FICHA TÉCNICA

Detecção de Contas Laranjas

Onde fraude, AML e inteligência cibernética se encontram

lynxtech.com

Lynx

Sobre a Lynx

Fundada há 30 anos como uma organização sem fins lucrativos por especialistas em inteligência artificial da Universidade Autônoma de Madri, a Lynx fez a transição para o mercado em 2023, trazendo soluções de ponta baseadas em IA para prevenção de fraudes e combate a crimes financeiros. Nossa tecnologia avançada identifica riscos em tempo real, simplifica tarefas e permite que as organizações se concentrem no que realmente importa. Reconhecida pelas principais instituições financeiras, a Lynx ajuda seus clientes a economizar até **US$ 1,6 bilhão anualmente**, protegendo mais de **76 bilhões de transações** e mais de **330 milhões de consumidores.**
Nosso modelo exclusivo "Modelo Adaptativo Diário" garante precisão incomparável, mantendo as baixas taxas de falsos positivos, algo em que somos líderes do setor, impulsionando a eficácia na prevenção de crimes financeiros.

Nossa missão

Liderar o combate à fraude e aos crimes financeiros por meio de tecnologias avançadas de IA, inovação contínua e profundo conhecimento do setor.
Com a prevenção de fraudes e crimes financeiros, ajudamos a aumentar a **confiança**, a manter a **integridade** dos sistemas financeiros macroeconômicos e a **proteger** você contra danos.

Benefícios

+ de 76 bilhões
de transações protegidas anualmente

+ de 330 milhões
de usuários protegidos a cada ano

< 50 milissegundos
para 99,99% das transações processadas*

+ de 2.400
de transações por segundo*

US$ 1,6 bilhão
de instituições financeiras protegidas

* Desempenho conhecido em cenários onde a conexão é feita por meio de sockets TCP/IP e a solução está instalada localmente.

O problema

- As instituições financeiras (IFs) enfrentam **dificuldades para identificar e prevenir fluxos de dinheiro ilícito em tempo real**, o que resulta em perdas financeiras e riscos de conformidade.
- Grupos criminosos usam **laranjas para lavar dinheiro ilícito** usando contas laranja.
- **Ataques automatizados** e o uso de aprendizado de máquina por Grupos de Crime Organizado (OCGs, na sigla em inglês) **tornam a detecção cada vez mais difícil.** Com ataques bem-sucedidos, os OCGs ampliam suas ações, o que gera um **surto de atividades criminosas** e na geração de mais fundos de origem criminosa.
- As instituições financeiras ficam sobrecarregadas com a Fraude de Pagamento por Push Autorizado **(APPF, na sigla em inglês)**, que **têm impacto no resultado final por conta de custos com fraude, operações e reclamações de clientes.**

A magnitude do problema

A **Europol afirma** que mais de 90% das transações identificadas como conta laranja estão vinculadas ao crime cibernético.[1]
Em 2023, fraudes e esquemas de fraude bancária totalizaram US$ 485,6 bilhões em perdas projetadas globalmente.[2]
Os crimes financeiros estão aumentando e as laranjas são facilitadores em tempo real do crime organizado. Em 2023, estima-se que US$ 3,1 trilhões em fundos ilícitos tenham circulado pelo sistema financeiro global[3], conforme relatado pela Nasdaq.
Os **cinco principais tipos de fraude de falsidade ideológica** em 2023 foram impulsionados pela inteligência artificial, redes de lavagem de dinheiro, identidades falsas, roubo de contas e verificações forçadas.[4]
No mundo todo, houve um **aumento em 10x no número de deepfakes** detectados em todos os setores de 2022 a 2023.[5]
As **atividades criminosas** responsáveis pela geração de fundos ilícitos abrangem desde ataques de phishing e malware até várias formas de fraude, como golpes em leilões online, fraudes no comércio eletrônico, comprometimento de e-mail corporativo (BEC, na sigla em inglês), golpes românticos, fraudes em reservas e outros tipos.
Os **criminosos estão organizados** e usam os mais recentes avanços em inteligência artificial para orquestrar ataques complexos contra instituições financeiras e seus clientes.
Os **criminosos precisam de contas laranja** para movimentar dinheiro ilícito. Nesse sentido, pode-se encarar isso como uma cadeia logística da organização criminosa.

Ao identificar fundos ilícitos e contas laranja em tempo real, interrompemos o braço logístico e impedimos que o dinheiro ilícito chegue ao monstro, o crime organizado.

De acordo com a Europol, **mais de 90% das transações de mula de dinheiro estão vinculadas ao crime cibernético.**

1 Europol. **2/3** Nasdaq. **4/5** Sumsub.

A solução

A **Detecção de Mulas de Dinheiro da Lynx** usa o aprendizado de máquina supervisionado para identificar fontes ilícitas de fundos e contas laranja em tempo real.
Ao combinar dados de transações de entrada e saída, a Lynx oferece uma visão abrangente do usuário para prevenção proativa de fraudes e detecção de intermediários em esquemas de lavagem de dinheiro.

Bloqueie a conta. Devolva os fundos fraudulentos aos legítimos proprietários. Impeça que o dinheiro chegue às mãos dos criminosos.

O que ele faz?

- Analisa cada transferência/transação recebida em tempo real.
- Fornece uma visão completa do cliente, incluindo todas as transações e contas com potencial de risco.
- Atribui uma pontuação de risco à transferência/transação com base na probabilidade de associação com fontes de fundos ilícitos, como APPF.
- Sinaliza e bloqueia automaticamente qualquer atividade adicional em contas identificadas como contas laranja.
- Gera alertas para ação imediata pelas equipes de prevenção a fraudes e lavagem de dinheiro.
- Atualiza o modelo diariamente usando o procedimento de Modelo Adaptativo Diário (DAM, na sigla em inglês) para obter a máxima precisão e minimizar os falsos positivos, permitindo o bloqueio em tempo real de contas e fundos utilizados por contas laranja.
- Se for identificada a prática de lavagem de dinheiro, um alerta imediato é enviado para a equipe de combate à lavagem de dinheiro. Reconhecer que o laranja é uma forma de lavagem de dinheiro e denunciar essa prática em tempo real não só garante a conformidade regulatória para a instituição financeira, mas também ajuda as autoridades policiais a identificar e deter esses criminosos.

Modelos Adaptativos Diários

Os modelos adaptativos diários representam o mais recente avanço na prevenção de fraudes.
Os **Modelos Adaptativos Diários (DAM) da Lynx** são continuamente atualizados usando os padrões mais recentes de comportamento genuíno dos usuários e de fraudes. Os perfis de autoaprendizagem utilizam dispositivos de usuários reais, transações com cartões, pagamentos recebidos e informações de localização. O enriquecimento de dados em tempo real, facilitado pelo banco de dados em memória da Lynx, permite a identificação rápida e precisa de comportamentos e atividades fraudulentas.
Com o modelo adaptativo diário, você **reduz a fricção** e impede **que mais fraudes sejam cometidas.**

Vantagens da detecção de contas laranja pela Lynx

- **Defesa em tempo real:** o modelo de contas laranja da Lynx combina transações de entrada e saída, permitindo identificar se a conta que recebe e/ou envia fundos é uma conta usada para lavagem de dinheiro. Por exemplo, o modelo pode identificar fontes irregulares de fundos recebidos pela conta, potencialmente provenientes de APPF ou outros tipos de fraude, sinalizando a conta como uma conta laranja.
- **Redução de perdas:** identifica mulas com precisão. Isso reduz a fadiga causada por alertas, reclamações e riscos. Combata o risco financeiro identificando a conta laranja em tempo real e impedindo seu funcionamento. A regulamentação PSR do Reino Unido, de 7 de outubro, exige que o reembolso por fraudes APPF (golpes) seja dividido em duas partes iguais entre as instituições financeiras remetentes e recebedoras. A Lynx identifica as fraudes APPF recebidas e impede que os fundos sejam enviados, reduzindo significativamente as perdas.
- **Modelos personalizados (DAM):** a Lynx desenvolve modelos específicos para cada instituição financeira, que são atualizados automaticamente diariamente. Os modelos adaptam-se automaticamente aos riscos, comportamentos, produtos e dados da instituição financeira. Permite maior precisão, cobertura completa e redução da carga de trabalho em comparação com os modelos estáticos tradicionais (dados apenas de transações).
- **Visão holística:** centralize o monitoramento de transferências de entrada e saída com uma única solução, oferecendo pontuação em tempo real e uma visão abrangente completa.
- **Independente ou como parte de uma solução:** o modelo de mula de dinheiro da Lynx pode ser usado como um componente independente para fornecer pontuações em tempo real a uma solução de prevenção de fraudes já existente. Isso pode ajudar a aumentar a precisão na detecção de fraudes, abordando esse desafio específico de forma eficaz, sem a necessidade de integrações complexas, apoiando assim as instituições financeiras de maneira eficiente. Ou utilize o modelo de mula de dinheiro da Lynx como parte da solução abrangente de prevenção de fraudes da Lynx para identificar com precisão fraudes e mulas em transferências de entrada e saída.

Ao participar desta luta, você não está só fazendo o seu trabalho.

Você está protegendo o futuro de milhões de usuários legítimos.

Ação imediata necessária

Nova regulação

O Código do Modelo de Reembolso Contingente (CRM, na sigla em inglês) exige a divisão do reembolso entre as instituições financeiras remetente e receptora no Reino Unido.
Como forma de prevenção, as instituições financeiras devem implementar a análise de perfil para pagamentos recebidos. Essa medida permite que as empresas impeçam a movimentação subsequente de fundos caso haja suspeita de que os fundos creditados sejam provenientes de um golpe APPF.[5]

Atividade criminal mais sofisticada

- O aumento das identidades sintéticas, impulsionado pela ampla adoção da inteligência artificial, simplifica a criação de contas bancárias fraudulentas para criminosos.
- Os criminosos se aproveitam dos avanços da inteligência artificial para orquestrar ataques complexos com recursos mínimos, utilizando bots e mídias sociais para ampliar o alcance.
- Embora o processo de integração digital vise simplificar o processo de identificação e verificação (ID&V), sua adoção também abriu brechas que favoreceram a proliferação de contas laranja, especialmente com o aumento das deepfakes.
- O Crime como Serviço (CaaS) impulsiona o aumento de violações de dados, roubo de identidade e fraudes em novas contas, à medida que grupos criminosos oferecem serviços por assinatura para ataques avançados.

Tendências bancárias no Reino Unido

- Os pagamentos em tempo real permitem que os criminosos movimentem rapidamente os lucros ilícitos a uma velocidade sem precedentes e sem serem detectados.
- Todas as transações bancárias, incluindo cadastro de clientes, solicitações de produtos, aprovações e transações, ocorrem em tempo real.
- **A Autoridade de Conduta Financeira do Reino Unido** destaca *"Observamos casos em que as empresas estão cadastrando clientes que compartilham um único dispositivo sem uma justificativa clara. Isso condiz com o comportamento típico de um usuário "laranja", indicando um possível uso não autorizado da conta."*
- A ausência de identidades digitais robustas dos clientes, apoiada por perfis de dispositivos, dados de geolocalização e biometria comportamental durante o processo de integração e interações subsequentes com a instituição financeira, representa um risco significativo.

Próximos passos

Dê um fim às mulas, dê um fim ao crime

As contas laranja são um elo crucial na cadeia do crime financeiro, facilitando a movimentação de fundos ilícitos em todo o mundo. Ao interrompermos esse fluxo do crime, não só protegemos inúmeras vítimas, como também enfraquecemos a capacidade operacional das organizações criminosas.

Seu impacto

Imagine um mundo onde as quadrilhas criminosas não conseguem operar porque seus canais financeiros são bloqueados a cada passo.

Experimente um POC e **descubra quanto você poderia economizar!**

Quantas contas laranja não detectadas ou inativas você tem?

Quanto você poderia economizar na sua empresa?

5 *Lending Standards Board* (Conselho de Padrões de Empréstimo no Reino Unido).

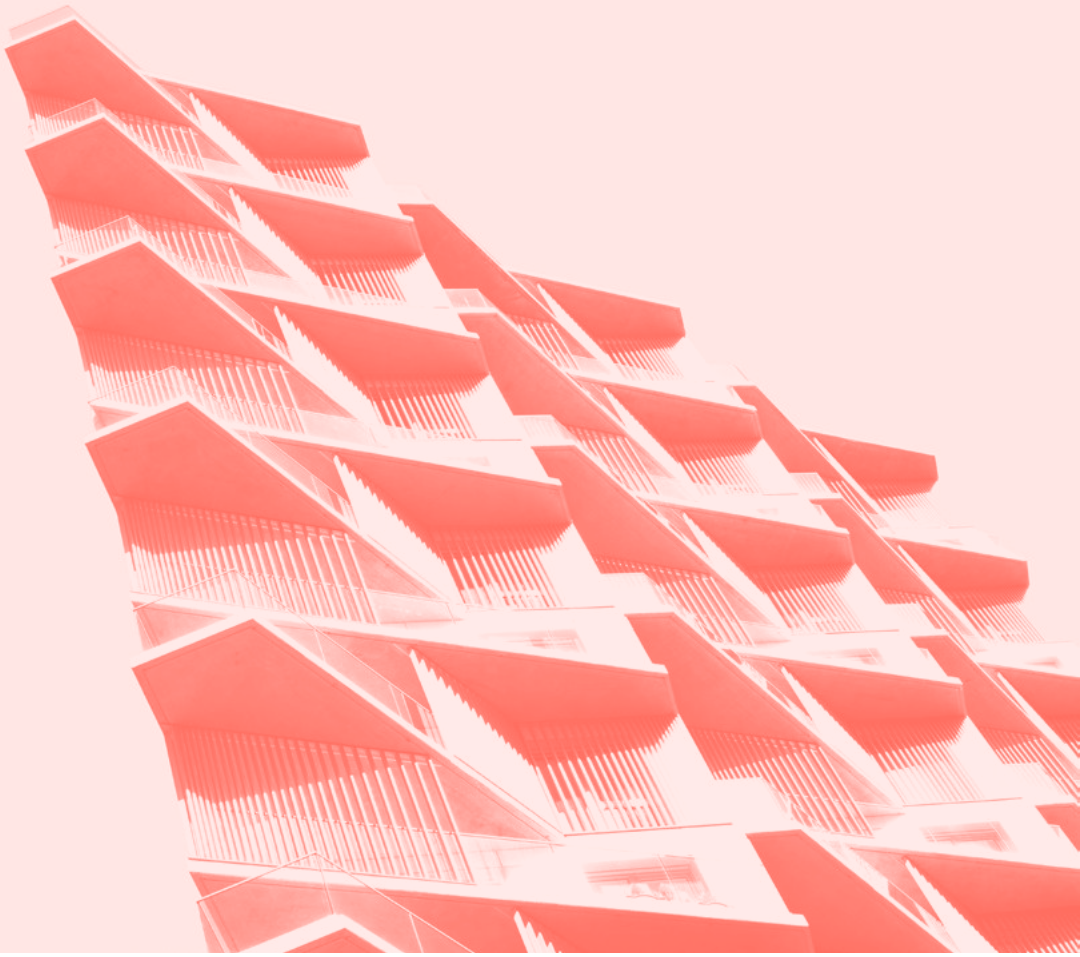
Recursos do produto

- Modelos de aprendizado de máquina de autoaprendizagem rápida que melhoram a precisão a cada dia.
- Modelos de comportamento financeiro pré-configurados que são atualizados automaticamente.
- Monitoramento do comportamento financeiro em tempo real.
- Monitoramento do tráfego de saída e entrada de APPF em tempo real.
- Visão abrangente e completa do cliente e gerenciamento de alertas.
- Regras avançadas e fáceis de usar, configuráveis por meio de uma interface de usuário (sem necessidade de programação).
- Painéis e relatórios de consulta e resposta em tempo real.
- Multicanal: cartões, dispositivos móveis, internet banking, caixas eletrônicos, agências, pagamentos P2P, corporativo, adquirentes, telefonia.
- Automação de fluxos de trabalho a partir de alertas.

Especificações técnicas

- Opções de implantação SaaS ou local.
- Conformidade com PCI-DSS e ISO27001.
- API de autopublicação para fácil integração.
- Arquitetura otimizada em tempo real para fluxo de autorização.
- Código de baixo nível e bancos de dados em memória.
- Tempo de resposta em tempo real (99,99%)*.
- Modelos de dados extensíveis.
- Controles de governança de modelo robustos.
- Otimizado em relação a Fraude vs. Atrito (VDR vs. Fraude vs. Fricção) (VDR vs. tFPR).

* Implantação local usando socket TCP/IP: tempo médio de resposta em milissegundos.



Desenvolvido por

Lynx

Sobre a Lynx

A Lynx utiliza IA avançada para prevenção de fraudes, aprimorada ao longo de 25 anos. Originada no programa de ciência de dados da **Universidade Autônoma de Madri**, a Lynx é confiável para as principais instituições financeiras do mundo na redução significativa de perdas relacionadas a fraudes. Processando mais de **66 bilhões de transações por ano**, a abordagem orientada por IA da Lynx identifica riscos em tempo real e capacita as organizações a se concentrarem no que realmente importa.

Reconhecimentos

Gartner
Recognized in the 2024 Market Guide for **Fraud Detection in Banking Payments**

Gartner
Recognized in the 2025 Market Guide for **Anti-Money Laundering**

Gartner
Named as a Sample Vendor in the 2025 **Emerging Tech Impact Radar**

Chartis
Financial Crime and Compliance50 2024

Chartis
RiskTech Quadrant®
Category Leader
Enterprise Fraud Solutions, 2024

Chartis
RiskTech Quadrant®
Category Leader
Payment Fraud Solutions, 2024

Chartis
RiskTech Quadrant®
Best of Breed
Name and Transaction Screening Solution, 2024

CBINSIGHTS
Fintech 100
2024

Solução antifraude do ano no FStech Awards

datos INSIGHTS
Risk Insights Spotlight Q4 2024

Best Intiative in Utilising Data or AI at the PAY360 Awards 2025

Chartis – Top 50 Retail Banking Analytics, 2025

* **Gartner, Market Guide for Fraud Detection in Banking Payments**, 11 December 2024. **Gartner, Market Guide for Anti-Money Laundering**, 5 August 2025. **Gartner, Emerging Tech Impact Radar: 2025**, 23 January 2025. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

Entre em contato

Site: lynxtech.com
E-mail: info@lynxtech.com