transmit security

SERVICE BRIEF

Simplify Workflow Orchestration with Identity Decisioning

Easily adapt decisioning to changing business needs by creating **no-code custom rules in minutes**.

Complex decisioning logic hinders teams' ability to integrate, test, deploy, and manage rule sets. Simplifying the development and management of decisioning rules enables more accurate threat detection while reducing operational costs.

Challenge

Risk signals from siloed solutions are hard to correlate & analyze

To detect sophisticated attacks, businesses must stitch together multiple risk signals, often using multiple solutions that make data correlation complex, labor-intensive and prone to errors.

Customizing business logic extends time to value

New risk detection solutions must be tested and tuned to adapt to unique business needs, resulting in a protracted time to production and even longer time to develop meaningful results.

Cumbersome programmatic rules are difficult to understand

As rules grow more complex, it becomes harder to decipher their purpose, order and versioning — further complicating their ongoing maintenance and improvement.

Solution

Centralized decisioning service for creating logical, boolean rules

Implement unique business logic by entering a handful of parameters:

1. **Select a rule type** from multiple services that enable input from a range of identity events.
2. **Create rule conditions** by choosing the identity attributes to validate.
3. **Add a boolean operator and input value** for each attribute — for example, a range of IP addresses or country codes.
4. **Select a decision** of Trust, Allow, Challenge or Deny to determine how requests that meet the conditions should be handled.

Rules are evaluated according to priority, which can be set in the UI or API.

[1](ISC)2

Key Use Cases

Optimize detection rates

Leverage centralized decisioning that consolidates a wide range of risk signals to improve fraud detection and quickly update rules for ongoing improvement.

Reduce customer churn

Leverage internal intelligence to create dynamic allowlists that minimize friction and false positives for trusted customers, resulting in fewer dropoffs.

Improve visibility & analytics

Gain a grouped view of events matching a specific rule to view and tune its impact on performance, UX & security.

Speed up development

Reduce the need for complex coding and get better control and visibility over decisioning with easy-to-use APIs or a no-code UI. Safely deploy new rules by simulating them without changing code.

Customize business logic

Easily create and instantly apply rules to meet specific use cases, such as credit score screening, or adapt to evolving threats based on specific insights.

Simplify compliance

Meet regulatory guidelines by denying or requesting an alternate ID when a document issued within a foreign country is provided for ID verification.

Native Integration with Advanced Security and Risk Intelligence Services

Leverage a no-code UI or easy-to-use APIs to write and orchestrate rules that leverage the advanced security and risk intelligence capabilities of three natively integrated services:

- **Detection and Response** uses machine learning (ML) to analyze a broad range of telemetry with behavioral biometrics, bot detection, app activity, global intelligence and other detection methods and delivers transparent recommendations based on the full context of applications and their users.
- **Data Validation** instantly evaluates the reputation and authenticity of end users' data by simultaneously comparing the information against multiple external databases for use cases like KYC, credit score evaluation and preventing stolen identities.
- **Identity Verification** extracts data from government documents that are evaluated for authenticity within seconds using 150+ weighted ML analyses and a database of 10,000+ documents, then compared to user selfies for liveness and matching based on large training datasets.

Don't give fraudsters time to adapt

Evolving threats require a fast response from fraud teams, but waiting for engineers to build out new rules gives attackers time to change their tactics and successfully avoid detection. By eliminating the need for coding, Identity Decisioning lets fraud teams safely deploy rules to target new attacks as soon as they're discovered, the visibility to quickly evaluate their impact and the flexibility to continue adapting as new evasive tactics emerge.

KuppingerCole ANALYSTS

Transmit Security Named 'Overall Leader'
in three ranking reports: Fraud Reduction Intelligence, Passwordless Authentication and CIAM Platforms.

Identity Attributes by Service

Detection and Response
- IP address
- User ID
- Browser name
- OS version
- Country of origin
- Device fingerprint

Data Validation
- Full name
- Phone number
- Email address
- Physical address
- Date of birth
- SSN

Identity Verification
- Age
- Document type
- Document country
- Document region
- Expiration date

Rules examples

Whitelist internal IPs
- Rule type > RTFBB
- Conditions > IP
- Operator > In
- Input value > IP range
- Decision > Trust

Deny risky phone numbers
- Rule type > Data Validation
- Conditions > Telesign Score API Reason Code
- Operator > In
- Input value > Code number
- Decision > Deny

About Transmit Security

Transmit Security gives businesses the modern tools they need to build secure, trusted and end-to-end digital identity journeys to innovate and grow. CX-focused, cybersecurity-conscious leaders rely on Transmit Security's CIAM platform to provide their customers with smooth experiences protected from fraud across all channels and devices. Transmit Security serves many of the world's largest banks, insurers, retailers, and other leading brands, collectively responsible for more than $1.3 trillion in annual commerce. For more information, please visit **www.transmitsecurity.com**.