callsign®

GET ON

INTELLIGENCE BEYOND RECOGNITION

Decision

Policy Manager & Engine

Product Sheet

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.

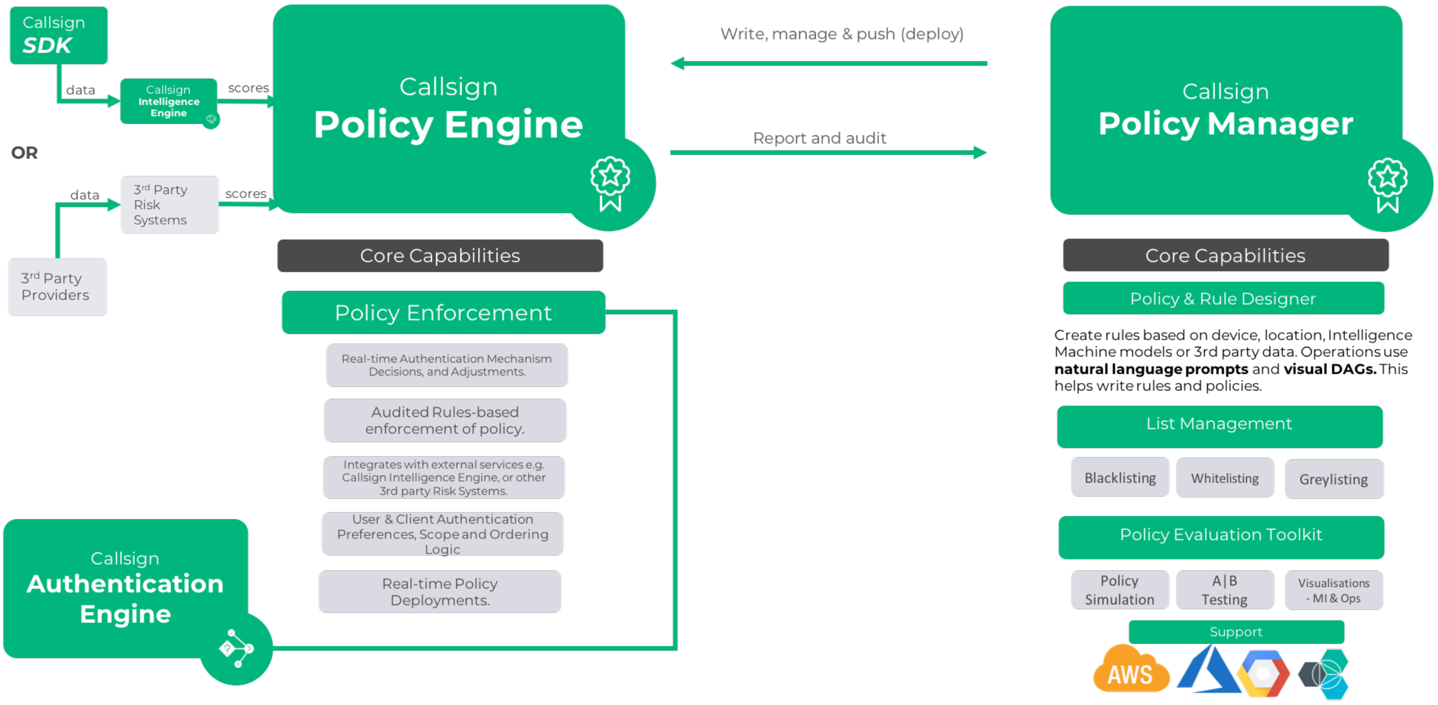
Organizations often struggle finding the right balance between customer experience and security. Turn the dial too far one way and you sacrifice the other. But finding the right balance is necessary to solving this this paradox. Organizations need the ability to turn the dials up and down as required, 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.


Callsign SDK
data
Callsign Intelligence Engine
scores
OR
data
3rd Party Risk Systems
scores
3rd Party Providers
Callsign Policy Engine
Core Capabilities
Policy Enforcement
Real-time Authentication Mechanism Decisions, and Adjustments.
Audited Rules-based enforcement of policy.
Integrates with external services e.g. Callsign Intelligence Engine, or other 3rd party Risk Systems.
User & Client Authentication Preferences, Scope and Ordering Logic
Real-time Policy Deployments.
Callsign Authentication Engine
Write, manage & push (deploy)
Report and audit
Callsign Policy Manager
Core Capabilities
Policy & Rule Designer
List Management
Blacklisting
Whitelisting
Greylisting
Policy Evaluation Toolkit
Policy Simulation
A|B Testing
Visualisations - MI & Ops
Support
AWS

Create rules based on device, location, Intelligence Machine models or 3rd party data. Operations use **natural language prompts** and **visual DAGs.** This helps write rules and policies.

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.

callsign

GET ON

INTELLIGENCE BEYOND RECOGNITION

Intelligence

Product Sheet

What is Authentication?

Authentication is the act of given a user permission in order to perform a task. This is often done at the point of access using a single factor such as username and password, although, this method doesn't stop the bad guys. Multi-factor authentication is a much more secure way of establishing identity.

What is Passive Authentication?

Passive authentication, or identification, is the collection of information in the background to verify identity. Using thousands of available data points, such as a user's location, device, typing cadence, mouse movement or swipe.

What is active Authentication?

The opposite of passive authentication is active authentication. Active authentication occurs when a user is asked to do something to prove they are who they say they are, such as provide a password, pin, or a prompted biometric scan.

What is Verification

Verification is the act of verifying identity. Proving that the user is in fact who they say they are.

Solving the challenge of knowing that your users really are, who they say they are

Industries such as e-commerce and finance are seeing increasing incidents of cross channel fraud, as fraudsters exploit security blind spots in one channel to commit fraud in another. For example, account takeover use recently skyrocketed, climbing 45 percent in Q2 2017*.

With an average 4% of purchases affected by account takeover, organizations need to verify in real-time that their users are who they say they are. To achieve this, identity checks need to be non-rules based so the bad guys cannot overcome them, whilst being dynamic enough to reduce additional friction to the customer experience.

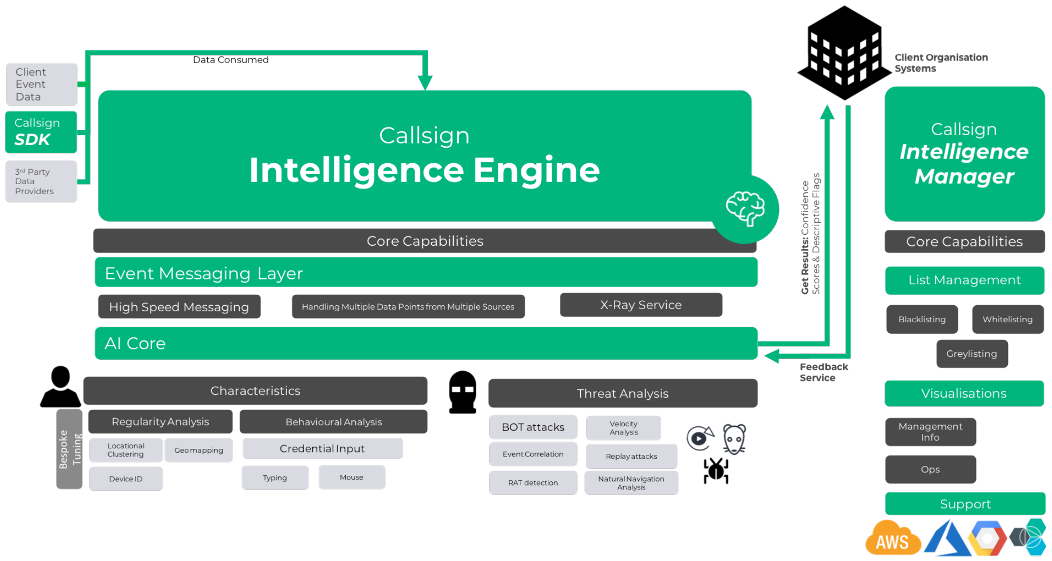
How Callsign can help:

The Callsign Intelligence Engine delivers the perfect balance between security and usability. It uses thousands of data-points including behavioral patterns (e.g. keyboard & mouse patterns), location data, biometric data (e.g. fingerprint / facial recognition) and device data, to determine that someone's behavior is within their normal pattern.

This means the authentication journey can be tailored dependent on the factors at the time. For example, a user's characteristics when making a high value transaction via a laptop at home will vary slightly from conducting the same request via a mobile device on a train abroad. In this case additional authentication checks may be requested without needing to block the transaction.

However, if another individual was to attempt to access the account, the characteristics would likely be different and so the transaction can be blocked. As we pull from multiple data sources, we can verify, in real-time, whether users behavior fits in with their normal pattern. If it is, they can continue. If not, additional authentication steps can be dynamically introduced.

* (Global Fraud Index 2017)



How it works

The Callsign Intelligence Engine determines a confidence score based on the behavior of the user and how effectively we can trust the information provided. This is broken down into two categories – recognition and trust.

Recognition

This is whether the behavior patterns throughout the transaction are consistent with that identity profile. This data is captured across three areas:

- **Device:** Characteristics and ID information - e.g. web & hardware fingerprint
- **Location:** Where is the transaction taking place - e.g. location
- **Behavior:** What are the user characteristics - e.g. movement, pressure and keystrokes (wrist strength, muscle memory, size of hand)

Overall, the Callsign Intelligence Engine is looking for behavior that is 'out of character' such as different input methods or, the mobile device being in a completely different location to the computer.

Trust

To run an effective policy, information needs to be accurate and trustworthy. We conduct ongoing passive analysis on various data points which include:

Threats	Location	Device
• Malware • BOT & Replay attacks • Remote Access Takeover (RAT) Detection	• Are they in the office on VPN? • Can they physically be in that location • Is location spoofing taking place?	• Has the phone been cloned? • Has a SIM swap recently taken place? • Has the device been registered as lost / stolen?

Based on the data points collected, the Callsign Intelligence Engine determines a confidence score using statistical modelling and machine learning techniques. This score is then pushed to the Callsign Policy Engine, driving it to request the appropriate checks through the Callsign Authentication Engine. The user's response is fed back, and the journey can continue.

In a constantly evolving world these data points are reassessed and adjusted as more information becomes available. This reduces considerable friction on the user, as additional data / authentication requests are only requested when what is available doesn't meet the required threshold set by the business depending on their risk appetite.

The Callsign Intelligence Engine can fit into any business model and can integrate with multiple data sources. It is:

- API driven: It calls out to internal and external sources to get the required data
- Cloud hosted: Save on server requirements and implementation issues

The Callsign Intelligence Engine puts the user at the heart of the authentication journey, ensuring they are who they say they are at the point of transaction without adding additional friction.

GET ON

INTELLIGENCE BEYOND RECOGNITION

Authentication

Product Sheet

What is Authentication?

Authentication is the act of given a user permission in order to perform a task. This is often done at the point of access using a single factor such as username and password, although, this method doesn't stop the bad guys. Multi-factor authentication is a much more secure way of establishing identity.

What is Single Factor Authentication?

Single Factor Authentication is the process of authenticating a user against one type of credential, this is often a password or PIN.

What is Two-Factor Authentication?

Two-factor authentication (2FA) or dual-factor authentication is the process of authenticating a user using a combination of their password / PIN alongside something unique to the user. This is often a token or one-time password (OTP).

What is Multi-factor Authentication?

Multi-factor authentication (sometimes referred to as Strong Customer Authentication (SCA) is the process of authenticating a user against multiple factors. This is often from the following:

- Something you own – e.g. payment card or mobile phone
- Something you know – e.g. password or PIN
- Something about you – e.g. biometrics and behavioural

Solving the problem of customer satisfaction vs security

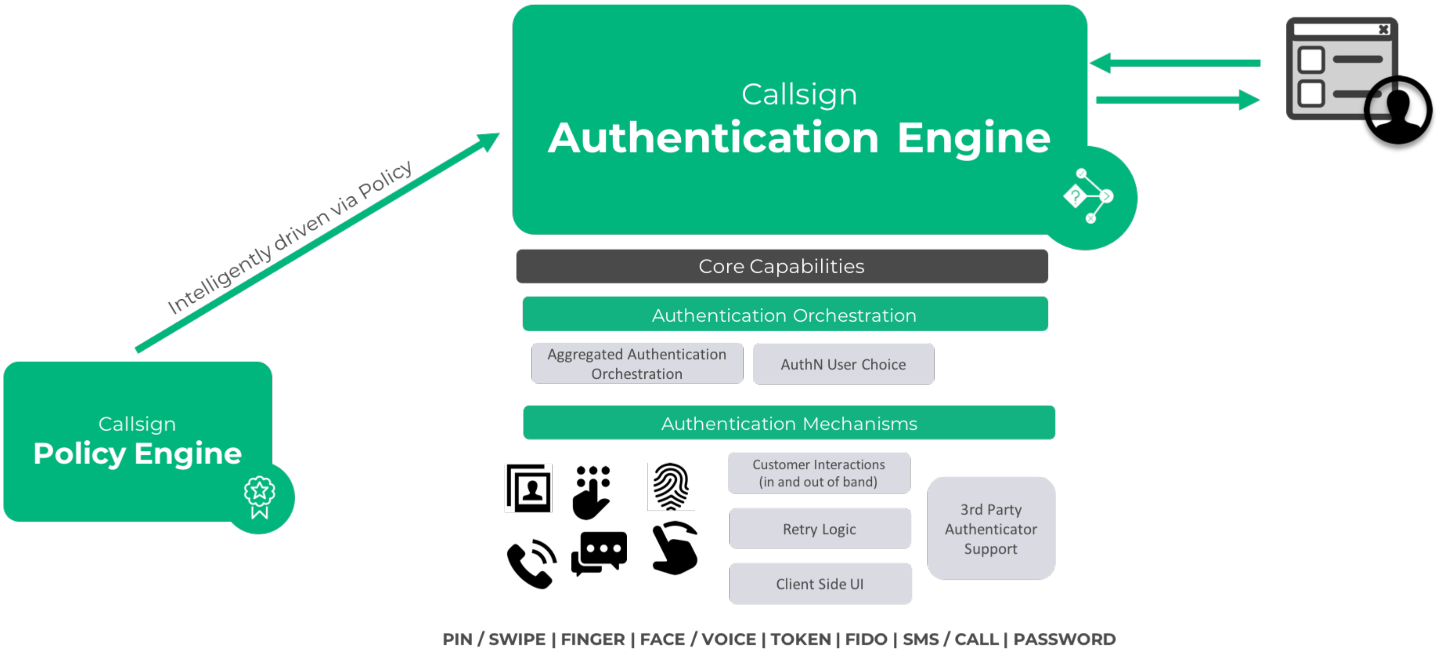
Finding the right balance between customer experience and secure authentication has always been a challenge. Turn the dial too far to the left, and you begin to sacrifice security over the user. Too far to the right, and customer satisfaction is sacrificed.

By applying continuous authentication throughout the transaction, identity can be verified with minimal disruption to the user journey. This also allows for the appropriate authentication checks to take place based on user data, rather than applying a catch-all authentication process for the entire customer-base.

How Callsign can help:

The Callsign Authentication Engine orchestrates the authentication request at each relevant point during the transaction, so that digital identity can be validated throughout. The level of authentication required is determined by a confidence score derived from our Callsign Intelligence Engine and is pushed through by the Callsign Policy Engine.

A higher score denotes a greater the assurance of the user's identity being valid. For example, if input methods and locational data are recognized behavioual patterns, then the score will be greater. If one of those factors is not deemed as recognizable, such as a change in keystroke, then the score may be lower.


Callsign
Authentication Engine
Intelligently driven via Policy
Callsign
Policy Engine
Core Capabilities
Authentication Orchestration
Aggregated Authentication Orchestration
AuthN User Choice
Authentication Mechanisms
Customer Interactions (in and out of band)
Retry Logic
Client Side UI
3rd Party Authenticator Support
PIN / SWIPE | FINGER | FACE / VOICE | TOKEN | FIDO | SMS / CALL | PASSWORD

How it works

The Authentication Engine can be programmed using any key factors that the organisation wants to provide to their users. With the most extensive solution, Callsign offers the following factors:

- **Something you know:** PIN, Password, SMS / Call
- **Something about you:** Biometric & Behavioural - fingerprint, face, voice, swipe
- **Something you have:** Tokens, Fast ID Online (Fido), Laptop. Phone

If the user can't authenticate via a certain method, or if additional authentication is needed, the policy will adapt in real-time by tying authentication journeys and use cases to the policy. For instance, if the user doesn't have biometric functionality on their mobile device, an alternate authentication method can be requested. Being API driven, multiple data sources can be incorporated to help determine this.

The Authentication Engine puts customer experience at the centre. Administrators are able to select the authentication methods that suit the needs of their business, whilst the user's authentication journey is friction free as they move seamlessly between devices.

callsign

GET ON

INTELLIGENCE BEYOND RECOGNITION

Telecoms Data

What is Telecoms Data?

Mobile providers often have large amounts of data stored pertaining to individuals. This data can be used to validate a user's identity by checking the information provided at the point of transaction against a range of factors. These include whether the phone has been reported lost or stolen, is on call divert or there has been a SIM swap recently. This data can help detect fraudulent activity that is often missed in traditional authentication checks.

Protecting Data Privacy

Validating against Telecoms data only uses a series of yes / no responses. The User's data is checked and validated against the information held by the operator, meaning that a user's data isn't shared with any third-party sources during the transaction.

Helping to prevent fraudulent activity using third-party data sources

Increased authentication and verification checks can add friction to the user experience. Using additional, third-party data points allows for organizations to use passive authentication methods to help validate identity, without the need of increasing friction via additional requests to their users.

Callsign checks the data provided by the user against their telecoms data to verify identity, and flag any potentially fraudulent activity.

How Callsign can help:

Callsign uses Telecoms data to help validate user identity, not only at the point of registration but throughout the customer lifecycle. When a user provides their phone number at the point of registration, this data is validated against multiple attributes including:

- SIM Swap - has this taken place recently
- Call divert - has this been put in-place on the number associated with this account?
- Fraud checks - whether the phone has been cloned or reported lost / stolen
- Is the phone number associated with the account?

Using telecoms data in a silo can often lead to false positives and isn't a catch-all method to fraud prevention. In these cases, it means added friction to the customer experience with added checks, and verification methods needed to prove identity.

At Callsign we combine telecoms data with thousands of additional data points in the Callsign Intelligence Engine. This validates a customer's identity, not only at the point of registration but throughout their lifecycle. Utilizing this with the Callsign Policy Engine can ensure that the appropriate checks can be run without the need for call-backs. This catches threats such as bots and fraudulent activity without the cost of additional resource.

With continuous authentication, combined with telecoms data, organizations can build trust around an individual, without needing to apply unnecessary friction to their customer's experience when conducting a transaction.

This product is currently only available in the UK.

callsign®

GET ON

INTELLIGENCE BEYOND RECOGNITION

Web & Mobile SDK

Product Sheet

What is an SDK?

A software development kit (SDK) is a set of software development tools that allows for the Callsign software to be integrated with third-party apps or websites.

What is Authentication?

Authentication is the act of given a user permission in order to perform a task. This is often done at the point of access using a single factor such as username and password, although, this method doesn't stop the bad guys. Multi-factor authentication is a much more secure way of establishing identity.

What is Multi-factor Authentication?

Multi-factor authentication (sometimes referred to as Strong Customer Authentication (SCA) is the process of authenticating a user against multiple factors. This is often from the following:

- Something you own – e.g. payment card or mobile phone
- Something you know – e.g. password or PIN
- Something about you – e.g. biometrics and behavioural

Providing access to thousands of data points to prove identity

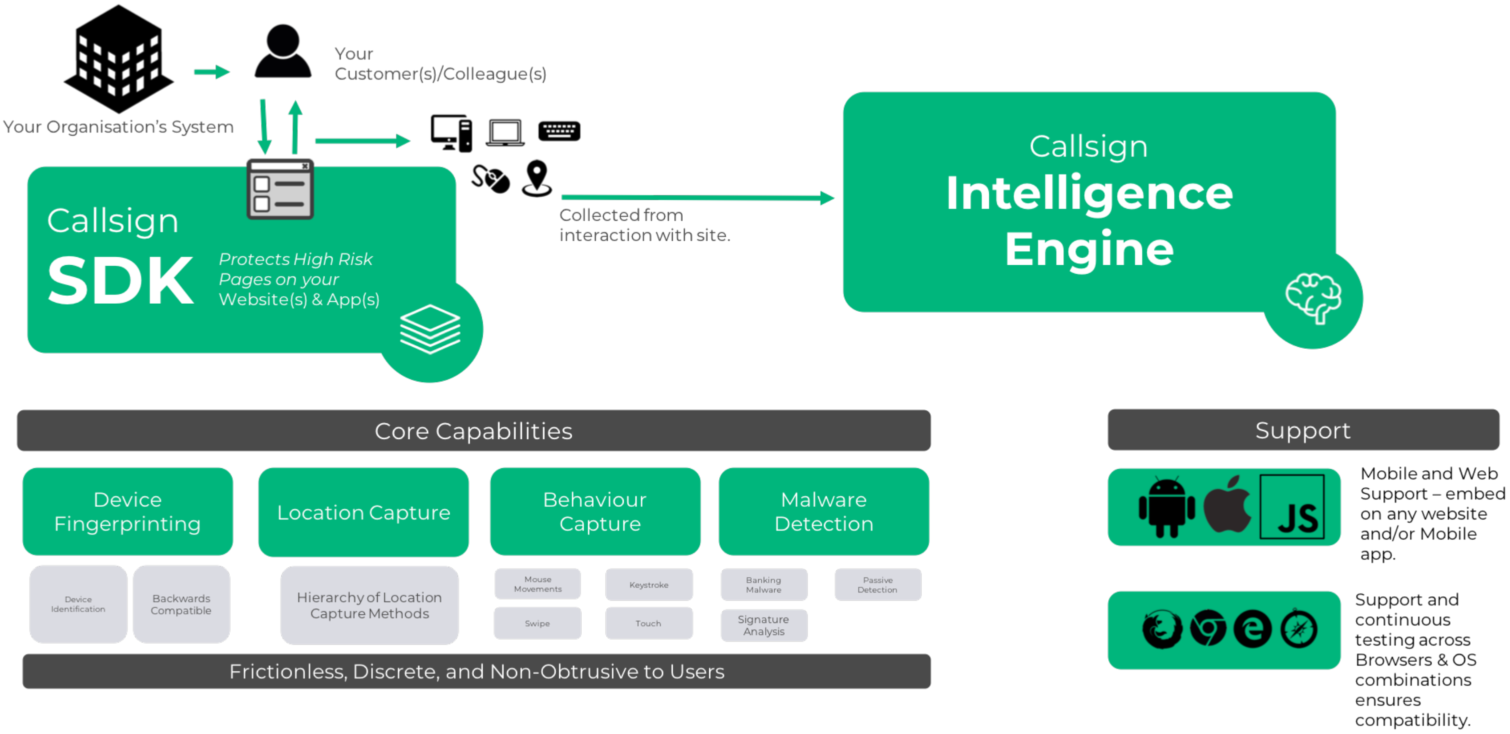
Managing customer experience throughout the authentication process is an important factor for any organization. Make the process too arduous and you run the risk of losing customers. Organizations need to also ensure that users trust the application they are using to submit details, without having to use multiple sources to validate identity.

Using data points such as such as location, muscle memory & wrist strength helps to build a greater understanding of the user's identity, without adding additional friction to their journey via additional authentication methods.

How Callsign can help:

Callsign's SDKs can be embedded into any app or website to collect device, location and behavior information from a user's interaction with an app or web page. This information is passed through to the Callsign Intelligence Engine, which designates a confidence score that the Policy Engine uses to deliver the appropriate authentication method.

Using the Callsign SDK ensures that organizations are getting the intelligence they need without impacting customer experience.



Your Organisation's System
Your Customer(s)/Colleague(s)
Callsign SDK
Protects High Risk Pages on your Website(s) & App(s)
Collected from interaction with site.
Callsign Intelligence Engine
Core Capabilities
Device Fingerprinting
Device Identification
Backwards Compatible
Location Capture
Hierarchy of Location Capture Methods
Behaviour Capture
Mouse Movements
Keystroke
Swipe
Touch
Malware Detection
Banking Malware
Passive Detection
Signature Analysis
Frictionless, Discrete, and Non-Obtrusive to Users
Support
JS
Mobile and Web Support – embed on any website and/or Mobile app.
Support and continuous testing across Browsers & OS combinations ensures compatibility.

How it works

The Callsign SDK feeds data from multiple sources to the Platform, which via the Policy Manager, drives the appropriate authentication method based on the confidence score derived from the Intelligence Engine. Types of data collected include:

- Device identification & fingerprinting
- Location data
- Behavior actions including mouse, keyboard and touch characteristics (wrist strength, muscle memory, size of hand)
- Threat detection, such as banking malware and passive malware detection

The Data collected is focused on attributes that are useful for asserting identity or distinguishing anomalous behavior. Making it discrete and non-obtrusive to the user so that they receive a friction free experience when conducting the transaction.

With ongoing support and testing across browsers & OS combinations, organizations can be assured of compatibility with their systems. Developers can also benefit from a full suite of support and tools via our dedicated Callsign developers' site. Being cloud based the SDK and Callsign Platform is easy to implement with minimal impact on infrastructure.

callsign®

Product Sheet

GET ON

INTELLIGENCE BEYOND RECOGNITION

Electronic Identity & Verification (eID&V)

Protecting Data Privacy

Validating against Telecoms data only uses a series of yes / no responses. The User's data is checked and validated against the information held by the operator, meaning that a user's data isn't shared with any third-party sources during the transaction.

What is Know Your Customer (KYC)?

This is a process that financial institutions and other regulated companies must perform in order to make sure their customers really are who they say they are.

The intention of the Know Your Customer (KYC) process is to prevent bad guys from using banks to launder money either intentionally or unintentionally.

Banks must ensure that they have obtained relevant identification data on their customers to verify their identity. This information needs to be both independent, and reliable.

Helping organizations know their customers

Know Your Customer (KYC) is a process that financial institutions and other regulated companies must perform in order to make sure their customers really are who they say they are. Institutions must ensure that they have obtained relevant identification data on their customers to verify their identity. This information needs to be both independent, and reliable.

Traditionally, this would have been offline, with customers waiting in line to verify their identity in a branch. But, as Bob Dylan said, "the times they are a changin'"; users are looking for ways to manage their finances online, from transactions to opening new accounts. How can organizations cater to this new customer journey, whilst proving that the user really is who they say they are?

Advancements in electronic identity and verification (eID&V) are not only moving previously offline only transactions online, they are also making them quicker. Users can now open a bank account in 15 minutes on their phone, a huge step forward in customer experience.

Electronic Identity and Verification (eID&V)

Our eID&V capability supports numerous proofs of identity documents including passports, drivers licenses and birth certificates. We cross reference this documentation and facial recognition confirmation against multiple first and third-party data sources including telecommunications, police, electoral and governmental databases.

Working directly with our Policy & Intelligence Engines the appropriate eID&V checks are only triggered when necessary and documentation can be referenced in future transactions should it be required. This ensures that the documentation is validated on record and can be called upon at any time.

With eID&V, institutions can prove identity whilst removing friction and helping their customers Get On.