APPSIAN

DATA SHEET

Application Security Platform for SAP

Application Security Platform for SAP

APPSIAN

Appsian's Application Security Platform offers SAP users a contextual, granular-level approach to securing their SAP environments

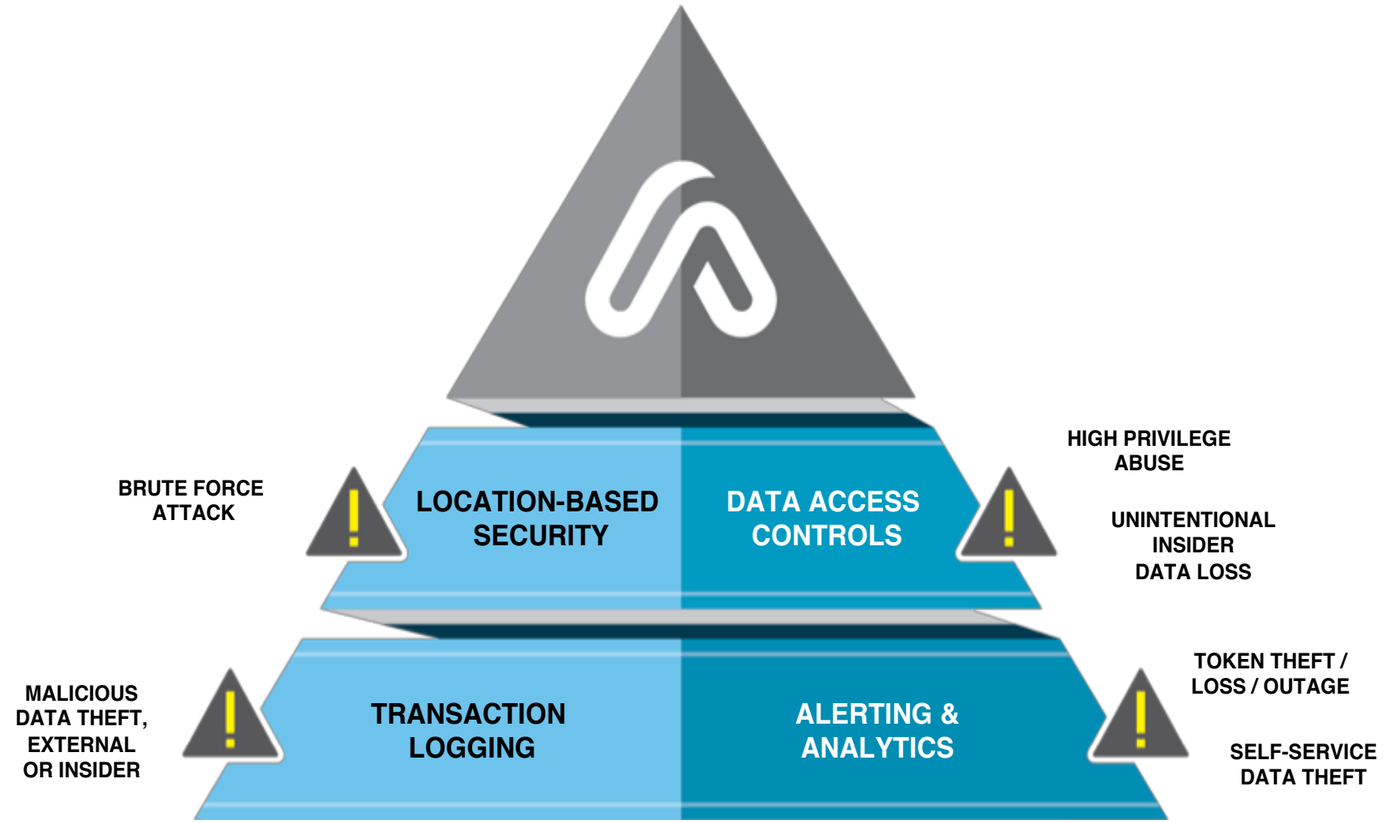
Key Use Cases

Deploy dynamic context-based access controls
Improve security across SAP without impeding productivity by enforcing context-specific policies that balance security priorities with usability demands

Gain direct visibility into SAP activity
Enhance SAP logging capabilities to provide insight into user activity at the transaction and field levels for both standard and custom transactions

Perform forensic investigations with full context
Capture a complete audit trail of user activity enriched with user attributes and tagged with SAP data attributes

Expedite detection and response with visualized analytics
Equip your security operations center with real-time visualized dashboards fed with enriched logs to quickly spot suspicious activity and drill down to root out issues.



Access Control

Protect sensitive data from unauthorized access by enforcing granular, context-aware security policies in SAP. Implement preventive controls that enforce access rules based on known business risks, such as separation of duties.

Control access to SAP based on:

- User attributes
- Data attributes
- Activity type
- IP address
- User activity trends

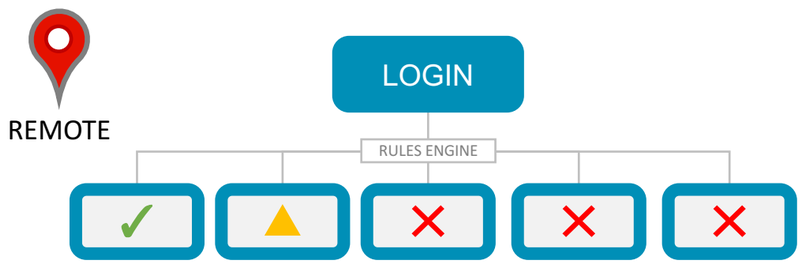
Enforce granular access policies such as:

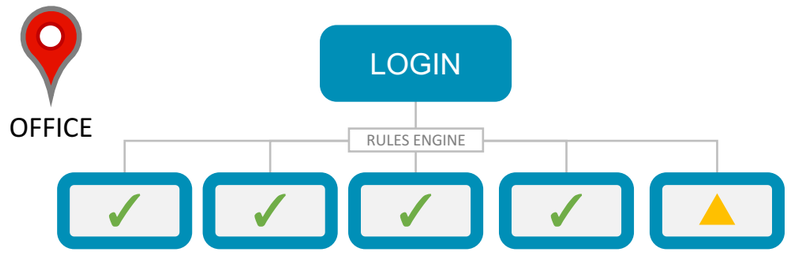
- Allow/block access to SAP transactions and sensitive fields
- Allow/block execution of conflicting business processes through mitigation and process controls
- Allow/block specific user actions (i.e. running queries, exporting reports)

Privileged Access Management

Improve control and visibility of your highest risk user accounts.

- Controlled access for shared batch or admin accounts





Data Loss Prevention

Prevent unauthorized exposure of sensitive information and protect against insider data leakage with dynamic, context-aware DLP policies for SAP.

Dynamic DLP Policies

- Configure access control rules to enforce policies in SAP that can restrict transactions based on user and data attributes
- Block / stop the download of data, for example, from outside a corporate network.
- Enforce access control rules uniformly across both standard and custom transactions or data fields

Data Masking and Redaction

- Deploy context and attribute-based policies for dynamic data masking
- Mask / Redact fields in SAP based on the context of access
- Implement Sensitive Data Masking policies in prod. and non-prod. environments

Click-to-View Field Masking

- Prevent unnecessary exposure of sensitive data while still allowing users to view data with expressed intent
- Use click-to-view to unmask data, or require a MFA challenge before data is revealed
- Log all click-to-view actions to have a structured record of sensitive data access

Secure SAP Reports

Prevent exfiltration of sensitive data records through Quickviewer or Queries by enforcing access controls by role or location, or by requiring a MFA challenge for reauthentication.

Improve GDPR Compliance

Reduce the exposure of PII with dynamic data masking for sensitive fields within SAP. Click-to-view functionality protects against unnecessary exposure while logging intentional access of sensitive information.

Protect Non-Production Environments

Implement masking functionality across non-production environments to control access for development or testing teams. Further secure remote resources with location-based access controls.

Activity Logging

Appsian's Application Security Platform enhances SAP's default logging capabilities by providing transaction-level activity logs that capture granular, real-time information on who a user is, what they're trying to access, and where they're coming from.

Capture granular log data such as:

- User ID
- Transactions Performed
- Fields Accessed
- IP Address
- Application Server
- Date & Time

Creation of Targeted Logs

- Activity for specific content (i.e. PII)
- For specific roles (i.e. administrators, 3rd parties, etc.)
- Click-to-view activity of masked sensitive data

Flexible and configurable logging

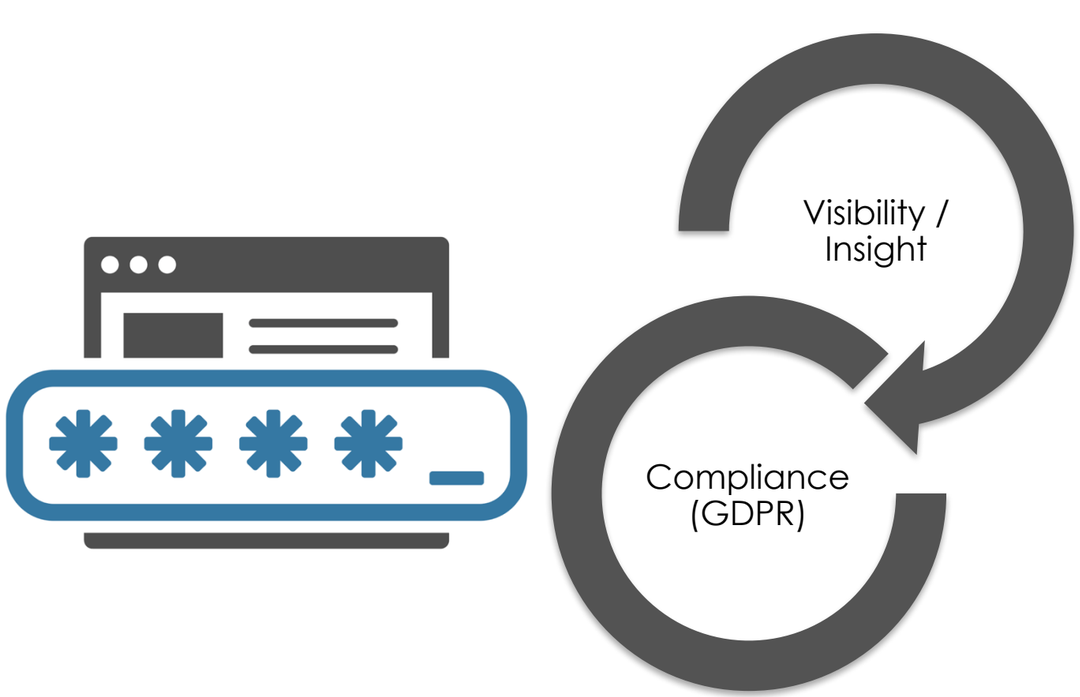
Regulatory Compliance

Direct visibility necessary for compliance

- View and record all activity inside SAP to align to compliance requirements such as GDPR, CCPA., and more.

Improve auditing capabilities

- Eliminate much of the complexity that comes with database audits and provide streamlined methods for administrators to run reports and perform audits



Real-Time Analytics

Accelerate threat detection, reporting and response with pre-configured dashboards. Real-time data trends are aggregated, enriched, and visualized with Appsian Security Analytics

Log Enrichment Process

Appsian uses an in-depth understanding of SAP to correlate user activity with common actions that organizations should be aware of – eliminating the time consuming need to translate unstructured logs into actionable information.

Data Loss Prevention

- Trending data by sensitivity
- Trending privileged user access
- Security changes tracking

Incident Response

- Forensics at User ID and IP levels
- Detect breaches / attacks in real-time

Critical Insights for Data Privacy Compliance

- View real-time access trends of sensitive data such as personally identifiable information (PII) and protected health information (PHI)
- Drill down to see all access of specific records

Improve Post-Breach Forensics

- Execute a rapid response to possible security threats
- Eliminate much of the manual work required for performing audits
- Remain compliant with new data privacy regulations (ex. GDPR)

Unified Rules Engine

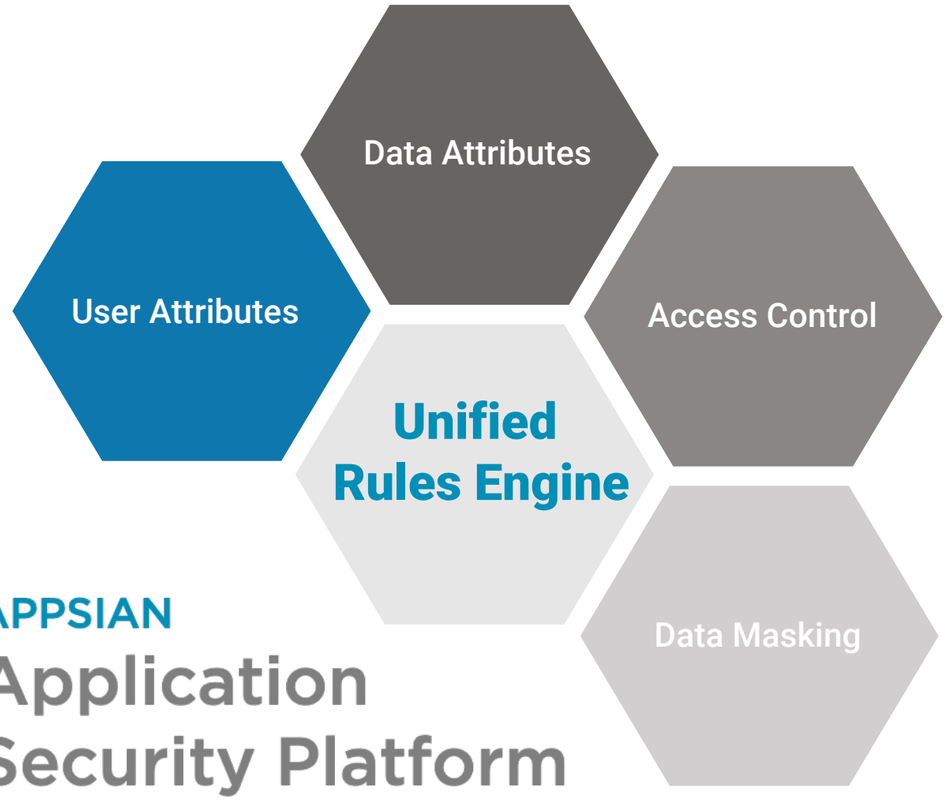
Appsian's Application Security Platform leverages a centralized rules engine to apply contextual policies throughout SAP. Residing natively inside the SAP architecture, the rules engine can combine both master and transactional data in SAP with user and contextual access data to enforce granular security policies

Policy Templates
Utilize pre-built templates for common roles, use cases, or compliance requirements to expedite implementation

Versatile Configuration
Create custom policies with contextual logic to conform to any corporate or regulatory requirement

Native to Your SAP Environment
Incorporate artifacts within SAP to build policies specific to your organization's SAP environment (i.e. customizations)

- Combine DLP and access control rules to enforce granular policies
- Dynamic policy framework leverages triggers and response actions
- Build policies using Boolean logic, nested rules, and rule groups
- Selectively target or exclude specific users and define exception rules



Application Security Platform for SAP

APPSIAN

Process Flow