DECK TÉCNICO

# Biometria Comportamental contra o Account Takeover

Por que o modelo de verificação mais usado hoje parou de separar quem é cliente de quem é fraudador, e o que o mercado está testando no lugar dele.


Deck técnico | Koin Antifraude

# 94%

**das tentativas de login**

**vem de bots**
não de humanos

## Login virou o ponto de entrada favorito do crime digital

Invadir sistemas dá trabalho. Testar uma lista de senhas vazadas contra um formulário de login, não. É por isso que a apropriação de conta (account takeover) deixou de ser um incidente pontual para virar o método preferido de ataque em escala.

94% das tentativas de login observadas na rede da Cloudflare vêm de bots, não de humanos, com registro de uma média de 6,9 bilhões de tentativas suspeitas de login por dia em rede[1].

O impacto financeiro acompanha esse volume. De acordo com o Estudo de Fraude de Identidade 2026 da Javelin Strategy & Research, o account takeover foi a categoria de fraude mais cara para o consumidor americano em 2025, ultrapassando US$ 15 bilhões em perdas e afetando 6 milhões de vítimas, um crescimento de 18% em relação a 2024[2].

Segundo dados do Estudo Koin-Gmattos 2026, que acompanha 59 das principais lojas online brasileiras desde 2021, mais de 42% dos crimes cibernéticos no Brasil já utilizam alguma ferramenta de inteligência artificial em sua execução[3], incluindo a validação em massa de números de cartão de crédito, justamente o primeiro passo de um ataque de credential stuffing (preenchimento de credenciais).

# Recorte do mercado brasileiro

O Estudo Koin-Gmattos 2026[3] traz um retrato direto do tamanho do problema no mercado local:

A fraude online no Brasil deve gerar

**R$ 8,1 bilhões**

em perdas projetadas para lojistas em 2026,
alta frente aos R$ 7,8 bilhões estimados em 2025.

América Latina e Europa registram a pior taxa relativa de fraude online do mundo, **4,1%** das vendas online resultam em fraude, contra 3,1% na América do Norte.


Segundo dados da Polícia Federal citados no estudo, mais de **42%** dos crimes cibernéticos no país já utilizam inteligência artificial em sua execução.

# A autenticação estática não segura mais o account takeover

Senha, código fixo e pergunta de segurança validam algo que o fraudador também pode ter: uma credencial. Quando essa credencial vaza, a autenticação estática vira uma porta destrancada, o sistema aprova o invasor com a mesma confiança que aprovaria o titular.

**Três caminhos diferentes levam ao mesmo resultado:**

01

### Vazamento, reuso e teste em massa

Bases vazadas testadas em massa contra o login. A senha certa não prova que é o dono da conta.

02

### Clone, desvio e interceptação

Clonagem de chip (SIM swap) e página falsa (phishing) em tempo real capturam o segundo fator no momento exato do uso.

03

### Sessão sequestrada

Cookies e tokens roubados replicam uma sessão já autenticada, sem passar pelo login de novo.

> Todos os três casos têm em comum que a credencial é válida, mas o comportamento não é do titular.

# Mais autenticação nem sempre significa mais segurança

A resposta mais comum ao aumento de fraude é adicionar camadas: reenviar senha, confirmar por aplicativo, responder pergunta de segurança. Cada camada nova de ação pede esforço do usuário, e cada esforço extra é um ponto onde ele pode simplesmente desistir da compra.

> **Ninguém deveria escolher entre segurança e experiência. É preciso entregar as duas ao mesmo tempo, sem depender do esforço do usuário para diferenciar quem é consumidor de quemé fraudador.**

EQUILÍBRIO ENTRE VALIDAÇÃO E EXPERIÊNCIA

**33%**

dos usuários evitam a autenticação em duas etapas por atrapalhar a jornada de compra[4]

**63%**

das operações online reduziram fraude após adotar biometria avançada[5]

**1 em cada 5**

**tentativas de fraude biométrica já envolve algum tipo de deepfake**

Ou seja, o próprio ponto de verificação (o rosto, a voz, a foto) **deixou de ser prova suficiente de identidade** quando usado sozinho.

# Verificar "quem a pessoa diz ser" também está ficando mais frágil

Não é só a senha que perdeu força como prova de identidade. Em 2024, a Gartner projetava que, até 2026, **30% das empresas** passariam a considerar suas soluções de verificação facial não confiáveis quando usadas isoladamente, em razão do avanço de ataques com deepfake (imagem, áudio ou vídeo gerado por inteligência artificial que imita uma pessoa real)[6].

Essa previsão está se confirmando. Segundo o Relatório de Fraude de Identidade 2026 da Entrust, 1 em cada 5 tentativas de fraude biométrica já envolve algum tipo de deepfake, com ataques de injeção crescendo 40% em relação ao ano anterior[7].

Ou seja, o próprio ponto de verificação (o rosto, a voz, a foto) deixou de ser prova suficiente de identidade quando usado sozinho.

A própria Gartner recomenda que, uma vez definida uma base mínima de controles, as empresas incluam sinais adicionais de risco e reconhecimento, como identificação de dispositivo e análise comportamental, para aumentar a chance de detectar ataques ao processo de verificação de identidade.

A tendência do mercado é somar camadas de reconhecimento contínuo, como comportamento e dispositivo, e não apenas confiar em um único ponto de verificação, por mais sofisticado que ele seja.

# Da verificação pontual à observação contínua

Se um ponto único de verificação, seja senha, biometria facial ou código de segurança, pode ser vazado, clonado ou enganado, a resposta não é empilhar mais um ponto isolado de verificação em cima dos que já falharam.

> **É parar de depender de uma prova única e passar a observar o comportamento de forma contínua, ao longo de toda a sessão.**

**É por isso que parte do mercado de segurança digital está migrando de um modelo para o outro:**

### VERIFICAÇÃO PONTUAL (o padrão de hoje)

- Confirma a identidade uma vez, no momento do login
- Depende do que o usuário digita ou recebe
- Aplica o mesmo nível de exigência para todo mundo
- Perde visibilidade assim que a sessão começa

### OBSERVAÇÃO CONTÍNUA (o que vem sendo testado)

- Acompanha sinais durante toda a sessão, não só na entrada
- Observa características que não podem ser copiadas nem digitadas
- Reserva a exigência extra só para onde o risco realmente aparece
- Aprende com padrões observados em volumes maiores de transações

A diferença entre os dois modelos é que a autenticação deixa de ser um evento único, verificado uma vez e esquecido, e passa a ser uma camada estratégica, observada o tempo todo. Não é uma camada extra somada às que já existem. É a mudança de lógica que torna as fraudes descritas até aqui mais difíceis de escalar.

# O que isso muda na prática

Quando a verificação para de ser um evento isolado, três coisas mudam para quem opera o negócio:

- Menos clientes legítimos são barrados por engano, porque a decisão não depende de uma única resposta certa ou errada
- A exigência extra aparece só quando o padrão observado foge do esperado, não para todo mundo, o tempo todo
- O sistema fica mais difícil de enganar com uma credencial isolada, porque ela deixa de ser suficiente sozinha

## O CAMINHO

01 ·

### CAPTURE

Coleta de sinais

→

02 ·

### CORRELATE

Insight engine

→

03 ·

### COMMAND

Decisão automatizada

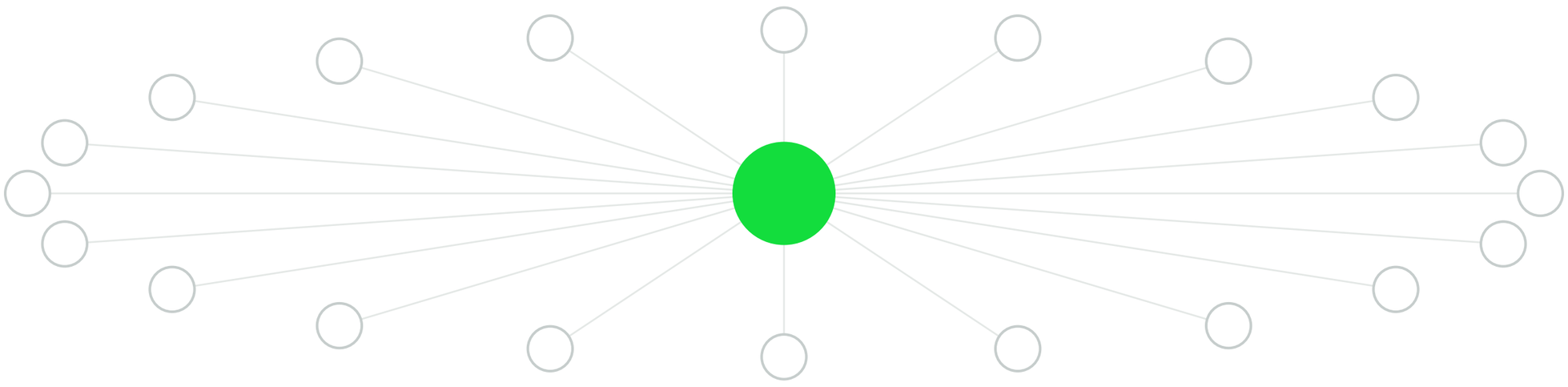
# 200+

variáveis de identificação
por dispositivo

## Device Intelligence: uma identidade que sobrevive ao disfarce

Entre todos os sinais observados durante uma sessão, o dispositivo é um dos mais estáveis, ele não depende do que o usuário digita ou recebe, e não desaparece quando a sessão termina. É esse sinal que sustenta a observação contínua (descrita anteriormente), e que permite reconhecer um comprador, ou um fraudador, mesmo quando ele tenta se disfarçar.

O mesmo dispositivo é reconhecido sob mais de 100 identidades diferentes tentadas para escapar da detecção, independentemente do disfarce.



### Identificação avançada do dispositivo (fingerprinting)

Combina atributos de hardware, software, rede e configuração para gerar uma identidade estável do dispositivo, mesmo com troca de IP, cookies limpos ou navegador anônimo.

### Resistência à falsificação de sinal (spoofing)

Sinais de baixo nível (não apenas cookies ou user-agent) tornam a falsificação de identidade cara e detectável em tempo real.

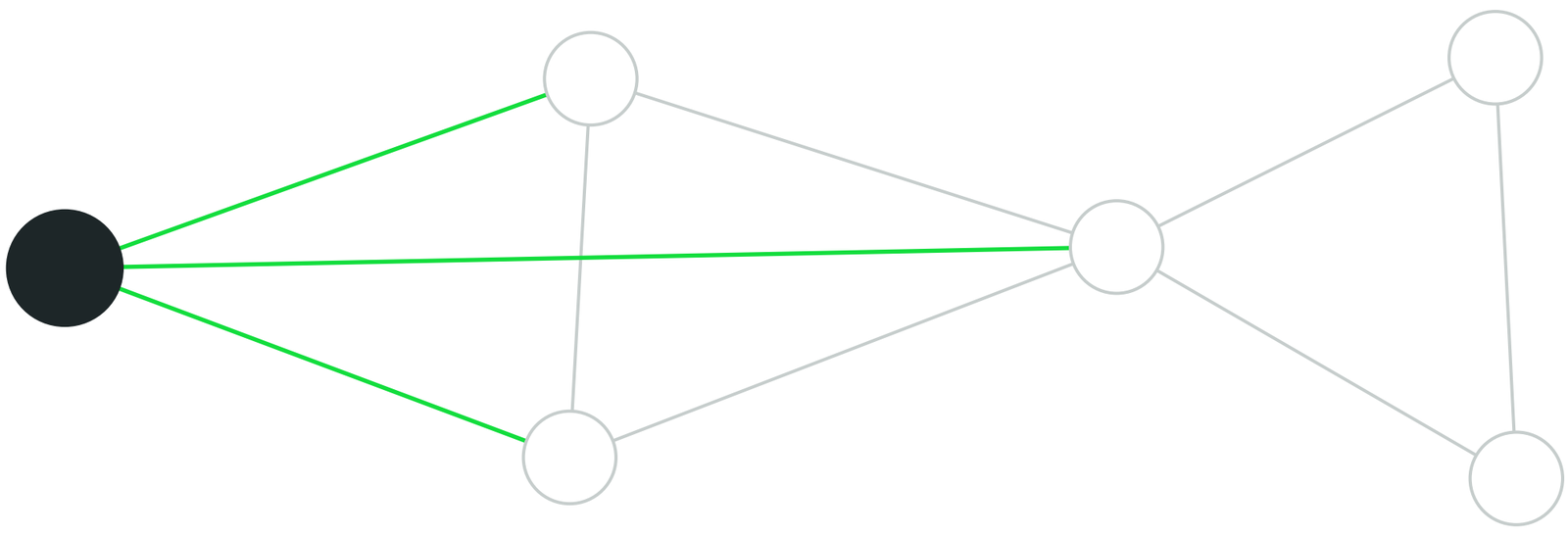
### Persistência entre sessões

Um dispositivo malicioso identificado hoje continua reconhecido amanhã. O histórico não se perde a cada nova tentativa de acesso, e é o que transforma o dispositivo em um fator persistente de identidade, não em um dado descartável a cada login.

Essa mesma identidade que resiste ao disfarce dentro de uma operação é o que abre caminho para reconhecer o risco também fora dela: um dispositivo identificado em um comércio soma histórico à inteligência que protege as próximas operações que ele tentar acessar.

# Rede comportamental: a proteção não fica isolada no seu checkout

Cada transação analisada alimenta uma inteligência de rede compartilhada. Um dispositivo ou padrão comportamental sinalizado como fraude em uma operação passa a ser reconhecido como risco em todas as outras, em tempo real.



- Se um dispositivo cometer fraude em outra operação hoje, a rede já sabe disso amanhã, sem esperar você ser a próxima vítima.
- A rede não apenas bloqueia: um dispositivo com histórico positivo em qualquer operação recebe aprovação acelerada nas demais.
- Proteção entre comércios (cross-merchant) em tempo real, sem exigir integrações adicionais do seu time técnico.

# Positivação por reconhecimento: proteger sem adicionar problema

O objetivo técnico não é bloquear mais, é decidir melhor. Um dispositivo já reconhecido como legítimo não precisa repetir etapas de verificação a cada nova compra.

### Dispositivo reconhecido

Histórico positivo, sinais consistentes com o comportamento esperado do titular.

→ Aprovação acelerada, sem etapa extra de autenticação.

### Sinal fora do padrão

Comportamento, dispositivo ou contexto divergem do que se espera daquele comprador.

→ Verificação adicional é acionada só aqui, de forma direcionada.

# Termos que você viu por aqui

Esse material usou alguns termos técnicos do dia a dia de segurança digital. Aqui está um guia rápido para simplificar a consulta:

- **Apropriação de conta (Account Takeover)** - Quando alguém que não é o dono de uma conta consegue acesso a ela e passa a agir como se fosse o titular.
- **Vazamento, reuso e teste em massa (Credential Stuffing)** - Ataque automatizado que testa, em massa, combinações de login e senha vazadas em outros sites, na esperança de que o usuário tenha reutilizado a mesma senha.
- **Código de verificação (OTP)** - O código numérico enviado por SMS, e-mail ou aplicativo para confirmar uma ação, como um login ou uma compra.
- **Clonagem de chip (SIM swap)** - Golpe em que o fraudador transfere o número de telefone da vítima para um chip sob seu controle, passando a receber os códigos OTP dela.
- **Página falsa (Phishing)** - Tentativa de enganar alguém para que revele dados sensíveis, geralmente por meio de páginas ou mensagens que imitam uma empresa real.
- **Cookies e tokens de sessão** - Pequenos arquivos que mantêm um usuário "logado" enquanto navega. Se forem roubados, permitem que outra pessoa continue a sessão sem precisar fazer login de novo.
- **Autenticação em duas etapas (MFA)** - Camada extra de verificação além da senha, como um código enviado por SMS ou aplicativo.
- **Biometria comportamental** - Análise de como uma pessoa interage com um dispositivo ou aplicativo (não só quem ela diz ser), usada para diferenciar um usuário legítimo de um fraudador.
- **Identidade do dispositivo (Device fingerprinting)** - Técnica que reconhece um dispositivo por um conjunto de características técnicas, mesmo que o usuário tente disfarçar sua identidade digital.
- **Falsificação de sinal (Spoofing)** - Tentativa de falsificar um sinal técnico (dispositivo, localização, identidade) para enganar um sistema de verificação.
- **Deepfake** - Imagem, áudio ou vídeo gerado por inteligência artificial que imita a aparência ou a voz de uma pessoa real.

O questionamento que precisa ser feito para o time:

# Quanto da verificação que sua operação aplica hoje existe para proteger contra fraude e quanto existe porque sempre foi feito assim?

Esse é o tipo de pergunta que times técnicos de operações de alto volume têm se feito ao repensar a camada de autenticação. Vale a reflexão antes de qualquer decisão de arquitetura.

Consulte outros materiais de Antifraude no Hub de Conteúdos da Koin.

**ACESSE AGORA**

Conteúdo preparado pelo time de Antifraude da Koin - AI Driven.

DESTRAVA COM A Koin

[1] Cloudflare 2026 Threat Intelligence Report, 2026. · [1a] Cloudflare, 2026. "Announcing Cloudflare Account Abuse Protection".

[2] Javelin, 2026. The Illusion of Progress. · [3] Estudo Koin-Gmattos, 2026.

[4] Prove, 2026. Relatório da Identity sobre o estado da autenticação multifatorial (MFA). · [5] Experian, 2020. Global Identity & Fraud Report.

[6] Gartner, "Gartner Predicts 30% of Enterprises Will Consider Identity Verification and Authentication Solutions Unreliable in Isolation Due to AI-Generated Deepfakes by 2026. · [7] Entrust, 2026 Identity Fraud Report.