

Event verification desk

Event Desk organizes a claim. It keeps sources, evidence, missing context, and confidence notes clear. The basic desk runs on the device. Team features use separate Worker services.

WHERE IS DATA PROCESSED?

Core work is local, with a separate consent-led network step

GOAL

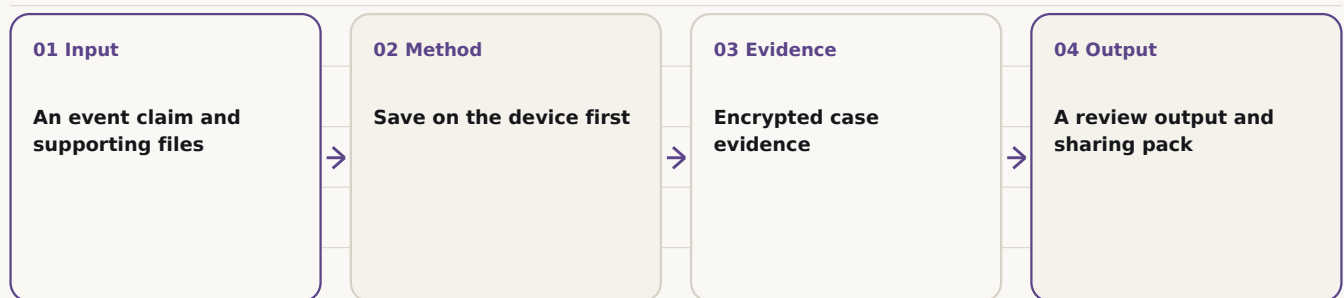
Structures an event claim, encrypts it on the device, and builds a review output.

WHO IS IT FOR?

For teams that need to keep an event claim, its sources, missing context, and decisions in separate records.

TECHNICAL FLOW

Input, method, evidence, and output



Event verification desk

HOW DOES IT WORK?

Step 1

Structure the claim

The claim and source URL use separate fields. What the source says also has its own field. So does what the source does not show.

Step 2

Save on the device first

The basic packet can stay in localStorage or be downloaded as text. A server is not required.

Step 3

Check team access

For Pro and team features, the Worker checks access on the server. It checks the session, workspace, role, and plan.

Step 4

Encrypt sharing on the device

Team messages and shared files are encrypted with AES-256-GCM in the browser. The key is not sent to the server.

Step 5

Queue service work

The Worker stores structured records and ciphertext in D1. Queues and Cron run scheduled work.

Step 6

Build review output

Evidence packets, comments, decision history, and report outputs are linked to the same case record.

LIMITS

The desk is not for live people tracking, private-account access, or unauthorized access. Encryption does not correct a bad sharing decision.