk Context
- Driven by ABAC Policies and Scale Across all T-Codes
- No Need for One-to-One User or T-code Mappings
- Source Attributes from Other Solutions in your IT Stack
- SAP-Native Add-On
- Time and Cost Savings



The Power of Pathlock's Dynamic Access Controls

Pathlock's Dynamic Access Controls revolutionizes SAP security by addressing the limitations of traditional access control models. It streamlines SAP security by simplifying role provisioning, particularly crucial during ongoing S/4HANA migrations, and adapting to changing regulatory requirements and cyber threats. DAC ensures that authorized users get the access they need while restricting access in risky situations. This approach enables organizations to achieve fine-grained data governance, prevent cybersecurity threats, and ensure compliance. Automated policy enforcement reduces the manual workload on security teams, enhancing data security and significantly saving costs.

DAC also supports Dynamic Data Masking and other preventative security controls like Data Scrambling, Data Filtering, Data Loss Prevention, Dynamic Data Classification, and Session Logging, providing a comprehensive approach to data security, governance, and cybersecurity risk prevention. Ultimately, DAC enables you to only allow access to sensitive data under optimal conditions that are aligned to your specific security and governance policies – without hindering user productivity and operational efficiency.

About pathlock

Pathlock Cloud protects leading ERP systems and enterprise business applications and the critical business processes they power. Our Application Access Governance product helps companies enforce GRC controls and take action to prevent loss. Enterprises can manage all aspects of application governance in a single, unified platform, including risk reporting and management, user provisioning and temporary access elevation, ongoing user access reviews, and audit preparation.

One Tabor Center, 1200 17th St, Suite 880
Denver, CO 80202
Phone: +1 469.906.2100
info@pathlock.com

©Pathlock. All Rights Reserved. All logos, company names and product names, mentioned herein, are property of their respective owners.