Protect Critical SAP Transactions and Address Business Risks

Pathlock Security Platform for SAP

Pathlock enables SAP customers to effectively address the risks associated with ERP business transactions. By adding sophisticated controls that strengthen access policies and enhance logging & analytics capabilities – unauthorized activities that lead to fraud, theft, and error are prevented.

Pathlock's solutions leverage a 'data-centric' approach, designed to overcome the limitations of SAP's native security and compliance features. Thus, allowing organizations to fully align their enterprise information security policies with business objectives.

| Secure Access | Mitigate Risk | Detect Threats | Simplify Compliance | Streamline Audits |

Avoid Losses from Fraud and Theft
Fraud costs enterprises ~7% of annual revenue. Protect your bottom line with advanced prevention and detection capabilities that stop fraud in SAP business transactions

Prevent Unauthorized Data Exfiltration
Prevent data leakage from both privileged accounts and normal end-users by limiting what data can be exfiltrated and ensuring data can only be exfiltrated from SAP in secure environments

Limit Financial Risks from Policy Violations
Avoid losses from violated business policies inside key SAP transactions. Limit edits, revisions, and submissions (w/o proper documentation) that lead to unnecessary financial losses

Avoid Non-Compliance Penalties
Automate manual, time consuming audit and remediation processes that are required for new and upcoming data privacy mandates

Platform Overview

Pathlock Security Platform delivers a contextual, granular-level approach to securing SAP access. Residing natively in the SAP App Server, the solution requires no additional hardware and its direct integration delivers unparalleled capabilities.

IMPROVE CONTROL

Adaptive Data Access Control

- Extend Fine-Grained Access Controls that Consider Attributes & Context
- Protect Sensitive Data with Centralized, Policy-based Data Masking
- Minimize Financial Risks with Field-level Rate-limiting Controls
- Prevent SoD violations with supplementary ABAC Polices

ENHANCE VISIBILITY

Real-Time Data Analytics

- Gain Full Visibility into User, Data, and Transaction Activity with Context
- Streamline Manual Audit and Compliance Processes
- Enable Non-Technical Employees with Simple Self-Service Reports
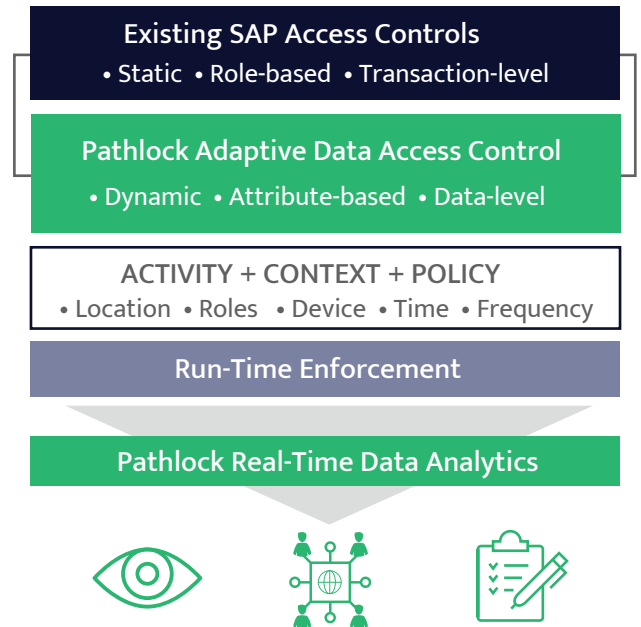- Leverage Real-Time Insights to Quickly Detect Unauthorized Activity

How It Works

Two core components work together to form Pathlock Security Platform. First, **Adaptive Data Access Control** serves as an additional authorization layer within SAP. This allows your business to strengthen controls and further extend policy logic to include **field-level values** (e.g. expense or purchase values) and **access context** (i.e. network, location, time, transaction count, + more).

Pathlock's dynamic access control policies then account for previous user activity and the varying business criteria to make authorization and risk management decisions at run-time.

The second component, **Real-Time Data Analytics**, captures this activity, enriches the data, and sends the information to its centralized reporting tool for further risk analysis. Granular details on user behavior and transaction activity can be exported into reports, used in real-time monitoring dashboards, and trigger remediation workflows and configurable alerts.

VISIBILITY | CONTROL | COMPLIANCE

Existing SAP Access Controls
- Static • Role-based • Transaction-level

Pathlock Adaptive Data Access Control
- Dynamic • Attribute-based • Data-level

ACTIVITY + CONTEXT + POLICY
• Location • Roles • Device • Time • Frequency

Run-Time Enforcement

Pathlock Real-Time Data Analytics

About Pathlock

The Pathlock platform protects the leading ERP systems and enterprise business applications and the critical transactions they power. Our application governance solutions help 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.

pathlock