

Takedown

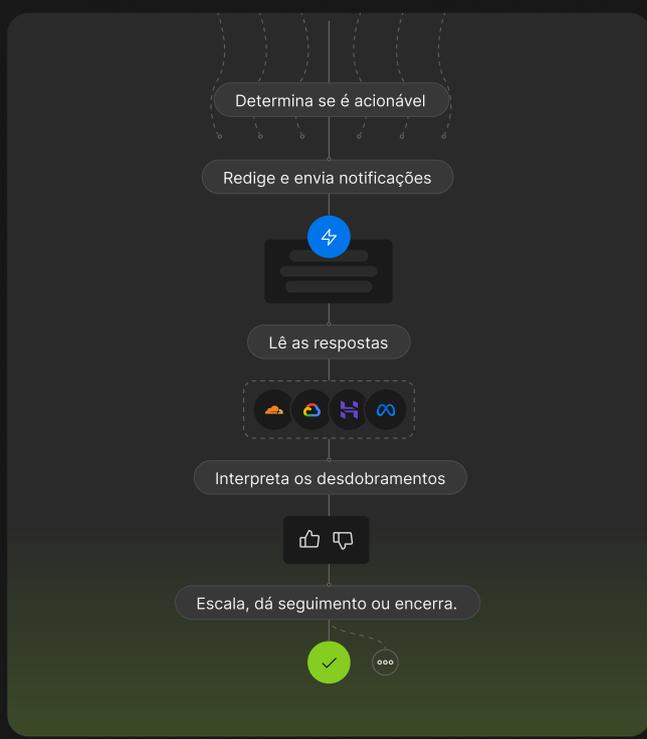
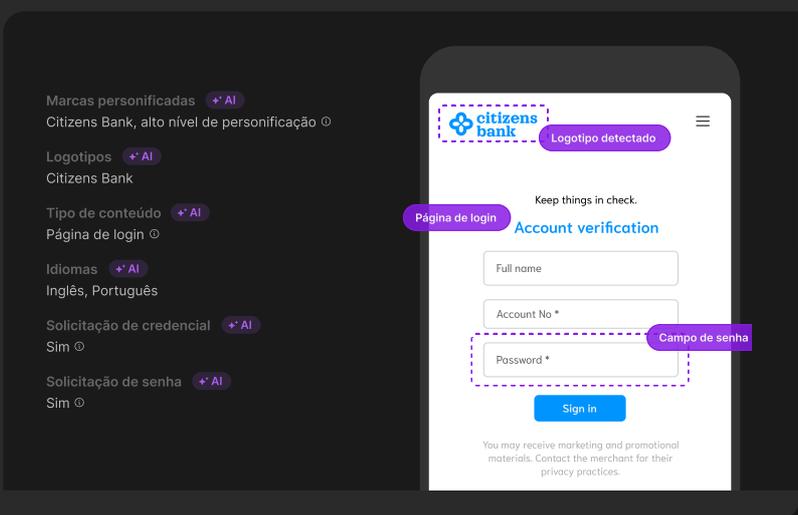
Takedown agêntico: elimine ameaças com a velocidade, autonomia e precisão da IA.

Conteúdos nocivos em plataformas colocam sua marca, receita e dados em risco. O takedown agêntico da Axur detecta, classifica e elimina ameaças com rapidez, precisão e sem interrupções.

IA como motor, não como recurso.

Nosso modelo proprietário de IA detecta abusos de marca em ativos visuais — mesmo sem palavras-chave, logos ou menções diretas à sua empresa.

Clair entende o contexto visual, sinaliza conteúdos infratores e alimenta essas decisões em um fluxo de takedown totalmente agêntico.



Da detecção à decisão, com autonomia total

O takedown agêntico da Axur é capaz de:

- Determinar se a ameaça é acionável, filtrando falsos positivos, conteúdos legítimos e fraudes fora do escopo de atuação;
- Redigir e enviar notificações;
- Ler as respostas de hosts e plataformas;
- Interpretar os desdobramentos;
- Agir de acordo para escalar, dar seguimento ou encerrar o caso.

Tudo isso com a mínima intervenção humana. É assim a nova geração de takedowns.

Sim, o **melhor** takedown. E temos provas disso.

✦ Takedowns com 1 clique ou automáticos

Nada de prints, explicações ou comprovações. Basta clicar — ou configurar fluxos com IA para acionar takedowns de forma totalmente automática.

✦ 98,9% sucesso

Não enviamos apenas alertas. Eliminamos ameaças. Escale sua resposta com uma plataforma que já executou mais de 2 milhões de takedowns.

✦ Web Safe Reporting

Acione diretamente os principais órgãos responsáveis pela exibição da “tela vermelha” em páginas maliciosas, antes mesmo que o conteúdo seja removido.

✦ Garantia de 15 dias

Removemos. E se o link voltar a aparecer em até 15 dias, uma nova remoção pode ser solicitada sem custo adicional.

✦ Notificação em <5min

Quanto antes o provedor recebe o pedido, menor a janela de exposição. É por isso que temos os melhores SLAs para envio da primeira notificação.

Phishing

Domínios similares

Fraudes com a marca

Pirataria

Fraudes com VIPs

Se sua proteção atual ainda não cobre esse nível de automação, vale considerar dar o próximo passo.

✦ 9h mediana de uptime

A automação é o principal motivo por trás do nosso alto índice de sucesso e baixo tempo de exposição.

✦ Acompanhe todo o processo

Visualize cada etapa do takedown em tempo real: envio de notificações, status de remoção e tempo médio de resposta — tudo ao seu alcance.

✦ Pague apenas por takedowns concluídos

Sim, deveria ser o padrão, mas não é: outros provedores cobram por notificação, mesmo que nada seja removido.

⚡ +1k takedowns por dia

✓ Resolvido! Takedown finalizado.

02/03/2025 às 23h17

✉ 1 notificação enviada, 1 resposta

✓ Hostinger ▾

Recebido em 02/03/2025 às 23h14

➔ Hostinger ▾

Primeira notificação enviada em 02/03/2025 às 22h59

⬤ Ameaça movida para tratamento

02/03/2025 às 22h58

⚡ Takedown solicitado automaticamente

02/03/2025 às 22h58

Regra de automação Phishing - Takedown

Ir para Automações

⬤ Ameaça detectada

02/03/2025 às 22h50

Mais de 86% das detecções são gerenciadas **sem toque humano.**

Experimente a nova geração de takedowns

Agende uma demo

Descubra todas as soluções em axur.com

Gartner
Peer Insights. **4.8**
★★★★★



AXUR