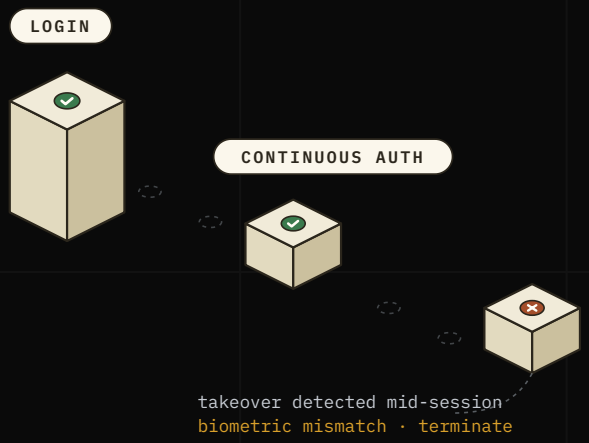
LOCI

EXECUTIVE BRIEF · NOVEMBER 2025

The gate is not enough. Guard the whole session.

The future of account takeover prevention: from static gatekeeping to continuous, intelligent identity assurance. AccessGate validates who is behind the keyboard, not just what they know.



EXECUTIVE SUMMARY

The future of account takeover prevention

Account takeover (ATO) remains one of the most persistent and damaging threats to digital businesses. Traditional defenses rely on static gates like passwords and multi-factor authentication (MFA), which attackers increasingly bypass through phishing or session hijacking.

THE BLIND SPOT

Once past the gate, the attacker is invisible.

This brief outlines a paradigm shift: moving from **static gatekeeping** to **continuous, intelligent identity assurance**. Our solution, **AccessGate**, fuses behavioral biometrics with network, device, and identity intelligence to verify identity not just at login, but with every interaction. It runs at the global edge, returns a real-time, explainable decision on each request, and renders stolen credentials useless by validating *who* is behind the keyboard, not just *what* they know.

The engine: a fused behavioral model

The prevention engine does not rely on a single check. It fuses distinct layers of intelligence into a dynamic risk profile: a "brain" that operates invisibly in the background, building a high-fidelity model of legitimate user behavior while instantly flagging anomalies that indicate a takeover.

Biometric correlation engine

Attackers can mimic *what* a user does, but they cannot replicate the *subconscious correlations* in *how* they do it. Rather than looking at isolated metrics like "typing speed," this layer analyzes the subtle relationships between behaviors: for a specific user, high typing speed might naturally correlate with specific mouse movement curves. A bot or human attacker might match the speed but fail the correlation test, typing fast with zero errors or moving the mouse in unnaturally straight lines. The system detects this "unnatural" combination as a biometric mismatch.

Resilient learning system

User behavior changes over time. A static system becomes obsolete; a naive learning system can be "poisoned" by an attacker slowly changing behavior to avoid detection. The model employs a smart learning rate that adapts based on the "surprise" of new data: consistent behavior is learned quickly, while radically different behavior is sharply down-weighted so it barely influences the profile. This prevents sophisticated attackers from "grooming" the system to accept their fraudulent behavior as the new normal.

THE ENGINE, CONTINUED

Context, networks, and the full signal picture

Contextual pattern recognition

Legitimate users have habits: they log in at certain times, from specific regions, using familiar devices. This layer calculates a "predictability score" for every action, building a probability map of a user's typical hours, locations, and device choices. It distinguishes between a user who is naturally unpredictable (a traveler) and a user who is historically stable but suddenly acts erratically. A valid login from a new device at 3 AM might be technically correct but contextually impossible for a specific profile, triggering an immediate alert.

Ecosystem graph

Sophisticated fraud often involves "fraud rings": groups of attackers managing hundreds of fake or stolen accounts from a single location. This layer looks beyond the individual user to the entire network, analyzing device fingerprints and the similarity of behaviors across accounts. If ten different accounts are accessed from the same device fingerprint, or five "different" users exhibit identical typing rhythms, the system flags the entire cluster as a fraud ring, stopping the attack before it scales.

Beyond behavior: the full signal picture

Behavior is the hardest signal for an attacker to fake, but it is not the only one. AccessGate fuses behavioral intelligence with the surrounding context of each request, so a takeover that slips past one layer is caught by another:

NETWORK & LOCATION
Datacenter, VPN, proxy, Tor, and known-fraud address reputation, plus impossible-travel detection. Threat lists refresh from live sources, not hard-coded.

DEVICE & AUTOMATION
Device fingerprinting and emulator/automation detection: a genuine returning device vs. a spoofed or scripted one.

IDENTITY & VELOCITY
Email and phone reputation, carrier and line-type checks, and velocity controls that catch scripted bursts from a single source.

BEHAVIORAL BIOMETRICS
The four-layer engine: the core differentiator.

WHY FUSION WINS

No single signal decides the outcome. They are fused into one risk profile, which is why the system is resilient: an attacker who defeats one control still has to defeat the others simultaneously.

FROM SIGNAL TO DECISION

Graduated, explainable, tunable

Intelligence is only useful if it drives a clear, defensible action. For every interaction, AccessGate returns:

- **A graduated response, not a blunt yes/no.** Depending on risk: *allow* (the silent, frictionless default), *step-up challenge* (verify only when risk warrants it, avoiding MFA fatigue), *block*, or, mid-session, a *terminate* decision your platform enforces.
- **Explainable reasons.** Each decision ships with the specific signals behind it, so fraud and risk analysts can review, tune, and defend it. No black box.
- **Tunable to your risk appetite.** Signal weights and thresholds are configurable per organization: conservative for high-value transactions, lighter-touch elsewhere, without code changes.

Continuous auth vs. multi-factor authentication

MFA is a critical security layer, but no longer sufficient as a standalone defense against ATO.

FEATURE	TRADITIONAL MFA (THE GATEKEEPER)	CONTINUOUS BEHAVIORAL AUTH (THE GUARD)
Security model	Static and punctual: validates identity once at the front door. Once inside, the user is implicitly trusted.	Dynamic and continuous: validates identity with every interaction. Trust is re-evaluated in real time.
User experience	High friction: interrupts the user to find a phone, enter a code, or scan a finger. Leads to MFA fatigue.	Zero friction: runs silently in the background. The user is never interrupted unless confirmed fraud is detected.
Threat coverage	Prevents unauthorized entry but cannot detect session hijacking or coerced access.	Detects takeover even after login: a mid-session behavior change triggers a real-time terminate decision your platform enforces.
Blind spots	Vulnerable to phishing (real-time proxy) and MFA fatigue attacks.	Resilient to credential theft: even with the password and OTP, an attacker cannot replicate the victim's behavioral biometrics.
Best use case	Initial login / high-value transactions.	The entire user journey, ensuring session integrity from start to finish.

GETTING SMARTER OVER TIME

Learning from your traffic, safely

AccessGate is not a static engine that decays the day it ships. It improves continuously from your own real traffic:

- **Per-user baselines that adapt** as legitimate behavior naturally evolves, while resisting attacker manipulation.
- **A dedicated machine-learning anomaly layer**, trained on your own live behavioral data, that learns the shape of "normal" for your population and flags novel patterns no hand-written control anticipates.
- **Validation-first rollout.** New models run in shadow mode first, scoring every live session against real outcomes, and only influence decisions once proven.

VALIDATION FIRST

Shadow mode is how accuracy rises without exposing your users to an unproven model: score everything, affect nothing, until the evidence is in.

Built for the edge, built for trust

- **Global edge performance:** the full intelligence pipeline runs at the network edge, delivering instant decisions that add no friction.
- **Per-tenant isolation:** every organization's behavioral profiles and data are strictly segregated.
- **Privacy by design:** support for data-subject export and deletion, so behavioral intelligence operates within your regulatory obligations, not around them.

TRUST BOUNDARIES

Isolation and privacy guarantees are properties of the architecture, so behavioral intelligence stays inside your regulatory obligations by construction.

The business value

- **Higher accuracy:** multiple independent behavioral, contextual, and network signals fused, with an ML anomaly layer validated in shadow mode before it can affect a single decision.
- **Lower false positives:** friction drops because the system learns each individual's "normal," even if it's unconventional.
- **Resilient baselines:** the adaptive learning system actively resists manipulation by attackers.
- **Real-time, explainable decisions:** every decision ships with its reasons, and all of it runs at the global edge.

Security moves from a one-time check
to a continuous guarantee.

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. Emerging markets face unique fraud tactics and regulatory pressure; with Loci, your team turns data, behavior, and controls into real-time, explainable decisions that protect and grow your business.

SEE IT GUARD A LIVE SESSION

A walkthrough of AccessGate on your highest-risk journeys, from login to mid-session takeover detection. Read this brief online at runloci.com/brief/account-takeover-prevention.

LOCI FRAUD AI · EXECUTIVE BRIEF · NOVEMBER 2025 runloci.com · sales@runloci.com