

Impedindo ataques de Account Takeover

A fraude de Account Takeover é uma tática lucrativa e de baixo risco para os fraudadores e uma ameaça crescente para instituições financeiras e comércio eletrônico. Os cibercriminosos são adeptos do uso de credenciais roubadas, malwares, phishing, de acesso remoto via cavalos de Tróia e outras tecnologias de ataques para assumir contas de clientes e sessões bancárias. O valor médio das perdas de aquisições de contas financeiras é de quase US\$12,000¹. É crucial para as instituições financeiras evitarem apropriações de contas e afetar os resultados financeiros e degradar a experiência do cliente.



A Feedzai ficou em 15º lugar na lista da Forbes das empresas de Inteligência Artificial mais promissoras.



A Feedzai é eleita a melhor fornecedora de plataforma de Machine Learning e prevenção de fraude e prevenção à lavagem de dinheiro.



Feedzai recebeu o prêmio Top 21 de inovação da RegTech.

Mantenha a segurança de seus clientes detectando e evitando ataques de Account Takeover



Conheça o cliente em tempo real

A plataforma de detecção e resposta de fraude da Revelock, uma empresa Feedzai, evita ataques de Account Takeover em todos os pontos da sessão online do cliente, coletando e analisando continuamente os comportamentos do cliente em tempo real e acionando ações automatizadas quando uma atividade anômala é detectada.



Garanta que os clientes sejam reais

Conheça seu usuário. A plataforma Revelock FDR usa BionicID™ para identificar clientes legítimos e detectar agentes mal-intencionados, garantindo o acesso a cada interação do usuário.



Aumente a lealdade e reduza os custos de prevenção de fraude

Conhecer o seu usuário em cada interação evita a fraude e, ao mesmo tempo, melhora a experiência do cliente, eliminando as autenticações progressivas. Essa prática minimiza perdas de receita e custos de call center, diminuindo alertas e chamadas de suporte.



Aumente o custo dos ataques de Account Takeover para fraudadores

Detecte e interrompa fraudes de forma transparente, aumentando o custo e a complexidade para que os fraudadores realizem ataques de Account Takeover com sucesso.

¹ Security.org, Relatório Anual de Tomada de Conta de 2021: Prevalência, Conscientização e Prevenção, fevereiro de 2021

Características principais



Biometria comportamental

BionicID™ identifica cada usuário exclusivamente com base na análise de milhares de parâmetros, incluindo o comportamento de um cliente (por exemplo, se está usando um smartphone, qual o tipo de movimentos do mouse, como pressiona as teclas, etc.), perfil do dispositivo, análise de aplicativo, rede e dados de geolocalização.



Hybrid AI

BionicID™ é suportado pela tecnologia Hybrid AI que permite que você realmente conheça seu usuário e retome o controle. Protegemos os usuários em todos os pontos da jornada da transação, desde a abertura da conta e transações até o logout.



Experiência silenciosa do cliente

Evite que os usuários experimentem atrito devido às ações de agentes mal-intencionados, sem sobrecarregar as equipes de operações com alertas.



Active Defense

O Active Defense oferece um conjunto altamente flexível de recursos de resposta que capacita os analistas de fraude a interromper automaticamente as ameaças de ID ativas, protegendo imediatamente os usuários quando ocorrem ataques de malware ou phishing e executa automaticamente medidas de resposta predeterminadas.



Respostas automáticas

Detecta e derrota acesso remoto via cavalos de Tróia projetados para sequestrar sessões de usuário. Implemente automaticamente medidas de segurança, incluindo notificação do usuário, autenticação avançada, logoff automático da sessão e bloqueios de conta.



Adquirentes que confiam no Feedzai



Pronto para ver nossa tecnologia em ação?

Agende uma demonstração

