

# Biometric Check

**Hardware-bound human verification for bot management,  
and the trust infrastructure for the agentic era.  
Part of the Cequence platform.**

## What is Biometric Check?

Biometric Check is a biometrically secure way to differentiate between humans (or their AI agents) and bots. It is a hardware-bound challenge mechanism within the Cequence platform that replaces broken challenge flows including CAPTCHAs, SMS OTPs, and email codes with a cryptographically strong, sub-second verification using the device's native biometric sensor (e.g., Touch ID, Face ID, Windows Hello).

When the Cequence behavioral engine flags a session as potentially automated, Cequence issues a WebAuthn challenge instead of blocking. The user's Secure Enclave creates a token. No biometric data leaves the device. No shared secret is transmitted. The result is a proof of humanity that cannot be farmed, forged, or automated at scale.

## Why existing mechanisms have failed

- ML models now solve image CAPTCHAs with accuracy exceeding humans
- SMS farms and SS7 vulnerabilities undermine phone-based OTPs
- Email codes add friction that kills conversion and drives abandonment
- Teams soften bot policies to avoid false positives, letting 5 attackers through to protect 1 customer

<1s

Verification Time

Zero

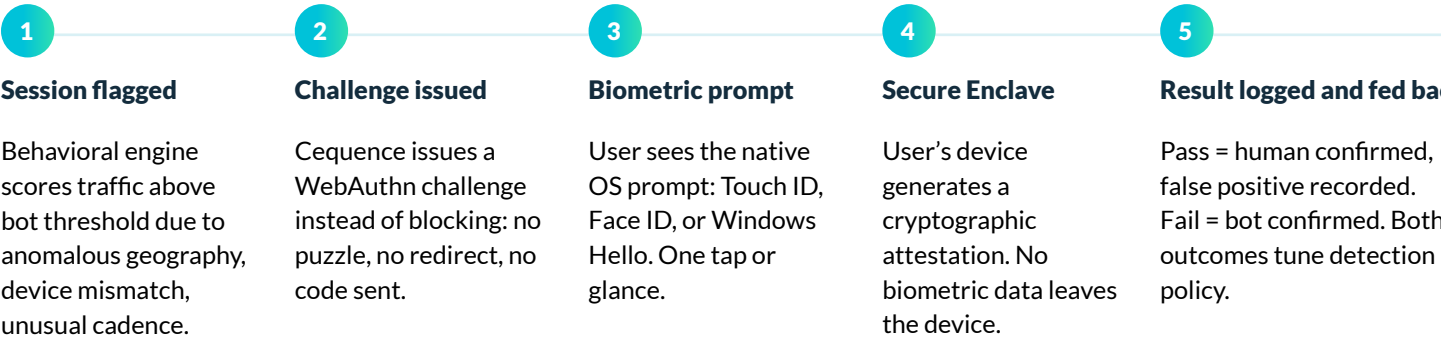
Shared Secrets  
Transmitted

5-15%

Typical FP Rate  
Recoverable



How it works



Features

**Challenge policy configuration**  
  
Set score thresholds, endpoint scope, and challenge behavior within Cequence's inline policy engine. Apply globally or per-endpoint.

**Native biometric prompt**  
  
The OS-native dialog (Touch ID / Face ID / Windows Hello) shown to the flagged user. No redirect, no UX degradation, no friction.

**False positive rate dashboard**  
  
Real-time pass/fail data surfaces your actual FP rate, the first measurable, evidence-based signal for detection policy calibration.

Use Cases

- Anomalous geography / travel scenario**  
A customer logging in from an unexpected country triggers a flag. Biometric Check recovers the session without exposing detection logic or requiring a support call.
- High-value endpoint protection**  
Gate checkout, account changes, and bulk data APIs with a biometric step-up, applied selectively by risk score.
- Agentic AI human-in-the-loop**  
When an AI agent hits a high-risk action boundary, Biometric Check surfaces the human principal for explicit re-authorization before the agent proceeds, breaking prompt-injection coercion chains.
- Detection policy tuning**  
Use pass/fail data to measure your actual false positive rate and calibrate detection thresholds with evidence, not estimates.

Technical Specifications

|                      |                                    |
|----------------------|------------------------------------|
| STANDARD             | WebAuthn / FIDO2                   |
| VERIFICATION LATENCY | < 1 second                         |
| KEY BINDING          | Hardware Secure Enclave            |
| BIOMETRIC DATA       | Never leaves device                |
| AUTHENTICATORS       | Touch ID, Face ID, Windows Hello   |
| DEPLOYMENT           | Cequence inline policy engine      |
| CHALLENGE SCOPE      | Per-endpoint or global             |
| SHARED SECRETS       | None transmitted                   |
| OUTPUT SIGNALS       | Pass / fail + FP rate metric       |
| VM / FARM RESISTANCE | Hardware-bound; can't be automated |

Threat Types Detected / Differentiated

Credential stuffing   Account takeover bots   Scalper & inventory bots   Automated checkout abuse   Login-stage scraping  
VM / headless browser farms   Prompt-injected agents   Unauthorized agentic actions