SOLUTION BRIEF

pathlock

Establishing a Data-Centric Cybersecurity Strategy for SAP

In the ever-evolving cybersecurity landscape, SAP customers traditionally prioritize perimeter defense mechanisms such as threat detection and vulnerability management. While these detective controls are crucial components of a robust cybersecurity strategy, the emergence of new threats highlights the need for a more comprehensive approach.

With hackers discovering unknown vulnerabilities and devising new attack vectors, the challenge lies in the impossibility of accounting for all potential attack paths. Driven by the wealth of data housed in SAP systems, they are often the prime target of attacks. In fact, research has found that two of three SAP environments are breached from the outside.

While SAP's role-based access control (RBAC) is a cornerstone of its security architecture, these controls are inflexible and cumbersome to securely manage access given the range of roles required. As organizations and systems scale, hundreds of new and duplicate roles accumulate, making it impossible to keep track of who has access to what. When this is the case, if a user's credentials are compromised or an attacker successfully circumvents perimeter security measures, a plethora of the associated role-based permissions becomes exploitable. This vulnerability exposes sensitive SAP data and increases the risk of costly exfiltration. The fact that 74% of SAP breaches involve access to privileged accounts only further emphasizes the security flaws of an RBAC security model.

Recognizing these challenges, it is imperative for organizations to implement a data-centric cybersecurity strategy for SAP. Unlike traditional approaches that may fall short in the face of emerging threats, a data-centric strategy serves as a failsafe when other detective security measures have failed.

Securing the Data Layer is Key

The essence of a data-centric strategy lies in its focus on safeguarding the core asset: the data itself. By implementing attribute-based access controls (ABAC) and other preventative controls directly at the data level, organizations can mitigate the risk of unauthorized access and data loss even if perimeter defenses are breached. This approach ensures that even in the event of compromised credentials or sophisticated attacks, the critical data remains obfuscated and protected.

A key advantage of a data-centric strategy is its adaptability to the dynamic nature of cyber threats. As attack methods evolve, the strategy can be updated and refined via dynamic policies to address emerging challenges across all user roles and data fields. This proactive approach enhances the overall data security for production and non-production SAP systems, providing a multi-layered defense against constantly evolving cyber threats.

7 Key Pathlock Capabilities That Enable a Data-Centric Approach

Protecting data that resides within your SAP applications requires a multi-pronged approach. Pathlock enables this by providing multiple, layered controls at the point of access, the application and database layers, and the page and field levels.

Attribute-Based Access Controls (ABAC)

Allows you to finely control user access to SAP applications, data, and transactions by considering various attributes (citizenship, certifications, location, IP address, data sensitivity, etc.), enabling organizations to adapt to changing business needs and enforce more precise access policies.

Dynamic Data Masking

Protects your sensitive information by limiting access to certain data fields in production environments based on dynamic user attributes. This regulates user access on a need-to-know basis and enforces least-privilege SAP data security.

Data Scrambling

Encrypts or obfuscates sensitive data in non-production systems, when data is in transit, or when direct access to the database is possible. This protects your replicated test data from unauthorized access and exfiltration.

Secure Your SAP Data with Pathlock

Pathlock's Dynamic Access Controls (DAC) module ensures that authorized users receive the access they need but are restricted when the context of their access is indicative of risk. This dynamic approach enables organizations to only allow access to sensitive data under optimal conditions that are aligned to your specific security and governance policies.

Our masking module utilizes a combination of access context and user attributes to determine permissions, and in turn, dynamically masks specific data fields depending on your policies. Deployment is a breeze with our flexible, one-to-many rules engine that allows you to deploy a sophisticated data privacy strategy with ease – across thousands of data fields and user roles.

Data Loss Prevention (DLP)

Prevents the unauthorized transmission of sensitive data outside your SAP environment. By controlling what data is downloadable, monitoring and blocking risky downloads, and triggering alerts, you can eliminate the risk of costly data leaks and ensure compliance with regulations like GDPR, ITAR, SEC Cyber Rule, and SOX.

Attribute Enrichment

Sourcing contextual attributes from all applications in your IT stack improves access control security and aligns policies for your SAP environment with the policies from the rest of your IT application infrastructure, reducing manual role management efforts and enabling role standardization.

Dynamic Policy Management

Enables authoring and management of ABAC policies for dynamic authorization across multiple applications using a single, unified interface. This eliminates the need to modify every GUI T-code or Fiori app to implement ABAC controls.

Data Access Logging and Alerts

Automatically log critical events or user access to sensitive data and leverage real time insights to quickly detect unauthorized activity. Automated alerts enable non-technical users with simple self-service reporting workflows.

Benefits

Pathlock helps simplify SAP data security and compliance by offering a solution that is easy to implement and can be customized based on your unique business needs. Designed specifically for SAP, the solution can be installed using your existing SAP resources without the need for additional hardware and with minimal storage requirements.

Eliminate Role Explosion and Proliferation

Pathlock's Dynamic Access Controls (DAC) module leverages an ABAC model to eliminate the need for excessive roles to address conditional and complex user authorizations. This enables dynamic role assigning, eliminates creation of one-off and duplicate roles, and overall streamlines access control across all users in all systems.

Enforces Data Security in Non-Production Environments

Organizations often rely on external auditors, consultants, and contractors for SAP system support. However, sensitive test data in non-production environments poses security risks. Implementing an ABAC policy, scrambling sensitive data, and using dummy data for external access ensures the security of duplicate data.

Data Security for Migration Projects

Amid digital transformations and S/4HANA migrations, there are user authorization and data security concerns with shifting architectures. The dynamic ABAC model addresses these by eliminating role re-design projects, enhancing access control policies, and protecting production and test data during migrations.

No Overhead Maintenance of Policies

Once ABAC security policies are defined, there is little to no required maintenance on a per-role basis. This ensures access controls effectively and securely scale with the business.

Automated Audit Reporting

OOTB workflows and templates enable tamper-proof, audit-ready reporting and analysis. Contextual logs and activity logging deliver attestations and demonstrates data privacy and regulatory compliance.

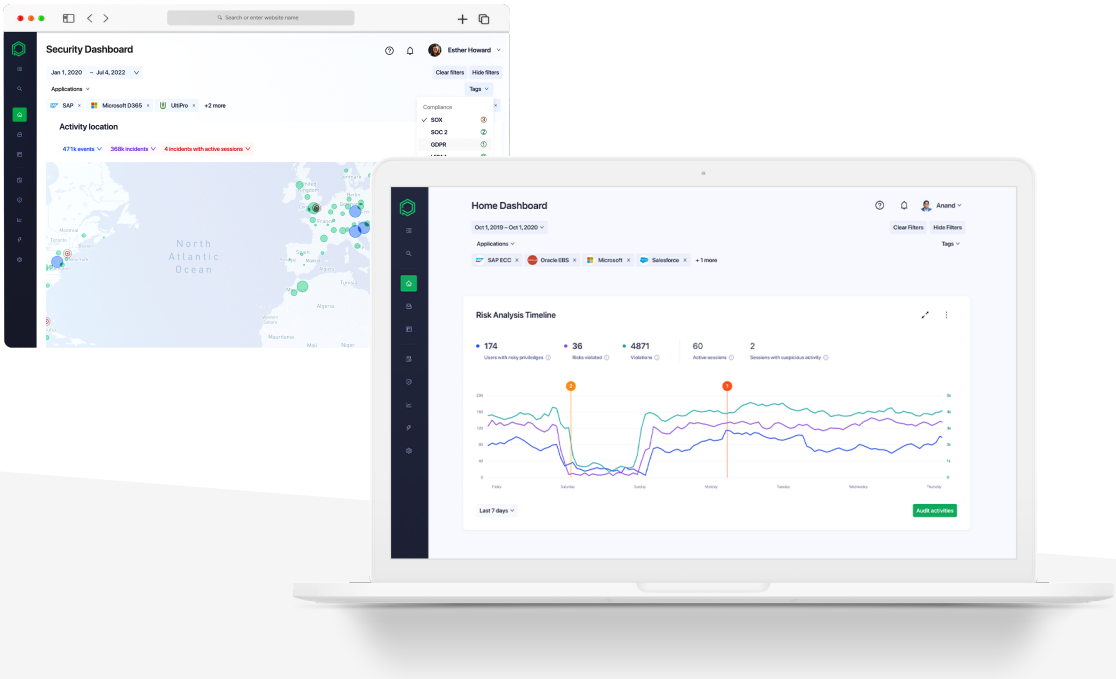
Automate Risk Prevention

The module automatically blocks risky transactions as defined in the dynamic ABAC policies and enforces strict data loss prevention (DLP) mechanisms. It triggers automated alerts and blocks unauthorized activities, ensuring secure user access and data transfers.

Achieve a Zero Risk Application Landscape

Pathlock DAC enables a least-privilege strategy for SAP data security and access control. The module empowers customers to preventatively secure their business-critical applications by protecting sensitive data and dynamically governing user access, enabling a true Zero Risk environment.

Benefits



About pathlock

The Pathlock Cloud protects the leading ERP systems and enterprise business applications and the critical transactions they power. Our application governance product helps companies enforce GRC controls and take action to prevent loss. Enterprises can manage all aspects of application governance in a single platform, including user provisioning and temporary elevation, ongoing user access reviews, control testing, transaction monitoring, and audit preparation.

For more information, visit www.pathlock.com » or get in touch » with us for a demo.

8111 Lyndon B Johnson Fwy, Dallas, TX 75251
Phone: +1 469.906.2100
info@pathlock.com