callsign®

GET ON

INTELLIGENCE BEYOND RECOGNITION

Product Sheet

Decision

Policy Manager & Engine

What is a Policy

A policy is where the organization defines authentication and verification journeys of users, their activities and the content they perform them in.

It is applied dynamically via a series of rules that form multiple connected decision trees.

What is a dynamic policy?

A static policy offers everyone the same choice of authenticators for a transaction - regardless of how risky they look, or what preferences they have. This makes it difficult to trade-off between security, ease-of-use and cost.

A dynamic policy adapts in real-time. It can build on the information it has by calling external services to discover things like the user's risk profile, their location, their device and their preferences. It can then suggest the right authenticator the user for their transaction - so a low-risk user with a simple transaction might be offered a convenient and straightforward authenticator (or even a choice of authenticators), whereas a high-risk user will be asked for more demanding proof.

Helping organizations solve the identity paradox

Organizations are facing an identity paradox:

- Regulation requires that privacy can be managed by individuals e.g. GDPR and PSD2.
- Organizations are obliged to securely collect & manage any identity data they hold & be accountable for proving how they use and secure it.
- Users want a friction free experience and are prepared to trade limited privacy information for a more seamless experience.

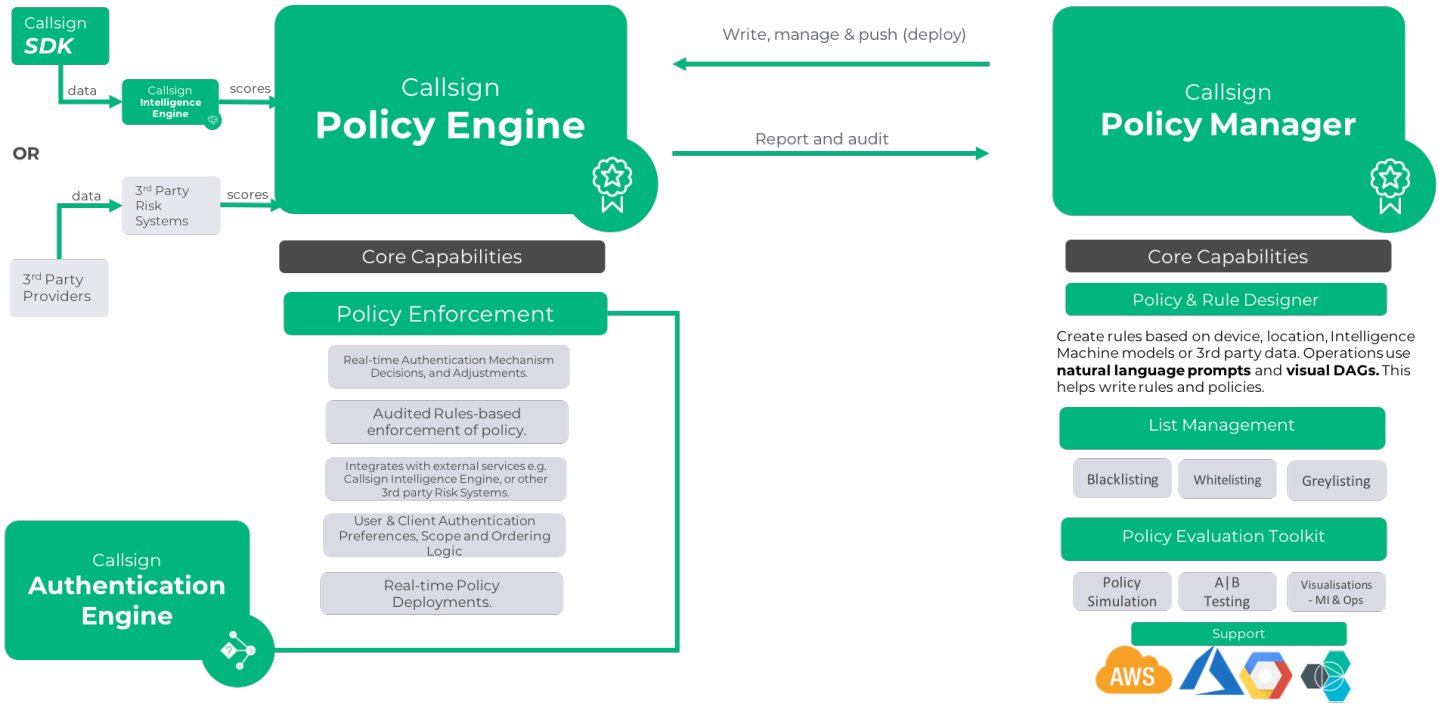
Organizations often struggle finding the right balance between customer experience and security. Turn the dial too far one way and you sacrifice the other. But finding the right balance is necessary to solving this this paradox. Organizations need the ability to turn the dials up and down as required, without huge changes to IT infrastructure.

How Callsign can help:

The Callsign Policy Manager allows organizations to build policies based on multiple data points and presents the different authentication journeys in one place, giving organizations greater visibility into their authentication landscape. This transparency delivers huge cost and time savings as organizations can develop a policy that adapts based on the data available.

For instance, the system can recognize adversaries and block the transaction at the point of request, which means costly call backs, and passport and identity checks can be avoided. Simultaneously, teams can use system calls to third-party sources such as mobile providers and security companies to confirm data in real-time, reducing the dependence on active authentication methods.

By defining a continuous authentication journey, organizations can empower users to complete transactions with minimal disruption, with the knowledge that the policy is authenticating user identity at the appropriate levels where needed.



Policy Manager

Callsign Policy Manager enables organizations to build authentication journeys based around the key authentication factors they want to support for their users. The platform fully supports Strong Customer Authentication (SCA):

- **Possession:** Something you own - e.g. payment card or mobile phone
- **Knowledge**: Something you know - e.g. password or PIN
- **Inherence:** Something about you - e.g. biometrics or behavioural data

Using the tool, administrators define under what conditions these authentication factors are required, these are based on contextual intelligence including:

- **Who:** The type of user performing the action - e.g. demographics
- **What**: The action they are performing and through what channel
- **How:** Device, location & behavioural characteristics

When rolling out a new or amended policy, reducing impact on customers is vital. Using the Callsign Policy Manager, users can phase in changes, run simulations of the policy with legacy data and release to only a small percentage of users to test results and limit disruption. Once deployed, data is fed back to help reduce error rate and inform further policy changes. This ensures that any amendments to policies are robust without damaging customers experience.

Policy Engine

The Callsign Policy Engine drives the defined authentication journeys. Driven by APIs it calls out to internal and external intelligence sources to obtain the required context, which includes the overall confidence score assigned by the Callsign Intelligence Engine. This score is continually re-assessed as additional information becomes available.

Using this real-time data, the Callsign Policy Engine can call the Callsign Authentication Engine to deliver additional checks when required. The user response is fed back, and the authentication journey continues. Ultimately it produces an authentication outcome to be fed back along with the associated intelligence to the calling system, such as our SDK.