FACT SHEET

Socure

Sigma Device

Why You Need Sigma Device

Combining explicit user input data (DOB, email, phone) and implicit information from the device (IP, device, behavior) at the digital entry point is **the only way to perfect identity verification and fraud classification.**

Get insights to device and connection risk indicators to obtain device intelligence at critical points in the customer lifecycle.

Sigma Device provides **positive indicators for matching historic PII observations** to help identify low risk events and reduce friction for existing customers.

Sigma Device serves as **a key pillar of Socure's fraud prevention strategy** and helps prevent large-scale attacks, driven by both bot and human.

Sigma Device's sophisticated intelligence helps increase your fraud capture rates and **grows your auto-approvals significantly**.

Device ID-Only Products Fall Short on Maximizing Device Intelligence

Device products are common in identity and fraud verification. All rely on the same processes and contend with similar constraints:

- Web SDK (client-side JavaScript) device fingerprinting
- Browser API restrictions and death of third-party cookies
- Native SDKs for iOS and Android mobile app support
- IP geolocation and consent-based data collection

Socure Sigma Device goes beyond traditional approaches employed by legacy device fingerprint providers by constructing long-lived user correlations. This strategy ensures that Sigma Device delivers a high-fidelity signal even as device level identifiers change or deteriorate.

Socure's Sigma Device Delivers Powerful Differentiators

There are other device ID products available in the marketplace, but none are as potent to verify identity and combat fraud as Socure's Sigma Device. Here are reasons why Sigma Device is superior:

1

CORRELATION OF DEVICE DATA TO IDENTITY

To optimize performance, the Sigma Device model combines device data with identity information including name, email address, phone number, and other details provided during account opening. This allows for a one-stop shop for fraud prevention, with robust feature interaction.

2

DATA ENRICHMENT

Socure doesn't stop there. Sigma Device is also layered with 700 million rows of known good and known bad outcomes across all identity elements to improve accuracy and support better business decisions.

3

SIMPLE IMPLEMENTATION

Utilize the same API call you use for other Socure products to enable Sigma Device data collection. Front-end deployment can be completed in just hours.

4

END-TO-END ROADMAP

Sigma Device benefits from a consortium network effect that will support Socure's mission to develop the first verifiable, cross-industry digital ID in the U.S. Enabling this trust ecosystem means eliminating repetitive authentication processes, quicker time to revenue, and a vastly improved customer experience.

SOCURE'S SIGMA DEVICE VS OTHER PROVIDERS	Socure	Others
Correlation of Explicit User Input and Implicit Device Data	✓	✗
Native Integration with Broader Fraud Suite Delivering More Accurate Fraud Detection	✓	✗
End-to-End Roadmap to 1st Verifiable, Cross-Industry Digital ID	✓	✗
Simple Implementation/Single API	✓	✓
Javascript-Enabled Data Collection	✓	✓
Browser API Restrictions	✓	✓
Death of Third-Party Cookies	✓	✓
Device Data Enriched with Feedback Data	✓	?
Native SDKs for iOS and Android Mobile Apps	✓	✓
IP Geolocation	✓	✓

How Sigma Device Works

The Sigma Device module uses multiple approaches to:

1. Understand device attributes and their risk profile

2. Bind devices to customers, both probabilistically and deterministically

- For probabilistic binding, we use unsupervised ML learning to measure the "distance" of the current session from other sessions associated with the same user
- For deterministic binding, we tie back to different methods of device fingerprints, cookies, IP address, and return results

3. Uniquely identify devices

When this product is called via the API, reason codes are returned to help Socure customers approve safe interactions and identify those that are risky. Importantly, device signals will also be incorporated into the next version of Sigma Identity Fraud, to further improve accuracy and fraud capture.

To Incorporate Sigma Device in Your Consumer Workflow

- Web Support (client-side Javascript): Add code to all pages on your website and call the Socure API before making a decision about an account
- Native App (iOS and Android SDKs) and Native React Support: Integrate code to facilitate data collection and secure communication with Socure services
- Use the Socure API to call the Sigma Device module on its own or together with other Socure products for a more complete understanding of fraud risk

Next Steps

1

Request your Socure account team to enable Sigma Device for your account.

2

Review the implementation guide available on Socure's DevHub.

3

Schedule a technical review, create an implementation plan, and pick a go-live date.

4

Add the code to your front-end platform and begin calling the Sigma Device module.

For more information about Sigma Device, email us at salesinfo@socure.com.