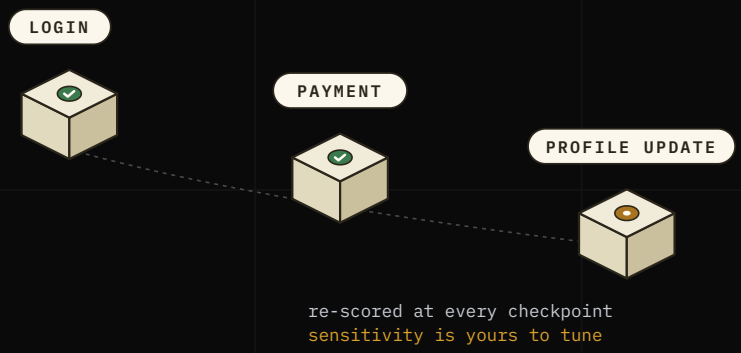
LOCI

TECHNICAL BRIEF · SESSION DEFENSE

Trust is not a token. It is re-earned, every action.

Continuous authentication and session defense: every sensitive interaction re-scored against the physics of the session, anchored to one signed session identity, with sensitivity your team tunes.



EXECUTIVE SUMMARY

Continuous authentication and session defense

Traditional fraud prevention operates on a "gated" model: rigorous checks occur at login, but once a session token is issued, the user is implicitly trusted for hours or days. This creates a dangerous vulnerability window for session hijacking (stolen cookies) and device handover (an authenticated user handing the device to a bad actor).

AccessGate implements **continuous authentication**: it re-evaluates risk on *every* sensitive interaction, not just at login. It does this by anchoring each interaction to a single, signed session identity, the **ASK** (Access Session Key), and re-scoring the "physics of the session" (biometric coherence, environmental stability, and pacing) live on every request.

THE GOAL

Ensure the entity holding the session token is the same entity that logged in.

Core architecture: live re-evaluation

Trust is recomputed, in full context, each time. Every checkpoint is scored fresh, from the user's persistent behavioral baseline plus the session's correlated history (device, network, and prior events, tied together by the ASK). There is no hidden running tally for an attacker to probe, groom, or quietly reset; each decision considers the whole session's story.

The three pillars

PILLAR A · CONTEXT

Environmental continuity. Sudden shifts in a session's environment mid-flight are primary indicators of token theft: the stability of the network context, the reputation of newly appearing addresses, and the consistency of the device identity are all evaluated within the active session.

PILLAR B · HUMANITY

Biometric coherence. Current behavior is compared against the user's established baseline. Divergent interaction dynamics suggest a remote-access tool or a different person; correlation-aware scoring means matching one metric is not enough. On mobile, motion-sensor plausibility separates real hands from emulated ones.

PILLAR C · PACING

Velocity and tempo. Navigation cadence, idle time, and input pacing are monitored across the session. Throughput beyond plausible human ranges, or long dormancy followed by a burst of high-value activity, raises risk on the next scored action.

ANCHOR · THE ASK

One session lineage. A signed session identity ties every checkpoint into a single, tamper-resistant story, so the journey is evaluated as a whole rather than as isolated events. It carries no personal information.

INTEGRATION MODEL

Checkpoints, anchored by one session identity

AccessGate does not passively watch. It enforces at defined **checkpoints**:

- **Login (the anchor).** On successful login, AccessGate anchors the session identity and establishes the behavioral baseline for the rest of the journey.
- **Critical actions (the gates).** High-value events such as payments, profile updates, and password resets are re-scored *before* the action is allowed, with action-specific sensitivity. Actions that typically begin an account takeover, like changing an email or password, run at the highest sensitivity; checkout flows run tuned to stop fraud without adding friction.
- **Passive heartbeats (the watchdog).** Ordinary navigation is scored with full session context, so a session exhibiting automation is caught on its next scored request.

Scoring fusion: how signals become decisions

Session signals are **fused into one global risk score**, not evaluated in isolation: network and reputation risks, behavioral and biometric penalties, and session-integrity anomalies weighted by the action being attempted. A suspicious session that stacks several independent signals, say a mid-session context change plus a biometric deviation on a profile update, moves decisively from "review" into "block."

TUNABLE BY DESIGN

The weights and thresholds behind this are configurable per organization and per action, so risk teams dial sensitivity to their appetite. We deliberately do not publish production values. Instead, the online edition of this brief includes an interactive sandbox where you set the weights yourself and watch the decision move: runloci.com/brief/continuous-authentication.

Authentication-method strength is priced in

Not all logins are equal. AccessGate adjusts the session's starting risk posture by how the user authenticated: device-bound passkeys establish the strongest posture, hardware keys and platform biometrics follow, and knowledge-based methods, especially password-only logins, start from a weaker posture. The same behavioral anomaly escalates faster for the weaker method.

SECURITY OUTCOMES

Threat vectors mitigated

THREAT VECTOR	WHAT GIVES IT AWAY	REPRESENTATIVE OUTCOME
Session hijacking (stolen cookie)	Session context changes mid-flight on an active session	Block: the session is invalid for the new context
RAT / remote desktop	Interaction dynamics diverge from the user's baseline	Step-up challenge
Account handover	Behavioral and motion-sensor deviation vs. the established baseline	Review: flagged for verification
Slow-drip automation	Pacing anomalies across the session	Terminate decision issued

How decisions are enforced: the trust boundary

AccessGate **decides**; your platform **enforces**. Every response returns an outcome (allow, review, block, and for session evaluation, challenge or terminate) that your systems act on: dropping the session, forcing step-up, or blocking the action. This clean boundary means AccessGate never has to hold your session state, and you retain full control of enforcement.

Explainability, governance, and resilience

- **Every decision is explainable:** responses include a machine-readable list of the exact signals behind the score, for analyst review and audit.
- **Per-tenant isolation:** each organization's behavioral profiles and session data are strictly segregated.
- **Privacy by design:** the session identity carries no personal information; data-subject export and deletion are supported.
- **Graceful resilience:** no single point of failure in the decision path; the machine-learning anomaly layer is additive, not load-bearing, running in shadow mode until proven against real outcomes.

A NOTE ON WHAT WE PUBLISH

This brief describes capabilities and design principles. Production scoring parameters are configured per organization and are deliberately not published; the online sandbox uses illustrative values so you can experience how tunable sensitivity behaves.

Trust becomes ephemeral: earned continuously,
withdrawn the moment the evidence says otherwise.

About Loci

Loci is the intelligence infrastructure for modern finance. Loci empowers every defender, analyst, and enterprise system to operate with confidence, clarity, and adaptive insight. With Loci, everyone becomes intelligent.

SEE IT ON YOUR SESSION FLOWS

A walkthrough of checkpoint scoring on your highest-risk actions, tuned to your risk appetite. Try the interactive sandbox at runloci.com/brief/continuous-authentication.

LOCI FRAUD AI · TECHNICAL BRIEF **runloci.com · sales@runloci.com**